MÀSTER INTERUNIVERSITARI EN SEGURETAT DE LES TECNOLOGIES DE LA INFORMACIÓ

ESTABLIMENT D'UN SITE SEGUR AMB HONEYNET ADJACENT

Desplegament virtualitzat en entorn stand alone

Alumne: Josep Caballé i Ràmia

Consultor: Jordi Guijarro Olivares

Centre: CSUC, Consorci de Serveis Universitaris de Catalunya

Període: Setembre 2016/Gener 2017


Júlia

RESUM

L'objectiu d'aquest treball és la implementació i fortificació d'un *site* destinat a l'intercanvi d'informació confidencial de manera controlada, així com la seva coexistència amb una xarxa esquer. Tota aquesta estructura serà bastida en un únic equip físic, que serà el que gestionarà els diferents servidors virtuals. Aquesta arquitectura, muntada a nivell de laboratori particular, serà totalment funcional i permetrà la seva escalabilitat a un entorn professional.

Els clients d'aquesta plataforma tindran la possibilitat d'accedir-hi tant des de dispositius de sobretaula com mòbils. Un cop validats, disposaran d'un entorn tipus fòrum on, segons els privilegis de què disposin, podran compartir informació en multitud de formats. La idea és garantir aquests accessos autoritzats, la resta seran derivats a un entorn simulat des d'on es supervisaran els rastres de la seva activitat.

Es tracta doncs d'esmerçar diferents tecnologies, que caldrà integrar, per a construir un entorn assegurat d'intercanvi d'informació, salvaguardat de possibles ciberatacs.

ABSTRACT

The aim of this project is to implement and to reinforce a site assigned to exchange confidential information in a controlled way, as well as make possible that this site can coexist with a honeynet. All this whole structure will be built in a unique physical equipment, that will manage all the virtual servers. This architecture, built in a private laboratory, will be totally functional and it may be scalable/built as well in a professional environment.

Customers in this platform may have the possibility to access from both desktop and mobile devices. Once logged in, there will be at the customer's disposal a kind of forum where, depending on the privileges of each user, they will be able to share information in a wide range of formats. The idea is to ensure these authorised accesses, the rest will be turned towards a simulated environment, from which their activity trails will be followed.

Then, it deals with using different technologies, which will be necessary to integrate, in order to build a safe environment to exchange information, protected from possible cyber attacks.

0. INDEX

1. ÍNDEX D'IL·LUSTRACIONS

2. GLOSARI

Backup: sistema físic i/o lògic de còpia d'un fitxer, conjunt de fitxers o del sistema sencer, actualitzat periòdicament, que permet restaurar les dades originals en cas de necessitat.

BBDD: conjunt estructurat de fitxers interrelacionats en què les dades s'organitzen segons criteris que en permetin l'explotació.

Crawling: algorisme esmerçat pel cercador que reordena i indexa les webs presentades a la seva interfície segons la informació extreta de cada pàgina.

Darknet: xarxa no indexada en cercadors d'abast comú que ofereix serveis específics per a una comunitat i d'accés restringit.

DCERPC (Distributed Computing Environment / RemoteProcedure Calls): és una crida de sistema a procediment remot desenvolupat per a entorns d'informàtica distribuïda.

Ethernet: arquitectura de xarxa que permet l'accés al medi, la comunicació, dels components informàtics.

Exploit: programari que aprofita un forat de seguretat o vulnerabilitat per a que un atacant en pugi beneficiar-se del sistema afectat.

FTP (File Transfer Protocol): protocol destinat a la transferència d'arxius que utilitza autenticació.

Honeypot: esquer informàtica concebut perquè sigui fàcilment vulnerable i atragui l'atenció amb l'objectiu de poder-ne observar el comportament i els mètodes d'atac.

Honeynet: desplegament d'un seguit de serveis i/o servidors amb capacitats de *honeypot* d'alta interacció, esdevenint una xarxa paral·lela en si mateixa.

Honeywall: maquina que actua com a encaminador de les peticions realitzades contra els diferents *honeypots* existents en la infraestructura.

HTTP (Hypertext Transfer Protocol): protocol que s'utilitza en cada transacció que es fa a la WWW. Està orientat als intercanvis i segueix un esquema de petició/ resposta entre clients, servidors i intermediaris.

IDS/IPS: sistema de detecció/prevenció d'intrusos que resideix en una xarxa. S'encarrega de supervisar les trames d'informació que hi circulen, tot actuant segons les regles definides en la seva configuració.

Iptables: eina que s'esmerça com a tallfocs en sistemes operatius Linux que permet filtrar i registrar l'activitat dels paquets que hi transiten.

IPSec: Conjunt de protocols que permeten l'intercanvi de dades de manera segura en una xarxa de telecomunicacions, utilitzant la capa del protocol d'Internet.

IP Spoofing: emmascarament de la IP real del endegador d'una comunicació per la de l'equip objecte de l'atac.

Iptables: utilitat de línia de comanda que esdevé un *firewall* del nucli del sistema operatiu Linux.

DNS (Domain Name System): sistema que permet consultar a una base de dades on hi són registrat els components de la xarxa juntament amb les IPs corresponents.

IPv4 (Internet Protocol, Versió 4): adreça de 32 bits que identifica a un ordinador en una xarxa.

IPv6 (Internet Protocol, Versió 6): adreça de 128 bits, successor del IPv4.

ISP (Internet Service Provider): empresa que es dedica a proveir Internet i d'altres serveis associats, als usuaris finals.

Mirroring / RAID1: tècnica consistent en redundar les dades sobre conjunts de parells de discs per assegurar-ne la informació continguda.

Malware: programari maliciós que cerca obtenir beneficis de manera il·lícita sobre l'equip infectat.

MongoDB: programari de codi obert, per a la creació i gestió de base de dades orientada a documents, escalable, d'alt rendiment i lliure d'esquema programada en C++.

Pentesting: test de seguretat que es realitza sobre un entorn informàtic per a detectar-ne les possibles vulnerabilitats.

Physhing: tècnica consistent en enganyar a la víctima per a obtenir dades sensibles per a cometre un frau econòmic.

Proxy: servidor intermediari que s'esmerça en les comunicacions a Internet i que pot servir per emmascarar l'adreçament origen de les mateixes.

Router: dispositiu intermediari destina a fer d'encaminador en les comunicacions entre diferents xarxes. Típicament, dispositiu que dóna accés a Internet en una xarxa de dispositius informàtics.

Signatura digital: funció resum aplicada a un arxiu que permet verificar i de demostrar l'autenticitat i l'autor d'aquest missatge.

SO/SSOO (Sistema/es Operatiu/s): programari encarregat de controlar les tasques essencials en un ordinador, com ara l'execució de programes i d'aplicacions, l'assignació de memòria interna i la connexió i desconnexió de perifèrics.

SSH (SecureSHel): intèrpret de comandes que permet accedir remotament a sistemes informàtics de manera segura.

SSL (Secure Sockets Layer):protocol de seguretat per a la capa de transport en les comunicacions a través d'Internet.

Subneting: tècnica consistent en segmentar les xarxes segons el seu adreçament IP.

TCP (Transmission Control Protocol): protocol que s'ocupa de supervisar la connexió i en segmenta la informació en paquets de dades.

Timestamp: referència temporal aplicada a un arxiu que inclou la data i hora en que s'hi ha operat i que és avalada per una entita certificadora.

TLS (Transport Layer Security): predecessor del protocol SSL encarregat d'assegurar les comunicacions per la xarxa mitjançant l´ús de criptografia.

Torificació: tècnica consistent en emmascarar l'adreçament IP en les comunicacions d'un procés darrera una connexió a la xarxa TOR.

UDP (User Datagram Protocol): protocol que no garanteix la seqüència de les trames trameses ni controla els errors, esdevé per tant un protocol no orientat a la connexió i s'utilitza per a transmissions on prima la baixa latència.

3. INTRODUCCIÓ

La motivació que m'ha portat a desenvolupar aquest treball Ad-hoc ve donada per l'encreuament de dues facetes sobrevingudes a la realització del Màster Interuniversitari en Seguretat de les TIC. En primer lloc, el fet que Consorci de Serveis Universitaris de Catalunya em proposés, arran de les pràctiques a realitzar en aquests estudis, el desplegament i anàlisi d'un sistema basat en *honeypots*, implementat dins la pròpia *Darknet*. En segon lloc, a partir d'una trobada amb un responsable de la Policia Local, que em va indicar la dificultat i la manca d'una estructura segura per a poder compartir informació sensible entre la jerarquia d'aquesta institució, i perquè no, amb d'altres cossos de seguretat. En extensió, caldria estudiar la possibilitat de poder estendre aquesta funcionalitat, no només a construir un repositori, sinó també a poder-se utilitzar com a canal d'intercanvi de comunicació en viu. Fruit d'aquestes dos escenaris, neix la idea de poder complementar ambdues situacions i destil·lar-les en un projecte comú.

4. OBJECTIU

L'objectiu marcat, s'estructura en la idea d'implementar un espai segur d'intercanvi d'informació sensible que cohabiti amb una xarxa tipus esquer per a recopilar informació sobre possibles ciberatacants.

Així doncs, per una banda es construirà un entorn amb accés restringit i fortament aïllat d'atacs de ciberdelinqüents, que permeti la publicació controlada d'informació. La idea doncs es desenvolupar un *site*, on calgui establir un canal segur per accedir-hi, disposi d'una validació pròpia i ataqui la seva BBDD de manera atomitzada. És a dir, per accedir a aquesta informació caldrà establir un canal intern segur, ja que es trobarà en un servidor aïllat de l'accés l'exterior. La pretensió és que els dispositius clients puguin ser tant estàtics, ordinadors en ubicacions fixes i conegudes, com dispositius mòbils. Per aquest motiu caldrà muntar una plataforma que suporti ambdós tipus de connexions i que ofereixi prestacions avançades a l'establiment d'un espai on publicar informacions estàtiques. Així doncs es cercarà l'establiment d'un espai dinàmic on poder realitzar converses en viu, traspàs d'arxius i que garanteixin una confidencialitat. En aquest sentit, cal cercar un espai on la plataforma de comunicació no depengui de la gestió d'una empresa tercera i les comunicacions que s'hi realitzin siguin opaques a ulls de l'operador de les telecomunicacions. Hem de pensar que encara que el contingut de les comunicacions no sigui accessible si es podrien traçar les comunicacions i establir pautes de conducta. Tan mateix, caldrà garantir-ne l'accessibilitat segura, la integritat de les dades, la seva confidencialitat i aquelles mesures de còpia de seguretat davant eventuals desastres.

D'altra banda, sota les mesures de protecció pertinents, establir una *honeynet* on emular l'entorn similar al de producció, amb l'objectiu d'atrapar activitats amb fins il·lícits que ens ajudin analitzar els mecanismes d'atac que s'esmercin. És important remarcar, que més enllà de capturar atacs indiscriminats, el que es cerca és poder atraure atacants discrecionals, que tinguin clar l'objectiu. Caldrà doncs deixar suficients credencials atacables, però no evidents, com per a despertar sospites, obrir només recursos imprescindibles i poder monitoritzar tota l'activitat maliciosa que hi succeeixi. Aquesta recol·lecció, a més de servir per a analitzar patrons d'atac també ens permetrà conèixer dades sobre els atacants, malgrat puguin ser emmascarades. Això també podria servir, en cas d'un hipotètic atac a la xarxa en producció, per a relacionar activitats sospitoses prèvies a la *honeynet* amb una intrusió al sistema fortificat.

5. COM FER-HO

Passem a enumerar el seguit d'eines que esmerçaran per tal d'assolir l'objectiu descrit. Cal esmentar que es tracta només d'un llistat d'elements on se'n justifica el seu ús. Durant la redacció de la memòria s'entrarà en més detall en les seves característiques i el seu funcionament.

5.1. Entorn De Treball

Tot aquest entorn serà desplegat en un laboratori particular, basat en un ordinador personal i una connexió a Internet mitjançant un *router* ADSL amb adreçament estàtic. Disposarem doncs d'un PC clònic amb les següents característiques principals:

5.1.1. Maquinari

- Processador: Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
- Placa base: ASRock H87 Pro4
- Memòria RAM: 8GB, DIMM DDR3 Synchronous 1600 MHz (0,6 ns)
- Targeta de xarxa: 1Gbps, Ethernet Connection I217-V
- Discs durs: 5
    - 1 x 3TB
        - Màquina física amb SO Ubuntu Desktop 14.04.05 LTS
            - SRV10:
                - VirtualBox Host 4.3.36_Ubuntu r105129
                - Modern Honeypot Network September 2016
                - Splunk 6.4.2
            - SRV99:Backup via NFS
    - 2 x 1TB (RAID1 Xifrat)
        - Màquina Virtual amb SO Ubuntu Server 14.04.05 LTS
            - Server52: MySql 5.5.52, iptables
    - 2x160GB (RAID1 Xifrat)
        - Màquines Virtuals amb SO Ubuntu Server
            - Server51: Moodle 3.1.1, iptables
            - Server02: Routing, iptables
            - Server13: Honeypot, Sensor: Dionaea
            - Server14: Honeypot, Sensor: Altres

Mentre que les característiques a ressaltar del *router* són:

- Model: Router ADSL Movistar, Model RTA01N_Fase2, Firmware RTK_V2.2.13, Velocitat 10Mbps / 256Kbps
- IP estàtica: 88.2.209.101, assignada internament al Domini: tfmjcr.tk

- Targeta de xarxa: 1Gbps (amb capacitat de segmentar una segona LAN/30 per a un enrutament alternatiu)
- Serveis a destacar: Virtual Server i NAT: permet obrir ports i redirigir-los a màquines internes

Durant les tasques de configuració s'hi accedirà via el programari d'accés remot TeamViewer, per tal de tenir accessible la màquina arreu. Cal indicar però que en un entorn de producció aquest seria eliminat, evitant així possibles escletxes per a intrusos.

