Estudi comparatiu d'eines de distribucions GNU/linux orientades a seguretat de xarxes

Alumne: Rubèn Illescas Saldaña
Enginyeria Tècnica en Informàtica de Sistemes
Àrea: GNU/Linux
Consultor: Ignaci Rius
Data Lliurament: Juny del 2014

RESUM

Aquest projecte pretén estudiar i analitzar tres distribucions linux (a partir d'ara seran anomenades *distros*), especialitzades en seguretat de xarxes.
En aquest estudi es descriurà les característiques tècniques de cada distro així com classificació de les seves eines principals.
Es duran a terme una sèrie de proves amb aquestes distros per tal de poder estudiar les seves eines, a través d'un laboratori virtual i amb un *LiveCD* (distro muntada en un disc dur virtual d'arrancada). A més s'instal·larà una màquina virtual de proves amb vulnerabilitats, per poder analitzar les diferents eines.
Aquestes proves seran les que ens faran poder verificar i estudiar l'entorn de treball de les distros així com les eines que incorporen per poder ser comparades finalment.

PARAULES CLAU
Distro, distribució, Backtrack, Pentoo, Wifislax, wifi, pentest.

ÍNDEX DE CONTINGUTS

ÍNDEX DE FIGURES

1. INTRODUCCIÓ

1.1. JUSTIFICACIÓ DEL PROJECTE

L'elecció d'aquest estudi no es deu al gran coneixement que tinc dels sistemes linux, sinó tot el contrari, per poder aprendre més sobre el món linux i en especial ser conscient de les eines que ofereixen les distros especialitzades en seguretat de xarxes.

Per què seguretat de xarxes? Avui dia accedim a tot tipus de connexions xarxes sense fils amb els nostres smartphones i computadores, ja siguin públiques o privades. Estar connectat a internet mitjançant *wifi* o per cable és un requisit per poder treballar o interactuar amb la informació. Les poques mesures que ens proporcionen les operadores telefòniques, fa que internet sigui un lloc insegur i de fàcil accés per a hackers informàtics.

L'estudi i anàlisi es pretén fer amb tres distros de sistemes operatius basats en linux i especialitzats en seguretat de xarxes.
S'ha escollit aquestes distros entre les tres principals originaries: Debian, Slackware i Red Hat. També s'ha tingut en compte la popularitat que tenen a nivell d'usuari i amb una àmplia gama d'eines.

- Backtrack versió 5 (basat en Debian).
- Wifislax (basat en Slackware).
- Pentoo (basat en Enoch, Red Hat)

S'ha considerat en escollir la distro Kali linux, successora de la distro Backtrack, però en lloc s'ha escollit aquesta última amb la versió 5, ja que aquesta és l''antecessora i originaria. Una altra raó per escollir aquesta distro i aquesta versió és que recentment s'ha instal·lat en la meva computadora la Backtrack 5 ja que s'ha cursat l'assignatura de Seguretat de Xarxes de Computadors de la UOC i aquesta distro era l'utilitzada en les pràctiques.
En el cas de les distros basades en Red Hat, no s'ha trobat cap que orientada a la seguretat de xarxes amb un mínim d'especialització, tot i que hi han moltes que contenen eines de testejos de penetracions. Per tant, s'ha escollit Pentoo, la qual esta basada en Enoch (Red Hat), que és una distro originaria i amb gran popularitat.

1.2. DESCRIPCIÓ DEL PROJECTE

En el següent document el lector trobarà una anàlisi de tres distros populars d'avui en dia, en concret BackTrack 5 r3, Pentoo RC2.1 i WifiSlax 4.8.
Cadascuna d'aquestes distros estan especialitzades en seguretat de xarxes, utilitzades per detectar les vulnerabilitats d'un sistema. Aquestes distros estan basades en:
Backtrack (Ubuntu), Pentoo (Gentoo), WifiSlax (Slax).
Es realitzarà una anàlisi profunda i detallada de les eines de cada distro per detectar les vulnerabilitats d'un sistema. Això no vol dir analitzar totes i cadascuna de les eines o programari que incorporen aquestes distros, sinó només aquelles necessàries per fer un test de vulnerabilitats d'un sistema informàtic. En aquest context l'anàlisi va destinat als usuaris de Linux no experts, com a alternativa a Windows per provar un nou sistema amb eines de seguretat de xarxes.
Així, en un primer apartat del document el lector trobarà unes quantes notes breus sobre la història i situació actual de GNU / Linux, i sobre les distros especialitzades en seguretat de xarxes per tal d'introduir al lector en aquest sistema operatiu abans d'entrar més de ple en l'anàlisi de les eines de cadascuna de les distros. Tanmateix s'explicarà que consisteix el procediment de *pentesting* i les seves fases, per tal de poder comprendre millor la prova que es realitzarà mes endavant al laboratori de proves.

Entrant ja en l'anàlisi podem dir que està dividit en quatre grans grups. Primer s'explica una descripció detallada de les tres distros. Es comentarà les seves opcions d'instal·lació, els recursos que utilitza així com les seves característiques tècniques.
En segon lloc, es farà una anàlisi de cadascuna de les seves eines, com estan classificades i agrupades i les seves funcions. Aquest procés es durà a terme a través dels manuals de cadascuna de les eines que incorporin les distros, així com informació trobada a internet i finalment verificada a l'ordinador portàtil on estaran instal·lades com a Màquines virtuals.
En tercer lloc, una vegada presentades i analitzades les tres distros es duran a terme unes sèries de proves en un laboratori virtual per testejar les vulnerabilitats d'una màquina virtual dissenyada per aquest propòsit amb cadascuna de les distros. Amb excepció de la distro Wifislax, s'executarà amb un *Live CD*, ja que de forma virtual no es pot utilitzar la targeta de xarxa en mode monitor per poder rastrejar xarxes sense fils al seu voltant. Tanmateix s'instal·larà un quarta màquina virtual vulnerable, per ser provada per les altres dos distros.
Aquestes proves es faran amb les eines de test de penetració i s'anotaran als resultats obtinguts per poder comprovar el maneig de les seves eines, on posteriorment s'estudiaran més profundament.
L'últim apartat el deixem per un estudi comparatiu de les eines de cada distro on es tindrà en compte els coneixements adquirits al llarg d'aquest projecte.

1.3. OBJECTIUS

L'objectiu principal del projecte és poder adquirir un coneixement general de les eines que incorporen les distribucions linux especialitzades en seguretat de xarxes. Això es vol aconseguir a través de l'estudi i anàlisi de tres distros enfocades en seguretat de xarxes.
Inicialment s'ha realitzat un estudi de les que existeixen avui dia i de les seves funcionalitats. S'ha pogut arribar a la conclusió que totes estan creades per trobar vulnerabilitats en sistemes informàtics principalment a través de la xarxa. En el cas de la distro Wifislax, trobem que conté més eines enfocades en trobar vulnerabilitats a través de la comunicació *Wi-fi*.

L'estudi i anàlisi comprendrà quatre fases:

1.- Explicació i presentació de les tres distros que s'estudiaran.

2.- Eines que contenen les distros per analitzar la seguretat d'una xarxa.

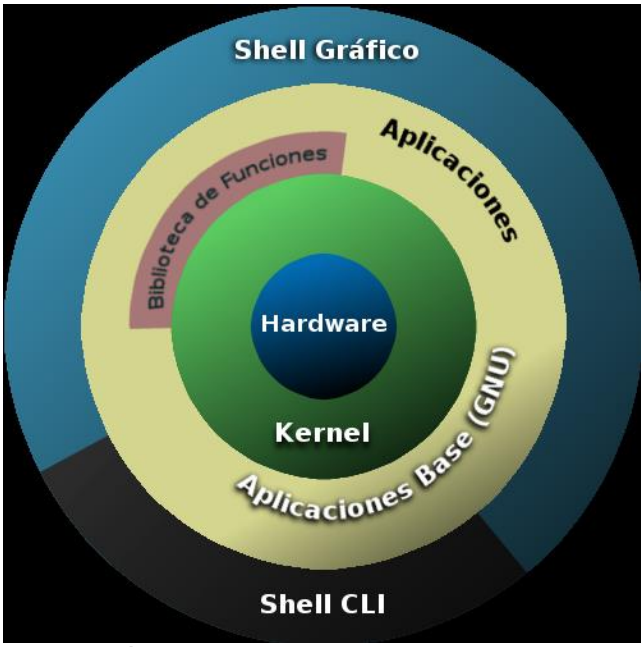
3.- Laboratori de proves *pentest,* on es faran proves amb les distros.

4.-Estudi de les eines de les tres distros i conclusió final.

2. HISTORIA I SITUACIÓ ACTUAL

2.1. QUE ÉS GNU/LINUX?

Una distro GNU / Linux és un conjunt de programari basat en el nucli Linux i altres eines de sistema GNU (Il·lustració 1). Actualment es poden trobar multitud de distros diferents, amb propòsits que van des de l'ús més general i quotidià, passant per l'opció multimèdia, i abastant fins a l'àmbit professional. Aquest projecte no pretén fer una anàlisi exhaustiva de totes les distros existents avui en dia, tasca titànica que requeriria massa temps i que resultaria en un resultat útil per a pocs.



Il·lustració 1: Arquitectura GNU/Linux

El projecte GNU ha donat fruit a molts programes de gran qualitat, molts d'ells utilitzats actualment:

– ***Bash***: L'intèrpret de comandaments per defecte de la majoria de distros GNU / Linux, basat en la shell d'Unix i compatible amb POSIX.

– ***Emacs***: un editor de text, creat en part per Stallman i que disposa d'una gran llista de comandes que es poden combinar en *macros*, facilitant la tasca.

– ***GCC***: La col·lecció de compiladors GNU, va passar de compilar únicament el llenguatge C a suportar C + +, Fortran i fins i tot Java. És el compilador per defecte de la majoria de les distros GNU / Linux, fins i tot dels sistemes BSD més moderns.

– ***GIMP***: Programa d'edició d'imatges, que suposa una alternativa a Adobe Photoshop en la majoria dels usos.

– ***GNOME***: Un dels entorns d'escriptori més utilitzats per les distros actuals, amb un gran èmfasi en la simplicitat, facilitat d'ús i eficiència.

– ***gzip***: Abreviatura de GNU Zip, creat el 1992 per substituir al programa *compress* de UNIX. Avui en dia és dels més usats, al costat de *bzip2*, encara que només permet comprimir, sense arxivar.

– ***Octave***: L'equivalent GNU a MATLAB, programat en el llenguatge C + + i amb un gran suport d'altres utilitats GNU.

- ***CVS*** : El sistema de control de versions (Concurrent Versions System) manté el registre de tot el treball i els canvis en els fitxers d'un projecte i permet que diferents desenvolupadors col·laborin amb més facilitat.

- ***Git***: és un programari de control de versions dissenyat per Linus Torvalds, pensant en l'eficiència i la fiabilitat del manteniment de versions d'aplicacions quan aquestes tenen un gran nombre d'arxius de codi font. Hi ha alguns projectes de molta rellevància que ja fan servir Git, en particular, el grup de programació del nucli Linux.

- ***Subversion (SVN)***: és un sistema de control de versions dissenyat específicament per reemplaçar el popular CVS. És programari lliure sota una llicència de tipus Apache / BSD i se'l coneix també com a svn per ser el nom de l'eina utilitzada en la línia d'ordres.

Una característica important de Subversion és que, a diferència de CVS, els altres arxius amb versions anteriors no tenen cadascun un número de revisió independent, en canvi, tot el repositori té un únic número de versió que identifica un estat comú de tots els arxius en un instant determinat del repositori que s'està treballant.

El nucli Linux és plantejat com un nucli monolític híbrid, això vol dir que s'engloben tots els serveis del sistema en el mateix " paquet" ; això provoca que calgui recompilar tot el nucli cada vegada que hi ha un canvi important. Els controladors de dispositius i les extensions del nucli s'executen en un espai privilegiat conegut com anell 0 , amb accés il·limitat al maquinari (alguns poden executar-se en espai d'usuari) . A diferència dels nuclis monolítics, Linux incorpora mòduls, que són controladors de dispositius i certes extensions del nucli. D'aquesta manera es pot afegir funcionalitat al sistema sense necessitat de detenir el funcionament del nucli.
Linux està escrit en el llenguatge de programació C, en la variant utilitzada pel compilador GCC (que ha introduït un nombre d'extensions i canvis al C estàndard) , al costat d'unes petites seccions de codi escrites amb el llenguatge assemblador, Perl i Python .
L'escriptori típic d'una distro Linux conté un nucli, eines i llibreries, programari addicional, documentació, un sistema de finestres, un administrador de finestres i un entorn d'escriptori, sovint sol ser GNOME o KDE. Gran part del programari inclòs és de codi obert o programari lliure i distribuït pels seus desenvolupadors tant en binari compilat com en forma de codi font, permetent als usuaris modificar o compilar el codi font original si ho desitgen. Moltes distros proveeixen un sistema d'instal·lació gràfica com ho fan altres sistemes operatius moderns. Distros independents com Gentoo Linux, T2 i Linux From Scratch proveeixen el codi font de tot el programari i només inclouen binària del nucli, eines de compilació i d'un instal·lador, que s'encarrega de compilar tot el programari de manera acord amb les especificacions del sistema.

2.2 BREU HISTÒRIA

GNU (GNU Is Not Unix) va ser iniciat per Richard Stallman en 1984 amb la intenció que fos lliure, és a dir, que tots els usuaris puguin modificar-lo i distribuir-lo, i alhora fer-ho compatible amb UNIX. La idea de còpia permesa (copyleft) està continguda en la Llicència Pública General de GNU (GNU GPL) de la Free Software Foundation (FSF), juntament amb altres, com ara la llicència de documentació lliure GNU (GFDL) o la llicència pública general reduïda de GNU (LGPL), una versió més permissiva amb l'ús de programari no lliure.
Stallman va fundar l'FSF en 1985 com a mitjà per proveir suport logístic, legal i financer al projecte GNU, que el 1990 ja disposava d'una base sòlida basada en l'arquitectura UNIX. Es va intentar utilitzar TRIX com a base del nucli que li faltava a GNU, però el seu disseny de trucades remotes a procediments i que únicament funcionava amb una arquitectura molt concreta van acabar per descartar-lo. Posteriorment, el projecte GNU va intentar usar el nucli Mach per a un nou projecte, anomenat Hurd i que acabaria estancat a causa de raons tècniques i conflictes personals entre els programadors originals. Finalment, el 1992 es va combinar el nucli Linux amb GNU, donant com a resultat el sistema operatiu lliure i funcional conegut avui dia com GNU / Linux.

2.3. ALGUNES CARACTERÍSTIQUES

Les dues principals característiques de GNU / Linux, principals mentre que marquen la diferència amb la resta de sistemes operatius existents, és que és lliure i que ve amb el codi font. La primera vol dir que és gratis, no hem de pagar cap llicència per instal·lar en tants equips com vulguem. La segona que qualsevol usuari amb els coneixements necessaris pot tenir la tranquil·litat de saber que fa un programa veient el codi font, a més de poder modificar aquest codi i distribuir-lo. Aquesta característica multiplicada per milers i milers de desenvolupadors al voltant del món fa que les millores siguin contínues.
Per destacar algunes característiques que ja no són exclusives de Linux, direm que és multitasca: permet executar diverses tasques simultàniament, o almenys donar la sensació a l'usuari que és així, lògicament una CPU només pot executar una tasca a la vegada; que és multiusuari:on diversos usuaris poden treballar o tenir sessions obertes simultàniament en un mateix equip i fins i tot treballar amb la mateixa versió d'una aplicació; i finalment destacarem una

eficient gestió de la memòria virtual que permet treballar a l'equip com si disposés de més RAM de la que realment té.

3. DISTROS ORIENTADES A SEGURETAT DE XARXES

Pen Test és com comunament es denomina als "Test de penetració" o en anglès "Penetration Test", i són en conjunt la forma d'anomenar a una sèrie de tècniques utilitzades per avaluar la seguretat de xarxes, sistemes de computació i aplicacions involucrades en els mateixos.

Aquestes tècniques es porten a terme amb un conjunt d'eines especifiques que incorporen certes distros de linux creades específicament per a aquest propòsit.
Les eines disponibles per efectuar aquestes proves de penetració passen per diversos graus de complexitat, i l'ús d'algunes d'elles pot ser tot un repte a la intel·ligència i sagacitat de l'atacant o "pentester". Entre elles s'inclouen des *scanners* de ports, complexos algoritmes per desxifrar claus, sistemes d'intrusió per força bruta, eines de *sniffing* de xarxes i penetració de tallafocs, així com també eines d'escaneig de vulnerabilitats d'aplicacions web i molt més.
Totes aquestes eines dissenyades sota un sistema operatiu linux, fan que el procés d'intent de penetració sigui molt més efectiu.
Aquestes eines solen estar agrupades en el que es coneix com "Toolkits" o jocs d'eines.
Alguns "toolkits" són molt famosos al medi per l'eficiència de les seves eines i per haver estat utilitzats en penetracions d'alt nivell a sistemes que es van considerar en el seu temps fortaleses impenetrables. Algunes més s'aconsegueixen fins i tot en format de LIVE CD o ISO, de manera que les eines ja estan integrades i instal·lades en un CD d'arrencada del sistema operatiu amb el qual treballen i són portàtils.

3.1. Procediment per fer un test de penetració

Comprèn múltiples etapes amb diferents tipus d'activitats en diferents àmbits i entorns. La profunditat amb que es duguin a terme les activitats dependrà de certs factors, entre els quals es destaca el risc que pot generar cap al client algun dels mètodes que s'apliquin durant l'avaluació.
Aquestes son les diferents fases de l'anàlisi, que es descriuen a continuació:

- *Fase de reconeixement:* Possiblement, aquesta sigui una de les etapes que més temps demani. Així mateix, es defineixen objectius i es recopila tota la informació possible que després serà utilitzada al llarg de les següents fases. La informació que es busca avarca des noms i adreces de correu dels usuaris del sistema, fins a la topologia de la xarxa, adreces IP, entre d'altres. Cal destacar que el tipus d'informació o la profunditat de la perquisició dependran dels objectius que s'hagin fixat en el test.
- *Fase d'escaneig:* Utilitzant la informació obtinguda prèviament es busquen possibles vectors d'atac. Aquesta etapa involucra l'escaneig de ports i serveis. Posteriorment es realitza l'escaneig de vulnerabilitats que permetrà definir els vectors d'atac.
- *Fase d'enumeració:* L'objectiu d'aquesta etapa és l'obtenció de les dades referent als usuaris, noms d'equips, serveis de xarxa, entre d'altres. A aquesta alçada del test, es realitzen connexions actives amb el sistema i s'executen consultes dins del mateix.
- *Fase d'accés:* En aquesta etapa finalment es realitza l'accés al sistema. Aquesta tasca s'aconsegueix a partir de l'explotació d'aquelles vulnerabilitats detectades que van ser aprofitades per la persona que fa el test per a comprometre el sistema.
- *Fase de manteniment d'accés:* Després d'haver-se obtingut l'accés al sistema, es busca la manera de preservar el sistema compromès a disposició de qui ho ha atacat. L'objectiu és mantenir l'accés a l'esmentat sistema perdurable en el temps.

Aquestes fases del test dx poden fer de dues formes:

1- Externa: l'objectiu és accedir en forma remota a l'equip i posicionar-se com administrador del sistema. Es realitzen des de fora del Firewall i consisteixen a penetrar a la Zona Desmilitaritzada (DMZ), en el cas que en tingui, per després accedir a la xarxa interna. Les principals proves d'aquesta fase son:

- Proves d'usuaris i la "força" dels seus passwords.
- Captura de trànsit.
- Detecció de connexions externes i els seus rangs d'adreces.
- Detecció de protocols utilitzats.
- *Scanning* de ports TCP, UDP i ICMP.
- Intents d'accés via accessos remots.
- En el cas d'una organització, anàlisi de la seguretat de les connexions amb proveïdors, treballadors remots o entitats externes a l'organització.
- Proves de vulnerabilitats existents i conegudes en el moment de realització del test.
- Prova d'atacs de Denegació de Servei.

2- Interna: aquesta fase es realitzarà en aquells equips que formin part d'una organització amb accés a diferents usuaris. Es tracta de demostrar quin és el nivell de seguretat interna. S'haurà d'establir que pot fer un atacant intern i fins on serà capaç de penetrar en el sistema com a usuari amb privilegis baixos. Aquest es compon principalment de les proves següents:

- Anàlisi de protocols interns i les seves vulnerabilitats.
- Autenticació d'usuaris.
- Verificació de permisos i recursos compartits.
- Test dels servidors principals (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilitat sobre les aplicacions propietàries.
- Nivell de detecció de la intrusió dels sistemes.
- Anàlisi de la seguretat de les estacions de treball.
- Seguretat de la xarxa.
- Verificació de regles d'accés.
- Atacs de denegació de servei

3.2. DISTRO BACTRACK 5

3.2.1. Característiques:

BackTrack és una distro GNU / Linux en format LiveCD pensada i dissenyada per a l'auditoria de seguretat i relacionada amb la seguretat informàtica en general. Actualment, tot i ser una distro antiga, encara té una gran popularitat i acceptació en la comunitat que es mou al voltant de la seguretat informàtica.

El seu nom va ser creat arran de l'algoritme de cerca "Backtraking".
Es va originar a partir de la fusió de dues distros de la competència, tant basats en Knoppix que es van centrar en les proves de penetració:
- WHax: desenvolupat per Mati Aharoni, un consultor de seguretat.
- Auditor Security Collection: un Live CD desenvolupat per Màx Moser que va incloure més de 300 eines de fàcil maneig organitzat.

En aquesta versió de Backtrack inclou nativament els gestors de finestres d'escriptori Gnome, KDE i Fluxbox.
Dona suport a arquitectures de 32 i 64 bit, ARM: facilitant l'anàlisi forense i la possibilitat d'executar-se en telèfons mòbils.
Conté el Kernel 3.2.6 amb suport millorat d'hardware.

Aquesta distro té una comunitat d'usuaris de més de 4 milions de descàrregues, amb un projecte de codi obert ("Open Source") iniciat per Mati Aharoni i Màx Moser i seguit per un equip de persones per tot el món.

La instal.lació està pensada per fer-la des d'una imatge (ISO) format LiveCD mitjançant:

- *LiveCD*: com a sistema operatiu amb memòria virtual des d'un CD en iniciar el sistema.
- *LiveUSB*: com a sistema operatiu amb memòria virtual des d'un USB pendrive en iniciar el sistema.
- *VMWare*: creant una màquina virtual amb VirtualBox (opció més recomanada).
- *Partició HDD*: instal·lació en una partició del disc dur com a sistema operatiu principal o secundari.

La descàrrega del fitxer. ISO es pot fer des de la pàgina oficial (http://www.backtrack-linux.org/downloads/) o altres servidors.

Il·lustració 2. Escriptori distro Backtrack 5 r3.

3.2.2 Programari:

Conté més de 300 eines de seguretat amb serveis públics que son tots de codi obert. Podem agrupar les eines que conté en les següents categories:

- Recull d'Informació
- Mapeig de Ports
- Identificació de Vulnerabilitats
- Anàlisi d'aplicacions web
- Anàlisi de xarxes de ràdio (WiFi, Bluetooth, RFID)

- Penetració (Exploits i Kit d'eines d'enginyeria social)
- Escalada de privilegis
- Manteniment d'Accés forense
- Enginyeria inversa
- Veu sobre IP.

Sota cadascuna de les categories principals, trobarem subtítols...

3.2.3. Avantatges

L'avantatge de Backtrack 5 (BT5) és que ofereix una sèrie d'eines de seguretat i forenses en un DVD en viu, a punt per utilitzar. Està basada en Ubuntu Lúcid (10.04 LTS) amb el nucli Linux 2.6.38 i alguns drivers apedaçats WiFi per permetre atacs d'injecció. Podeu descarregar la distro en un GNOME , KDE 4 i Flux box, la qual cosa permet a l'usuari descarregar l'edició amb l'entorn d'escriptori que desitgi. Per primera vegada en el moment del seu llançament, ofereix suport per arquitectures de 32 bits o 64 bits. Per primera vegada, el projecte també té una imatge per ARM, que es pot executar al telèfon intel·ligent o tauleta per provar la seguretat d'una xarxa sense fil.

El menú d'arrencada de BackTrack dóna diverses opcions. L'opció per defecte només s'inicia una sessió en viu (una consola "framebuffer), però també hi ha una manera de cautela que arrenca la distro sense generar cap tràfic de xarxa: cal habilitar la xarxa manualment més tard. Això és interessant si es vol ocultar la seva presència a la xarxa temporalment. Una altra bona opció és la manera d'anàlisi forense, que no munta automàticament les unitats de l'equip i tampoc no utilitza cap espai d'intercanvi que troba. Quan la investigació forense d'un sistema, el que garanteix que no accidentalment eliminar rastres ocults.

La versió 5 d'aquest programari és la primera que inclou el codi font complet dintre dels seus repositoris, de tal forma que aclareix qualsevol problema de llicències que s'hagi presentat fins la seva versió 4.

3.2.4. Inconvenients

Un desavantatge de BT5 és que no es pot actualitzar a la mateixa des BT4, si s'ha instal·lat i configurat una instal·lació BT4 anteriorment. D'altra banda, algunes eines interessants com Pyrit, que utilitza el poder de processament de la GPU per accelerar el trencament de contrasenyes WPA, i els escàners OpenVAS de vulnerabilitat, han caigut en BT5, tot i que poden anar de forma manual.

El punt més feble de BackTrack és la documentació. És escassa, fragmentària, i sovint obsoletes. Molts consells i tutorials que trobem a la pàgina web de BackTrack oficial i el seu "wiki" eren per a les versions anteriors i no funcionaven en BT5, i altres documents no expliquen quina és la versió que estaven parlant. No obstant això, també hi ha alguns documents molt detallats i molt bons en el lloc web, i, òbviament, la documentació és un treball en progrés, per la qual cosa depenent del que es necessita la quantitat d'informació trobada varia.

3.3. DISTRO PENTOO RC2.1

3.3.1. Característiques

Pentoo és una distro GNU/Linux comercialitzada en format Live CD i Live USB dissenyat per a proves de penetració i avaluació de seguretat en xarxes. Està basat en Gentoo Linux, i ofereix

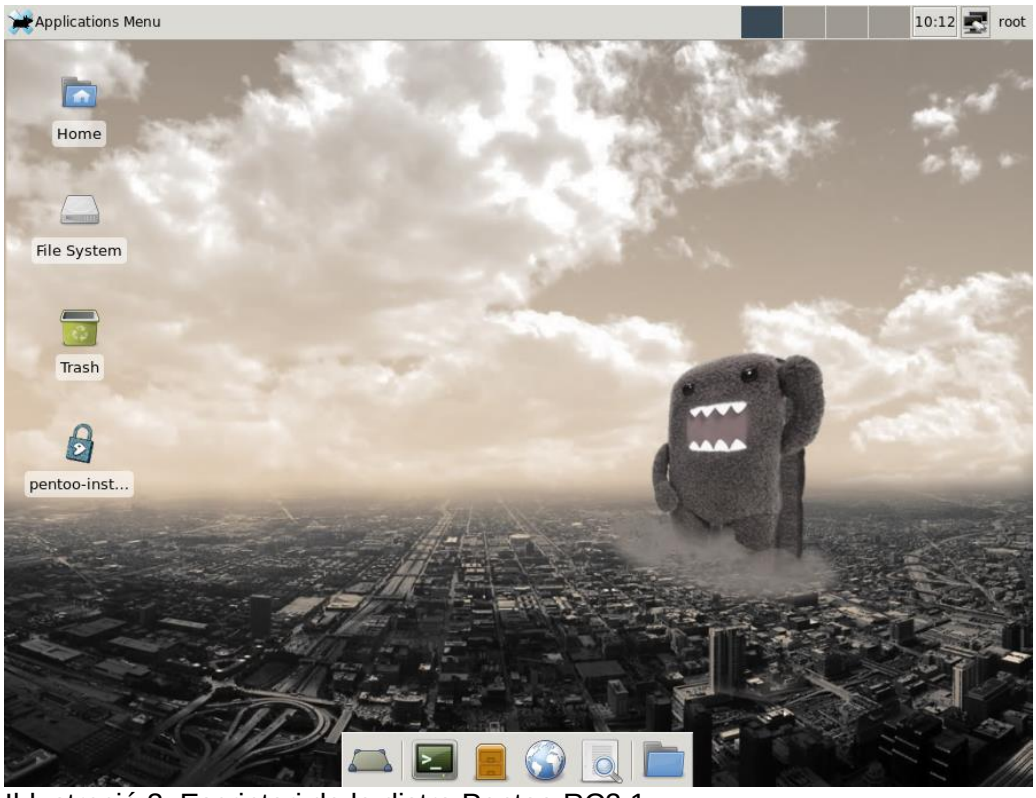
una arquitectura de 32 i 64 bits. Pentoo també està disponible com a plantilla per a un sistema operatiu Gentoo existent.
Compta amb controladors d'injecció de paquets amb correccions wifi, GPGPU cracking de programari (càlculs generals sobre les targetes de gràfics GPU en lloc de CPU), el qual és molt útil per desxifrar contrasenyes. Utilitza una superposició Pentoo, que permet a les eines que es construirà a la part superior d'una acumulació Gentoo estàndard.
Aquesta distro dona suport per xifrat de disc complet amb Luks si aquesta, està instal·lat al disc dur per donar major robustesa i seguretat.

El nucli Pentoo inclou GrSecurity i protecció PAX i amb un enfortit i personalitzat nucli que inclou afegits “patches aufs”.
Aquesta última distro llançada, inclou una versió 3.7.5 del nucli reconstruït i enfortit amb eines pròpies de Pentoo i molt especialment «enfortit» per als sistemes de 64 bits.

Pel que fa a la «Wifi stack» ella ha estat portada des de la versió més estable del nucli.
En la utilització de les seves eines fen un test de seguretat, donant la possibilitat d'anar guardant tot canvi que es vagi realitzant en un dispositiu USB (*pendrive*).
Si ja el té instal·lat, disposa també de les actualitzacions del sistema, la qual cosa fa més ràpid el seu funcionament.

El gestor d'escriptori que utilitza es Xfce wmel qual és més lleuger que GNOME i KDE. El seu objectiu és ser ràpid i servir pocs recursos del sistema, sense deixar de ser visualment atractiu i fàcil d'utilitzar.

Una característica pròpia d'aquesta distros és que suporta eines de desenvolupament per trencament de claus amb força bruta amb programació Cuda i OpenCL. Aquest tipus de programació permeten crear aplicacions amb paral·lelisme a nivell de dades i de tasques que poden executar tant en unitats centrals de processament com a unitats de processament gràfic, augmentant el rendiment de trencament per força bruta de qualsevol sistema treballant conjuntament amb les tècniques de GPGPU.



Il·lustració 3. Escriptori de la distro Pentoo RC2.1

El pre-configurat de la distro LiveCD alhora d'instal.lar-se es construeix de forma automàtica a partir de codi font i es personalitza amb la funcionalitat que l'usuari desitgi i sense les característiques innecessàries que vulgui evitar.

La descàrrega des de la seva pàgina oficial (www.pentoo.ch/donwloads) o altres servidors, en format ISO, dona les següents opcions:

- *LiveCD*: com a sistema operatiu amb memòria virtual des d'un CD en iniciar el sistema.
- *LiveUSB*: com a sistema operatiu amb memòria virtual des d'un USB pendrive en iniciar el sistema.
- *VMWare:* creant una màquina virtual amb VirtualBox (opció més recomanada).
- *Partició HDD*: instal·lació en una partició del disc dur com a sistema operatiu principal o secundari.

Pentoo no és altra cosa que Gentoo amb una plantilla pentoo superposada. Aquesta superposició està disponible en layman pel que l'única cosa que ha de fer, si li interessa i és usuari de Gentoo, s'ha d'escriure a la consola de comandes:
layman-L and layman-a pentoo

3.3.2. Programari

Algunes d'aquestes categories i eines són:

- *Analyser*: En aquesta categoria tenim eines d'anàlisi de tràfic de xarxa i diversos tipus de detectors, és a dir, programari que " ensuma " (del terme anglès *sniff*) diferents paquets de xarxa. El *sniffer* per excel·lència és Ethereal.
- *Bluetooth:* Aquí podem veure diferents eines d'auditoria, anàlisi i administració d'aquest protocol. Particularment *BlueSniff* és un *sniffer* de paquets bluetooth.
- *Cracker / Bruter*: En aquesta categoria principalment hi ha una varietat d'eines per vulnerar contrasenyes, tant de sistemes windows com GNU / Linux. En cas de voler realitzar atacs per diccionari, també tenim disponible una llista de paraules (en anglès). Els més coneguts són el mític "John the Ripper " i " Hydra ".
- *Fingerprinter*: Aquí tenim una àmplia varietat de diferents eines per a diferents tipus de fingerprinting, per exemple smtpmap per a diferents tipus de protocols de correu electrònic, Blueprint per Bluetooth, Siphon per a Sistemes Operatius i molts més.
-*Forging / Spoofing*: Eines diverses per ARP spoofing, DNS spoofing, traci, etc.
- *Misc*: Aquí tenim eines que no entren en una altra categoria, per exemple Firewall Builder és una eina per configurar i administrar Tallafocs, MAC Changer adreces MAC.
- *Pentest / MITM*: En aquesta categoria tenim eines particulars de tests de penetració i altres que apliquen la tècnica MITM (Man In The Middle) inventada per Kevin Mitnick. Per exemple Cisco - *Torch*: és un escàner, trencador de contrasenyes per força bruta i testejador de vulnerabilitats per a la majoria dels dispositius CISCO. D'altra banda Yersinia és una *suite* per a problemes de seguretat a diferents protocols de xarxa.
- *Proxy:* aquí disposem d'aplicacions proxy, per exemple Burpproxy que captura tot el trànsit del navegador web i permet modificar els paquets, o bé Paros, una utilitat que corre totalment a java i permet interceptar trànsit http i https per després modificar-lo i testejar diferents aplicacions web.
- *Scanner*: En aquesta categoria trobem diferents tipus d'escàners, tant de ports com ara nmap o bé de vulnerabilitats com Nessus. També tenim la utilitat Firewalk que no permet avaluar a grans trets les regles d'un firewall per veure si estan ben configurades.
- *Wireless*: Aquí podem trobar tot tipus d'eines per al protocol 802.11, tant per rastrejar paquets, vulnerar el protocol WEP, detectar falsos punts d'accés, etc.
- *Docs*: En aquesta carpeta tenim moltíssima documentació sobre les diferents eines que componen les categories esmentades anteriorment.

- *Fingerprints DV*: Aquí disposem de bases de dades per a les diferents eines que realitzaven diferents tipus de fingerprints (Sistema Operatiu, dispositius, etc.).
- *Network tools*: Una utilitat que integra diferents tipus d'eines simples que són molt útils al moment d'analitzar l'entorn on s'està treballant. Per exemple *whois, traceroute, escaneig de ports*, etc.

3.3.3. Avantatges

Aquesta distro és l'única que permet un alt nivell de personalització. Es pot desar el fitxer / etc., / root, plugins de Nessus i ExploitTree + i personalitzar el mòdul. Atès que l'arxiu / etc es carrega a l'inici del *rc init*, es pot personalitzar el que es vulgui en ell.
Pentoo permet fer eleccions, de forma fàcil i cada vegada, l'usuari sap el que està fent i el que ha de fer. És un control complet sobre el sistema. Les distros basades en Gentoo té la més completa documentació i la millor comunitat.

3.3.4. Inconvenients

No ofereix ZFS al menú durant la instal·lació. ZFS és un sistema d'arxius que destaca per la seva gran capacitat, integració dels conceptes anteriorment separats de sistema de fitxers i administrador de volums en un sol producte, nova estructura sobre el disc, sistemes d'arxius lleugers i una administració d'espais d'emmagatzematge senzilla.
Encara que Pentoo ofereix millores visuals amb el seu últim llançament, li manca tenir un instal·lador GUI per permetre que més persones ho instal·len sense la por de llegir la guia.

3.4. DISTRO WIFISLAX 4.8

3.4.1. Característiques

Wifislax està basat bàsicament i principalment en SLAX (basat en la distro Slackware Linux).
Està especialitzada en l'auditoria de xarxes sense fils (Wireless) a més de posseir eines de gestió i ús quotidià com, Reparadors d'arrencada, processadors de text, etc.
En aquesta distro es vol mantenir la idea principal que l'enfocament de la seguretat ve efectuat sobre les xarxes sense fils, per tant conté una gran quantitat d'eines orientades a les xarxes sense fils tot i que n'està dotat també amb moltes ajustades a la seguretat en general.
El nucli Linux és la versió 3.13, apedaçat per a una millor auditoria "wireless", així com el "Canal 1" correcció d'errors. Moltes de les aplicacions de seguretat incloses també es van millorar i es van agregar diverses de noves.
Els dos escriptoris disponibles, KDE i Xfce 4.10 4.10.5, vénen des de l'original, Slackware 14.1 repositori.

Il·lustració 4. Escriptori distro Wifislax 4.8.

Les diferents formes d'instal.lació es configuren totes a partir de la descàrrega des de la seva pàgina oficial (http://www.wifislax.com/descargas-depositfiles) o altres servidors en format ISO:

- *LiveCD:* com a sistema operatiu amb memòria virtual des d'un CD en iniciar el sistema.
- *LiveUSB*: com a sistema operatiu amb memòria virtual des d'un USB pendrive en iniciar el sistema.
- *VMWare*: creant una màquina virtual amb VirtualBox (opció més recomanada).
- *Partició HDD*: instal·lació en una partició del disc dur com a sistema operatiu principal o secundari.

La instal.lació de WifiSlax 4.8 en un disc dur és la més complexa entre totes les opcions, però si fas servir aquesta distro sovint, és la més eficient. Funcionarà molt més ràpid i es podrà guardar totes les teves configuracions, contrasenyes, documents i processos sense acabar.

3.4.2. Programari:

- **SUITE aircrack-NG:**
Aquesta és la bíblia de l'auditoria de seguretat wireless.
En aquesta *suite* es basen gairebé totes (per no dir totes) les eines d'auditories que s'utilitzen avui en dia, per als atacs als protocols de seguretat i encriptació dels *routers* existents.
Aquesta *suite* consta entre altres, de les següents eines, les quals hem considerat les més comunes:

- *Airmon-ng: a*questa comanda, usat tal com ens mostra informació sobre el xip del nostre dispositiu *wireless*, si li afegim la variable *start* / *stop* posarà el dispositiu en mode monitor o administrador, segons quina s'utilitzi.
- *Airodump-ng: s*'usa per capturar les dades transmeses a través de les ones wifi, concretament les balises manades pels *routers* propers (Beacons) i els IVs (vectors inicials) dels paquets WEP.
- *Aireplay-ng:* s'utilitza per injectar paquets. La seva funció principal és generar trànsit per usar més tard amb aircrack-ng i poder *crackejar* claus WEP i WPA-PSK.
- *Aircrack-ng: s*'utilitza per desencriptar els paquets capturats i així obtenir la clau de la xarxa wifi.

Per a això li indicarem l'arxiu, que hem capturat prèviament amb *airodump-ng* i comences el procés de desxifrat, fins que ens digui si va trobar la clau o no, de ser negatiu el resultat, ens indiqués que seguim capturant paquets fins a un nombre X

- Eines d'auditoria (desxifrat WEP):

Explicarem l'ús de les següents de les eines més importants:

-*Airoscript:*és un *script* basat en *la suite aircrack-ng*, amb el qual es poden realitzar tots els atacs d'*aquesta suite* d'una manera automàtica (sense introduir un sol comandament).

- *Goyscript-WEP:* eina basada en *la suite Aircrack-ng* per a l'explotació de vulnerabilitats en el xifrat WEP.

- *MinidWep-GTK:* amb aquesta *GUI* es pot auditar, tant xarxes amb xifrats WEP, com xarxes amb xifrats WPA, fins i tot podrem usar "reaver".

- Eines per auditar xarxes amb xifrats WPA:

- *Goyscript WPA: script* per capturar *handshake*.

- *BrutusHack:* és un *script*, per passar diccionaris amb els paràmetres configurats prèviament a un *handshake*, prèviament capturat, i realitzar atacs de força bruta més ràpids.