5.1.2. Programari

Tot el programari esmerçat en aquest Treball de Final de Màster serà gratuït i de lliure distribució, si més no en la versió implementada en laboratori.

- **UBUNTU**, s'esmerçarà la distribució 14.04 LTS, tant per la SO *Host* com pels servidors virtuals que conformaran la granja on desplegar l'entorn de laboratori. S'escull aquest tipus de distribució "Long Term Support" ja que així es garanteix un cicle de vida de producte de sis anys. Malgrat haver una release posterior, 16.04, no s'esmerçarà, doncs òbviament pel temps que fa que roman en el mercat, ha tingut menys tests i per tant es disposa de menys documentació i *feed-back* en vers les seves implementacions.
- **VIRTUALBOX**, entorn de virtualització que permet disposar en una mateix màquina física de varis sistemes operatius i aplicacions corrent de manera concurrent. S'integra perfectament amb el sistema operatiu host escollit i permet una flexibilitat de configuració prou àmplia.
- **IPTABLES**, tallafoc integrat en el SO que ens permetrà tant establir tant les regles de tallafoc i NAT com realitzar *routing* quan s'escaigui.
- **OPENVPN**, programari que ens permetrà establir un túnel SSL, amb certificat inclòs, entre les dues màquines més crítiques de la infraestructura. D'aquesta manera s'asseguraran i fortificaran les comunicacions davant un possible intent d' intrusió.
- **MODERN HONEYPOT NETWORK (MHN)**, programari per a centralitzar la gestió de diversos sensors de *honeypots* distribuïts que conformaran la *honeynet* paral·lela.
- **SPLUNK**, programari recol·lector dels registres generats per la *honeynet* que ens permet flexibilitzar la monitorització i explotació de les dades obtingudes més enllà de la pròpia interfície del MHN.
- **MOODLE**, malgrat ser una eina pensada per a la gestió d'espais acadèmics virtuals, l'esmerçarem per construir el fòrum "DeepTicies", on es compartiran les informacions segons els rols designats. Aprofitarem la disponibilitat de l'eina que possibilita gestionar taulers i usuaris amb diferents granularitats, segons els permisos assignats. Cal indicar que en l'actualitat també disposa d'un client per a dispositius mòbils, això possibilita, la integració plena de plataforma

en aquests ginys. Alhora ens permet projectar la idea de poder ampliar les funcionalitats per a permetre l'intercanvi de dades/comunicació en temps real.

- **FOCA**, esmerçarem aquesta eina per a recopilar les dades de que disposen els cercadors sobre el nostre entorn. També ens permetrà analitzar, si és el cas, les metadades de possibles documents que se'n derivin.
- **NMAP**, programari que ens permet visualitzar quins ports són oberts, o filtrats, quins serveis hi ha actius darrera aquests. També ens donarà informació sobre el dispositiu que respon, com pot ser el sistema operatiu o la versió de *firmware* de que disposa.
- **OpenVas**, plataforma que detecta les possibles vulnerabilitats d'un sistema i que en puntua la serva transcendència segons la perillositat dels mateixos. A més, informa d'aquelles correccions a fer per tal de pal·liar el forat de seguretat que comporta.
- **MSFConsole**, utilitat que davant una vulnerabilitat ens permetrà, en cas de disposar-ne, d'utilitzar un *exploit*. És a dir, podrem atacar la vulnerabilitat del sistema amb una eina creada expressament per tal efecte.

5.2. Tecnologies a Desplegar

Donat que ens trobem amb un projecte heterogeni caldrà treballar amb diferents tecnologies i tècniques. El repte, és construir un espai segur on ha de conviure la part productiva d'intercanvi de coneixement amb l'esquer per a possibles intrusos que funcionarà de manera paral·lela. Passem doncs a justificar-ne la seva utilització, cosa que ens permetrà assolir tal fita.

- **Virtualització**, amb aquesta tècnica disposarem d'un seguit de màquines virtuals necessàries, agnòstiques de la seva condició, que actuaran talment com ho farien en un entorn físic. Així mateix fins i tot l'entorn de xarxa serà virtual, el que ens permetrà establir zones de treball diferenciades.
- **NAT (Network Address Translation),** tècnica que esmerçarem principalment per a redirigir peticions a serveis sobre adreçaments i ports que tinguem definits i personalitzats. Ens serà d'utilitat en dos àmbits, per una banda les peticions arribades al *router* des d'Internet i d'altra les comunicacions que passin pel tallafocs.
- **Firewall**, el tallafoc l'esmerçarem tant per a protecció com per l' aïllament entre la zona de producció i la que establim com a parany. A més, ens servirà per a donar servei cap a Internet als equips que conformin la *honeynet* i que per restriccions del *router* no poden disposar d'un adreçament directe que ho permeti.
- **Routing**, sota aquest concepte explotarem per una banda les característiques del *router* pròpiament dit i per una l'altra banda aquell servidor que faci l'enllaç entre la *honeynet* i Internet. En ambdós casos, permetrà obrir aquells ports que els serveis de cada servidor sol·licitin i redirigir-ne les peticions entrants, així com la

sortida a Internet si s'escau. Pel que fa al dispositiu físic podem dir que actuarà com a *honeywall*, encaminant cada accés extern a la plataforma en producció, si s'escau, o per al contrari, redirigint les peticions als *honeypot*.

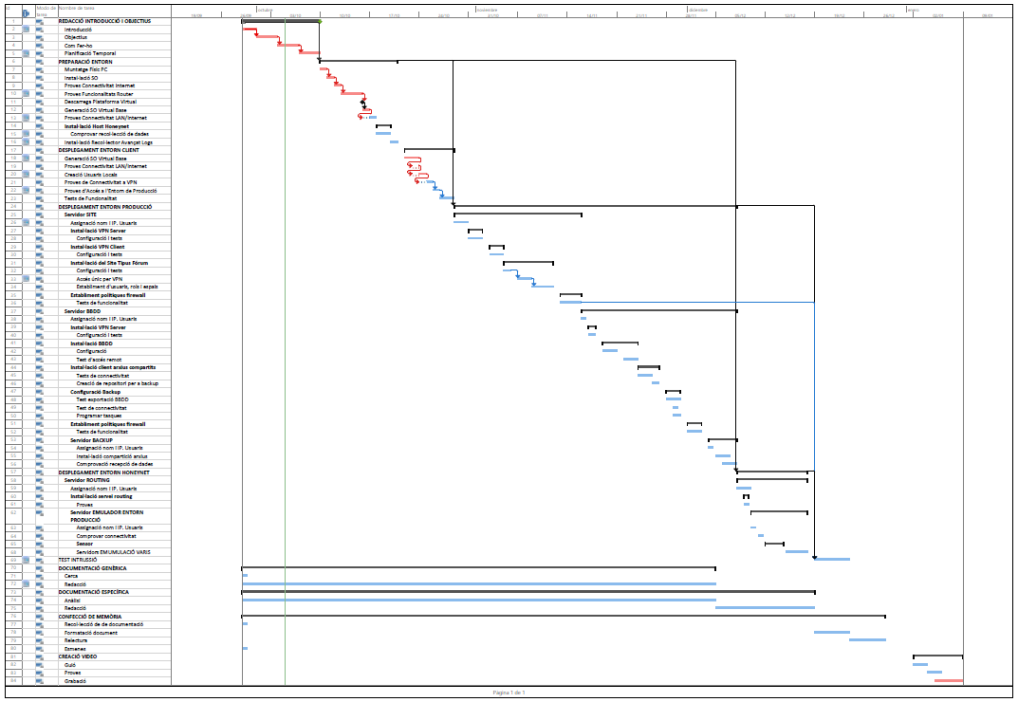
- **DMZ**, esmerçarem aquest terme per a designar les diferents zones de la xarxa aïllades entre si o bé que formen un subgrup basat en la possibilitat d'accedir, o ser accedides, per Internet. Així, ens trobarem amb una zona desmilitaritzada entre el *site* publicat i la BBDD que atacarà o bé entre la *honeynet* i el conjunt de màquines pertanyents al servei lícit ofert.
- **VPN**, l'establiment d'aquest canal de comunicació xifrat segur esdevé el pilar fonamental pel que fa a l'accés a l'espai de treball. S'establiran dos canals, un primer per a poder-se connectar al *site* de publicació i un altre que enllaçarà únicament aquesta màquina amb el servidor de la BBDD. D'aquesta manera es pot controlar quins clients s'hi poden connectar i que les comunicacions son robustes des del client fins a l'accés a les dades. Encara que hi hagués una intromissió en alguna de les màquines de l'ecosistema, no podria capturar les dades trameses.
- **RAID i Xifrat**, les màquines virtuals del projecte, el que inclou les dades sensibles de que disposen, seran desades en contenidors segurs. Així és replicaran les dades dels discs físics contenidors i se'n xifraran les dades continents. Això evitarà, tant que si un disc físic s'espatlla el sistema caigui o es perdin les dades, com que si s'accedís físicament a la màquina host es pogués accedir a les dades contingudes.
- ***Hardering***, s'utilitzaran mètodes, de vegades reiteratius, de protecció de les comunicacions i les dades per tal de garantir-ne la seguretat. Així doncs les comunicacions cap el *site* de publicació es faran en https, malgrat el canal ja serà segur VPN, i les transaccions de registres entre la *honeynet* i les eines d'explotació també en faran ús. D'altra banda, per tal de dificultar possibles identificacions dels serveis lícits oferts es redireccionaran els ports habituals d'ús
- ***Backup***, hi haurà un sistema de còpia de seguretat on exportar les dades de la BBDD, per tal d'esmorteir l'impacte d'una possible caiguda de l'equip encarregat de desar les dades. Aquesta còpia es desarà en un nou equip, només accessible pel servidor de dades i que idealment hauria de residir en una ubicació segura i remota.
- **NFS**, sistema d'arxiu de xarxa que mitjançant l'establiment de certs atributs de seguretat permetrà la comunicació en exclusiva entre un client de la màquina de la BBDD i l'equip de còpia per a poder transferir-ne el *backup*.
- ***Site* especialitzat**, caldrà desplegar un entorn que permeti la gestió d'usuaris i rols que permeti una granularitat en l'accés a les dades publicades. Aquest serà el producte al qual els clients es connectaran i publicaran les informacions sensibles, podent ésser consultades per la resta segons els privilegis de què disposin, L'organització serà en forma de fòrum, amb diferents taulells segons la temàtica a tractar.

La gestió, i responsabilitat dels usuaris propis de l'eina, recaurà en qui designi el cos com a gestor principal.

- **BBDD**, aquesta serà el cor i espai més protegit i aïllat del sistema, doncs és on residirà realment la informació sensible del sistema. Les seva protecció serà via la robustesa del canal de comunicació, l'establiment d'un usuari remot únic amb permís per a l'accés i manipulació de les dades dipositades i l'establiment d'un *backup* en condicions similars que no impliqui un curt circuit en la cadena seguretat del sistema establert.
- **Domini**, caldrà adquirir-ne un per tal de donar certa difusió i versemblança al "site fake" implementat en un dels *honeypot*, Adquiríem un domini que pugui ser indexat en Google i que ofereixi certes paraules claus a la cerca. Així, mirarem d'atraure als possibles atacants per estudiar el seu comportament i per obtenir dades que, en cas de rebre un atac a l'entorn de producció, ens puguin servir per a identificar l'atacant.
- ***Honeynet***, entorn paral·lel al de producció consistent en el desplegament de varis *honeypots* encarregats de simular uns serveis lícits que disposen d'uns sensors. Aquest, s'encarreguen de recollir la informació de les activitats fetes per possibles atacants de la plataforma en diferents registres. Dita informació serà processada posteriorment pel gestor principal dels *honeynet* i en extensió per un programari especialitzat en el tractament de fitxers del tipus registre.
- **Test d'intrusió**, el realitzarem com si d'una caixa grisa es tractés. És a dir, realitzarem atacs des de l'exterior, recorrent quan calgui a la informació de que disposem, per analitzar la resposta del sistema. Així doncs, farem dues tasques, una d'atac a cegues al sistema per a veure el comportament tant del *router*, que ha d'actuar com a *honeywall*, com de la *honeynet*. L'altra tasca, consistirà en realitzar un *pentesting* contra els serveis coneguts en funcionament, per a validar-ne la seva coherència pel que fa a la protecció. S'esmerçaran diferents vectors d'intrusió que pugin mostrar-nos alguna escletxa que permeti violar la seguretat del sistema. Ens centrarem en trobar vulnerabilitats pel que fa a l'espai de treball i estudiarem la resposta de l'entorn. Idealment, no hauríem de trobar cap referència específica al servei encapsulat dins la VPN, i si és el cas, caldrà indicar quines modificacions s'haurien d'implementar per a donar la mínima informació a l'atacant. És tracta doncs, de realitzar atacs passius, que deixaran un rastre que haurà de ser recollit pel nostre sistema. S'espera que les respostes obtingudes com a atacants o bé provinguin de la *honeynet* o bé, en el cas de serveis legítims, no revelin informació sensible del sistema fortificat. Per a fer-ho esmerçarem diferents eines, segons la fase del test en que ens trobem: recopilació d'informació a Internet, cerca de serveis actius, escaneig de vulnerabilitats, explotació de vulnerabilitats i neteja de registres de l'activitat del ciberatac.

6. PLANIFICACIÓ TEMPORAL

En el següent diagrama de Gantt hi ha la representació temporal de les tasques més significatives a desenvolupar.



IL·LUSTRACIÓ 1 - DIAGRAMA DE GANTT DISTRIBUCIÓ DE TASQUES

Finalment, per tal de tenir una millor visualització, passem a llistar la totalitat de les feines programades.

Nom de la tasca	Inici	Fi
REDACCIÓ INTRODUCCIÓ I OBJECTIUS	**Dij 29/09/16**	**Diu 09/10/16**
Introducció	Dij 29/09/16	Dis 01/10/16
Objectius	Dis 01/10/16	Dim 04/10/16
Com Fer-ho	Dim 04/10/16	Div 07/10/16
Planificació Temporal	Div 07/10/16	Diu 09/10/16
PREPARACIÓ ENTORN	**Dil 10/10/16**	**Div 21/10/16**
Muntatge Físic PC	Dil 10/10/16	Dim 11/10/16
Instal·lació SO	Dim 11/10/16	Dix 12/10/16
Proves Connectivitat Internet	Dix 12/10/16	Dij 13/10/16
Proves Funcionalitats Router	Dij 13/10/16	Dis 15/10/16
Descarrega Plataforma Virtual	Dis 15/10/16	Dis 15/10/16
Generació SO Virtual Base	Dis 15/10/16	Diu 16/10/16
Proves Connectivitat LAN/Internet	Diu 16/10/16	Dil 17/10/16
Instal·lació Host Honeynet	**Dim 18/10/16**	**Dix 19/10/16**
Comprovar recol·lecció de dades	Dim 18/10/16	Dix 19/10/16
Instal·lació Recol·lector Avançat Logs	Dij 20/10/16	Div 21/10/16
DESPLEGAMENT ENTORN CLIENT	**Dis 22/10/16**	**Div 28/10/16**
Generació SO Virtual Base	Dis 22/10/16	Diu 23/10/16
Proves Connectivitat LAN/Internet	Diu 23/10/16	Dil 24/10/16
Creació Usuaris Locals	Diu 23/10/16	Dil 24/10/16
Proves de Connectivitat a VPN	Dil 24/10/16	Dix 26/10/16
Proves d'Accés a l'Entorn de Producció	Dix 26/10/16	Dix 26/10/16
Tests de Funcionalitat	Dij 27/10/16	Div 28/10/16

DESPLEGAMENT ENTORN PRODUCCIÓ	**Dis 29/10/16**	**Dix 07/12/16**
Servidor SITE	**Dis 29/10/16**	**Dim 15/11/16**
Assignació nom i IP. Usuaris	Dis 29/10/16	Diu 30/10/16
Instal·lació VPN Server	**Dil 31/10/16**	**Dix 02/11/16**
Configuració i tests	Dil 31/10/16	Dix 02/11/16
Instal·lació VPN Client	**Dij 03/11/16**	**Div 04/11/16**
Configuració i tests	Dij 03/11/16	Div 04/11/16
Instal·lació del Site Tipus Fórum	**Dis 05/11/16**	**Dis 12/11/16**
Configuració i tests	Dis 05/11/16	Diu 06/11/16
Accés únic per VPN	Dil 07/11/16	Dim 08/11/16
Establiment d'usuaris, rols i espais	Dix 09/11/16	Dis 12/11/16
Establiment polítiques firewall	**Diu 13/11/16**	**Dim 15/11/16**
Tests de funcionalitat	Diu 13/11/16	Dim 15/11/16
Servidor BBDD	**Dix 16/11/16**	**Dix 07/12/16**
Assignació nom i IP. Usuaris	Dix 16/11/16	Dix 16/11/16
Instal·lació VPN Server	**Dij 17/11/16**	**Div 18/11/16**
Configuració i tests	Dij 17/11/16	Div 18/11/16
Instal·lació BBDD	**Dis 19/11/16**	**Dix 23/11/16**
Configuració	Dis 19/11/16	Dil 21/11/16
Test d'accés remot	Dim 22/11/16	Dix 23/11/16
Instal·lació client arxius compartits	**Dij 24/11/16**	**Diu 27/11/16**
Tests de connectivitat	Dij 24/11/16	Div 25/11/16
Creació de repositori per a backup	Dis 26/11/16	Diu 27/11/16
Configuració Backup	**Dil 28/11/16**	**Dix 30/11/16**

Test exportació BBDD	Dil 28/11/16	Dim 29/11/16
Test de connectivitat	Dim 29/11/16	Dim 29/11/16
PrograDim tasques	Dim 29/11/16	Dix 30/11/16
Establiment polítiques firewall	**Dij 01/12/16**	**Dis 03/12/16**
Tests de funcionalitat	Dij 01/12/16	Dis 03/12/16
Servidor BACKUP	**Diu 04/12/16**	**Dix 07/12/16**
Assignació nom i IP. Usuaris	Diu 04/12/16	Diu 04/12/16
Instal·lació compartició arxius	Dil 05/12/16	Dim 06/12/16
Comprovació recepció de dades	Dim 06/12/16	Dix 07/12/16
DESPLEGAMENT ENTORN HONEYNET	**Dij 08/12/16**	**Diu 18/12/16**
Servidor ROUTING	**Dij 08/12/16**	**Diu 18/12/16**
Assignació nom i IP. Usuaris	Dij 08/12/16	Div 09/12/16
Instal·lació servei routing	**Div 09/12/16**	**Div 09/12/16**
Proves	Div 09/12/16	Div 09/12/16
Servidor EMULADOR ENTORN PRODUCCIÓ	**Dis 10/12/16**	**Diu 18/12/16**
Assignació nom i IP. Usuaris	Dis 10/12/16	Dis 10/12/16
Comprovar connectivitat	Diu 11/12/16	Diu 11/12/16
Sensor	**Dil 12/12/16**	**Dix 14/12/16**
Configurar entorn web "ham"	Dil 12/12/16	Dix 14/12/16
Comprovar connectivitat amb host	Dix 14/12/16	Dix 14/12/16
Servidors EMUMULACIÓ VARIS	Dij 15/12/16	Diu 18/12/16
TEST INTRUSSIÓ	Dil 19/12/16	Div 23/12/16
DOCUMENTACIÓ GENÈRICA	**Dij 29/09/16**	**Diu 04/12/16**
Cerca	Dij 29/09/16	Dij 29/09/16
Redacció	Dij 29/09/16	Diu 04/12/16

DOCUMENTACIÓ ESPECÍFICA	**Dij 29/09/16**	**Diu 18/12/16**
Anàlisi	Dij 29/09/16	Diu 04/12/16
Redacció	Dil 05/12/16	Diu 18/12/16
CONFECCIÓ DE MEMÒRIA	**Dij 29/09/16**	**Dix 28/12/16**
Recol·lecció de de documentació	Dij 29/09/16	Dij 29/09/16
Formatació document	Dil 19/12/16	Div 23/12/16
Relectura	Dis 24/12/16	Dix 28/12/16
Esmenes	Dij 29/09/16	Dij 29/09/16
CREACIÓ VIDEO	**Dil 02/01/17**	**Diu 08/01/17**
Guió	Dil 02/01/17	Dim 03/01/17
Proves	Dix 04/01/17	Dij 05/01/17
Grabació	Dij 05/01/17	Diu 08/01/17

7. ESTUDI DEL MEDI

Passem a justificar l'elecció del productes esmerçats ens la realització d'aquest projecte. En cada cas es descriuran possibles alternatives existents en el mercat i se'n discutirà la seva idoneïtat per tal d'acabar fent l'elecció més pertinent segons les necessitats plantejades. Cal remarcar que ens recolzarem en programari lliure pel que fa al desplegament però tindrem especial cura de que disposi d'agents per a plataformes tant públiques com privatives per a garantir el seu desplegament entre els clients.

7.1. Espai De Treball

L'entorn de treball per a desenvolupar el producte es basa en un ecosistema virtual, on desplegar els diferents servidors amb els seus rols específics. Així, disposarem d'una màquina física que farà la funció de servidor dels *hosts* virtuals, encabirà discs xifrats i redundats a nivell de mirall i tindrà accés a Internet mitjançant una línia ADSL amb IP fixe. Aquesta sortida a la Xarxa es farà mitjançant un *router*, que alhora, realitzarà les funcions d'encaminador de les peticions entrants cap els serveis sol·licitats. Com es tracta d'establir un entorn segur, podem dir que serà la primera línia de protecció. En un segon nivell ens trobarem amb els servidors virtuals oferint els seus serveis. En aquesta capa cal destacar l'esforç per aïllar l'entorn de producció amb l'esquer. D'aquesta manera, caldrà muntar un canal VPN per a poder arribar al servidor de publicació, on un cop establerta la xarxa privada, només s'hi podrà accedir mitjançant la validació de les credencials personals. Aquest entorn ha de coexistir amb una xarxa esquer, formada per diferents servidors amb sensors disposats per a capturar les activitats malicioses. Els serveis oferts, seran accessibles mitjançant l'obertura dels ports pertinents en el *router*. S'haurà d'establir un tercer grau de profunditat pel que fa a la seguretat en remetre'ns a la ubicació de les dades. Aquestes, seran emmagatzemades en una base de dades només accessible pel servidor de publicació, que al seu torn haurà d'establir una nova VPN per a poder tenir-hi accés i que ja no tindrà capacitat de connexió amb Internet. Finalment, a nivell de redundància i seguretat de les dades, caldrà disposar d'un repositori extern de *backup*. El seu format serà un nou servidor virtual, amb un recurs compartit, que només serà accessible per un usuari destinat a realitzar les còpies de seguretat i que tampoc tindrà enllaç amb l'exterior. Cal destacar també el paper fonamental que jugaran els tallafocs en cada màquina desplegada. La seva tasca garantirà l'accés controlat només cap a aquells serveis oferts, aplicant polítiques per defecte restrictives de denegació.

Tal com hem esmentat, aquesta infraestructura virtual és la que es disposarà en discs durs redundats i xifrats. El fet d'esmerçar la tècnica de *mirroring* ens aporta disponibilitat mentre que el xifratge protegirà la incursió a les dades, en cas d'un possible accés físic no permès al hardware com podria ser un robatori. S'ha estimat convenient tenir en compte i donar rellevància a aquest aspecte doncs tota l'arquitectura lògica de seguretat

podria veure's compromesa si s'accedís físicament a la plataforma. Malgrat tractar-se d'una simulació a nivell de laboratori, s'ha volgut emular en el possible el que seria un desplegament real, si més no pel que fa a les tècniques de protecció esmerçades.

7.2. Canal De Comunicació

L'elecció del canal de comunicació és cabdal de cara a la realització d'aquest projecte. El més important de tot es fonamentar les comunicacions en un entorn segur, on mitjançant un mètode d'autenticació, es garanteixi el control d'accés a la plataforma. Pel que fa a les dades trameses, ha de permetre assegurar la integritat i confidencialitat d'aquestes i evitar la possibilitat de repudi de les mateixes. És a dir, que mitjançant la recopilació, i si és el cas una auditoria, sobre els registres d'accés, es pugui fer un seguiment sobre l'origen de les comunicacions. Donades aquestes premisses, ens trobem amb vàries solucions al mercat.

En un primer moment, donades les facilitats d'implementació es pensà en utilitzar la xarxa anònima TOR[i]. De fet, es tracta d'una estructura centralitzada que ofereix un servei per a disposar d'anonimat, pel que fa a les comunicacions. Aquesta es basa en un seguit de servidors, els *directory authorities*, que s'encarreguen de la gestió i recullen estadístiques sobre l'ús. Aquests equips, supervisen i avaluen els equips repetidors, *relays*, que conformen la xarxa, dispositius que seran els qui donin accés als clients finals a la infraestructura. TOR protegeix la informació, incloent l'adreça IP de l'emissor i el receptor, mitjançant un seguit de xifrats en diferents capes, això sí, només pel que fa als paquets TCP. Aquest han de realitzar un mínim de tres salts entre repetidors abans d'arribar al destí i es difereix el camí d'arribada dels diferents datagrames corresponents a cada comunicació. Treballa doncs en el que s'anomena "mode túnel". Cal tenir en compte però que el darrer salt és en clar ja que s'aïlla el darrer xifrat entre el node de sortida i el servidor requerit. En cas d'utilitzar un altre tipus de protocol, UDP/ o reduir la seguretat segons la configuració del navegador, es salta la protecció i els paquets arriben directament entre clients. Això significa que es produeix un *leak*, o el que és el mateix, hi ha un bypass en la transmissió que pot permetre capturar dades identificatives tant dels orígens com dels destins.

També cal remarcar a nivell de nomenclatura que s'utilitza un domini primitiu de primer nivell amb l'extensió *.onion*, seguit d'una setzena de caràcters alfanumèrics que conformen un nombre de 80 bits, generats a partir de la clau pública del servidor que hostatge el servei. Aquests no són indexats en un espai de noms tipus DNS, ja que la pròpia idiosincràsia de la xarxa estableix que els *sites* siguin protegits[ii] per mots de pas, disposin de codis que impedeixin la indexació tant en cercadors com en serveis de directori, programació dinàmica que eviti la utilització d'*html*, disposin de poc text, esmercin BBDD i no facin referencies directes a d'altres planes

web. Cal doncs saber a priori l'adreçament del lloc a consultar, associat a una IP interna de la xarxa TOR, per tal de poder-hi accedir.