- *Goyscript DIC:* és un *script*, per passar 4 diccionaris amb els paràmetres configurats prèviament a un *handshake*. L'eina detecta automàticament els *handshake* capturats amb Goyscript WPA i mostra una llista amb els que es té guardats, perquè es triï el que es vol utilitzar.

- *StrinGenerator: g*enerador de diccionaris, per atacar handshake de xarxes WPA.

Es pot crear els propis diccionaris amb les variables que es considerin oportunes per a cada cas.

-*WPA-gui-QT:* senzilla GUI per passar diccionaris amb *aircrack-ng*.

- *Airlin:* és un provador de claus contingudes en un diccionari de text pla, que comprova una a una cada clau del diccionari i valida contra l'AP, pel que no necessita *handshake*, però si necessita estar en línia.

- Eines per atacs al protocol WPS de xarxes WPA:

- *Wash:*eina per detectar objectius amb WPS activat.

- *Reaver:* és una eina per a atacs per força bruta al protocol WPS.

- *WPSPinGenerator:* eina que ens mostra els objectius amb WPS activat. Compara la seva adreça MAC amb la seva base de dades per comprovar si el *router* utilitza un *pin* amb patró conegut o genèric.

- *GOYscript WPS:* s*cript* per atacar el protocol WPS.

- Eines de Hacking en xarxa:

- *CookiesMoster:* GUI, per capturar les galetes, amb credencials d'accés dels dispositius que estiguin en la mateixa xarxa que s'analitza.

- *"El cazador cazado":* és un *script* per espantar els intrusos d'una xarxa que es vulgui protegir. S'aconsegueix que el client no desitjat, no pugui navegar i que cada vegada que intenti visitar una *web,* només aconsegueixi veure una pàgina que s'ha creat prèviament amb un missatge del tipus "No em robis la connexió, t'estic vigilant".

-*AirSSL:* eina per crear un AP fals.

3.4.3. Avantatges

Wifislax és únic en què més enllà de la inclusió de les proves de seguretat basada en Wi-Fi i la penetració de les eines del seu nucli també s'actualitza amb diversos drivers no oficials per assegurar-se que és compatible amb la major quantitat de maquinari wifi fora de la caixa. Això és molt important quan es tracta de provar i depurar la seguretat de les xarxes sense fils.

Pel que fa a les aplicacions, a estat dotat de certes eines molt importants per a l'auditoria *wireless* que seran de fàcil maneig per a tothom, com ara el *airoscript*, així com el mateix *airoscript*

específic i adaptat per a les *ipw2200* . A més estan incorporades una sèrie de llançadors gràfics per facilitar l'excés d'ús del teclat per a moltes eines, encara que no oblidar que aquests llançadors només aglutinen una ínfima part de les possibilitats de desenvolupament amb el treball amb comandaments bàsics. Aquests llançadors són *scripts* gràfics de molt fàcil ús.

3.4.4. Inconvenients

Un dels desavantatges que hi han és que no tots els *chipsets* de les targetes sense fils suporten *la suite* d'*aircrack-ng*, fins i tot hi *chipset* que són compatibles només amb algunes de les funcions del *aircrack-ng* o no pot funcionar.

4. ANÀLISI GENERAL DE LES EINES DE DISTROS ESPECIALITZADES EN SEGURETAT EN XARXES

El programari que conté aquestes distros, son majoritàriament eines per fer test de vulnerabilitats. A aquest conjunt d'eines se li anomena "Toolkits" i son programari que normalment és executat en una consola de comandes per l'usuari.
Aquestes eines les podem agrupar, segons la seva funcionalitat:

4.1. Escanejadors de ports:

El terme escàner de ports o escaneig de ports s'empra per designar l'acció d'analitzar per mitjà d'un programa l'estat dels ports d'una màquina connectada a una xarxa de comunicacions. Detecta si un port està obert, tancat, o protegit per un tallafoc.
S'utilitza per detectar quins serveis comuns està oferint la màquina i possibles vulnerabilitats de seguretat, segons els ports oberts. També pot arribar a detectar el sistema operatiu que està executant la màquina, segons els ports que té oberts.

- *Chkrootkit* : sistema d'exploració per *troians*, cucs i *exploits* (fragment de programari que aprofita una vulnerabilitat d'un sistema per aconseguir un comportament no desitjat del mateix) .
- *Detector de rootkit* : és un *rootkit* és un programari que permet un accés de privilegi continu a un ordinador, però que manté la seva presència activament oculta al control dels administradors en corrompre el funcionament normal del sistema operatiu o d'altres aplicacions.
- *Checkps:* detectar *rootkits* mitjançant la detecció de la sortida falsa i anomalies similars.
- *Caçadors antiRootkit*: exploracions per *rootkits*, portes posteriors i gestes locals.
- *Rkdet*: dimoni detector de *rootkits*. La intenció d'atrapar a algú la instal·lació d'un *rootkit* o executar un analitzador de paquets.
- *fsaudit* : *script* de Perl per analitzar els sistemes d'arxius i recerca de directoris d'aspecte sospitós.
- *COPS : Contrasenya del sistema Oracle i Computer*: controls de seguretat de UNIX. Els programes i *scripts* de *shell* que realitzen controls de seguretat. Les comprovacions inclouen permisos d'arxius i directoris, claus, els *scripts* del sistema, arxius SUID, comprovació de la configuració FTP, etc.
- *SATAN (Eina de Seguretat per l'Anàlisi de Xarxes)*: és una eina que recol·lecta una gran varietat d'informació sobre hosts de xarxa.
- *SARA: Assistent d'Investigació de l'auditor de Seguretat:* escàner de seguretat de xarxa de la vulnerabilitat de les injeccions de SQL, exploració remota, etc. (seguiment a l'eina d'anàlisi de SATAN).
- *Nessus* : és l'eina d'avaluació de seguretat "Open Source". Permet generar informes en HTML, XML, Làtex, i text ASCII; també suggereix solucions per als problemes de seguretat.
- *OpenVAS* : és un sistema d'avaluació de vulnerabilitat obert. Una branca de Nessus que és més lliure de les restriccions de llicència.

- *Argus*: és una eina d'auditoria de transaccions IP . Aquest dimoni llegeix els *datagrames* de la xarxa des d'una interfície especificada i genera registres d'estat de trànsit de la xarxa
- *Intersect Alliance:* identifica els intents d'accessos maliciosos i els no autoritzats.
- *nmap*: és un programa de codi obert que serveix per efectuar rastreig de ports i serveis que està executant una màquina. Identifica ordinadors en una xarxa, per exemple llistant aquelles que responen *ping*.
- *UnicornScan:* escaneja ports de forma ràpida i superficial. També vegi *onetwopunch.sh* automatitzar UnicornScans.
- *Portscanner:* és una aplicació de programari dissenyada per sondejar un servidor o host per ports oberts. Això és sovint utilitzat pels administradors per verificar les polítiques de seguretat de les seves xarxes i pels atacants per identificar serveis que s'executen en un host per tal de comprometre. Els tipus d'escanejadors de ports més importants son: TCP SYN ,TCP FIN , TCP ftp proxy, UDP recvfrom(), ICMP.

4.2. Generador de paquets:

Un generador de paquets o un paquet constructor és un tipus de programari que genera paquets aleatoris o permet a l'usuari construir paquets personalitzats detallades. Depenent del mitjà de xarxa i el sistema operatiu, els generadors de paquets utilitzen connectors directes, trucades a funcions NDIS, o accés directe al controlador en mode nucli d'adaptador de xarxa. Això és útil per implementacions de prova de piles IP per bugs i vulnerabilitats de seguretat.

- *Nemesis*: és un injectors de paquets simplificat. El *kit* està separat per protocols, i permet crear *scripts* útils de fluxos de paquets injectats des de simples *scripts* de *shell*.
- *lorcon:* és una eina de xarxa de codi obert. És una biblioteca per injectar paquets 802.11 (WLAN), capaç d'injectar a través de múltiples infraestructures digitals, sense la necessitat de canviar el codi de l'aplicació.
- *Aireplay-ng*: la funció principal és generar trànsit per a l'ús posterior en *aircrack-ng* per desxifrar les claus basades en WEP i WPA-PSK.
- *WinPcap:* és una eina per accedir a la connexió entre capes de xarxa en entorns Windows. Permet a les aplicacions capturar i transmetre els paquets de xarxa enllaçant la pila de protocols; i té útils característiques addicionals que inclouen el filtratge de paquets a nivell del nucli.
-*Arping:* envia i rep paquets UDP utilitzant el protocol ICMP.
- *Ipsend:* genera paquets TCP/IP
- *LibNet:* és una eina que genera els paquets TCP / IP amb un llenguatge de *scripting*. Això va ser escrit per provar quina mida fragments TCP que obtindrien a través de diversos filtres de paquets TCP / IP, com s'usa en els servidors de seguretat IP.

4.3. Analitzadors de paquets:

Anomenats també “sniffers”, és un programa d'ordinador o una peça de maquinari informàtic que pot interceptar i enregistrar el trànsit que passa a través d'una xarxa digital o part d'una xarxa. Com el flux dels corrents de dades a través de la xarxa, l' *sniffer* captura tots els paquets i, si cal, descodifica les dades en brut de paquets, que mostra els valors de diversos camps en el paquet, i s'analitza el seu contingut.

Eines Linux per a l'examen de la xarxa.

- *DSniff*- eines de xarxa d'auditoria i proves de penetració.
- *Wireshark:* és un analitzador de protocols utilitzat per realitzar anàlisis i solucionar problemes en xarxes de comunicacions, per a desenvolupament de programari i protocols, i com una eina didàctica. Compta amb totes les característiques estàndards d'un analitzador de protocols de forma únicament buida. Abans era conegut com Ethereal.

- *Tcpdump*: monitor de xarxa i adquisició de dades
- *KISMET*: 802.11a/b/g detector de xarxa sense fil, *sniffer* i un sistema de detecció d'intrusos.
- *DISC:* descobriment IP passiva i una eina de presa d'empremtes dactilars. S'asseu en un segment d'una xarxa per descobrir adreces IP úniques i identificar-los.
- *Yersina*: dissenyat per analitzar i provar les xarxes i els sistemes implementats. Dissenyat per aprofitar alguna debilitat en els diferents protocols de capa 2: Protocol Spanning Tree (STP), Cisco Discovery Protocol (CDP), Protocol d'enllaç troncal dinàmic (DTP), Protocol de configuració dinàmica d'amfitrió (DHCP), Hot Standby Router Protocol (HSRP), IEEE 802.1Q, Protocol d'enllaç Inter-Switch (ISL) i protocol d'enllaç troncal de BLAN (VTP).
- *Ippl:* és un dimoni que registra els paquets IP enviats a un ordinador. S'executa en segon pla, i mostra informació sobre els paquets entrants.
- *GnuSniff:* és un *sniffer* per monitoritzar múltiples processos, basat en escriptori GNOME que va ser escrit utilitzant libpcap.
- *Ettercap*: és un interceptor i enregistrador per LAN's amb *switch*. Suporta direccions actives i passives de diversos protocols (fins i tot aquells xifrats, com SSH i HTTPS).
- *Pdump:* aquesta eina fa moltes altres coses, com analitzar les dades en brut, analitzar contrasenyes o especificat paquets, "spoofing" (tècniques de suplantació d'identitat) com ara adreces MAC, modificar els paquets de xarxa, crea paquets ben dissenyats, etc.
-*WSA:* és una eina que audita automàticament una xarxa sense fil per a la configuració de seguretat adequada, per ajudar els administradors de xarxa a trobar les vulnerabilitats abans que els hackers intenten forçar l'entrada.

4.4. Encriptadors de comunicacions:

No son pròpiament eines de test de penetració, sinó de protecció de les comunicacions. Aquestes eines encripten les comunicacions ja sigui de veu o d'informació encriptant-los o utilitzant protocols de seguretat:

- *OpenSLL:* consisteix en un robust paquet d'eines d'administració i biblioteques relacionades amb la criptografia, que subministren funcions criptogràfiques a altres paquets com OpenSSH i navegadors web (per a accés segur a llocs HTTPS).
Aquestes eines ajuden al sistema a implementar el Secure Sockets Layer (SSL), així com altres protocols relacionats amb la seguretat, com el Transport Layer Security (TLS). OpenSSL també permet crear certificats digitals que poden aplicar-se a un servidor, per exemple Apache.
- *OpenSSH:* és un conjunt d'aplicacions que permeten realitzar comunicacions xifrades a través d'una xarxa, usant el protocol SSH. Permet accedir a una màquina remota i executar comandes. Proveeix de comunicacions xifrades i segures entre dos hosts no fiables sobre una xarxa insegura. També es poden redirigir connexions X11 i ports arbitraris de TCP / IP sobre aquest canal segur. La intenció d'aquesta eina és la de reemplaçar les comandes: 'rlogin ',' rsh' i rcp'.
- *Putty:* és un emulador de terminal lliure i de codi obert, amb consola de sèrie i aplicació de transferència d'arxius de xarxa. És compatible amb diversos protocols de xarxa, incloent SCP, SSH, Telnet, rlogin, i la connexió amb connexió directe.
- *GnuPG:* aquesta eina permet xifrar i signar les seves dades de comunicació, compta amb un sistema de clau versàtil de gestió, així com els mòduls d'accés per a tot tipus de directoris de clau pública. És una eina de línia de comandes amb funcions per a una fàcil integració amb altres aplicacions. Una gran quantitat d'aplicacions de *FrontEnd* amb biblioteques disponibles.
- *Nautilus:* és el gestor de fitxers oficials de l'entorn d'escriptori GNOME. Permet navegar pels teus arxius locals, així com pel protocol FTP, carpetes compartides windows Samba, servidors WebDAV i servidors SSH via GNOME VFS. També permet previsualització d'arxius en les seves icones, per exemple amb arxius de text pla, imatges, vídeos i so.
- *PPPTCP:* eina per establir una connexió directa entre dos nodes de xarxa. Pot proveir autenticació de connexió, xifrat de transmissió (usant ECP, RFC 1968), i compressió. Protocol PPP (*point-to-point-protocol)* és usat en diversos tipus de xarxes físiques incloent, cable serial, línia telefònica, línia troncal, telefonia cel · lular, especialitzat en enllaç de ràdio i enllaç de fibra

òptica com SONET. També és usat en les connexions d'accés a internet (comercialment anomenat "broadband").

4.5. Comprovadors d'integritat de fitxers:

Validen la integritat del sistema operatiu i els arxius de programari d'aplicació utilitzant un mètode de verificació entre l'estat de l'arxiu actual i l'estat de l'arxiu conegut per defecte. Aquest mètode de comparació sovint implica el càlcul del *checksum* criptogràfic de l'arxiu original per defecte i *checksum* criptogràfic calculat de l'estat actual de l'arxiu.

- *Tripwire:* és un comprovador d'integritat d'arxius i directoris. Ajuda a administradors i usuaris de sistemes monitoritzant alguna possible modificació en algun set de fitxers. Aquesta eina pot notificar als administradors del sistema, si algun arxiu va ser modificat o reemplaçat, perquè es puguin prendre mesures de control de danys a temps.
- *Nannie:* és una eina relativament simple, que se serveix de *stat* per construir una llista de com haurien de ser els fitxers (mida, *timestamp*, etc). Crea una llista que conté el nom de fitxer, el *inode*, informació d'enllaç, etc.
- *Chkrootkit:* permet localitzar *rootkits* coneguts, realitzant múltiples proves en les que busca entre els binaris modificats per aquest programari. Utilitza una consola la qual té eines comunes d'UNIX / Linux com les ordres *strings* i *grep* per buscar les bases de les signatures dels programes del sistema i comparant l'estat dels processos per buscar discrepàncies.

4.6. Diagnosticadors de xarxa:

Son eines per diagnosticar l'estat de les comunicacions en la capa d'IP i TCP i monitoritzar l'estat de la xarxa així com el seu consum de recursos per part dels usuaris que estan connectats a l'equip que es vol testejar.

- *Hping2:* és una eina d'observació per a xarxes, similar a *ping*. *Hping2* ensambla i envia paquets d'ICMP / UDP / TCP fets a mida i mostra les respostes. També té una manera *traceroute* bastant útil i suporta fragmentació d'IP. Aquesta eina és particularment útil en tractar d'utilitzar funcions com les de *traceroute / ping* o analitzar d'una altra manera, *hosts* darrere d'un *firewall* que bloqueja els intents que utilitzen les eines estàndards.
- *Iptraf:* és una eina basada en consola que proporciona estadístiques de xarxa. Funciona recollint informació de les connexions TCP, com les estadístiques i l'activitat de les interfícies, així com les caigudes de trànsit servidor de noms que es va a consultar. Forma part de *la suite* de programari de servidor de noms de domini BIND.
- *NetDiag:* aquesta eina de diagnòstic ajuda a aïllar problemes de connectivitat i xarxes mitjançant la realització d'una sèrie de proves per determinar l'estat del seu client de xarxa. Aquestes proves i la informació d'estat de xarxa clau que exposen, ofereixen als administradors de xarxa i personal de suport tècnic un mitjà més directe d'identificar i aïllar els problemes de xarxa. A més, pel fet que aquesta eina no requereix paràmetres o modificadors que s'especifiqui, suport tècnic, personal dels administradors de xarxa poden centrar-se en l'anàlisi de la sortida en lloc d'en formació d'usuaris com utilitzar l'eina.
- *Calamaris:* eina que analitza els arxius de registre entre una àmplia varietat de servidors Proxy web i genera informes pics d'ús, mètodes de peticions, informes d'estat de peticions internes i externes, destinacions de segon i alt nivell, tipus de continguts, i rendiment.
- *Big Sister:* és un sistema en temps real i de monitorització que consisteix en un servidor basat en web i un agent de supervisió. Pot monitoritzar els sistemes en xarxa, proporcionant una senzilla visió en temps real de l'estat de la xarxa actualTCP i UDP.
- *NetCat:* és una eina de xarxa que permet a través d'intèrpret d'ordres i amb una sintaxi senzilla obrir ports TCP / UDP en un *host* (quedant netcat a l'escolta), pot associar una *shell* a un port en concret (per connectar per exemple MS-DOS o l'intèrpret *bash* de Linux remotament). Pot forçar

connexions UDP / TCP (útil per exemple per realitzar rastrejos de ports o realitzar transferències d'arxius bit a bit entre dos equips).
- *Samspade:* és una que esta proveïda d'una interfície gràfica d'usuari (GUI) consistent i d'una implementació de diverses tasques d'investigació de xarxa útil. Útil per a moltes tasques d'exploració, administració i seguretat. Inclou eines com *ping, nslookup, whois, dig, traceroute, finger*, explorador de web cru, transferència de zona de DNS {"DNS zone transer"}, comprovació de "relay" SMTP, cerca en llocs web,etc.
- *Firewalk:* és una que utilitza tècniques de *traceroute* i valors TTL per analitzar les respostes de paquets IP per tal de determinar la porta d'enllaç ACL (Access Control List) filtres i xarxes del mapa. Es tracta d'una eina d'anàlisi de seguretat de xarxa activa de reconeixement que intenta determinar quines capa de protocols acceptarà un *firewall* determinat.
- *Dig:* (*Informació del domini Groper*) és una eina d'administració de xarxa per a consultar el sistema de noms de domini (DNS) servidors de noms. És útil per a verificar i solucionar problemes de DNS, i també per fer cerques DNS i mostrar les respostes que es retornen des del.

4.7. Tallafocs i encaminadors:

És un tipus de programari, no dissenyat per testejar sinó per donar protecció a un equip. Permet interceptar, manipular i filtrar paquets així com realitzar traducció d'adreces de xarxa (NAT) per IPv4 o mantenir registres de lòg.