Sota aquesta infraestructura es descartà la possibilitat d'establir un servidor *cyphernet*, ja que segons el descrit fins aquí, ens podríem trobar amb impediments crítics que garantissin l'accés fortificat. El fet que només s'hi pugui accedir amb coneixement de l'adreça específica, i naturalment el programari adient, no és res més que una mesura d'ofuscació que es possible comprometre i que en tal, cas faria accessible el servei des de tots els nodes integrants de la xarxa. Cal assenyalar també, que el pas per multitud de màquines *relay* no controlades tampoc dóna un marge de confiança pel que fa al tractament que puguin donar als paquets que gestionen. Així doncs es descarta la utilització d'aquest canal, compartit entre màquines desconegudes, per encabir-hi la plataforma de publicació del *site*.

Com alternativa immediata a la xarxa TOR ens trobem amb les xarxes P2P, la FreeNet, GNUNet ó en el nostre cas més concretament la I2P. Aquestes basen la comunicacions anònimes en el punt a punt, malgrat es valen d'uns equips *proxy* encarregats d'encaminar les peticions. Cada node participant de la xarxa esdevé un nou encaminador que composarà un determinat túnel. L'estuctura d'aquesta xarxa dota d'un major grau de privacitat i anonimat ja que no és accessible des de Internet. Cal esmentar que en la xarxa TOR, malgrat la dificultat que els cercadors tenen per a teixir una teranyina que desvetlli el contingut de la *Deep Web*, existeixen passarel·les que permeten certs accessos als infra-serveis. Això no passa pas en el cas de les xarxes *peer to peer* ja que esdevenen xarxes totalment aïllades de la Xarxa. Ara bé, es tracta d'una xarxa orientada al missatge, és a dir els participants són coneguts per altri, no pas les seves comunicacions. Els serveis que s'acostumen a donar són web, mitjançant els *eepsites*, clients BitTorrent i serveis d'encaminament segur per aplicacions terceres. L'adreçament, es basa en cada instància que es genera sobre I2P i que a l'hora depèn d'un arxiu que vincula el propi domini *.i2p*. Així es construeixen adreces on es combina l'adreça pròpia amb el port que dóna el servei. Si bé no existeix un servei tipus DNS clàssic sí que els encaminadors disposen del "SusiDNS", consistent en un arxiu pla que associa cada destí amb el corresponent Domini. En cas de no disposar de l'entrada sol·licitada s'escala la consulta als "jumps services" que són serveis d'adreçament distribuït. Cal esmentar finalment que qualsevol protocol és admès en aquest tipus de xarxa. Davant aquesta descripció, veiem com a una alternativa poc vàlida adoptar aquesta solució, doncs també ens veiem obligats a compartir l'entorn amb dispositius desconeguts. Això fa que no sabem quin tractament poden donar als paquets que passen per la seva interfície, malgrat el xifratge de que es doten les comunicacions. La identificació dels ens de l'entorn tampoc ens ajuda a pensar a poder-ne incloure un servei exclusiu i aïllat com el que es pretén en aquest treball.

Un cop arribat a aquest punt, hem vist com ni un entorn centralitzat ni un de punt a punt ens donava prou garanties. Malgrat això, amb una evolució d'aquest darrer sí que podria esdevenir el canal idoni per a disposar de

l'entorn cercat. És per això que s'explora finalment el desplegament d'una VPN com a canal de comunicació per accedir al *site* segur i a les seves dades confidencials des d'un entorn hostil com és el d'Internet.

7.2.1. Virtual Private Network

Escollim doncs desplegar l'entorn sota una xarxa privada virtual que basarà les comunicacions, entre el *site* i els clients remots, en l'establiment de túnels xifrats punt a punt. Aquesta tècnica s'anomena "tunneling", més concretament PPTP (Point to Point Tunneling Protocol), en la versió que corre sota la capa d'enllaç (Layer 2), i disposa de modificacions en aquesta tecnologia com l'L2F (Layer 2 Forwarding), el L2TP (Layer 2 Tunnel Protocol) o L2Sec (Layer 2 Security Protocol) . La seva especificació ens indica que les dades a enviar es divideixen en paquets que es xifren i s'encapsulen i que pateixen el procés invers en ser rebuts pel destinatari.

En la capa immediatament superior, la capa 3 o de xarxa, hi treballa la tecnologia IPSec, encarregada de cobrir la manca d'autenticiat i privacitat d'IPv4. Aquesta pot treballar en mode túnel, els paquets s'asseguren i reben una nova encapsulació de seguretat, o bé en mode transport, quan únicament es xifra i encapsula l'espai de dades del datagrama.

Finalment assenyalar que també es pot treballar sobre la capa 7 d'aplicació sota les funcionalitats d'SSL6 i TLS7. EL procediment és accedir a un web segur, https, que un cop validats ens permetrà l'accés a la VPN via túnel.

7.2.1.1. El producte: OpenVPN

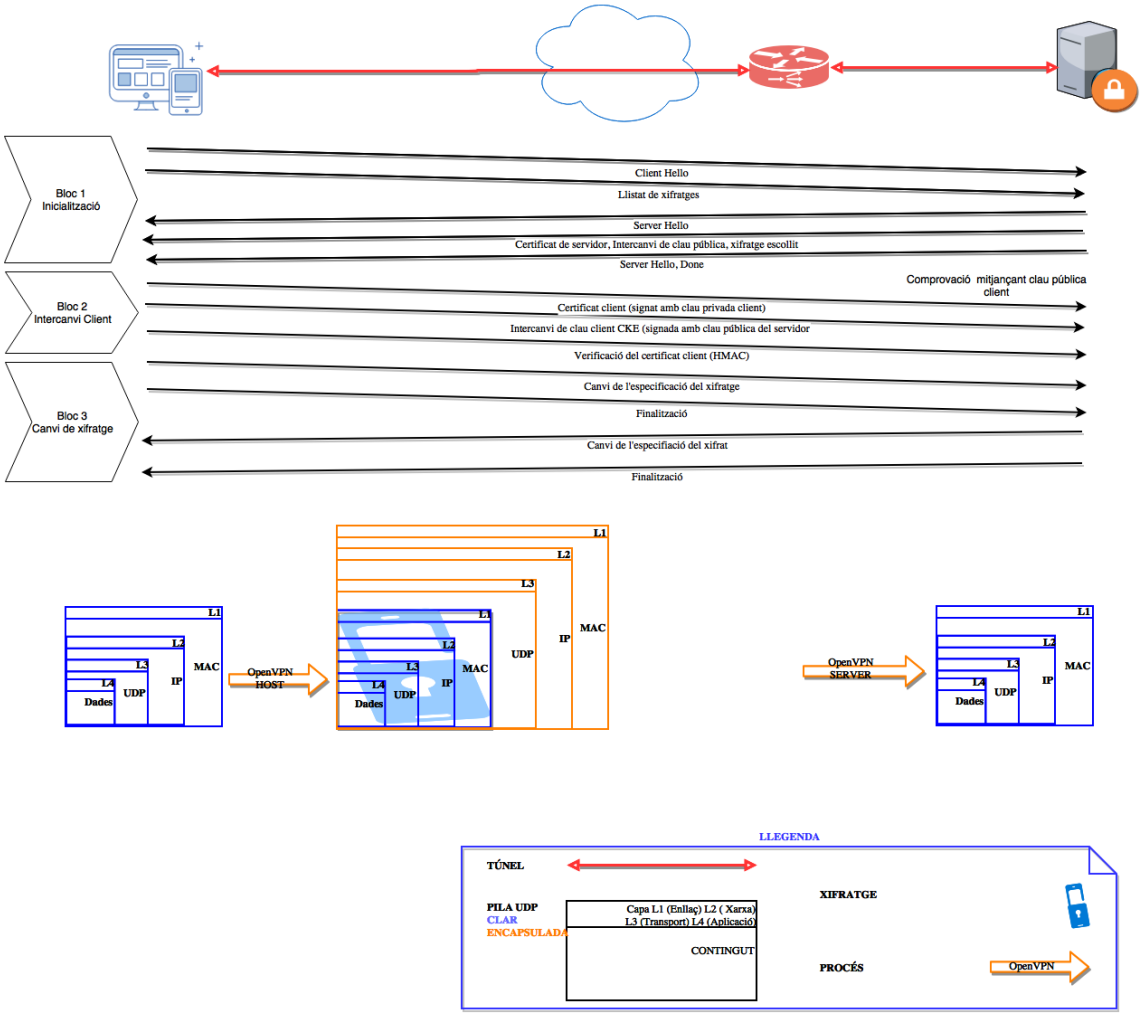
Concretant en el nostre cas, utilitzarem el producte OpenVPN[iii], que pot treballar tant a nivell de capa d'enllaç com de xarxa, i esdevé un producte multiplataforma. Aquesta versatilitat ens donarà gran marge de maniobra per a poder implementar el producte en multitud de dispositius. Pel que fa al tipus xifrat utilitzarem l'asimètric, basat en clau pública i clau privada sota el sistema criptogràfic RSA pel que fa als certificats i claus, corrent sobre SSL/TLS. D'aquesta manera obtindrem els següents avantatges:

- Protecció i Securització dels accessos: assegura l'accés, protegeix les dades i dóna un servei preventiu a possibles amenaces.
- Possibilita la connexió des d'arreu: assegura i protegeix l'accés des de qualsevol lloc on hi hagi connectivitat a Internet.
- Confidencialitat: desplegada per l'equip del producte i avalada per multitud d'aplicacions empresarials crítiques en funcionament.

L'establiment de la connectivitat d'aquesta estructura es basa en l'stàndard que s'anomena encaixada de mans (RSA/DH handshake) sobre SSL/TLS[iv]. En aquest cas consisteix[v] en l'enviament la comunicació de tres blocs de missatges:

1. El client inicia la comunicació amb un missatge "Hello" on indica el llistat de xifratges que suporta per a la generació de la seva clau. El servidor escull el xifratge a esmerçar i li comunica al client conjuntament amb el certificat de servidor i la seva clau pública.
2. El client envia el seu certificat, signat amb la clau privada que el servidor haurà de comprovar mitjançant la clau pública del client. Aquest a l'hora envia el *Client Key Exchange* (CKE), que ha hagut de signar-se amb la clau pública del servidor, pas imprescindible per a obtenir claus simètriques equivalents entre servidor i client que s'esmerçaran per a xifrar les comunicacions. Per tal de comprovar que els extrems de la comunicació són els lícits el client envia una funció resum de l'"encaixada" de mans", HMAC.
3. El servidor canvia l'especificació del xifratge a utilitzar, segons el marcat en el primer pas. Finalitza l'establiment de la fase de negociació, com ho feia el client, amb un HMAC. En aquest moment ja es disposa d'un túnel xifrat síncron entre dos punts.

A mode de resum gràfic, la següent il·lustració mostra la seqüenciació descrita en el paràgraf anterior, això com l'espai xifrat i encapsulat corresponent al datagrama.



IL·LUSTRACIÓ 2 - SEQÜENCIALITZACIÓ, XIFRATGE I ENCAPSULAMENT

Procediment a part, cal escollir quin protocol esmerçar. Si bé la utilització del protocol TCP esdevé més confiable pel que fa a aquestes connexions, ja que n'és orientat, el seu comportament exigeix l'enviament d'un paquet ACK per tal d'establir una comunicació, també el fa més traçable. Això és així doncs el més comú en un atac, durant la fase de *fingerprinting*, és cercar serveis oberts en ports que utilitzin aquest protocol. Tan mateix, un cop descoberta aquesta connectivitat, es poden esmerçar tècniques com les de MiTM, per a capturar el tràfic entre client i servidor. Per aquests motius, s'ha decidit fer la implementació sobre UDP, un protocol no orientat a connexió. Malgrat no tenir la garantia de que hi hagi una petició de reenviament en cas de no arribar correctament els paquets, poden haver-hi pèrdues, ens assegurem de generar menys trànsit que pugui ser capturat. A més, en cas d'escanejos estàndards de ports TCP, tipus NMAP, no sempre s'estableix com una opció de cerca de serveis oberts sobre UDP.

7.3. Plataforma De Publicació

L'elecció sobre l'eina on reposarà el *site* de producció no és trivial, doncs ens ha de donar confiabilitat, tant pel que fa al tractament dels usuaris com a l'emmagatzemament de les dades. Cal doncs, no només garantir la seguretat de la informació en totes les seves dimensions: confidencialitat, integritat, disponibilitat i autenticació, sinó anar una mica més enllà. És per això que es cerca un sistema que faciliti la tasca de gestió de la informació, lligada a una assignació de rols per evitar el repudi. Cal poder fer un seguiment sobre de cada acció feta sobre qualsevol objecte existent, tot identificat l'usuari, en la plataforma. La criticitat de les dades que pugui encabir és rellevant i s'ha de poder determinar el qui, el quan i quines accions s'han dut a terme. Una situació on es podria requerir la recopilació d'aquests registres seria en el cas que es produís una fuita de dades sensibles. Així mateix, serà imprescindible garantir un sistema de còpia de seguretat que permeti, en cas de desastre, poder retornar a un punt temporal anterior. Aquestes dades, han de restar igualment segures i fora de qualsevol possible intromissió, ja que en sí són l'essència del producte a protegir en el plantejament d'aquest treball.

Tan mateix, s'ha de contemplar l'heterogeneïtat de plataformes que poden arribar a tenir accés a l'entorn. Així doncs, és important disposar de mecanismes flexibles, que no tant sols puguin donar accés a la plataforma mitjançant una interfície web, sinó que s'adeqüin al client. Caldrà redimensionar i acoblar-se tant a dispositius de format fixe com a ginys mòbils que hi vulguin accedir. S'ha de recordar que es tracta d'un projecte que ha de donar servei segur tant com a repositori històric d'informació com d'un canal segur d'intercanvi de dades en viu.

7.3.1. Sistemes de Gestió de Continguts

Davant aquestes premisses, s'analitzaren diferents productes existents al mercat i que estaven funcionant en entorns amb necessitats anàlogues, malgrat la llunyania en el seu fet existencial.

Donat que la metodologia d'estudi que s'esmerça en la Universitat Oberta de Catalunya resideix en la utilització d'un campus virtual s'ha fet una aproximació alguna eina de les que s'esmercen en la gestió del mateix. Així doncs, s'ha vist com es fa menester de la plataforma OpenCMS[vi]. Aquesta eina esdevé un gestor de continguts que un cop implantat serà gestionat per quatre rols diferenciats d'usuaris. Així, editors, programadors administradors i usuaris seran qui disposin d'atributs diferenciats per a explotar el *site*. El seu motor de treball corre sobre Java, es desplega sota un servei Tomcat i la base de dades utilitzada és MySql. La informació continguda es tractada sota el metallenguatge XML que permet el seu tractament sobre qualsevol acció que s'hi vulgui donar. Si bé aquestes característiques donarien abast a les nostres necessitats, al no disposar de coneixements previs, la especificitat en la gestió de la plataforma ens fa descartar-la. Cal tenir un nivell de destresa suficient per a, entre d'altres, crear el *site*, afegir-li recursos, crear components, construir la interfície de treball i un seguit d'accions que demanen destresa. Donat que l'àmbit d'aquest TFM no és aprofundir en una eina de treball sinó construir un entorn segur, es descarta la seva utilització.

Un segon possible candidat fora MyBB[vii] (MyBulletinBoard), que bàsicament s'esmerça per a la gestió de fòrums sota una plataforma PHP i que treballa amb diferents BBDD consolidades, el que li aporta les característiques pròpies de seguretat de les mateixes. A més cal indicar que és un entorn força habitual a la *DeepWeb*, cosa que ens hauria de fer pensar en la seva robustesa i que és compatible en entorns ocults. A més, disposa de grans fonts d'informació pel que fa tant a la instal·lació com al tractament de multitud d'incidències que s'hi poden donar. El handicap que presenta aquesta opció és la poca versatilitat de que disposa pel que fa a dispositius mòbils, ja que no compta amb cap motor o eina especifica, sinó que s'adapta a l'entorn mitjançant la utilització de temes més o menys lleugers. Tampoc disposa d'un mòdul de comunicació en temps real d'origen, encara que té la possibilitat de fer enviaments privats a mode de missatge de text. Per tant cal adquirir-ne un en forma de *plug-in* que, si es vol integrar fàcilment i que tingui opcions esteses com l'adjunció d'arxius, acostuma a ser de pagament. Finalment indicar, que si bé disposa d'una gestió de diferents rols assignables a categories d'usuari, la granularitat amb que es poden modificar els seus atributs és menor a la plataforma escollida finalment per a desenvolupar aquest projecte.

7.3.2. Missatgeria Multimèdia Instantània

Si bé aquest apartat es podria considerar un afegit al Sistema de Gestió de Contingut, s'ha cregut adient dedicar-li un punt diferenciat donada la importància del mateix. És per això que s'aprofundirà en donar a conèixer les amenaces pateixen sistemes d'aquest tipus, especialment un dels més utilitzats i populars, el *Whatsapp*. Hom, es pot veure temptat d'esmerçar-lo per a trametre dades confidencials, sobretot després que l'Agost del 2016 l'empresa anunciés el xifrat de les seves comunicacions. Aquest fet però no és suficient com per garantir-ne la confidencialitat sobre les dades tractades. Tal i com es passa a apuntar[viii], existeixen un gran nombre de forats de seguretat que en desaconsellen el seu ús:

- Procés insegur en l'alta d'usuaris, la explotació malintencionada sobre els mecanismes de registre podria permetre llegir els missatges, i fins i tot enviar-ne, sobre el compte d'un tercer. Vaga dir que aquest tercer, la víctima, podria ser qualsevol membre del cos de seguretat.
- Robatori de comptes, mitjançant el començament d'un procés de registre, un atacant podria simular un canvi de terminal. Així, només amb la possibilitat de previsualització dels SMS de confirmació del terminal exposat, es podria activar el compte en un nou telèfon.
- Segrest de sessió, ajudant-se de l'opció de verificació per trucada, un atacant amb accés al dispositiu podria obtenir el codi de verificació, ja que no és possible evitar aquest avís malgrat estar blocat el telèfon lícit.
- Segrest de comptes, ajudant-se d'errors coneguts en el protocol de comunicacions SS7, que defineix els procediments pels quals una xarxa de telefonia intercanvia informació sobre una xarxa digital, es podria esmerçar una tècnica de MiTM. Es faria passar doncs el número de telèfon de la víctima per el de l'atacant i d'aquesta manera, s'assoliria la captura i gravació de trucades, SMS o detecció de dispositius.
- Esborrament insegur de converses, cosa que permetria en cas d'accés físic al dispositiu, mitjançant la utilització de tècniques forenses, l'accés al registre de les converses. Això es degut a que veritablement no s'esborra la informació sinó que queda marcada com a espai lliure a omplir.
- Emmagatzemament en BBDD, aquesta és realitza en local en format SQLite i actualment xifrada. Tot i això, si un atacant hi tingués accés, potser amb algun troià o algun altre mètode per accedir-hi, seria possible accedir a la totalitat de les dades del compte. Això és així degut a que el xifrat incorporat, l'*.crypt12* és vulnerable.
- Còpies de seguretat desateses, aquestes es realitzen al núvol i no se'n té un control exhaustiu. Per exemple, en el cas d'aquells continguts esborrats en el dispositiu segueixen residents en les còpies fetes en anterioritat. Una irrupció en el compte de correu personal d'algun usuari en podria revelar les dades.

- Versions "tunejades", descarregar-se una versió no oficial del producte implica un risc major ja que es desconeix l'autor de l'aplicatiu i quines intencionalitats hi ha al darrera. Aquestes instal·lacions acostumen a requerir l'accés a les nostres dades sense tenir cap garantia que no se'n farà un mal ús.
- Physhing mitjançant Whatsapp web, un atacant poc enganyar demanant que s'escanegi un codi QR amb un aplicació pròpia, quan en realitat es redirigit a la sol·licitud d'un nou inici de sessió per codi QR de Whatsapp. En aquest moment es desaran les credencials i dades de sessió desades i seran reutilitzades per accedir al seu compte de manera il·legítima.
- Utilització de versions antigues, en les anteriors versions no es tingué prou cura i es podia arribar a conèixer el contingut de les converses, el número de telèfon i la ubicació. La utilització d'aquest programari primerenc exposa les dades a les vulnerabilitats descrites.
- Difusió d'informació sensible durant la connexió inicial, ja que en aquest estadi s'intercanvia informació sobre: SO del client, versió de l'aplicació en ús i el número de telèfon dels participants. Aquesta informació pot quedar exposada, en clar tractant-se de versions anteriors o xifrades a hores d'ara. Malgrat aquest xifrat d'extrem a extrem el número de telèfon segueix sortint en clar, tot i que codificat en binari. Per tant, no es pot dir que s'ha produït una millora en la seguretat sinó que s'ha emmascarat la informació. Això incideix especialment amb la necessitat de fer ús d'una VPN per tal de ocultar aquestes dades.

7.3.2.1. El producte: Moodle

Així doncs, finalment s'opta per l'elecció de Moodle[ix], una eina orientada al desenvolupament de plataformes d'aprenentatge sota un entorn robust segur. Malgrat diferir el seu àmbit d'aplicació amb el del nostre treball, les seves característiques ens permeten establir un espai controlat per a la publicació d'informació sensible. L'eina disposa a priori de diferents rols: manager, creador de cursos, professor, professor no editor, estudiant, convidat i usuari autenticat. Tots aquest disposen de diferents privilegis pel que fa a la publicació i visualització de contingut i es pot fer una equivalència als nivells de gradació que es poden menester en un entorn policial. A més, se'ns permet crear nous rols d'usuari, assignant-los els atributs escaients, gràcies a un sistema granular de permisos força detallat. A més disposa d'un nivell de filtrat adient que amb una simple consulta, sobre atribut o grup ens retorna qui disposa de certa capacitat o rol. Pel que fa a la gestió de cursos, que en el nostre cas esdevindrà els taulell de publicació d'informacions segmentades segons temàtica, és molt complerta. El propi aplicatiu permet d'una manera senzilla, assignar, o prohibir, als diferents rols totes aquelles capacitats que creguem adients. Tan mateix, compta amb la possibilitat de realitzar plantilles de cursos, cosa que evitarà haver de mirar per a cada nova publicació els permisos que definim com a estàndards. La creació de blocs també és possible i pot donar una dimensió

més enllà de la publicació de notícies rellevants. Així doncs també podria esdevenir un espai de compartició d'informació més a nivell d'investigació o estudi. Cal esmentar que també és possible la creació d'etiquetes, fet transcendent sobretot a l'hora de cercar informació determinada en un espai que es pretén vagi augmentant significativament al llarg de temps. A més, es pot gestionar un calendari tant per rebre notificacions programades com per a definir espais temporals de publicació de certes notícies al taulell.

Finalment esmentar que disposa d'un xat propi que permet l'intercanvi de missatges de text en temps real. Aquesta eina és imprescindible en el nostre entorn, ja que es vol desplegar un espai que permeti la comunicació immediata quan es realitzin actuacions *in situ*. Donat que té limitacions pel que fa a l'enviament de material multimèdia i a la gestió de grups que puguin interactuar de manera aïllada, caldrà esmerçar un *plugin* extra. Aquest afegit, ens permetrà utilitzar, o crear, un grup d'usuaris destinats a una acció determinada per a que puguin intercanviar missatges de text, fotografies, documents i informacions. És a dir, es disposaria d'un espai de missatgeria propi no depenent de terceres companyies i, donades les característiques del canal de comunicació esmerçat, opac a l'operador de telefonia mòbil.

7.4. Xarxa Esquer

Tal com s'ha esmentat, paral·lelament a la xarxa de producció s'implementarà una xarxa esquer destinada a recopilar informació sobre possibles accessos il·legítims. Aquests tipus de xarxes, anomenades *honeynet*, es basen en l'establiment de serveis que simulen entorns reals i que per si mateixes conformen una xarxa autònoma. Aquests són implementats en màquines, els equips *honeypot*, que disposen diferents serveis que emulen entorns reals, sobretot pel que fa a la resposta a les peticions que s'hi projecten. És a dir, es crea un entorn el qual quan un atacant fa una recerca d'informació, intenta validar-se en l'entorn, hi infereix comandes o mira d'accedir a les fonts de dades, espera rebre uns resultats per part del sistema. L'objectiu, és recollir totes les accions en registres que un cop desats podran ser analitzats per tal de trobar pautes sobre el comportament s'emprenen per tal d'atacar les infraestructures. Així, queden al descobert eines i tàctiques esmerçades per a comprometre el sistema que han de servir per a prevenir futurs atacs, tant siguin provinents directament d'humans com de programari maliciós. D'aquí rau la importància d'intentar simular l'entorn real per a poder acotar els resultats a la tipologia de la nostra xarxa. No es tracta doncs de rebre atacs indiscriminats per a recol·lectar molta informació, sinó posar a l'abast dels atacants uns esquers accessibles que els atraguin per emprendre aquelles activitats que realitzarien contra l'entorn real. S'ha de considerar però no deixar en clar, de manera evident, aquests serveis troianitzats, sinó no

excedir-se en el cel pel que fa a la seva protecció. S'ha de cercar un equilibri, per a no aixecar sospites, entre presentar un espai totalment vulnerable i un que sigui extremadament inaccessible. En aquest sentit és doncs on entren en joc varis factors. Per una banda les "filtracions" per a les aranyes dels cercadors amb certa informació que pugui despertar interès d'atacants. Així escollir un domini amb un nom atractiu on hi resideixi una informació translúcida pot despertar l'interès de malfactors. En termes més concrets esdevindria la publicació a Google d'un domini escaient on per exemple hi figurés l'arxiu robots.txt on hi residís certa informació sucosa. Per altra banda, ha de ser possible, però no evident, poder-se validar en el *honeypot* i així possibilitar que l'atac tiri endavant. A més, amb tota la informació que es pretén recol·lectar també pot servir per a contrastar-la amb un possible atac, si mai es produís, contra l'entorn de treball legítim. El creuament de dades podria donar-nos més afinitat a l'hora d'assenyalar el possible origen d'un atac. Disposar d'un registre històric esdevingut a la *honeynet* pot completar la informació que els esdeveniments de la plataforma lícita ens pugui subministrar. Sempre poden haver-hi descuits o menor protecció darrera les accions dels atacants durant les diferents fases de les seves tècniques de penetració.