- *NetFilter:* és un potent filtre de paquets el qual és implementat en el nucli Linux estàndard. L'eina *iptables* és utilitzada per a la configuració i filtrat de paquets així com la seva modificació, i tots els diferents tipus de NAT (Network Address Translation).
- *IPtables:* és l'eina més popular construït sobre Netfilter, la qual actua com tallafocs que permet no solament filtrar paquets, sinó també realitzar traducció d'adreces de xarxa (NAT) per IPv4 o mantenir registres de *lòg*.
- *Firestarter:* és una eina de tallafocs que utilitza el sistema (iptables / ipchains) Netfilter inclòs en el nucli Linux. Firestarter posseeix una interfície gràfica per configurar regles de tallafocs i altres opcions. També monitoritza en temps real tot el tràfic de xarxa del sistema, a més de facilitar el redireccionament de ports, compartir la connexió a internet i el servei DHCP.
- *SINUS Firewall:* és un filtre de paquets TCP / IP que es distribueix sota la GNU. És un tallafoc que inclou: Filtrat de tots els camps de la capçalera dels IP, TCP, UDP, ICMP, paquets IGMP, RIP intel · ligent i suport FTP, interfície d'administració gràfica per a la configuració de diversos servidors de seguretat, regles dinàmiques, prevenció del paquet i la falsificació d'adreces, i moltes més funcions.
- *Click:* és una eina per dissenyada per gestionar totes les fases de les transacciones IP en l'intercanvi de paquets i inclou suport per manipular-los així com de programació i gestió de cues.

4.8. Escàners CGI:

Un escàner de CGI és un programa que busca vulnerabilitats conegudes en els servidors webs i els programes d'aplicació de les proves en contra de les peticions HTTP CGI coneguda (interfície de passarel · la comuna). CGI, que és part de HTTP, és un mètode estàndard per als servidors webs per aprovar sol · licituds dels usuaris als programes d'aplicacions web i enviar dades de tornada dels programes per a l'usuari.
La limitació més important dels escàners de GCI és el fet que sovint no detecten la presència de vulnerabilitats que no es defineixen prèviament.

- *Linuxforce:* Auto-auditoria AdminForce CGI - Analitzador script CGI per trobar deficiències de seguretat.
- *Whisker:* és un escàner que ens permet posar a prova servidors d'HTTP pel que fa a diverses forats de seguretat coneguts, particularment, la presència de perillosos *scripts* i programes que

utilitzin CGI. *Libwhisker* és una biblioteca per *perl* (utilitzada per Whisker) que ens permet crear escàners de HTTP a mida.
- *Nikto:* és un escàner de servidors de web que busca més de 2000 arxius CGI potencialment perillosos i problemes en més de 200 servidors. Utilitza la biblioteca LibWhisker però generalment és actualitzat més freqüentment que el mateix Whisker.
- *Achilles:* és una eina designada per comprovar la seguretat d'aplicacions web. Achilles és un servidor intermediari, que actua com una "persona-en-el-mig" (man-in-the-middle) durant una sessió d'HTTP. Aquesta eina intercepta les dades en una sessió d'HTTP en qualsevol direcció i li dóna a l'usuari l'habilitat d'alterar les dades abans de ser transmesos.

4.9. Trencadors de contrasenyes:

És un programari que consisteix a desxifrar la contrasenya de determinades aplicacions triades per l'usuari. Es busca codificar els codis de xifrat en tots els àmbits de la informàtica. Es tracta del trencament o desxiframent de claus. D'aquesta forma es comprova la robustesa de les contrasenyes dels programes que s'utilitzen en l'equip.

- *AirSnort:* AirSnort és una eina per LANs sense fils (WLAN) que recupera les claus de xifrat.
- *John The Ripper:* és una eina ràpida, actualment disponible per a molts sistemes operatius de Unix. El seu propòsit principal és detectar contrasenyes basades en Unix febles. Suporta diversos tipus de *hashes* de contrasenya que són comunament trobats en diversos sistemes operatius d' Unix.
- *Hydra:* és un programari que s'utilitza per trencar les contrasenyes dels sistemes de *login* de diferents serveis com HTTP, FTP, TELNET, IMAP, SMB, SSH, etc. d'una manera molt fàcil i ràpida fent usos de diccionaris.
- *Brutus:* trencador de contrasenyes remotes, ràpid, el qual admet fins a 60 connexions, pot arribar a 2500 paraules per segon. Actua sobre els següents serveis: HTTP (Autentificació bàsica),HTTP (HTLM /CGI), POP3, FTP, SMB (netBIOS), TELNET i NETBUS.
- *MySql Brute Force:* aquesta eina permet als usuaris dur a terme atacs de força bruta sobre una base de dades MySQL Server. Aquesta utilitat totes les possibles combinacions dels noms d'usuari i contrasenyes finalment aconseguint la clau.
- *Aircrack-ng:* és una suite de programari de seguretat sense fil. Consisteix en un analitzador de paquets de xarxes, un trencador de contrasenyes de xarxes WEP i WPA/WPA2-PSK i un altre conjunt d'eines d'auditoria sense fils. Dins aquesta suit, les eines més utilitzades per a l'auditoria sense fil són: Aircrack-ng (desxifra la clau dels vectors d'inici), Airodump-ng (escaneja les xarxes i captura vectors d'inici), Aireplay-ng (injecta trànsit per elevar la captura de vectors d'inici), Airmon-ng (estableix la targeta sense fil en mode monitor, per poder capturar i injectar vectors).

4.10. Sistema de detecció d'intrusos:

(IDS de les seves sigles en anglès Intrusion Detection System) és un programa usat per detectar accessos no autoritzats a un computador d'una xarxa. Aquests accessos poden ser atacs d'usuaris hàbils ("crackers"), o de "Script Kiddies" que usen eines automàtiques.
El IDS sol tenir sensors virtuals (per exemple, un *sniffer* de xarxa) amb els quals el nucli de l'IDS pot obtenir dades externes (generalment sobre el tràfic de xarxa).

- *eXpert BSM IDS:* és un sistema basat en *host* que proporciona la supervisió de seguretat en temps real per a servidors d'aplicacions crítiques i estacions de treball. Proporciona una completa base de coneixements per a la detecció d'ús indegut d'informació privilegiada, la política de violacions, ús indegut privilegi o la subversió, la manipulació il · legal de recursos, i altres violacions en qüestions de legalitat. Aquest component s'empaqueta i distribueix com una solució de detecció d'intrusió completa, preveu la recollida de dades, anàlisi de detecció d'intrusos, una interfície de gestió d'alertes, i les directives de resposta detallades.
- *Snort:* és Sistema de poc pes (per al Sistema), capaç de realitzar anàlisi de trànsit en temps real i registre de paquets en xarxes amb IP. Pot realitzar anàlisi de protocols, recerca i identificació de

contingut i pot ser utilitzat per detectar una gran varietat d'atacs i proves, com per exemple *buffer overflows,* escanejos indetectables de ports, atacs a CGI, proves de SMB, intents de reconeixements de sistemes operatius i molt més. Snort utilitza un llenguatge flexible basat en regles per descriure el trànsit que hauria recol · lectar o deixat passar, i un motor de detecció modular.
- *SHADOW:* (*Secondary Heurístic Analysis for Defensive Online Warfare*) és una simple combinació de *tcpdump i Perl* que en realitat funciona com un NIDS (Sistema de detecció d'intrusos en una Xarxa) rudimentari però es va fer més potent utilitzant snort i / o *scripts* de *Perl* processament.
- *Lids:* un sistema de detecció i defensa d'intrusions pel nucli Linux.
- *Nidsbench:* és un conjunt d'eines de pes lleuger i portàtil per a sistemes de detecció d'intrusions de xarxa en prova. Implementa diversos atacs coneguts en contra de supervisions de xarxes passives i permet les simulacions d'atacs de rastreig a la xarxa.
- *Fragroute:* intercepta, modifica, i reescriu el trànsit de sortida, implementant la majoria dels atacs de xarxa. Entre les seves característiques, es troba un llenguatge de regles simple per retardar, duplicar, descartar, fragmentar, superposar, imprimir, reordenar, segmentar i altres operacions més en tots els paquets sortints destinats a un *host* en particular, amb un mínim suport de comportament aleatori o probabilístic.

4.11. Redirectors de ports i proxys:

És un programa per protegir un equip davant de connexions insegures a la xarxa. S'utilitza per transmetre el trànsit i les connexions a les xarxes d'ordinadors, com un "proxy". L'ús d'aquestes eines permet a un usuari ocultar la font original de la connexió de l'usuari, proporcionant privacitat, així com la capacitat per utilitzar el trànsit a través d'un lloc específic.

- *Fpipe:* la funció d'aquesta eina és la redirecció de ports, el qual crea un "túnel" per on redirigeix els ports, amb la possibilitat d'utilitzar ports UDP i TCP , fàcil d'utilitzar i efectiu.
- *WebFilter:* eina per monitoritzar el trànsit HTTP a la xarxa i bloquejar el contingut inadequat. Pot observar i respondre a les sol · licituds de dues maneres principals. Un mètode, requereix que el programari de filtrat de Web per a ser integrat amb altres dispositius de xarxa, com ara servidors proxy o portes d'enllaç. L'altre mètode requereix que el programari de filtrat web per instal·lar en un servidor independent i es col · loca a la xarxa de les màquines que vol filtrar.
- *Squid:* aquesta eina fa les funcions de *proxy* i dimoni de memòria cau de les webs. Compta amb una àmplia varietat d'usos, des de l'acceleració d'un servidor web mitjançant l'emmagatzematge en memòria cau de peticions repetides; per a l'emmagatzematge en memòria cau de webs, DNS i altres recerques de la xarxa d'ordinadors de grup de persones que comparteixen els recursos de xarxa; per ajudar a la seguretat pel tràfic de filtratge, etc. Encara que s'usa principalment per HTTP i FTP, Squid inclou compatibilitat limitada amb diversos altres protocols, incloent TLS, SSL, Internet Gopher i HTTPS.
- *Stunnel:* és una eina dissenyada per treballar com un embolcall de xifrat SSL entre un client remot i un servidor local (executable per inetd) o remot. Pot ser utilitzat per agregar funcionalitat SSL a dimonis utilitzats comunament com POP2, POP3, i servidors IMAP sense canvis en el codi del programa. Negocia una connexió SSL utilitzant la biblioteca d'OpenSSL o la SSLeay.
- *Bnc:* és una peça de programari que s'utilitza per transmetre el trànsit i les connexions a les xarxes d'ordinadors, com un intermediari. El seu ús permet a un usuari ocultar la font original de la connexió de l'usuari, proporcionant privacitat, així com la capacitat per utilitzar el trànsit a través d'una ubicació específica.

4. 12. Eines de propòsits variats:

- *E-Security Audit ToolKit:* és un conjunt d'eines dissenyades per ajudar en l'auditoria i revisió

dels elements comuns d'un sistema basat en xarxa o infraestructura. Aquest conjunt cobreix qualsevol aspecte en xarxes, servidors de seguretat, accés al sistema, accés a dades, *routers*, gestió virus, internet, etc.
- *Bastille:* és un conjunt d'*scripts* basats en Perl que endureixen un sistema. Es basa en una sèrie de preguntes que l'usuari ha de respondre, depenent d'aquestes respostes, l'eina configurarà certs paràmetres de l'ordinador per protegir-lo.
- *Kerberos:* és un protocol d'autenticació de xarxes d'ordinador que permet dos ordinadors en una xarxa insegura demostrar la seva identitat mútuament de manera segura. Ofereix autenticació mútua: tant client com servidor verifiquen la identitat un de l'altre. Els missatges d'autenticació estan protegits per evitar *eavesdropping* i atacs de *Replay*.

5. LABORATORI DE PROVES

Per entendre el funcionament bàsic de les distribucions analitzades, es realitzarà tres proves amb cadascuna de les distribucions estudiades. Una de les proves es realitzarà en el laboratori virtual, en el qual es testejarà un sistema operatiu, **Metasplotable 2.0.0**, amb la distro **Backtrack 5** per tal de trobar vulnerabilitats i explotar-les. L'altra prova que es durà a terme en el laboratori virtual, consistirà en trobar accés a un sistema operatiu per tal de poder rastrejar el tràfic web generat. Aquesta es realitzarà amb la distro **Pentoo RC2.1**.
Com a última, es trobarà la clau d'accés a una xarxa sense fil des de la distro **Wifislax 4.8** instal·lada en un *LiveCd.*
Amb aquestes proves es pretén descriure el procés de *pentesting* que es durà amb detall i anotar els resultats obtinguts per tal de poder estudiar millor les eines de cadascuna de les distro i així poder complementar d'aquesta forma l'estudi comparatiu d'aquest projecte.

5.1. Composició del laboratori de proves

El laboratori de proves consta d'un equip en el qual estan instal.lats les distribucions estudiades com a màquines virtuals i un sistema operatiu on es farà un pentest instal.lat en el mateix equip com a màquina virtual. Totes les màquines virtuals seran instal.lades amb VirtualBox versió 4.3.10.

Equip de proves: PC portàtil ASUS model A55V

- **Hardware:**

Processador: Intel Core i7-3610QM (4x2,30 GHz / 6 MB caché).
Monitor / Resolució: 15,6" glossy / 1366x768.
Memòria RAM / HDD: 8 GB RAM DDR3 /500gb
Targeta gràfica: nVidia GeForce GT 610m con 2 GB DDR3.

- **Software:**

Sistema Operatiu: Windows 7 Home Premium (2009) Service Pack 1 de 64 bits.
VirtualBox Oracle BM versió 4.2.18

Encaminador amb connexió ADSL:

- Comtrend AR-5387un

Màquina virtual: sistema operatiu Metasploitable-2:

Aquest sistema operatiu és una versió d'Ubuntu Linux intencionalment vulnerable dissenyada per provar eines de seguretat i demostrar vulnerabilitats comuns. Esta pensada per ser instal.lada a una màquina virtual compatible amb VMWare, VirtualBox, i altres plataformes de virtualització comuns. Per defecte, les interfícies de xarxa de Metasploitable es troben lligades als adaptadors de xarxa NAT i Host-only, i la imatge no es recomanable exposar-se a una xarxa hostil.

- Especificacions tècniques:
- Memòria RAM: 512 MB
- Acceleració: VT-x/AMD-V, Nested Pagin, PAE/NX
- Memòria vídeo: 12 MB /3D
- Emmagatzematge: Controlador SATA (8GB)
- Adaptador de xarxa: Intel PRO/ 1000 MT Escriptori (Adaptador només anfitrió, "VirtualBox Host-Only Ehternet Adapter"). Mode promiscu.

Màquina virtual: distribució Backtrack 5 r3:

- Especificacions tècniques:
- Memòria RAM: 2048 MB
- Acceleració: VT-x/AMD-V., paginació anidada
- Memòria vídeo: 64 MB/3D
- Emmagatzematge: Controlador SATA (20GB)
- Adaptador de xarxa: Intel PRO/ 1000 MT Escriptori (Adaptador només amfitrió, "VirtualBox Host-Only Ehternet Adapter")

Màquina virtual: distribució Pentoo RC2.1:

- Especificacions tècniques:
- Memòria RAM: 2048 MB
- Acceleració: VT-x/AMD-V, paginació anidada
- Memòria vídeo: 64 MB /3D
- Emmagatzematge: Controlador SATA (30 GB)
- Adaptador de xarxa: Intel PRO/ 1000 MT Escriptori (Adaptador només amfitrió, "VirtualBox Host-Only Ehternet Adapter"). Mode promiscu.

Màquina virtual: distribució Wifislax 4.8:

- Especificacions tècniques:
- Memòria RAM: 1024 MB
- Acceleració: VT-x/AMD-V, paginació anidada
- Memòria vídeo: 32 MB
- Emmagatzematge: Controlador IDE primari (6,24 GB)
- Adaptador de xarxa: PCnet-FAST III Escriptori (Adaptador només amfitrió, "VirtualBox Host-Only Ehternet Adapter"). Mode promiscu.

5.2. ANÀLISI AMB BACKTRACK:

La prova es realitzarà un laboratori virtual on constarà d'un sistema operatiu Metasploitable 2.0.0 instal.lat en una màquina virtual amb Virtual Box versió 4.3.10.
Es procedirà a realitzar una petita prova de *pentest* amb la distro Backtrack 5 en Metasploitable-2 (apartir d'ara en endavant nombrarem així al sistema operatiu on es fan les proves) per escanejar i trobar vulnerabilitats.

La prova consistirà en dos parts:

Primera part:
en fer un escaneig dels ports i serveis amb l'eina *Nmap*. (Aquesta fase inicial és comú a la majoria de distros especialitzades en seguretat de xarxes)

Segona part:
S'escollirà una vulnerabilitat significativa que es trobi i s'aplicaran els *exploits* per atacar-les. S'anotaran els resultats per ser posteriorment analitzats i estudiats.

S'utilitza l'eina *Nmap* per escanejar els ports d'un sistema informàtic i esbrinar el tipus de sistema operatiu de la màquina atacada.

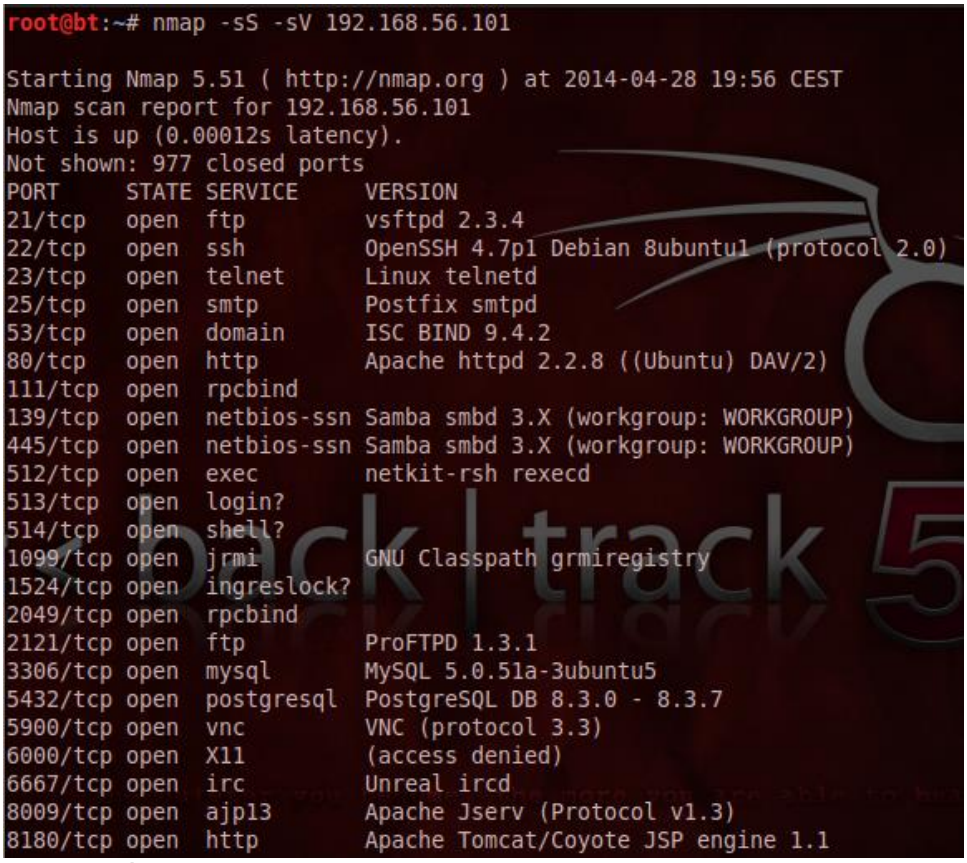
5.2.1 Primera part:

Primer de tot s'inicia en el PC de proves les dues màquines virtuals, Metasploitable-2, per ser analitzada, i la distro amb la qual es farà l'atac, BackTrack 5 r3.
Es comprova la IP de la màquina Metasploitable-2, amb la comanda *ifconfig*, i observem eth0: 192.168.56.101. Aquesta serà la IP sobre la qual es farà l'atac des de la màquina Backtrack 5.
Seguidament es fa la crida de l'eina *nmap* versió 5.51 a Backtrack 5. Això ho podem fer amb el menú desplegable (Applications> BackTrack>Information Gathering>Network Analysis>Identify Live Hosts>nmap), o bé des de la consola de comandes:

Nmap –sS –sV 192.168.56.101

Les opcions de crida de la comanda Nmap tenen els següents significats:

-sS: s'obre una connexió TCP complerta. S'envia un paquet SYN, si arriba un SYN/ACK s'envia un senyal RST (reiniciat) per tancar la connexió i d'aquesta forma fer l'escaneig sense deixar rastre.
-sV: sondeja les versions del programari que escolta als ports



Il·lustració 5. Captura de pantalla de la comanda nmap.