7.4.1. Classificació

Davant aquestes premisses cal escollir el producte adient per a desplegar la nostra xarxa *honeynet*. En el mercat hi ha multitud d'eines que es poden classificar segons dos criteris principalment: el seu objectiu o la seva interacció. Passem doncs a esmentar breument les característiques ambdós per tal d'afinar en la selecció del programari a instal·lar.

- Objectiu[x] (concepte desenvolupat per Marty Roesch, desenvolupador del programari Snort)

    - *Honeypot* de producció, són fàcils d'utilitzar i s'utilitzen per a capturar informació limitada. Treballen en el mateix entorn que el serveis de producció i són destinats a millorar la seguretat de l'entorn per així mitigar el risc de patir un atac. Obtenen una informació menor dels atacants pel que fa a les eines esmerçades i el seu entorn.
    - *Honeypot* de recerca, presenten més dificultat pel que fa al seu desplegament i manteniment. El seu objectiu és recol·lectar major informació sobre la motivació i tàctiques que esmerça l'atacant. Es tracta d'aprofundir en l'anàlisi dels mecanismes d'intrusió per aprendre a protegir-se'n, per la qual cosa necessiten capturar dades de manera més extensa. La manera d'aconseguir-ho és oferir un entorn altament interactiu i controlat, cosa que ens oferirà més informació de l'atacant, com es comunica i de quines eines es serveix. Cal però un esforç més gran per a controlar i administrar aquest tipus d'infraestructures

doncs l'atacant disposa d'una superfície d'atac major, i conseqüentment més perillosa.

- Interacció [xi] (Mokube and Adams, 2007)

    - Baixa, caracteritzats per la senzillesa pel que fa a la instal·lació i al poc risc pel sistema que representa la seva explotació. És tracta d'un servei emulat, on l'entorn no disposa realment de sistema operatiu ni de programari executable. Això disminueix notablement les accions a realitzar per l'atacant i en conseqüència les dades a recopilar. Esdevé un recurs fàcil de mantenir i desplegar. El producte NetSec o Honeyd serien un exemple d'aquest tipus, de fet aquest darrer funciona com a servei afegit al SO més que com a programari. El seu àmbit defineix dins l'emulació de serveis dels protocols TCP/UDP, com poden ser l'FTP, SSH, ICMP, HTTP o l'SMTP.
    - Mitja, l'àmbit de treball virtual és el mateix que en el cas dels equips de baixa interacció però disposen d'un ventall major de serveis a emular. Així arriben a emular SO, cosa que permet realitzar llençar comandes al sistema per part de qui realitza una penetració però sense conseqüències per al medi. D'aquesta manera és possible recopilar un major nombre d'accions i procediments d'atac en el registre del *honeypot*. Dos coneguts productes són Nepenthes i Mwcollect que exposen vulnerabilitats per tal de recollir les accions que el *malware* realitza contra la plataforma.
    - Alta, en aquest cas és tracta d'una aplicació real que treballa sota un SO també real, no hi ha doncs emulació. Permeten doncs una recol·lecció important i vehement del que pot arribar a fer l'atacant, o *malware* en qüestió. Per contra, la superfície d'exposició és major amb la conseqüent perillositat que això suposa per al sistema. Cal ubicar-los, doncs, en *subnets* separades de l'entorn de producció. El seu desplegament, manteniment i supervisió representen una càrrega de feina molt superior als dos *honeypots* de gamma inferior. Les dades capturades poden ser explotades posteriorment per d'altres programaris amb capacitats més dedicades a l'anàlisi i explotació de registres. Un dels programaris que s'estableixen en aquesta categoria és l'anomenat Sebbek. Aquest, captura cada interacció que comet l'intrús, el seu *kernel* pot desar quines accions s'han realitzat fins aconseguir l'accés al sistema. També esdevé una eina útil en cas de voler analitzar tràfic xifrat, ajudant-se d'eines d'anàlisi de xarxa, pot reconstruir fluix de dades de sessions i descobrir tant objectius com activitats de l'atacant.

Així doncs, donat l'abast d'aquest TFM optem per l'elecció d'una *honeynet* de producció que es basarà en la implementació de diferents *honeypot* de baixa o mitja interacció. En la seva implementació, però, es mirarà

d'aproximar-se a l'abast, pel que fa a l'explotació de les dades recol·lectades de dades, a una alta interacció.

El seu desplegament es farà en un entorn virtual autocontingut dins la mateixa infraestructura que l'espai de producció. Així caldrà garantir, mitjançant tallafocs, *VPNs* i l'ús de tècniques d'ernrutament, l'aillament entre la xarxa de treball i la *honeynet*.

7.4.1.1. El producte: Modern Honey Network

Aquest producte neix de la companyia Anomali INC amb la pretensió de simplificar les tasques d'instal·lació i gestió de diferents *Honeypot*, tant d'interns com d'externs. El programari suporta l'estàndard *HPFeeds*[xii], un protocol genèric que possibilitat l'intercanvi de dades compartides i que pot ser cridat des de qualsevol llenguatge de programació. En aquest cas s'utilitza per enllaçar la informació recollida pels diferents *Honeypot* amb programari destinat a l'anàlisi de dades, com és el cas de l'Splunk. També comunica amb un mòdul de representació gràfica sobre les dades recollides que es presenten sobre un mapa mundial, l'anomenat *honeymap*. A més interactua amb Mnemosyne, mecanisme destinat a sincronitzar les dades recollides amb el contenidor de les mateixes, el mongoDB. Aquesta BBDD esdevé el magatzem del producte i pot ser consultada tant per aplicacions terceres com pel propi usuari. En aquest darrer cas, es disposa d'una aplicació web que ens presenta els resultats obtinguts i permet la gestió del producte. Així, la interfície ens ofereix la possibilitat de gestionar les següents àrees, dividies en menús:

- Map: ens mostra el mapa esmentat on poder veure en viu l'orígen dels atacs soferts.
- Deploy: espai on podem seleccionar l'script que volem desplegar, tant sigui en el servidor com en un sensor que li enviï la recol·lecció de les dades. Ara com ara disposem de:
  - Ubuntu – Suricata: IDS/IPS veloç que pot analitzar, entre d'altres els protocols: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, HTTP, SSL, TLS, SMB, SMB2, DCERPC, SMTP, FTP, SSH, DNS
  - Ubuntu – Glastopf: desplegament de baixa interacció que emula milers de vulnerabilitats donant la resposta esperada als exploits atacants.
  - Ubuntu – Shockpot: aplicació web que emula patir la vulnerabilitat CVE-2014-6271.
  - Raspberry Pi – Dionaea: script específic per al desplegament de Dionaea sobre dispositius de maquinari Raspberry Pi.
  - Ubuntu – Snort: IDS/IPS analitzador de xarxa de gran abast de codi obert que permet supervisar, i crear esdeveniments, sobre tot el tràfic escollit com a objectiu.

    - Ubuntu - p0f: eina que utilitza empremtes passives per a identificar el sistema operatiu rere les connexions TCP establertes.
    - Ubuntu – Conpot: sistema de baixa interacció destinat a controlar protocols desplegats en ambients industrials.
    - Ubuntu/Raspberry Pi – Kippo: script específic per al desplegament de Kippo sobre dispositius de maquinari. Raspberry Pi. Kippo actua com a un heneypot d'interacció mitja dissenyat per desar esdeveniments d'atacs per a força bruta sobre SSH amb una interfície prou depurada.
    - Ubuntu – ElasticHoney: eina de cerca dissenyada per a enganxar atacants que mirin d'explotar vulnerabilitats del tipus RCE.
    - Ubuntu – Amun: honeypot de baixa interacció que es troba discontinuat en aquests moments.
    - Ubuntu – Wordpot: emulador d'una plataforma dissenyada sota Wordpress.
    - Ubuntu – Dionaea: sistema de baixa interacció que exposa multitud de serveis com MSSQL, SIP, HTTP, FTP, TFTP, etc. Entrarem més en detall sobre aquest script durant la redacció de la present memòria, doncs és l'escollit per a desenvolupar la pràctica proposada.
- Attacks: en aquest menú podrem filtrar les atacs rebuts segons el tipus de sensor esmerçat, l'script, la data, el port o l'adreça supervisada. La informació bolcada segons el filtre aplicat serà el país i la IP de l'atacant i sobre quin el protocol i port està mirant d'obtenir accés.
- Payloads: aquest espai servirà per a que, en cas que un atacant hagi utilitzat programari per a mirar d'explotar algun servei exposat, se'ns mostri la petició del mateix. Així doncs podrem obtenir la informació de la data, el sensor encarregat de la supervisió, la IP atacant, el port atacat, la prioritat, la classificació i la signatura de l'arxiu maligne.
- Rules, aquest menú es subdivideix en dos apartats:
    - Manage Activate/Desactivate: permet activar o desactivar regles específiques que entren en funcionament en escollir un script. Això possibilita escollir de manera més granular quins serveis es publiquen.
    - Sources: possibilita afegir repositoris des d'on cercar noves regles per a descarregar.
- Live Render: mostra les regles actuals de que disposa el programari, a nivell d'un IDS. Pre-Rendered: permet descarregar les regles existents.
- Sensor, menú subdividit en dos apartats
    - View Sensors: visualització dels dispositius on s'hi ha instal·lat un sensor. Apareix la informació dels scripts actius, on apareix la informació de la màquina on s'ha instal·lat, l'adreçament, el tipus de sensor, el seu identificadors i el nombre d'atacs totals patits.

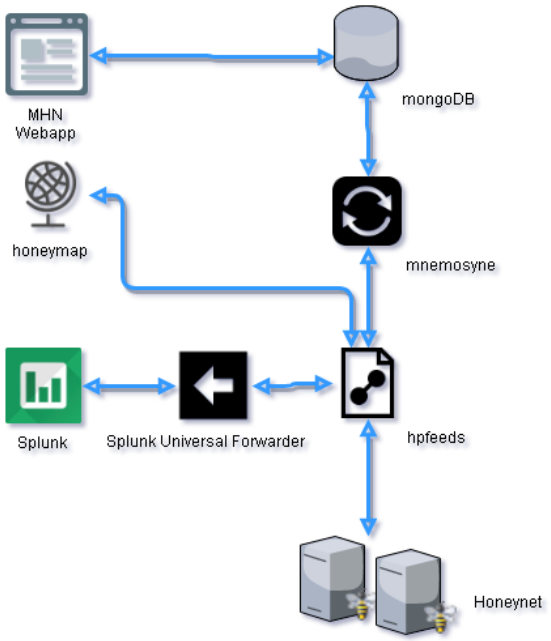
- Add Sensor: permet afegir nous sensor instal·lats en màquines diferents. Cal indicar que en el cas d'afegir en "local" noves funcionalitats, apareixerien de manera automàtica en la visualització.

- Charts: visualització de gràfiques referents al desplegament del sensor Kippo. Aquest ens permetria observar els principals: usuaris, mots de pas, usuari/password i atacants.

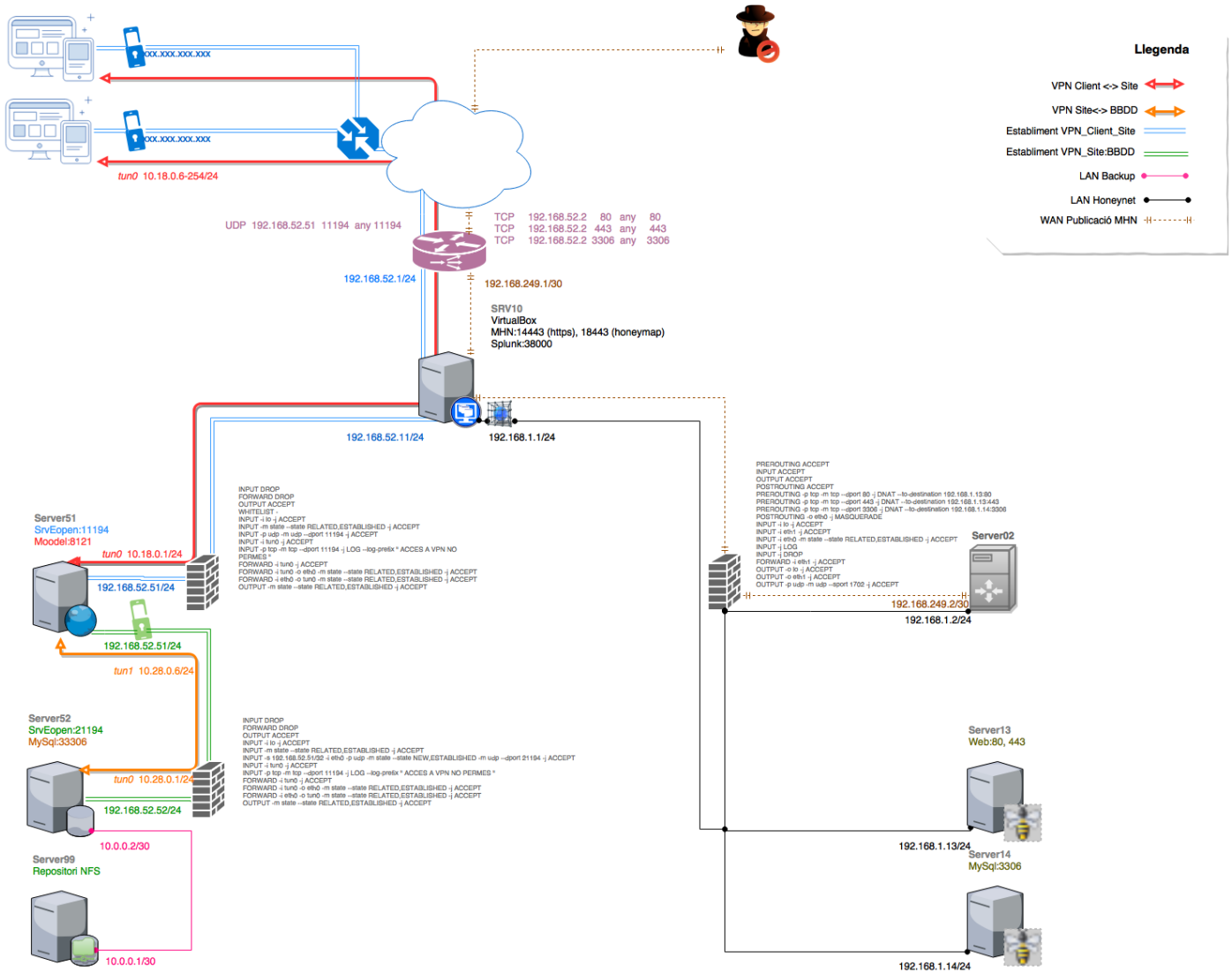
En definitiva esmentar que es tracta d'un producte que es permet desplegar a mida diferents *honeypot* mitjançant l´ús de sensors per a construir la nostra *honeynet*.