Es pot observar a la il·lustració 5 un llistat de tots els ports escanejats, el seu estat (obert/tancat/filtrat/no-filtrat) , el tipus de serveis que donen i la versió del programari que utilitza cada servei. En aquest cas, Metasploitable-2 és un sistema operatiu pensat per fer proves, per tant es troben molts ports oberts.

Un altre aspecte interessant de les opcions de *nmap* per saber, és el tipus de sistema operatiu de la màquina atacada. Amb aquesta comanda obtenim la informació:

nmap -O 192.168.56.101

Il·lustració 6: captura de pantalla de la comanda nmap -O.

Es pot observar a la il·lustració 6, que aquesta comanda ens retorna un llistat dels ports, el seu estat i el servei que donen així com el tipus de sistema operatiu i un interval de números de la seva versió. En aquest cas, informa que és linux 2.6.x sense poder determinar amb precisió la versió exacta fent una aproximació entre 2.6.9-2.6.31.

5.2.2 Segona part:

En aquesta segona part de la prova s'escull una de les vulnerabilitats trobades amb *Nmap* i treure'n profit per *hackejar* la màquina atacada amb el programari *Metasploit* que incorpora la distro Backtrack 5. La finalitat principal quan es vol atacar un sistema es prendre control total amb privilegis d'administrador (*root*), tot i que això sovint es difícil, sempre s'intenta poder controlar alguna part del sistema amb alguna vulnerabilitat. S'escull la trobada al port 21 que ofereix el serveix *ftp* la qual es gestiona a la màquina Metasploitable-2 amb el programari vsftpd 2.3.4 segons ens informa el nostre escaneig anterior. La raó per escollir aquesta es que és força comú en els sistemes operatius, malgrat que també es la més revisada i protegida.

A la màquina virtual Metasploitable-2 es buscarà l'*exploit* corresponent al programari vsftpd versió 2.3.4 del servei ftp i aprofitant que el port és obert, es prendrà control amb privilegis *root* de la consola *shell* d'aquest sistema.

Es començarà fent una crida des de la consola *shell* a *msfconsole* amb la qual s'entra en una interfície de comandes de *metasploit*.
Des d'aquí es busca la vulnerabilitat trobada amb *nmap* del programari *vsftpd*, amb la comanda *search vsftpd.*
Una vegada trobada i confirmada amb la versió del programari, amb la comanda *use <ruta> <nom exploit>* es força aquesta vulnerabilitat del sistema i s'entra en una altra interfície.

Amb la comanda *show options*, es mostra les possibles opcions d'aquest exploit: RHOST <IP> i RPORT <port>, amb les quals es configura l'*exploit* on s'atacarà.
Una vegada fet això amb la comanda *show payloads*, es mostra quin programari es pot utilitzar per aprofitar aquesta vulnerabilitat ja forçada amb l'*exploit*, i introduir-la en la màquina atacada, amb la configuració prèvia amb les comandes RHOST i RPORT.
Amb la comanda *set <nom payload>* es configura el programari i amb la comanda *exploit* s'executa, entrant en la consola *shell* de la màquina atacada amb els permisos *root.*

La finalitat del programari *Metasploit* inclòs a les distros orientades en seguretat de xarxes és trobar les vulnerabilitats o errors presents en qualsevol programari son aprofitades per produir efectes inesperats en els equips, un cop descobert aquest error es desenvolupaven petits programes (*exploits*) per forçar de forma específica aquesta errada al sistema.

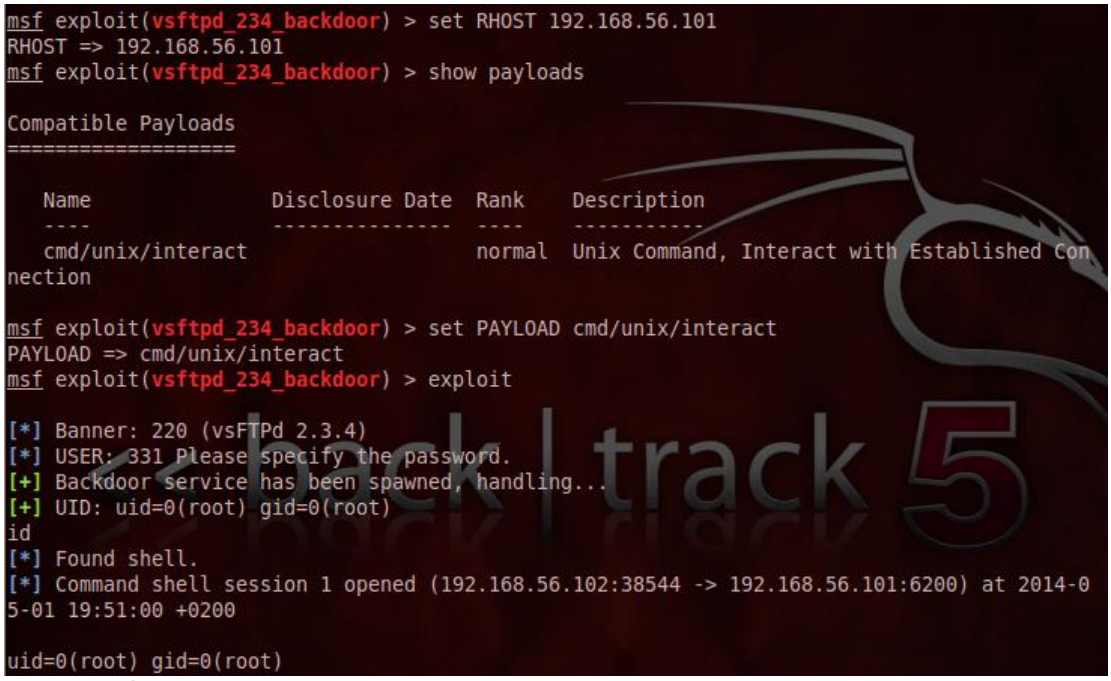
Una vegada que s'aconsegueix que el programari produeixi aquest error s'aprofita perquè l'equip faci les funcions que l'atacant vulgui.
Aquesta part del programari que proporciona una funció davant un error és el *Payload*, el qual pot ser utilitzat per diferents *exploits* i un mateix *exploit* pot utilitzar diversos *payloads.*

S'ha tingut que actualitzar la versió *Metasploit 3.7* que portava originàriament la distro Backtrack 5, a la versió 4.9.2 ja que no contenia *l'exploit vsftpd 2.3.4* per atacar la vulnerabilitat del port 21 amb servei *ftp* de la distro *Metasploitable-2*.

Es comença des de la consola de comandes, la crida de *Metasploit:*
> *msfconsole*, on seguidament sobre interfície:

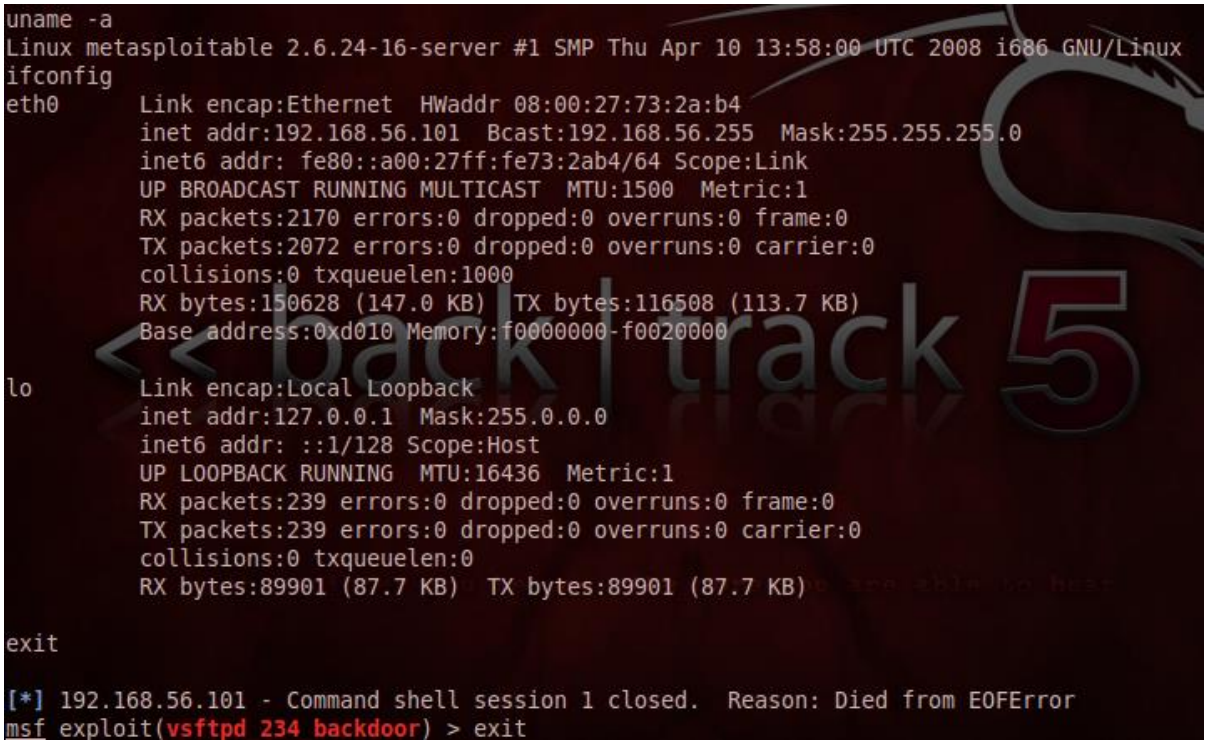
Il·lustració 7. Captura de pantalla de l'eina Metasploit.

A la il·lustració 7, s'observa com es troba amb la comanda *search, l'exploit* vsftpd_234_backdoor, el qual podem verificar que correspon amb la versió de *vsftpd v2.3.4*. Tanmateix podem observar les diferents opcions de l'exploit una vegada s'ha carregat amb la comanda *use <ruta i nom de l'exploit>.*



Il·lustració 8. Captura de pantalla de l'exploit vsftpd.

A la il·lustració 8 observem la configuració de l'*exploit* amb RHOST i el *payload* que posteriorment s'utilitzarà. Una vegada s'ha entrat remotament a la consola de comanda de la màquina Metasploitable-2, mirem els permisos que s'han obtingut amb la comanda *íd* observant que son permisos *root* (d'administrador).



Il·lustració 9. Captura de pantalla a la consola Metasploit i la comanda *uname*.

A la il·lustració 9 s'observen comprovacions efectuades dintre de la consola *shell* de la màquina Metasploitable-2 connectada remotament. Es verifica amb la comanda *uname -a* la versió del

sistema operatiu (Linux Mestasploitable 2.6.24-16) i la seva IP (192.168.56.101), on es veu efectivament que la prova s'ha dut amb èxit.

5.3. ANÀLISI AMB PENTOO:

En aquesta prova estudiarem unes de les tècniques de *pentesting* la qual consisteix en enverinar les taules ARP (*ARP spoofing*).
El ARP Spoofing, també conegut com *ARP Poisoning* o *ARP Poison Routing*, és una tècnica usada per infiltrar-se en una xarxa *ethernet* commutada (basada en *switches* i no en *hubs*), que pot permetre a l'atacant llegir paquets de dades a la LAN (xarxa d'àrea local), modificar el trànsit, o fins i tot aturar-lo.
El principi de l'*ARP Spoofing* és enviar missatges ARP falsos (falsificats, o *spoofed*) a la targeta de xarxa *Ethernet*. Normalment la finalitat és associar l'adreça MAC de l'atacant amb l'adreça IP d'un altre node (el node atacat), com ara la passarel·la predeterminada (*gateway*). Qualsevol trànsit dirigit a l'adreça IP d'aquest node, serà erròniament enviat a l'atacant, en lloc cap al seu destí real. L'atacant, pot llavors triar, entre reenviar el trànsit a la passarel·la predeterminada real (atac passiu o escolta), o modificar les dades abans de reenviar (atac actiu).
En el nostre cas farem un atac passiu, observant el tràfic de la màquina atacada amb el programari *Wireshark* que incorpora Pentoo.

En aquesta prova utilitzarem dues màquines virtuals, l'atacant (distro Pentoo) i la víctima (distro Wifislax). S'escolleix la distro Wifislax, per poder observar el tràfic web que es genera amb el seu navegador Firefox.

http://systemadmin.es/2009/12/como-hacer-arp-spoofing

Comencem esbrinant la IP de la nostra víctima la distro de Wifislax (com s'observa a la Il·lustració: 192.168.1.118) i observem que a les taules ARP només tenim la MAC del *router* (192.168.1.1)

```
wifislax ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:CF:60:EE
          inet addr:192.168.1.118  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1239 errors:0 dropped:17 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:94094 (91.8 Kb)  TX bytes:1276 (1.2 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

wifislax ~ # arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1f:a4:84:f3:87   C                     eth0
wifislax ~ #
```

Il·lustració 10. Captura de pantalla a la consola de comandes de wifislax.

Fem el mateix procés per saber la IP de la màquina atacant la distro Pentoo (192.168.1.117).

```
pentoo ~ # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.117  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe93:abca  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:ab:ca  txqueuelen 1000  (Ethernet)
        RX packets 1238  bytes 94064 (91.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2162 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 10  bytes 668 (668.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 668 (668.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pentoo ~ #
```
Il·lustració 11. Captura de pantalla de la consola de comandes de Pentoo.

Configurarem el nostre sistema, perquè reenviï tots els paquets als seus veritables destinataris mitjançant la comanda *echo*:

```
pentoo ~ # echo 1 > /proc/sys/net/ipv4/ip_forward
pentoo ~ #
```
Il·lustració 12. Captura de pantalla de la consola de comandes de Pentoo.

Ara es procedeix a enverinar les taules:
Amb l'aplicació *arpspoof -i <interface> -t <objectiu IP>* a la consola de comandes s'indica que la MAC atacant és la MAC associada a la IP del *router*:

```
pentoo ~ # arpspoof -i eth0 -t 192.168.1.1 192.168.1.118
8:0:27:93:ab:ca 0:1f:a4:84:f3:87 0806 42: arp reply 192.168.1.118 is-at 8:0:27:9
3:ab:ca
8:0:27:93:ab:ca 0:1f:a4:84:f3:87 0806 42: arp reply 192.168.1.118 is-at 8:0:27:9
3:ab:ca
8:0:27:93:ab:ca 0:1f:a4:84:f3:87 0806 42: arp reply 192.168.1.118 is-at 8:0:27:9
3:ab:ca
8:0:27:93:ab:ca 0:1f:a4:84:f3:87 0806 42: arp reply 192.168.1.118 is-at 8:0:27:9
3:ab:ca
8:0:27:93:ab:ca 0:1f:a4:84:f3:87 0806 42: arp reply 192.168.1.118 is-at 8:0:27:9
3:ab:ca
```
Il·lustració 13. Captura de pantalla de la consola de comandes de Pentoo.

A continuació fem el mateix però en paral.lel amb el (*gateaway*).

```
pentoo ~ # arpspoof -i eth0 -t 192.168.1.118 192.168.1.1
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
8:0:27:93:ab:ca 8:0:27:cf:60:ee 0806 42: arp reply 192.168.1.1 is-at 8:0:27:93:a
b:ca
```

Il·lustració 14. Captura de pantalla de la consola de comandes de Pentoo.

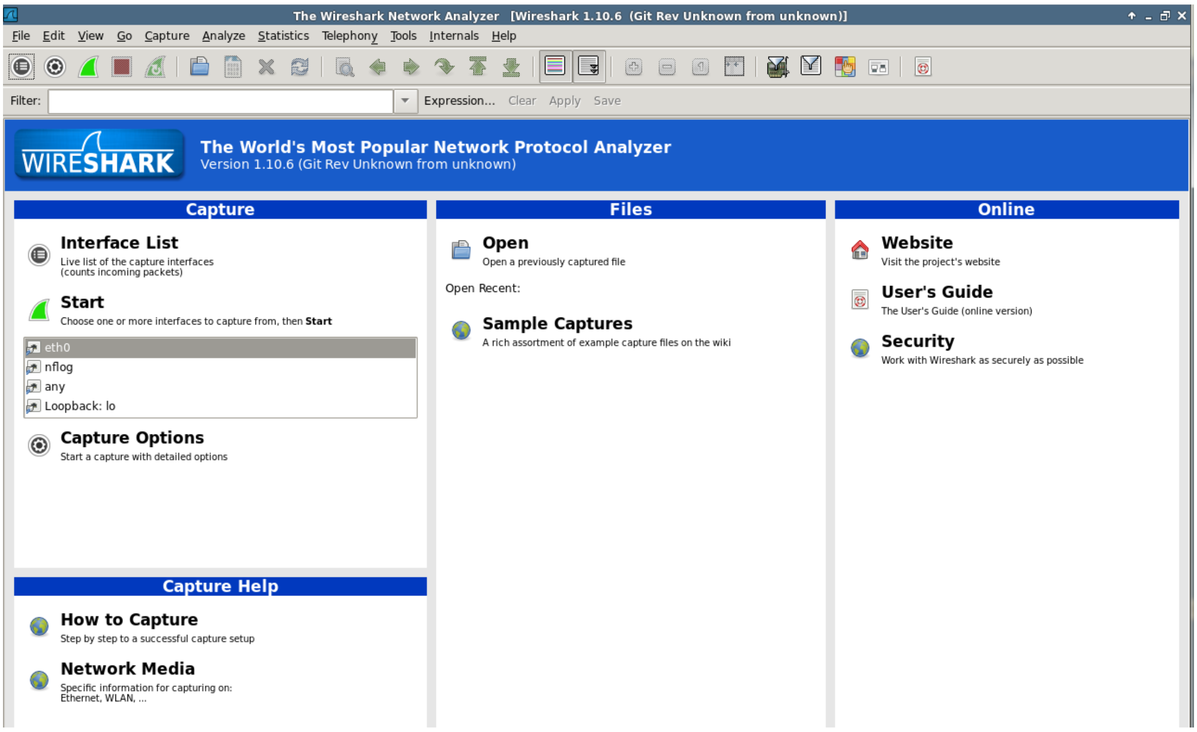
Es pot observar a la il·lustració 14 que a les taules de la distro atacant (Pentoo) esta associada la MAC de la víctima (192.168.1.118).

```
pentoo ~ # arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.118            ether   08:00:27:cf:60:ee   C                     eth0
192.168.1.1              ether   00:1f:a4:84:f3:87   C                     eth0
```

Il·lustració 15. Captura de pantalla de la consola de comandes de Pentoo.

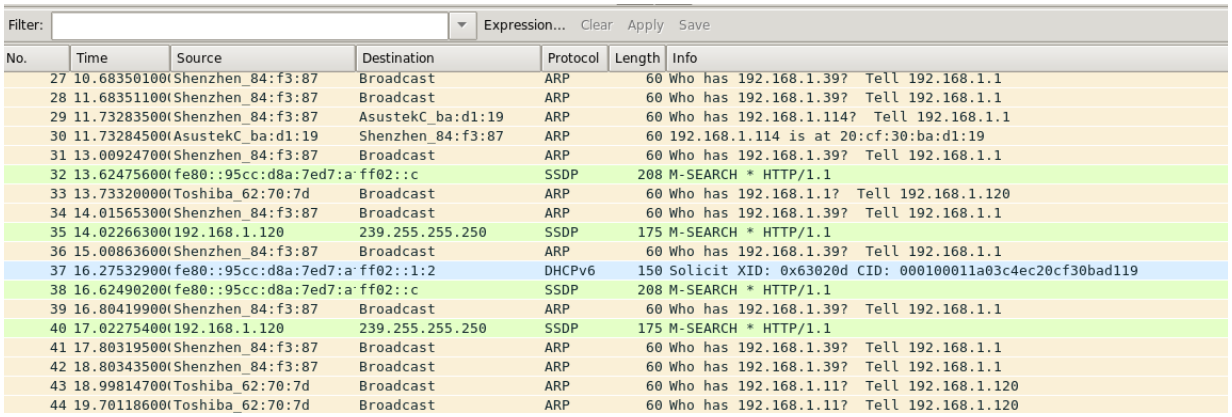
S'executa el programari Wireshark que es troba al menú de la distro Pentoo:

Pentoo > Analyzers > Wireshark



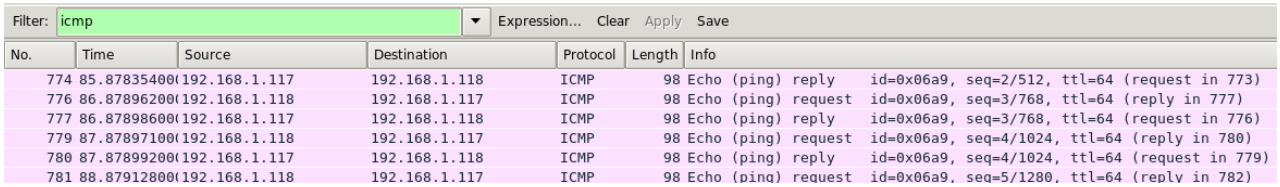
Il·lustració 16. Captura de pantalla del programari Wireshark de Pentoo.

S'escolleix l'opció de monitorització de la interfície *eth0* i observem tot el tràfic que circula a la il·lustració 17.



Il·lustració 17. Captura de pantalla del tràfic del programari de Wireshark de Pentoo.

Per poder comprovar que observem el tràfic de la màquina Wifislax, des d'aquesta s'executa des de la consola de comandes l'aplicació *ping 192.162.1.117* que és la IP de la màquina Pentoo. Tanmateix es filtra el tràfic ICMP que s'observa a *Wireshark.*
A la il·lustració podem observa les demandes de *ping* que realitza la màquina amb IP 192.168.1.118 a la màquina 192.168.1.117.

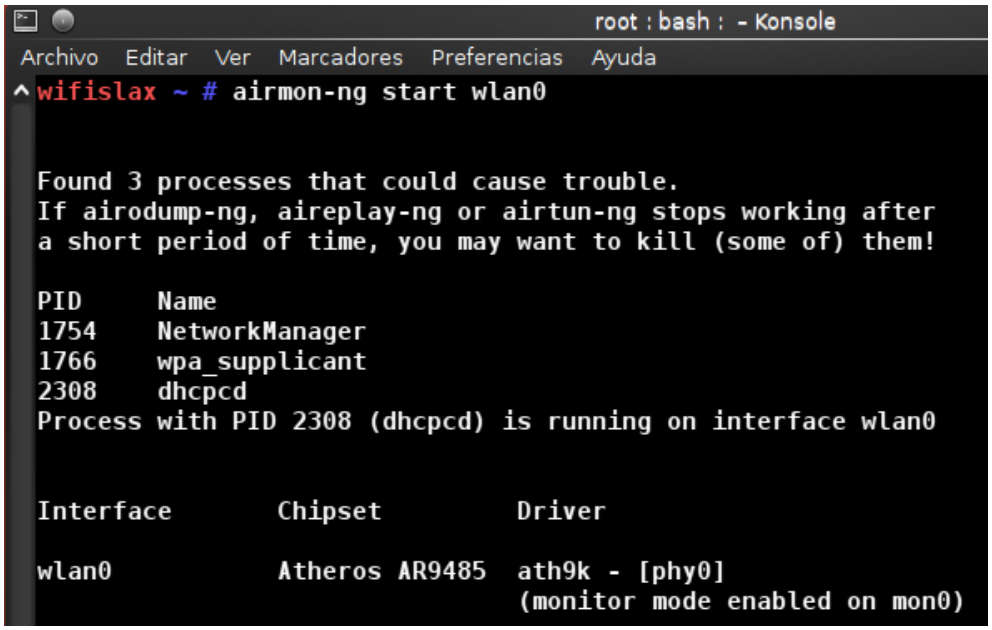


Il·lustració 18. Captura de pantalla del tràfic del programari de Wireshark de Pentoo.

5.4 ANÀLISI AMB WIFISLAX:

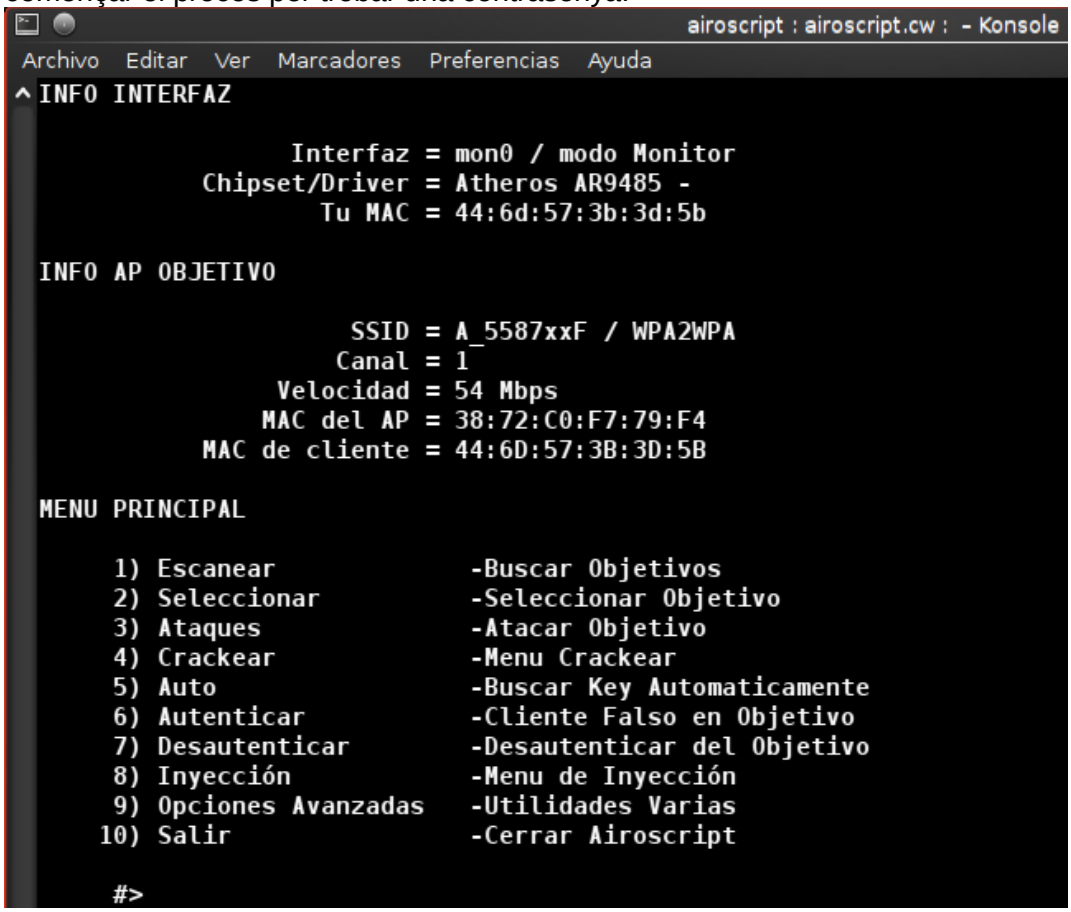
En aquesta prova estudiarem la tècnica de trencament de contrasenyes de *Wifi.*Per fer-ho utilitzarem la distro Wifislax instal·lada en LiveCD, ja que amb la configuració de màquina virtual, no es possible posar la targeta de xarxa sense fil de la computadora en mode monitor. L'*script* amb el que es treballarà es troba al menú principal: *Wifislax > Suite aircrack-ng > airoscript wifislax.*
Aquest programari pot desencriptar les contrasenyes WEP/WPA/WPA2 de xarxes sense fils mitjançant la captura de paquets, amb la posterior desencriptació amb l'ajuda de diccionaris de força bruta.
Aquest *script* engloba les diferents aplicacions necessàries que incorpora *la suite aircrack-ng* per poder fer una auditoria de seguretat de xarxes sense fils. Les eines que conté més destacades son: *Airmon-ng (*informació del xip de la targeta de xarxa sense fil*), Airodump-ng* (captura les dades transmeses per les ones *wifi*)*, Airplay-ng* ("ataca" la màquina escollida)*, Aircrack-ng* (desencripta els paquets trobats de la màquina escollida per trobar la contrasenya)*,* les quals s'agrupen en un menú a la consola de comandes.
S'utilitza al laboratori de proves l'equip portàtil ASUS i l'encaminador ADSL, descrits anteriorment. L'encriptació de la clau d'accés a la xarxa a través d'aquest encaminador es WPA/WPA2 i s'utilitza la contrasenya: "password123" amb nombre de xarxa: A_5587xxF.

Es comença posant el xip de la targeta de xarxa sense fil de la màquina en mode monitor. Tot i que es pot fer des del menú de l'*script airoscript*, es farà amb la comanda *airmon-ng start wlan0* per demostrar que aquest *script* és un recull de les diferents aplicacions que la componen.



Il·lustració 19. Captura de pantalla de la consola de comandes de Wifislax.

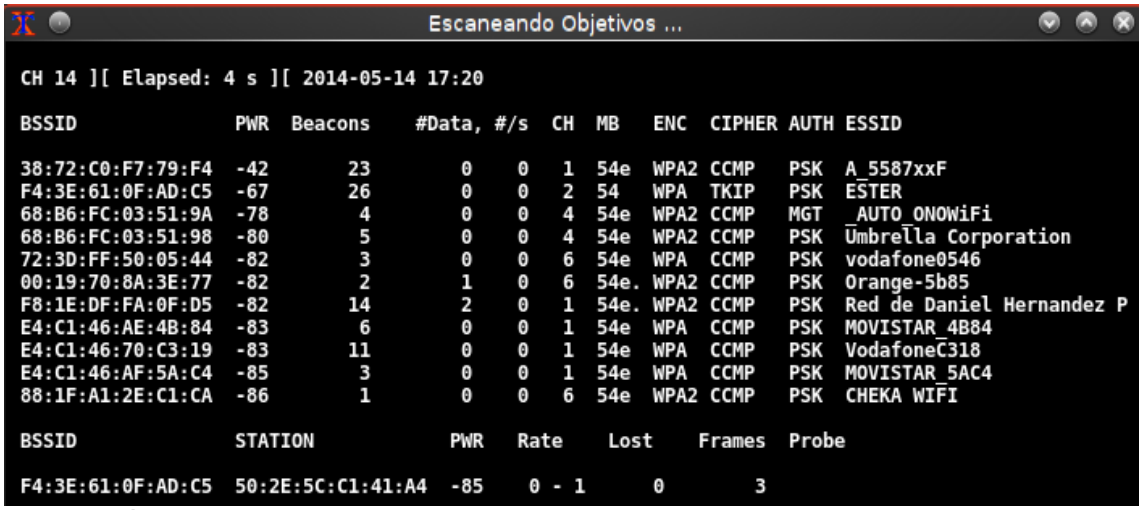
S'executa l'*script airoscript* i s'observa a la il·lustració 19 el menú amb les diferents opcions per començar el procés per trobar una contrasenya.



Il·lustració 20. Captura de pantalla del menú airoscript de Wifislax.

Se selecciona l'opció 1 per escanejar les xarxes sense fils existents en el radi d'abast del xip de la targeta. En aquest procés l'*script* utilitza l'eina *airodump-ng.*
Amb això es pretén capturar les dades transmeses per algun *host* connectat a la xarxa que es vol

atacar a través de les ones *wifi*, concretament les balises enviades pels *routers* propers (*beacons*) i els Ivs (vectors inicials) dels paquets WEP/WPA/WPA2.



Il·lustració 21. Captura de pantalla de l'escaneig d'objectius al programari airoscript.

A la il·lustració 21 s'observa la finestra que s'està escanejant, on ens trobem els següents valors:
BSSID = Mac de l'encaminador
PWR = Senyal de la xarxa (a més alt valor negatiu, millor cobertura)
Beacons = Paquets que s'estan enviant.
# Data = IB s
# / s = IB s / segon
Ch = canal
MB = La capacitat de la targeta, (54,48 ...)
ENC = Tipus de xifrat (WEP, WPA)
Cipher = Tipus de codificació de la xarxa
AUTH = Format de xifrat.
ESSID = Nom de la xarxa.

D'aquest escaneig s'obté les diferents xarxes que es van trobant (ESSIDs) i a la part de sota, les màquines connectades a algunes d'aquestes xarxes. S'escollirà una xarxa que necessàriament tingui una màquina connectada a alguna xarxa, i principalment que tingui un número elevat negatiu de PWR i de *beacons*. L'indicador PWR ens informa de la potència del senyal: com més negatiu sigui el nombre més bona és el senyal rebuda. L'indicador *bacons*, dels paquets que s'estan enviant a través d'aquesta xarxa, per tant com més alt sigui aquest nombre, més fàcil serà "atacar-la".

El normal a l'hora de llançar aquesta eina, és especificar el canal i la xarxa cap a la qual anem a dirigir la captura de paquets, per això especificarem el canal, el nom de la xarxa i el nom del fitxer amb què anem a guardar la captura, per després utilitzar l'eina de desincriptació: *aircrack-ng* per treure la clau.

El següent pas és escollir una xarxa que compleixi bons requisits i llançar un atac, amb l'opció 3 del menú (que pertany a l'eina *aireplay-ng*).

La seva funció principal és generar trànsit per usar més tard amb *aircrack-ng* i poder trencar claus WEP i WPA-PSK. Hi ha diversos atacs diferents que es poden utilitzar per fer desfer autenticacions amb l'objectiu de capturar un paquet *handshake* WPA, el qual es genera quan un client es connecta a la xarxa.
Aquest paquet només s'aconsegueix desautenticant a un client legítim de la xarxa, i quan es torna a connectar amb l'eina *airodump-ng*, capturarem aquest fitxer

.Els diferents “atacs” que es realitzen sobre la xarxa escollida son els següents:

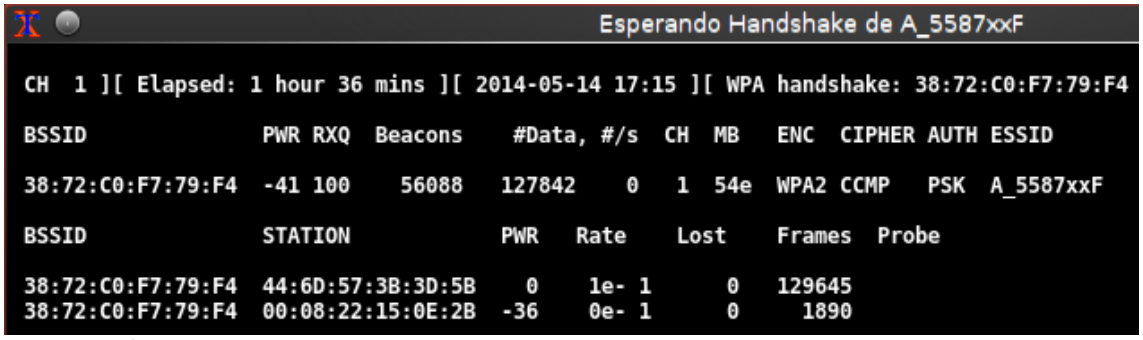
Atac 1. Serveix per desautenticar un client connectat a l'AP (punt d’accés) que s’està atacant. Això és especialment útil quan la xarxa té xifrat WPA , ja que s'aconsegueix que el client s'hagi de tornar a autenticar i així poder capturar el *handshake* (protocol de començament de comunicació entre dos processos informàtics).

Atac 1 . Autenticació falsa. Aquest atac s'utilitza quan no hi ha un client legítim connectat a la xarxa. D'aquesta manera es crea un client fals que s'associés l'AP i així es pot llançar els atacs corresponents.
És indispensable per llançar els atacs 2 ,3 i 4

Atac 2 . Reinjecció Interactiva de paquets. Aquest atac permet triar el paquet que es reinjecta a l'AP .

Atac 3 . Injecció de paquets ARP Automàticament. Aquest atac és el més efectiu, quan hi ha un client legítim connectat, un cop es llança l'atac l'aplicació intentarà aconseguir un paquet ARP i quan ho aconsegueixi , començarà a reinjectar-se’l a l’AP generant així un trànsit que permetrà pujar els IVs a una velocitat alta.

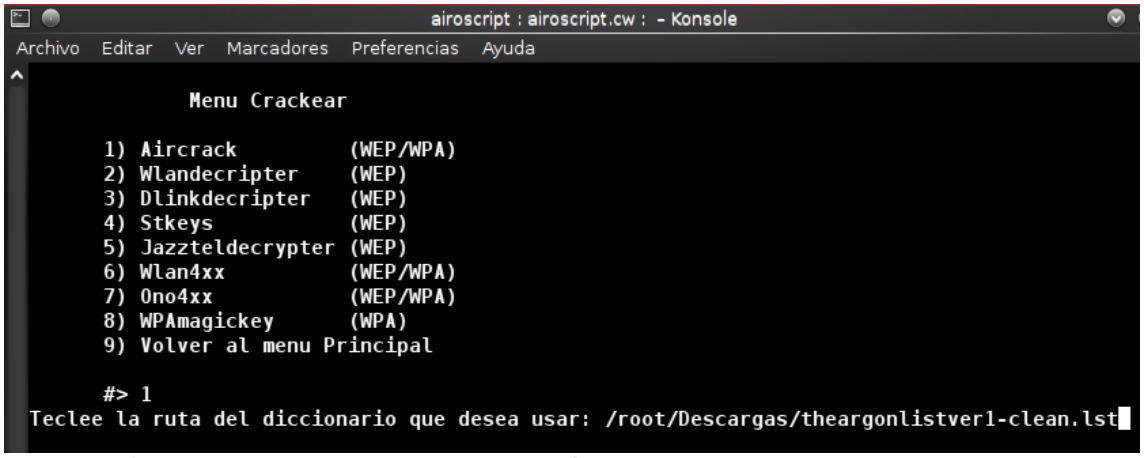
Atac 4 . Atac per saturació al *router* víctima. Es molt poc efectiu , ja que els routers identifiquen l'atac i no llença paquets de resposta. Però quan el AP és vulnerable s'aconsegueix obtenir la clau WEP d'una manera relativament ràpida .



Il·lustració 22. Captura de pantalla de l’obtenció del paquet *handshake* de airoscript.

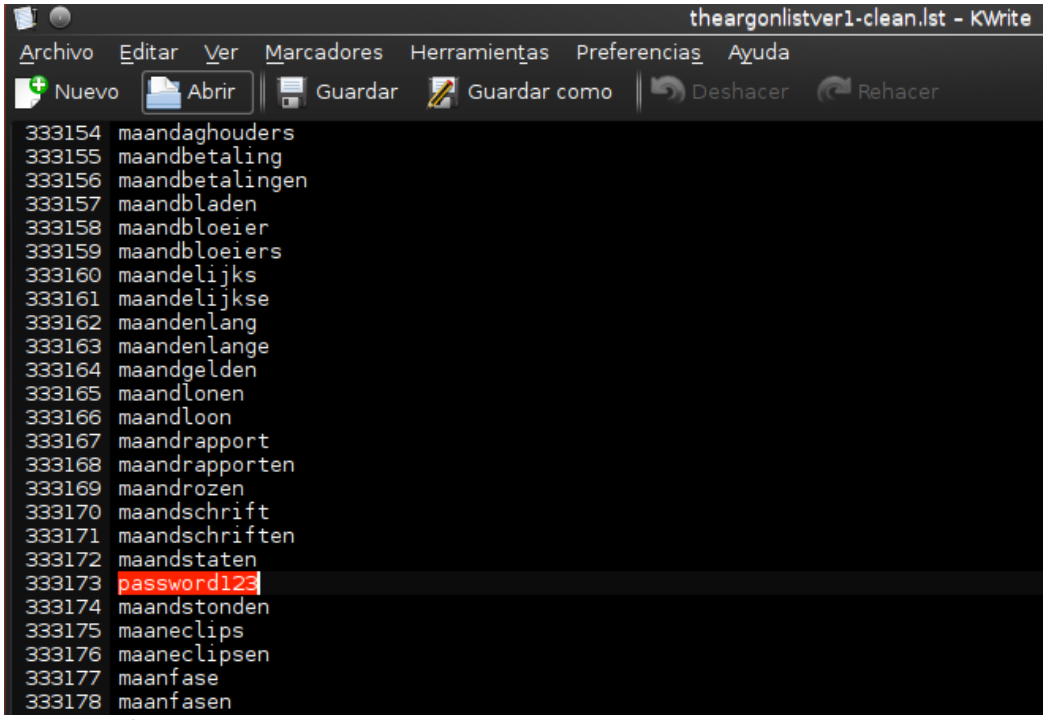
A la il·lustració 22 s’observa a la capçalera superior, l’obtenció del paquet *handshake* WPA (38:72:C0:F7:79:F4) després d’una hora i trenta sis minuts realitzant diferents atacs.