7.4.1.2. El producte: Splunk

Malgrat la vistositat i presentació de dades que ens aporta el Modern Honey Network el tractament de les mateixes és poc flexible. Per tal de poder explotar les dades, monitoritzar-les i estudiar-ne l'enginyeria operacional que ens aporten, cal un producte més específic. Així, tal com contempla el propi MHN dins la seva instal·lació s'opta pel desplegament d'aquest programari[xiii]. Mitjançant el mòdul *The Splunk Universal Forwarder*, basat en el protocol *hpfeeds*, es traspassaran els registres recollits pels diferents *Honeypot* a aquest aplicatiu. Cal doncs, que els sensors recullin les dades, les emmagatzemin en un arxiu local de registre i s'enviïn a l'adreça i port designat per l'Splunk que resta a l'espera de rebre-les. Amb aquesta informació es podran construir diferents consultes i presentar les dades d'una manera escaient per a poder fer l'anàlisi de les mateixes. De fet, ja existeix un mòdul[xiv] extern desenvolupat que efectua aquesta tasca i que és modificable a conveniència.



IL·LUSTRACIÓ 3 – INTEGRACIÓ SPLUNK EN L'ENTORN MHN



IL·LUSTRACIÓ 4 – ESQUEMA DE XARXA FINAL

A la il·lustració que precedeix aquest text, es reflecteix l'escenari dissenyat per a fer front a tots els ítems apuntats en aquest projecte. A nivell físic, dins el que esdevé la infraestructura pròpia, disposem d'un encaminador, que tanmateix actuarà com a tallafocs i d'un ordinador destinat tant a tractar i recopilar les dades dels sensors, mitjançant el programari MHN i Splunk, com a encabir els servidors virtuals, sota l'entorn de VirtualBox. Aquests es distribueixen gràficament en dues àrees, segons a l'entorn a que pertanyen, corresponents a la part esquerra i dreta de l'esquema. Així es pot observar com el sector a l'esquerra de la imatge pertany a l'entorn de producció, mentre que el dret està assignat a la xarxa *honeynet*. Abans d'entrar en el detall del funcionament, cal assenyalar el canvi de adreçament dels ports estàndard i l'esforç per a implementar canals de comunicació segurs. En l'esquema doncs s'han assenyalat els aspectes més rellevants i diferencials en cada ubicació que en fan referència, a més d'altres descriptius. No ens trobem amb una interpretació exhaustiva de cada component, sinó a la interpretació gràfica d'aquells punts més rellevants. Agafant doncs aquesta referència, anem a descriure cadascun dels elements que hi trobarem i com es comuniquen entre els seus afins.

Començant per la zona esquerra, la zona de producció, veiem que està formada per tres servidors amb rols diferenciats: el de publicació (Server51), el de BBDD (Server52) i el de còpia de seguretat (Server99). Dels tres, la única màquina accessible des de l'exterior és la de publicació, això sí de manera ofuscada ja que es tracta d'una *Darknet*. Per accedir-hi, és imprescindible establir una connexió VPN, sota el programari OpenVPN, que un cop generada possibilitarà realitzar la identificació unívoca d'usuari dins el *site* DeepTicies*,* bastit mitjançant Moodle. El procediment, es basarà en una validació de credencials d'usuari del SO host amfitrió i disposar del certificat de client, que opcionalment pot requerir els subministrament d'una clau de pas. Un cop establert el túnel serà possible ingressar en la plataforma, mitjançant la introducció de les credencials d'usuari pertinents, i així tenir accés als recursos assignats a cada usuari en qüestió. Es pot observar com hi ha un primer canal (canonada blava) destinat a establir la connexió virtual que permetrà generar un túnel específic (línia vermella) entre els clients i el *site*. El tallafoc, resta preparat per si mai es volgués aplicar una política més restrictiva d'accés per adreçament d'origen. Seguint aquest mateix esquema visualitzem una segona xarxa virtual privada (canonada verda). Aquesta a VPN permet establir un nou túnel (línia carbassa), que s'utilitza per a comunicar de manera exclusiva, i amb el recolzament tallafocs, el portal DeepTicies amb la corresponent BBDD, bastida per una instància de MySQL. Finalment assenyalar que una nova connectivitat (línia verda) permet de manera exclusiva, gràcies al tallafocs, disposar d'un repositori NFS per a realitzar una exportació de la base de dades, a mode de garantir la còpia de seguretat diària de la mateixa. Indicar, tanmateix que idealment aquest servidor es trobaria en una ubicació aïllada d'aquest entorn físic per tal de complir amb totes les garanties inherents a un *backup*.

Pel que fa a la zona dreta de l'esquema definirem el que és l'espai dedicat a la *honeynet*. Aquesta és formada per tres servidors, un que fa les funcions

d'enrutament (Server02) i dos amb funcionalitats de *honeypot* (Server13 i Server14). En aquest cas, i degut a les característiques del *router* del laboratori, també hi ha una única màquina accessible des de l'exterior que és la dedicada a l'encaminament. Disposa de dues targes de xarxa, una amb accés a Internet (línia discontínua marró) i una altra per a comunicar-se amb els equips de la *honeyne*t (línia negra). El *firewall* intern, l'*Iptables*, conté les regles que permeten l'encaminament d'aquests equips cap a l'exterior i alhora manté aïllades les màquines respecte la xarxa de producció. Aquests servidors doncs, disposen dels serveis esquers oberts i poden accedir a l'equip amfitrió físic, que tal com hem comentat, recull les dades capturades per a ser analitzades. Així el primer *honeypot* disposa d'un sensor Dionaea que emula el servei web DeepTicies i el segon farà les funcions de MySql. En aquest punt s'implementa una xarxa exclusiva i aïllada per a comunicar la honeynet amb l'equip gestor dels registres (SRV10).

Finalment apuntar que a nivell d'adreçament, cada sector específic compta amb la seva xarxa diferenciada. Més que parlar de *subneting* el que s'ha optat és per l'aïllament per IP lògic total. Així la xarxa de producció compta per a establir el canal virtual amb l'adreçament: 192.168.52.x/24, cada túnel esdevé independent i respectivament disposa de les IPs: 10.18.0.x/24 i 10.28.0.x/24. Mentre que pel que fa a l'espai reservat a la *honeynet* de l'adreçament extern és el 192.168.249.x/30 i internament el 192.168.1./x/24.

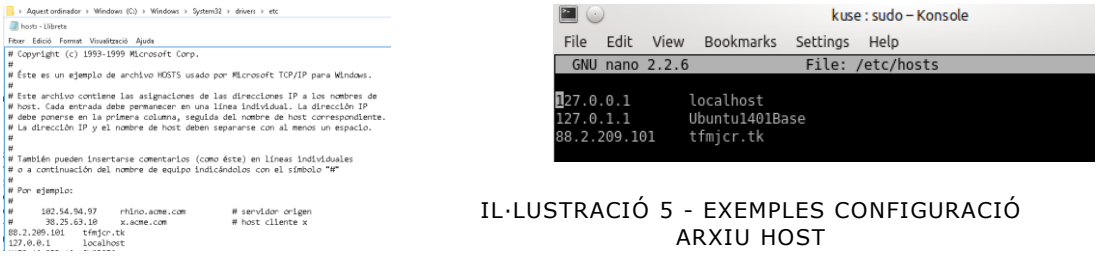
9. IMPLEMENTACIÓ

En els següents apartats posarem en relleu aquells punts de la configuració més destacats, pel que fa a la seguretat, sobre les eines desplegades per tal de construir l'entorn. Cal indicar que no es tracta d'una formulació, fil per randa, de les passes a realitzar per a la seva implementació, ja que sobre aquest aspecte Internet n'és ple de manuals. El propòsit és indicar aspectes puntuals en la configuració de cada àrea: Sistemes Operatiu[xv], Router[xvi], Iptables[xvii], VirtualBox[xviii], OpenVPN[xix], Moodle[xx], MHN[xxi] i Splunk[xxii]. El que es vol recollir en aquesta memòria són les especificitats per a construir un entorn segur, no pas una guia d'instal·lació estàndard de cada producte. Informació que d'altra banda està prou nodrida fent una senzilla cerca en el buscador. Així, s'indicaran les modificacions més rellevants fetes en cada instal·lació, deixant per l'espai d'annex la integritat dels arxius tractats.

9.1. Domini: tfmjcr.tk

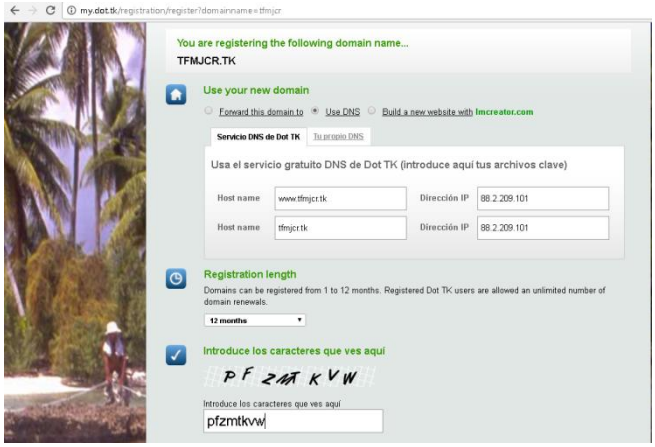
S'ha escollit el domini tfmjcr.tk ja que és descriptiu sobre el *treball de final de master de josep caballe ràmia* (tfmjcr) i té un període de gratuïtat (tk).

Qualsevol referència feta a aquest domin,i des d'una màquina integrant de l'entorn de producció, s'enllaça amb l'adreçament 88.2.209.101 que cop establert el túnel esdevé l'adreça 10.18.0.1. Això s'aconsegueix mitjançant la modificació de les entrades *hosts* d'aquelles màquines participants.



IL·LUSTRACIÓ 5 - EXEMPLES CONFIGURACIÓ ARXIU HOST

A nivell de resolució de DNS externs, cap la possibilitat d'adquirir el domini, amb un període limitat de gratuïtat que inclou la resolució de noms. Cal avaluar però, la idoneïtat de fer-ho, ja que això suposa exposar-ho al món i afavorir la inclusió d'informació accessible, de la que caldrà estudiar-ne el detall a publicar.



IL·LUSTRACIÓ 6 - ADQUISICIÓ DEL DOMINI TFMJCR.TK

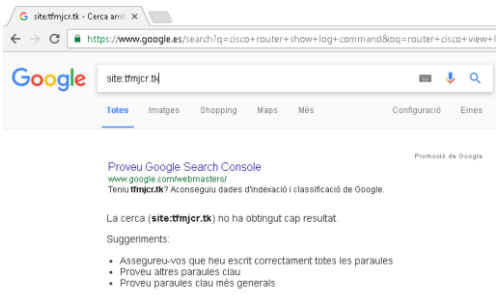
Mentrestant una simple cerca en un DNS mundial d'aquest domini ens retornarà un adreçament extern.

```
> tfmjcr.tk
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  tfmjcr.tk
Address:  195.20.45.125
```

IL·LUSTRACIÓ 7 - RESOLUCIÓ DNS DE GOOGLE SOBRE TFMJCR.TK

S'ha de tenir present que l'objectiu de l'entorn que fa les funcions d'esquer, no és pas la captura indiscriminada d'atacs, sinó detectar aquells que actuen amb premeditació sobre el nostre entorn. És a dir, poder recollir informació d'aquells atacs dirigits que com a tals començaran cercant la porta d'entrada a l'entorn exposat.

Un excés de dades evidents, com pot ser la indexació en cercadors d'informació rellevant, pot despertar sospites. No seria gaire pertinent que, un *site* d'intercanvis d'informació sensible dels cossos de seguretat, fos publicat per exemple a google.com.



IL·LUSTRACIÓ 8 - RESULTAT DE LA CERCA TFMJCR.TK A GOOGLE.COM

9.2. Encaminador

Aquest dispositiu actua com a enllaç entre les dues xarxes ha implantar i Internet. Per això s'ha extremat la cura en el filtratge de les comunicacions, sobretot pel que fa a les entrants. Així, actuant en l'espai de publicació, tant sols s'ha mantingut obert el port 11194 contra el servidor de publicació. D'aquesta manera es garanteix que la única entrada al servei web sigui mitjançant l'establiment d'una VPN. Pel que fa a l'entorn on resideixen els *honeypot*, s'han obert en exclusivitat els ports 80 i 443 per a emular un *site* amb publicació i el port 3306 que dóna el servei *fake* a la suposada base de dades que el suporta.