El següent pas es procedeix al desxiframent d’aquest paquet mitjançant l’opció 4 del menú *airoscript* (el qual utilitza l’eina *aircrack-ng)*.
Una vegada es prem l’opció 4, utilitzem l’opció 1 del menú *crackear*, el qual ens proporciona l’eina mencionada anteriorment. Les altres opcions donen alternatives a la utilització d’altres eines de desxiframent, en el nostre cas utilitzem *aircrack-ng*.
A la il·lustració 23 es pot observar que s’ha d’utilitzar un diccionari creat prèviament, de possibles paraules clau, per realitzar un desxiframent de “força bruta”. S’utilitzarà un diccionari de caràcter general baixat d’internet de l’adreça: http://ns2.elhacker.net/wordlists/



Il·lustració 23. Captura de pantalla del menú airoscript de Wifislax.

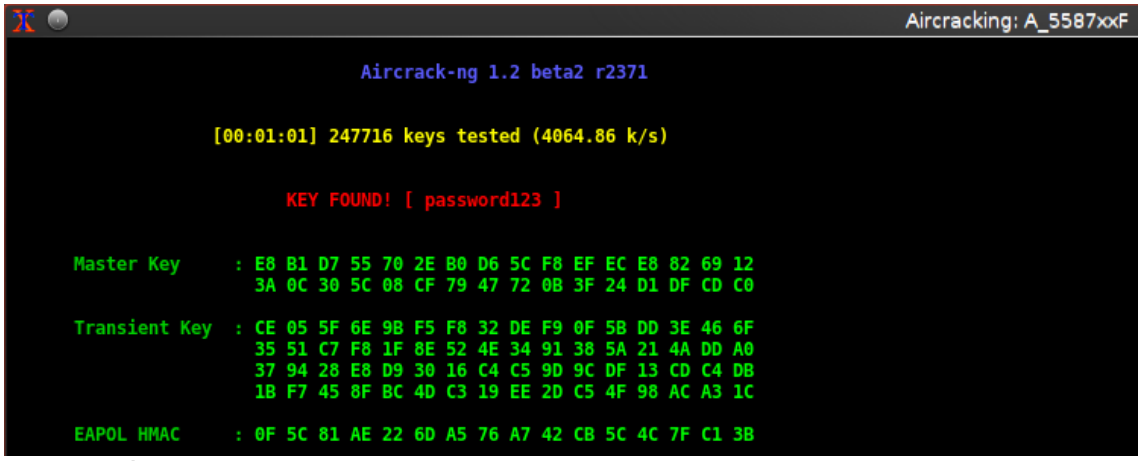
S'introdueix la clau coneguda prèviament d'accés a la xarxa "atacada" com a una de les paraules clau del diccionari a la posició 333173 tal i com es veu a la Il·lustració.



Il·lustració 24. Captura de pantalla de l'arxiu diccionari de l'eina *aircrack-ng*.

En aquest moment l'eina *aircrack-ng* comença a fer un "atac" de força bruta amb l'ajuda del diccionari, per trobar alguna coincidència en els paquets handshake WPA i les claus del diccionari. En el cas de l'encriptació amb WPA/WPA2, l'única opció per desxifrar la clau és a través per la comparació entre les paraules clau del diccionari i els paquets *handshake* capturat, la qual cosa pot prendre molt temps i un ús exclusiu de la CPU. En el cas d'encriptació WEP, el desxiframent es fa per aproximació estadística, augmentant per cada comparació que es fa la probabilitat de trobar una coincidència, i per força bruta amb ajuda d'algun diccionari de paraules clau.

Així, s'observa a la il·lustració 25 que es troba la clau d'accés a la xara sense fil escollida: password123, en un temps de 1 minut i un segon, i havent empleat 247716 claus per comparar.



Il·lustració 25. Captura de pantalla de l'eina *aircracking* trobant la contrasenya.

6- ESTUDI COMPARATIU DE LES EINES DE LES DISTROS DE SEGURETAT:

Una vegada realitzada la descripció de cada distro en els apartats anteriors i efectuada les proves de laboratori, es passarà a explicar les diferencies de les aplicacions que incorporen i destacar per tant els punts on més diferencies s'han trobat. És cert que alguns d'aquests punts ja han sigut comentats anteriorment durant la presentació, però no en el format de comparativa que apareixen en aquest apartat.
En concret, es destaca quines eines tenen, com estan agrupades les aplicacions als menús de l'entorn gràfic, en quin tipus d'eines s'enfoca més cada distro i com estan d'actualitzades.
No es pretén enumerar i explicar cadascuna de les aplicacions de cada distro, ja que contenen un nombre molt elevat i moltes d'elles, son aplicacions complementàries d'altres o de suport per altres tasques de caràcter irrellevant. Per tant es procedirà a comentar les eines més destacades de cadascun.

6.1 Eines de Backtrack 5:

Les eines es troben organitzades en un menú gràfic desplegable que es troba a la part esquerra superior. L'agrupació principal és de la següent manera, al final de cada grup es menciona les eines noves més rellevants que incorpora aquesta nova versió de Backtrack:

- ***Information Gathering*** : reuneix les aplicacions que ajuden a obtenir tota la informació prèvia necessària abans de l'atac, buscar els serveis actius, les versions d'aquests, nombre de màquines, etc. (dnmap, address6, jigsaw, uberharvest, sslcaudit, VoIp honey, urlcrazy).

- ***Vulnerability Assessment***: en aquesta categoria es troben les aplicacions per buscar vulnerabilitats d'un objectiu. (lynis, dotdotpwn).

- ***Exploitation Tools*** : eines per explotar vulnerabilitats trobades. Aquesta distro posseeix un nombre elevat d'*exploits* respecte a la resta, destacant una nova categoria inclosa (Pysical *exploitation*), la qual esta enfocada en fer proves *hardware*, amb una eina molt potent: *Arduino Ide*.

- ***Privilege Escalation***: aquestes eines permeten des de nivells inferiors accedir a un nivell superior per tal d'augmentar els privilegis d'un usuari o apoderar-se de l'altre. (smarphone-pentest-framwork, creddump, johnny, ophcrack).

- ***Maintaining Access***: un cop aconseguit explotar una fallada, de vegades, cal mantenir aquest accés. Per a això, es pot utilitzar diverses tècniques que es troben agrupades en aquesta secció.

Aquesta categoria, conté menús desplegable molt ben estructurats per la comprensió de l'usuari. (powersploit, sbd, u3-pwn, msfencode, webshells).

- ***Reverse Engineering***: aquí es troben aplicacions per fer enginyeria inversa. (android-sdk, mercury, ollydbg)

- ***RFID Tools***: eines per tecnologies d'identificació per radiofreqüència. Tot i que és poc utilitzada, l'ús d'aquesta tecnologia és cada vegada més elevat. Aquí es troben totes les aplicacions necessàries per fer un *pentesting* complert. (spooftooph, bluepot, brute force hitag2, reset hitag2 tag).

- ***Stress Testing***: consisteixen bàsicament en estressar a una màquina. Generalment es refereixen a atacs de denegació de serveis. (denial6, hping3, smurf6, dos-newip6, flood_advertise6, flood_router6)

- ***Forensics***: categoria relacionada al món de la informàtica forense. Conté eines bastant potents per fer anàlisi forense (rifiuti2, cmospwd, darkstat, ptk).

- ***Reporting tools***: eines per documentar i reportar tot procés. (casefile, keepnote, magictree, maltego).

- ***Services*** : aquesta distro permet de manera molt còmoda instal·lar alguns serveis o dimonis com Apache, MySQL, ssh, etc. (Snort service).

- ***Miscellaneous*** : aplicacions que de gran utilitat i suport per a altres amb objectius més concrets. Aquesta categoria conté nombroses eines molt interessants a diferencia d'altres distros, com per exemple l'eina *SSLTunnel*, fent ús de servidors per fer-los servir com a *proxies*.

A la il·lustració 26, es pot observar el tipus de menú desplegable basat en *KDE*, on s'agrupen les diferents eines:

Il·lustració 26. Captura de pantalla del menú d'eines de Backtrack 5.

Backtrack 5 r3 conté un repertori d'eines variades i enfocades per testejar la seguretat de qualsevol sistema informàtic. Apart de contenir un gran nombre elevat d'eines, és de les distro que millor té classificades per cateogires, facilitant sobretot als usuaris que utilitzen per primera vegada aquesta distro. Es troba fàcil i intuïtivament les eines que es volen utilitzar.

BackTrack s'omple amb una col · lecció d'unes 300 eines de seguretat de codi obert, que es poden trobar organitzades en diferents submenús i on cada submenú es subdivideix al seu torn en subcategories. Aquest tipus de desplegament, és un dels més estructurats de totes les distros que s'estan estudiant. Això fa que sigui més fàcil visiblement per trobar una eina determinada, o obtenir un resultat concret. Els desenvolupadors han afegit un toc especial als elements del menú d'utilitats de la consola de comandes: en fer clic en un element del menú, s'obre una finestra de terminal amb l'eina que mostra el seu ús, per exemple, amb l'opció-*help.* Tot i així en aquesta distro la majoria de les eines encara s'han d'executar des de la consola de comandes amb el seu nom i paràmetres. Conté pocs *scripts i/o suites* per englobar conjunt d'eines per utilitzar en un mateix propòsit.

Un dels inconvenients de Backtrack és que la documentació és escassa i sovint obsoleta i l'actualització des de la versió anterior no s'admet, sinó que s'ha de reinstal·lar la distro completament.
És un sistema operatiu que es va deixar d'actualitzar degut a l'aparició del seu successor (*Kali Linux*), per tant la majoria de les eines estan obsoletes des del llançament de l'última versió (1 d'agost de 2012). En la prova de laboratori que s'ha fet en aquest projecte amb Backtrack, s'ha tingut que actualitzar l'eina *metasploit* per poder portar la prova a terme.
Backtrack des del seu inici a l'any 2006, fins al 2012 ha tingut 12 actualitzacions de les seves distribucions, amb una mitja de dos per any, per tant entre cada actualització l'usuari havia d'actualitzar manualment les eines per tal de comprovar si s'havien millorat.

Les eines de Backtrack estan enfocades per fer un test de penetració general. Degut a què aquesta versió és obsoleta, es troba que les eines dedicades al test de vulnerabilitats en xarxes sense fil estan una mica desfasades. Malgrat això, aquesta distribució està pensat per ser molt estable per poder ser utilitzat, no només com a *pentester*, sinó com a sistema operatiu principal.

6.2 Eines de Pentoo RC2.1:

Les eines de test de penetracions es troben a la part superior esquerra en un menú desplegable, com l'anterior distro comentada. La majoria d'aquestes eines són d'execució en consola de comandes. Es troben agrupades al menú de la següent manera:

- ***Analyser*** : en aquesta categoria tenim eines d'anàlisi de tràfic de xarxa i diversos tipus de rastrejadors de xarxa. El *sniffer* per excel · lència és *Ethereal*. Aquest analitzador de paquets conté una gran quantitat d'analitzadors de protocols, els quals son executats quan un paquet d'informació arriba a la interfície, el risc d'un error en el codi de l'analitzador podria permetre l'execució de codi extern. Per raons de seguretat, els desenvolupadors d'aquest programari van llançar l'analitzador de protocols *Wireshark*, el qual té menys privilegis, permetent el mode "superusuari".

- ***Bluetooth***: aquí podem veure diferents eines d'auditoria, anàlisi i administració d'aquest protocol. Particularment BlueSniff és un *sniffer* de paquets força potent.

- ***Cracker / Bruter*** : en aquesta categoria principalment hi ha una varietat d'eines per vulnerar contrasenyes, tant de sistemes windows com GNU / Linux. En cas de voler realitzar atacs per diccionari. Els més coneguts són el mític "John the Ripper " i " Hydra ", també comuns a la distro Backtrack 5.

- ***Database*:** aquí es troben eines dedicades a buscar vulnerabilitats a les bases de dades de sistemes informàtics a través de les estructures d'accés de SQL. Un dels programes característics d'aquesta categoria es *SQLNinja*, una eina específica per explotar vulnerabilitats d'injecció SQL en una aplicació web que utilitza Microsoft SQL Server com *back-end*. El seu objectiu principal és proporcionar un accés remot al servidor de la base de dades, fins i tot en un ambient molt hostil.

- *Exploit:* aquesta categoria agrupa les eines d'explotació de vulnerabilitats. Aquí es troba la popular *MSF Console*, i altres més. L'eina *Inguma* és inclosa en aquesta distro a diferència de les altres, la qual ofereix nombroses eines per a la recollida d'informació i l'auditoria de destinació. Aquesta eina és d'una de les més desenvolupades i actualitzades per buscar vulnerabilitats.

- ***Footprint*:** aquí tenim una àmplia varietat de diferents eines per a diferents tipus de *fingerprinting* (reconeixement d'aplicacions i la seva versió d'un sistema informàtic), per exemple *smtpmap* per a diferents tipus de protocols de correu electrònic, Blueprint per Bluetooth, Siphon per a Sistemes Operatius i molts més. Degut a la bona actualització de les eines d'aquesta distro, aquí trobem les eines més indicades per fer un test de *fingerprinting*, ja que la versió de les aplicacions dels sistemes informàtics s'actualitzen amb molta freqüència.

- *Forensics*: son eines enfocades en l'anàlisi forense. Es troba un gran repertori d'eines en aquesta distro, la qual cosa mostra que està més especialitzada en aquest tipus de tècniques que Backtrack 5 i Wifislax. Aquesta categoria conté l'eina *Autopsy*, la qual és una eina d'entorn gràfic molt potent per recuperar informació en sistemes informàtics.

- ***Forging***: eines diverses per ARP spoofing , DNS spoofing , traci , etc .(Fragroute, Hping, Nemesis, Rain)

- Fuzzers: son eines que intenten descobrir les vulnerabilitats de seguretat mitjançant l'enviament d'entrada aleatòria a una aplicació. Les eines d'aquesta categoria son molt semblants a les de la distro Backtrack 5, sense haver-hi cap de rellevant.

- ***Misc*** : aquí tenim eines que no entren en una altra categoria, per exemple Firewall Builder és una eina per configurar i administrar tallafoc, MAC Changer realitza *spoof* en adreces MAC. (Curl, Honeyd, Macchanger, Snort, Vncviewer)

- ***MITM*** : en aquesta categoria tenim eines particulars de tests de penetració i altres que apliquen la tècnica MITM (Man In The Middle) inventada per Kevin Mitnick. Per exemple Cisco - Torch és un escàner, trencador de contrasenyes per força bruta i un testejador de vulnerabilitats per a la majoria dels dispositius CISCO. D'altra banda Yersinia és una *suite* per a problemes de seguretat a diferents protocols de xarxa.(Dsniff, Ehhercap, Sslstrip).

- ***Mobile*:** en aquesta categoria es troben eines per accedir a telèfons mòbils mitjançant cable *usb* i analitzar la seva seguretat. Aquesta categoria és un exemple de la potencialitat d'aquesta distro, la qual esta pensada per cobrir quasi totes les necessitats en sistemes informàtics. Es troben eines com *APKtool* (per compilar i descompilar aplicacions Android), *Ifuse* (per accedir al sistema de fitxers d'un Iphone o Ipad sense "jailbreak"), etc.

- *Proxy*: aquí disposem d'aplicacions *proxy*, per exemple Burpproxy que captura tot el trànsit del navegador web i permet modificar els paquets, o bé Paros, una utilitat que corre totalment en Java i permet interceptar trànsit http i https per després modificar-lo i testejar diferents aplicacions web. (3proxy, Burpsuite, Pivoxy, Proxystrike)

- ***RCE*:** aquí es troben les eines d'enginyeria inversa. Aquestes tècniques es basen en l'acte d'imaginar el que faria un programari, per la qual cosa no hi ha codi font disponible. Amb això no

s'aconsegueix detalls exactes del programari, però es pot entendre força bé sobre com es va implementar. A diferència de les altres distros, aquesta categoria conté moltes més eines més concretes per cada tipus de programari.

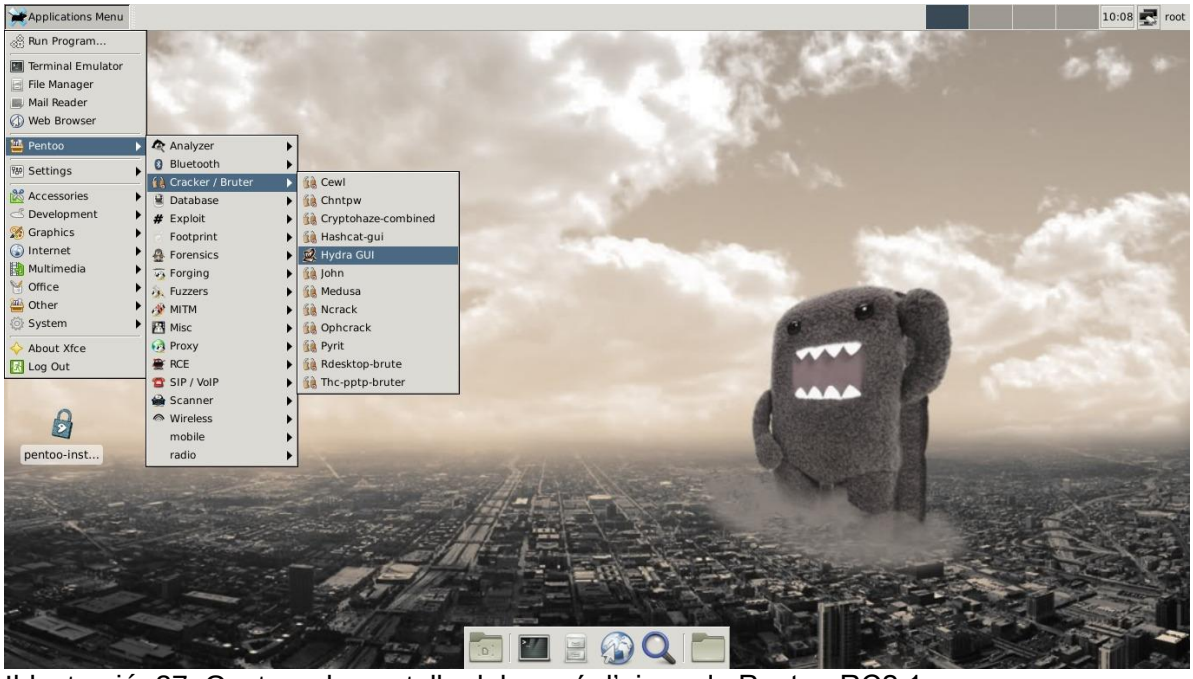
- *Scanner* : en aquesta categoria trobem diferents tipus d'escàners, tant de ports com ara *nmap* o bé de vulnerabilitats com Nessus. També tenim la utilitat Firewalk que no permet avaluar a grans trets les regles d'un tallafoc per veure si estan ben configurades. (Nikto, Wapiti, AutoScan, Firewalk, Nessus, Nmap, Scanrad)

- *SIP / VoIP*: aquí es troben eines per poder testejar els paquets d'àudio sobre xarxes basades en *IP*. Hi ha diferents tipus d'eines amb suport d'autenticació: provador d'opcions, trencadors de força bruta, analitzador de la confiança de la xarxa, delegació i provador de registres, etc. No s'ha trobat una gran diferencia respecte la distro Backtrack en aquest tipus d'eines.

- ***Wireless*** : aquí podem trobar tot tipus d'eines per al protocol 802.11 , tant per rastrejar paquets, vulnerar el protocol WEP, detectar falsos punts d'accés, etc. (Aircrack-ng, Airoscript, Cowpatty, Wepattack)

- ***Radio*:** aquí es troben les eines per testejar les tecnologies basades en radiofreqüència. S'estan implantant cada vegada més en les distros enfocades en seguretat. Aquesta eina serveix per revisar les etiquetes d'aquest tipus de tecnologia. Serveix per manipular les dades emmagatzemades en etiquetes RFID, targetes de la proximitat, etc. Un comandament a distància d'obertura de garatge, seria un aparell sensible d'inseguretat per poder ser testejar amb aquestes eines.

A la il·lustració 27, es pot observar el tipus de menú desplegable amb administrador de finestres *enlightenment*:



Il·lustració 27. Captura de pantalla del menú d'eines de Pentoo RC2.1.

La llista d'eines incloses en aquesta distribució supera les 1400. Moltes de les eines que es troben en aquesta distro son personalitzades, la qual cosa fa que siguin més adaptades al seu *kernel*, el qual també esta força enrobustit.

Les eines estan actualitzades al màxim, ja que s'instal · len amb *ebuilds* (processament per lots

especialitzat creat per compilar i instal·lar programari d'una forma automàtica) versionats i obertes, pel qual fa possible descarregar les últimes versions d'aquestes i encara tenir les instal·lacions controlades per l'administració de paquets.
Des de la seva creació a l'any 2005 fins a l'actual data, han hagut 8 actualitzacions de Pentoo, incloses les seves eines, amb una mitja d'una actualització per any. Tot i així, és una de les distros on s'actualitzen les eines automàticament, independentment de l'actualització del seu sistema.

Es pot realitzar qualsevol tipus de test de penetració amb aquesta distro. Tot i el gran número elevat d'eines que conté, les més importants son les de trencament de claus mitjançant força bruta amb tecnologia CUDA (utilitza la GPU de la targeta gràfica la qual és molt més ràpida que la CPU) i el programari *pyrit,* millorant el trencament de WPA d'una forma molt més ràpida que la resta d'aplicacions.
Tanmateix, inclou moltes eines especialitzades en les pràctiques de seguretat preventiva, com Autopsy, Sleuthkit, etc., totes elles agrupades al menú a la part de *Forensics.*

6.3 Eines de Wifislax 4.8:

Les eines de tests de penetracions es troben a la part inferior esquerra en un menú desplegable sota el nom de Wifislax, com l'anterior distro comentada. Es troben agrupades al menú de la següent manera:

- ***Cifrados***: es tracta d'una bona col · lecció de xifrats per a moltes de les xarxes sense fils actuals ordenats per operador, entre altres utilitats diverses per desxifrar xarxes wifi.

- ***Crda-Tx-Power-Config***: aquestes eines ens permeten canviar la configuració de la potencia de la propagació d'ones (dv) de la targeta *wifi*.

- ***Credenciales****:* aquí es troben les eines que busquen en el radi del dispositiu de connexió sense fil les credencials de client de les xarxes trobades (nom de la xarxa i tipus de clau que utilitza)

- ***Diccionarios***: aquí es troben els generadors de diccionaris de diferents aplicacions per ser utilitzats pels trencadors de contrasenyes.

- ***Forensics***: aquí es troben tres aplicacions bàsiques per l'anàlisi forense: *bulk_extractor, Dumpzilla i Grampus Beta.* Només amb aquestes eines es pot realitzar una anàlisi forense superficial.

- ***Gestores de Conexion*** : conté utilitats essencials per gestionar recursos: interfícies de xarxa, utilitats com *wicd* , wifi radar i un assistent per a xarxes sense fil propi de wifislax.

- ***Hardware-Tools****:* compendi d'eines per configurar manualment la targeta de xarxa i controlar els seus paràmetres, com la *MAC*, el radi d'abast de l'antena, el mode monitor, etc.

- ***Redes***: utilitats per realitzar atacs bàsics contra segments de xarxa, incloent utilitzats molt conegudes en altres distros com: *Ettercap*, *Macchanger, Wireshark, Zenma.*

- ***Suite Aircrack-ng****:* com el seu nom indica, conté *la suite* completa de *aircrack – ng*, pensada per trencar contrasenyes de xarxes sense fil. Aquesta eina és la més rellevant, ja que facilita a usuaris inexperts el seu ús.

- ***Testing***: aquí es troben eines de caràcter general, com trencadors de número *hash*, de test d'intrusions, informació *DNS,*etc.

- ***Wireless*** : conté algunes utilitats per realitzar tasques concretes sobre xarxes sense fils com ara escanejos per SSID , geolocalització, etc . Inclou eines com ara Kismet i FeedingBottle

- ***WPA*** : conté una bona col · lecció d'eines enfocades exclusivament a atacs contra xarxes WPA , inclou eines molt conegudes per altres distros com ara *Pyrit , CowPatty , genpmk , John the Ripper* , entre d'altres.

- ***WPA – WPS***: conté *Reaver* (implementa un atac de força bruta contra configuració protegida *Wi-Fi* (WPS)) i algunes utilitats incloses en aquest apartat per realitzar atacs contra xarxes sense fils amb WPA i WPS habilitat.

A la il·lustració 28, es pot observar el tipus d menú desplegable on s'agrupen les eines a la categoria *Wifislax:*

Il·lustració 28. Captura de pantalla del menú d'eines de Wifislax 4.8.

Les aplicacions estan especialitzades la gran majoria en auditoria de xarxes sense fil, on les més usades son les de trencament de contrasenyes de xarxes sense fil.També compren les eines per realitzar anàlisi forense i varies etapes relacionades amb les proves de test de penetració. Aquest compendi d'eines son molt bàsiques, pensades per fer proves sencilles, dintre de l'ambit de la securetat sense fil.
La majoria de les aplicacions son *scripts* on s'agrupen diferents eines pensades per ser executats per l'usuari a través d'un menú gràfic a la consola de comandes, la qual cosa facilita molt el seu ús, ja que moltes de les proves d'auditoria de xarxes sense fil requereixen diferents passos per arribar a un resultat final.

Incorpora les últimes versions de les eines més utilitzades*: aircrack-ng, wifi cracker, wireshark, i kismet*, i un gran nombre de controladors de xarxa, pensats per cobrir qualsevol tipus de targeta *wifi* utilitzada. Les eines son actualitzades automàticament a cada nova actualització sortida al

mercat. La primera va ser llançada al 2011 (Wifislax 4.1) i les cinc posteriors fins a l'actual al març d'aquest any.
Per actualitzar les eines s'ha de fer a través de la consola de comandes i descarregar-les manualment.
El fet que aquesta distro és molt popular en el món de la seguretat sense fil, fa que tingui una gran comunitat d'usuaris i per tant, la correcció d'errades (*bugs)* i noves actualitzacions, és molt bona.

7- VALORACIONS I CONCLUSIONS

7.1 – Valoracions:

S'ha pogut arribar a la conclusió després de fer un estudi de les eines que s'utilitzen en una prova de vulnerabilitats, en les explicacions sobre el procediment d'un *pentest*, en les proves de laboratori i en l'estudi de les eines de cada distro que totes tres contenen les eines bàsiques per fer una prova de vulnerabilitat en un sistema informàtic senzill, com pot ser en una computadora, un *smartphone* o una xarxa sense fil.
Moltes de les eines més usades són comunes a les tres distros, on l'única diferencia pot ser que estiguin més o menys actualitzades, el seu accés des del menú, o que estiguin agrupades en *scripts*.

La millor distro en la meva opinió és Pentoo RC2.1, tot i que en realitzar proves de trencament de contrasenyes de xarxes sense fils amb tecnologia CUDA, el fet de necessitar una targeta gràfica amb aquesta tecnologia no ha fet possible aquesta prova. En qualsevol cas, te moltíssimes coses positives i sense dubte, és una distro que val la pena provar sempre abans de decidir-se definitivament per una altra.
Per un costat el gran nombre d'eines que inclou, fa que aquesta distro sigui la millor opció per escollir alhora de fer un test de penetracions en qualsevol sistema informàtic.
Les eines més utilitzades, com trencament de contrasenyes de xarxes sense fils, anàlisi forense o trobar vulnerabilitats en pàgines web, estan suportades i ben actualitzades.
Per una altra banda, el programari *Pyrit*, de trencament de contrasenyes, utilitzant tecnologia CUDA, és un dels millors en aquesta distro.
Malgrat que és una distro complexa i de gran pes per la memòria de l'ordinador degut al gran nombre d'eines que incorpora, considero que té un gran futur amb el recolzament de tota la comunitat que aporta coneixement i millores contínues.

La distro Wifislax 4.8 podria ser la millor si ens ajustéssim als resultats de les proves de laboratori, ja que el fet que incorpora molts *scripts* per les seves eines, fa que el seu ús sigui fàcil i ràpid, a més que les seves eines estan categoritzades de forma pràctica per ser trobades.
No obstant, en l'estudi de les seves eines, es pot observar que estan molt enfocades en la seguretat de xarxes sense fils, dotant a aquesta distro amb eines molt bàsiques i escasses per altres tipus de test de vulnerabilitats, com de pàgines web, base de dades o anàlisi forense.
Per trobar documentació a internet sobre les seves eines i procediments, hi ha una gran comunitat que aporta millores i recolzament i la majoria en idioma espanyol.

En quant a Backtrack 5 r3, m'ha agradat molt l'estructura del menú d'eines i les seves categoritzacions. Disposa de molts menús i submenus amb les eines força agrupades per famílies.
És una distro molt estable per ser utilitzada com a sistema operatiu principal i disposa de totes les eines principals per realitzar un test de vulnerabilitats sobre qualsevol sistema informàtic.
Malgrat estar desactualitzat, i per tant ni s'ha considerat com a millor opció per ser utilitzat en un test de vulnerabilitats, es considera una distro referent degut al gran recolzament per part dels desenvolupadors i la comunitat que la recolza, fent possible obtenir una distro molt potent. L'exemple d'això és la creació de la seva successora, Kali Linux.

7.2- Conclusions:

La idea principal d'aquest projecte ha estat una: establir una base a un nivell bàsic- mitjà sobre quines eines podem trobar en les distribucions GNU / Linux més usades avui dia. Sens dubte no ha estat l'únic objectiu. Per a aquest projecte s'ha necesitat un llarg procés de recollida d'informació, filtratge i organització d'aquesta informació. Mitjançant l'estudi de viabilitat es va plantejar una primera aproximació a l'elaboració del PFC, establint les bases d'aquest mitjançant la divisió en fases de la informació recollida, així com la seva posterior anàlisi i contrastació.
Aquesta divisió del projecte en diverses fases es pren totalment imprescindible per poder afrontar amb èxit el projecte . En segmentar el treball, s'obté una millor visió de quant esforç i dedicació representarà el projecte.
El món de la seguretat informàtica és més complex cada dia que passa, i intentar abastar tot pot suposar un repte insuperable. Aquest projecte pretén apropar el lector a aquest immens món mitjançant l'estudi de les eines de tres distribucions considerades importants i representatives.

Després de l'anàlisi teòrica de les eines i les distros ha estat convenient verificar certs aspectes empíricament. Per això s'ha fet servir l'eina VirtualBox que ha permès virtualitzar dos de les distros. Per l'altra s'ha tingut que utilitzar un *Live CD*, ja que de forma virtual ha estat imposible fer una de les proves planejades. És evident que hi ha infinitat de detalls de verificar en les distros: estructura del sistema operatiu, gestió de paquets, arquitectures suportades, ús dels recursos, etc. Malgrat això, aquest projecte s'ha centrat en les eines incorporades en cada distro, com estan d'actualitzades, enfocament respecte a les eines i la seva accesibilitat.

Per finalitzar el projecte, diré que ha suposat un repte major del que esperava. He comprès finalment que una bona planificació val més que res i és un dels pilars de tot bon treball. Si hagués dedicat més temps al projecte al principi del semestre, aquestes últimes setmanes haurien estat molt més suportables. La idea inicial era fer un estudi comparatiu més exhastiu de les eines i del *kernel* de les distros estudiades i utilitzar més distros per comparar. Al mon de la seguretat informàtica i del *hacking ètic*, existeixen un nombre elevat de sistemes molt especialitzats per testejar vulnerabilitats molt concretes, ja siguin xarxes sense fils, smartphones, tecnologies basades en radiofreqüència, etc. El fet que aquest projecte només duri un semestre, no ha fet possible un estudi tan ampli i profund, i per això la tasca inicial de planificació del projecte ha estat més complex del que em pensava. Com a punt final, diré que malgrat que no he realitzat un estudi més rigorós amb més distros, em sento satisfet per tot el coneixement que m'ha aportat aquest treball de fi de carrera, sobretot amb el laboratori de proves, on és realment com s'aprenen millor els coneixements.
Vull puntualitzar que la documentació trobada a internet mitjançant el buscador Google, ha estat aportada la gran majoria per usuaris en fase de descobriment i aprenentatge d'aquestes eines. En tractar-se de temes que freguen la il·legalitat en l'ús d'aquestes eines en el cas que s'utilitzin de forma fraudulenta, hi ha poca documentació oficial i segura, de tal forma que per verificar qualsevol tema trobat aquí, s'ha tingut que contrastar amb diverses fonts de diferents orígens.

8-GLOSSARI DE TEMES:

adreces IP -Adreça de 32 bits assignada a una estació o host que defineix una xarxa i a un equip.
Poden ser privades (per a Intranets sense connexió a Internet) o públiques (les que connecten equips a Internet). Existeixen els següents tipus:
-Classe A: xarxes molt grans, amb 8 bits a xarxa+24 bits per estacions
-Classe B: xarxes grans, amb 16 bits a xarxa+16 bits per estacions
-Classe C: xarxes petites, amb 24 bits a xarxa+8 bits per estacions
-Classe D: xarxa especial per multidifusió
-Classe E: xarxa especial reservada

Distro - Nom habitual simplificat que se'ls dóna a les distribucions de GNU / Linux.
Encaminament/routing - Procés complex per definir la ruta a l'equip de destinació entre xarxes. També anomenem així la ruta en si mateixa.
ICMP- protocol que pertany al conjunt de protocols TCP/IP, que permet l'emissió de missatges d'errors entre estacions d'una xarxa.
Host- Tot aquell maquinari que incorpora una tarja de xarxa, encara que per accepció mes general
s'identifica amb un PC o estació.
Ping – Comanda que envia un paquet ICMP tipus eco a *un host* remot i espera una resposta d'aquell, avaluant si hi ha connexió i d'altres paràmetres.
Proxy - Un programa o dispositiu que realitza una acció en representació d'un altre. El seu ús més habitual és la de servidor *proxy*, servint per permetre l'accés a Internet a tots (o alguns) dels equips d'una organització.
Router o encaminador- maquinari que s'encarrega de direccionar el tràfic d'una xarxa. Edemes pot incorporar altres funcionalitats com p. Ex fragmentar paquets d'informació
Script - Arxiu de procés per lots, amb comandes emmagatzemats en un arxiu habitualment en text pla.
SSID - Nom inclòs en tots els paquets d'una xarxa sense fils per identificar-los com
part d'aquesta xarxa. El codi consisteix en un màxim de 32 caràcters que la majoria de les vegades
són alfanumèrics. Tots els dispositius sense fils que intenten comunicar-se entre si
han de compartir el mateix SSID.
traceroute – Funcionalitat que mostra l'encaminament d'un paquet des del seu origen fins a la seva destinació.
tracert – Comanda Windows per fer un **traceroute**
WEP/WPA/WPA2 - Protocols de seguretat utilitzats en xarxes Wifi.

9- BIBLIOGRAFIA

Per a dur a terme l'anàlisi i disseny del projecte s'ha consultat la documentació a internet de pàgines web oficials i no oficials:

9.1. DOCUMENTACIÓ OFICIAL:

Pàgina Web oficial Pentoo: www.pentoo.ch

Blog oficial Pentoo: http://pentoo.blogspot.com.es/

Pàgina Web Backtrack 5: http://www.backtrack-linux.org/

Pàgina Web Wifislax: http://www.wifislax.com/

Tutorial *metasploit*: http://backtracktutorials.com/metasploit-tutorial/

VirtualBox Oracle BM: https://www.virtualbox.org/

Descàrrega de la distro Metasploitable 2:
http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

9.2. DOCUMENTACIÓ NO OFICIAL:

9.2.1. Eines de seguretat:

Eines de seguretat informàtica de xarxes: http://sectools.org/tag/crypto/

Programari penSSH: http://es.wikipedia.org/wiki/OpenSSH

Programari de monitorització d'integritat de fitxers: http://en.wikipedia.org/wiki/File_integrity_monitoring

Programari Visualroute: http://visualroute.visualware.com/

Programari de monitorització de tràfic de xarxa: http://blog.desdelinux.net/ntop-o-como-monitorear-tu-trafico-de-red/

Programari Iptables: http://es.wikipedia.org/wiki/Netfilter/iptables

Programari cgscanner: http://www.cgisecurity.com/questions/cgiscanner.shtml

Programari de trencadors de contrasenyes: http://es.wikipedia.org/wiki/Password_cracking

Programari Bouncer: http://es.wikipedia.org/wiki/Bouncer

Programari d' IDS: http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

9.2.2. Documentació sobre backtrack 5:

Guia de l'usuari: http://www.binary-zone.com/course/BZ-Backtrack.usage.pdf

Historia de Backtrack 5: http://en.wikipedia.org/wiki/BackTrack

Característiques de Backtrack 5: http://jheffner.hubpages.com/hub/Backtrack-Install

Característiques de Backtrack 5: http://www.slideshare.net/mariuszantal/backtrack5-linux#

Orígens de Backtrack 5: http://www.identi.li/?topic=36195

Orígens de Backtrack 5: http://eniac-system.blogspot.com.es/p/historia-backtrack.html

Programari Metasploit de Backtrack 5 : http://highsec.es/2013/07/conociendo-metasploit-parte-i-exploit-basico/

Programari Metasploit de Backtrack 5: http://ns2.elhacker.net/timofonica/manuales/Metasploit-v0.3.pdf

Avantatges i desavantatges de la distro Backtrack 5: http://www.linuxuser.co.uk/reviews/backtrack-5-review-if-youre-serious-about-pentesting-dont-leave-home-without-it/2

Llista d'eines Backtrack 5 r3: http://secpedia.net/wiki/List_of_tools_in_BackTrack

9.2.3. Documentació sobre Pentoo:

Entrevista al creador de Pentoo: http://www.securitydistro.com/security-interviews/interview-with-pentoo-writer-michael-zanetta

Característiques de Pentoo RC2.1: http://www.gustavopimentel.com.ar/2013/03/pentoo-liberacion-de-la-primera-rc-de-la-futura-version-2013-0/

Vídeo de presentació de Pentoo: http://code.google.com/p/pentoo/

Eines que incorpora Pentoo: http://www.dragonjar.org/pentoo-version-final-2009-gnulinux-para-test-de-penetracion.xhtml#

Arpspoofing amb distro Pentoo: http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing/

Llista d'eines Pentoo RC2.1: https://blackstack.org/t/pentoo-distro-pentest/221

Característiques eines Pentoo: http://sematove.wordpress.com/2010/01/04/pentoo-2009-disponible/

9.2.4. Documentació sobre wifislax:

Eines que incorpora Wifislax: http://foro.seguridadwireless.net/manuales-de-wifislax-wifiway/manual-basico-de-wifislax-y-sus-herramientas-de-auditoria/

Anàlisis i classificació d'eines de seguretat en xarxes:

Programari Port scanner: http://www.offensive-security.com/metasploit-unleashed

Classificació eines: http://www.yolinux.com/TUTORIALS/LinuxSecurityTools.html

Definicions d'eines: http://insecure.org/tools/tools-es.html

Trencament contrasenyes *Wifi*: http://www.wifislax.com/contenido/aplicaciones.php

Trencament contrasenyes *Wifi*: http://computerhoy.com/paso-a-paso/internet/tutorial-obtener-contrasena-tu-wifi-wifislax-9089

9.2.5. Distro Metasploitable:

Configuració de la distro: http://bitacoraderedes.wordpress.com/2013/09/02/atacando-e-improvisando-con-metasploitable-parte-1/

Vulnerabilitats de Metasploitable 2: http://alejo-0430.blogspot.com.es/2012/06/metasploitable-parte-1-identificacion.html

Exploit del servei *ftp*: http://oski02.wordpress.com/2013/01/07/vulnerar-servicio-ftp-con-metasploit/

Vídeo sobre *l'exploit* de ftp: http://www.dragonjar.org/metasploitable-2-guia-en-video.xhtml#

Tutorial de como atacar Measploitable 2:
http://bitacoraderedes.wordpress.com/2013/12/03/atacando-vnc-y-mas-en-metasploitable-2/