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address/WAN Interface	WAN Port	Action
SRV51_VPN_11194	udp	192.168.52.51	11194	any	11194	delete
VirtualServ4	tcp	192.168.249.2	80	any	80	delete
VirtualServ5	tcp	192.168.249.2	80	any	443	delete
VirtualServ5	tcp	192.168.249.2	3306	any	3306	delete

IL·LUSTRACIÓ 9 - CONFIGURACIÓ NAT DEL ROUTER

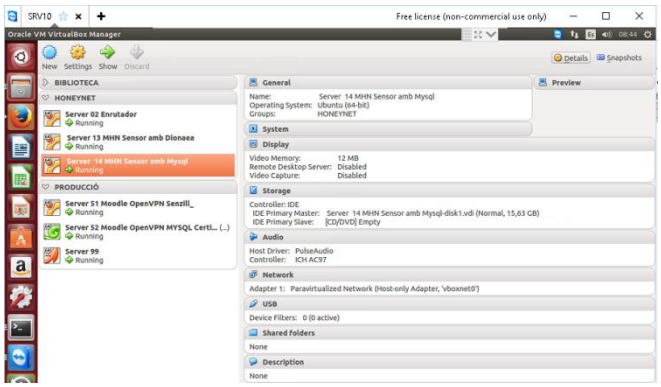
També ha calgut habilitar la possibilitat de realitzar encaminament per una segona interfície. Això ha permès muntar, l'espai independent i aïllat del de producció, format per les màquines honeypot que restaran a l'espera de rebre atacs. Cal observar que la màscara no s'ha pogut modificar, el que ha obligat a incloure un servidor tipus proxy[9.8.3].

IL·LUSTRACIÓ 10 - HABILITACIÓ SEGONA INTERFICIE DE XARXA AL ROUTER

El propi router disposa d'altres característiques avançades, equivalents a les que s'han desplegat a la xarxa, per exemple filtratge per MAC o establiment de VPN. Se n'ha descartat el seu ús, en favor de les configuracions dels servidors, ja que es tracta d'un dispositiu domèstic. Això el fa menys confiable, si més no a priori.

9.3. VirtualBox

La totalitat de les màquines que composen aquest projecte, exceptuant el SRV10, són virtuals. L'eina escollida per a tal empresa és el VirtualBox, instal·lat com a *host* al servidor físic, i hostatjant com a *guest* els servidors, tant de l'espai de producció com el de *honeynet*.



IL·LUSTRACIÓ 11 - ORGANITZACIÓ SERVIDORS VIRTUALS

Amb aquest equipament doncs, som capaços de gestionar set servidors que esdevenen la base per a desenvolupar el projecte. D'altra banda apuntar, que també s'ha esmerçat aquest programari en el dispositiu que emularà els equips clients. En aquest cas però, el host és Windows i els clients disposen d'una distribució KUbuntu.

9.3.1. Recursos

Cada servidor té les seves especificitats pel que fa als recursos assignats, destacant la ubicació física del disc virtual (.vdi). Així, aquells servidors més crítics s'han disposat en discs durs separats amb redundància, construïts sota mirall amb tecnologia RAID1. D'aquesta manera es disposa d'una

IL·LUSTRACIÓ 12 - UBICACIÓ LÓGICA DELS HDD .VDI

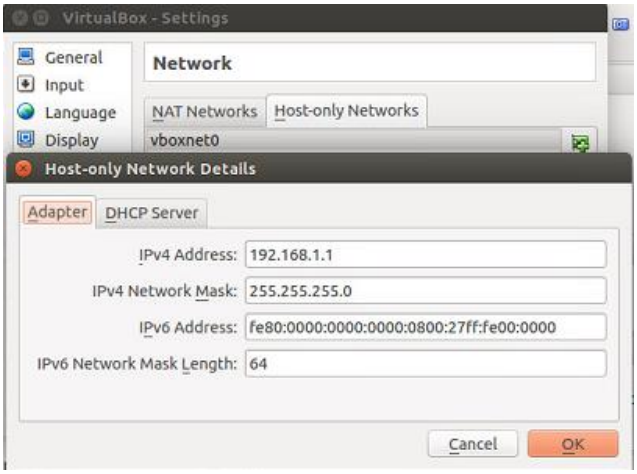
mesura de contingència davant els errors. Sobre aquestes unitats també s'ha aplicat el xifratge, preveient un possible atac físic sobre els mateixos. D'aquesta manera s'impediria l'accés a les dades per part de possibles accions no autoritzades sobre el maquinari. També cal destacar en aquest punt el sistema de muntatge d'arxius que s'ha esmerçat en les dues unitats que disposen de RAID.

Així, per una banda tenim el repositori CONTENIDOR, on s'ha muntat el RAID en mode clàssic i s'ha xifrat. Aquest espai és el destinat a encabir el servidor de publicació, Server51.

D'altra banda tenim el repositori DIPOSIT que esmerça el *Logic Volumen Managment Ver2*, basat en la creació d'un RAID que a l'hora conté l'espai lògic on s'emmagatzemen, i xifren, les dades. Amb aquest tipus de muntatge d'unitats és possible crear instantànies que poden ser utilitzades per a crear còpies de seguretat. L'avantatge d'aquest sistema és poder donar un servei interromput, on no calgui aturar serveis ni fer exportacions mitjançant eines depenents del sistema operatiu *guest*. Seria possible doncs, replicar un espai lògic remotament de manera instantània on una altra instància del Virtualbox arranqués les màquines. Així no caldria portar a terme processos de restabliment de sistemes operatius, programari i importació de dades. És per aquest motiu que allí s'hi encabirà el servidor de base de dades, Server52, i en el nostre cas aprofitant per a fer encabir també el servidor de còpies, Server99.

IL·LUSTRACIÓ 13 - UBICACIÓ FÍSICA DELS HDD

Un altre aspecte a destacar en la configuració és l'establiment d'una interfície virtual dedicada per a fer les funcions de xarxa independent. Aquesta esdevé el canal de comunicació entre el Server10, on hi resideixen els programaris d'explotació dels honeypots i la honeynet. Assolint així un aïllament respecte a la xarxa de publicació del s*ite* DeepTicies. Actua doncs com a tallafocs recolzant la tasca dels diferents Iptables[9.8.3] existents a la infraestructura.



IL·LUSTRACIÓ 14 - INTEFÍCIE EXCLUSIVA DE COMUNICACIÓ HONEYNET

9.4. OpenVPN

Mitjançant aquesta tecnologia es bastiran les comunicacions protegides i assegurades per on transitaran les dades sensibles. La seva arquitectura es basa en la tunelització de les comunicacions entre un dispositiu que actua com a servidor i els clients que s'hi connecten.

9.4.1. Server

Cada servidor virtual que desenvolupi aquest rol ha de tenir instal·lats els paquets *openvpn* i *easy-rsa*. El primer esdevé el motor propi que gestiona i permet realitzar les connexions VPN. El segon, s'utilitzarà per tal de disposar d'una autoritat de certificació particular, ja que per raons econòmiques generarem certificats autosignats. Malgrat això cal indicar que un entorn real s'aconsella la utilització dels serveis que ofereixen entitats certificadores públiques o privades.

Malgrat la configuració en ambdós servidors és molt similar, quan hi hagi alguna diferencia aquesta vidrà marcada pel color de fons, sent `SRV51` i `SRV52`

i) Generació de la clau

Primerament cal personalitzar l'arxiu `/usr/share/easy-rsa/vars`[13.1] que conté les dades amb les quals es personalitzarà en nostre entorn:

Valor	Definició
`export KEY_SIZE=2048`	Mode paranoic, durant la negociació s'utilitzarà el xifrat asimètric TLS a 2048 bits per a la generació del parell de claus públic/privada. Un cop

`export KEY_COUNTRY="CT"`
`export KEY_PROVINCE="BA"`
`export KEY_CITY="Barcelona"`
`export KEY_ORG="UOC"`
`export KEY_EMAIL="kuse@uoc.edu"`
`export KEY_OU="Treball Final de Master"`
 	
`export KEY_ xx=xxxx`
 	
`X509 Subject Field`
`export KEY_NAME="tfmjcr"`
	Personalització de les dades públiques en el certificat.

ii) Construcció de la clau de certificació

Amb les variables definides es passa a la construcció de la clau privada per a la nostra autoritat de certificació, l'arxiu ca.key [13.2]

iii) Intercanvi de claus Diffie Hellman[13.3] `/etc/openvpn/dh2048.pem`

Procés que permetrà que dues entitats, que no es coneixen prèviament, s'intercanviïn les respectives claus mitjançant un servidor públic.

iv) Generació de certificat `/etc/openvpn/tfmjcr.tk.crt`, sol·licitud d'aquest certificat signat `/etc/openvpn/tfmjcr.tk.crs` i clau privada del servidor `/etc/openvpn/tfmjcr.tk.key`[13.4]

Es genera, amb el xifratge RSA de 2048 bits escollit, la clau privada del servidor, que serà reconeguda per la nostra particular entitat d'autorització.

v) Configuració del servidor configurant l'arxiu `/etc/openvpn/server.conf`[13.7]

Valor	Definició
`port 11194` `port 21194`	Canvi del port per defecte com a mesura d'ofuscar el servei.
`proto udp`	Assignació del protocol a utilitzar en les comunicacions.
`dev tun`	Indiquem que cal establir un túnel *ethernet* amb clau asimètrica.
`ca ca.crt`	Referència a la ubicació de 'arxiu que esdevé l'entitat certificadora pròpia que hem establert.
`cert tfmjcr.tk.crt` `cert Server52.crt`	Referència a la ubicació de l'arxiu de certificat de servidor.
`key tfmjcr.tk.key` `key Server52.key`	Referència a la ubicació que conté la clau privada de servidor.
`server 10.18.0.0 255.255.255.0` `server 10.28.0.0 255.255.255.0`	Adreçament, modificat sobre les opcions per defecte, que s'esmerçarà en establir-se el túnel.
`tls-auth ta.key 0`	Activació del paràmetre de seguretat extra que exigeix a les connexions disposar de l'arxiu ta.key[13.5]. Aquest és format per una clau estàtica per tal evitar atacs de denegació de serveis i inundació de port mitjançant UDP.

`plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so /etc/pam.d/openvpn`	Extensió que validarà només als usuaris amb compte local dins el servidor.

vi) Generació del certificat de client [13.6], on de manera anàloga al servidor obtenim tres arxius corresponents al propi certificat `vpnuser01.crt`, a la seva sol·licitud `vpnuser01.csr` i el corresponent a la clau privada d'usuari `vpnuser01.key`. Aquest arxius seran implantats en el dispositiu del client destí en la carpeta corresponent, depenent de la distribució de SO utilitzada
Cal indicar que en la generació de les credencials es pot afegir una doble autenticació mitjançant diferents mètodes com pot ser esmerçant un mòdul de *google authenticator*. Aquest genera un codi QR amb un codi d'autenticació associat que s'ha de validar per part del client. En el nostre cas, a tall d'exemple i esmerçant la possibilitat que ens brinda durant la generació del certificat, l'usuari vpnuser02 a part de validar-se amb les seves credencials, haurà d'introduir un nou mot de pas, el *certificate challenge password*.

```
Thu Nov 24 10:20:15 2016 us=867080 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [P
KCS11] [eurephia] [MH] [IPv6] built on Dec  1 2014
Enter Auth Username:Agent03
Enter Auth Password:
Enter Private Key Password:
```

Si bé aquesta doble autenticació augmenta la robustesa del sistema també penalitza l'experiència d'usuari pel que fa a la interacció amb el connector.

9.4.2. Client

Cada dispositiu des d'on es vulgui realitzar la connectivitat ha de disposar el programari client oficial destinat a tal fi. Així per a sistemes Windows i Ubuntu cal descarregar-se l'aplicació des de la pròpia web del producte, mentre que en el cas de iOS necessitarem adquirir-lo des d'App Store, anàlogament al que succeeix en Android que s'ha de fer mitjançant el Play Store.

La ruta on ubicar els arxius necessaris per a realitzar la connectivitat dependrà del sistema operatiu que executi i de la instal·lació del client OpenVPN que s'hagi realitzat. Tot i això, com a tall d'exemple indicarem els directoris de treball segons la distribució escollida. Així, s'hauran de copiar els fitxers generats en el servidor que corresponen a: ca.crt, ta.key, vpnuserxx.crt, vpnuserxx.key.,de manera predeterminada a la ruta:

- Windows: `C:\Program Files\OpenVPN\config`
- Ubuntu: `/etc/openvpn`
- iOS: `/etc/openvpn (presumiblement)`
- Android: `/etc/openvpn (presumiblement)`

Indicar que en els dos darrers casos, els referents a dispositius mòbils bàsicament, les pròpies aplicacions disposen d'un mòdul d'importació dels esmentats arxius. Una altra opció seria utilitzar les eines pròpies que proporciona el menú de configuració per tal d'afegir una VPN.

Per a poder establir la connexió cal esmerçar un arxiu on indicar la configuració a utilitzar. Aquest pot tenir qualsevol diferents noms segons les especificacions del sistema operatiu, el nostre cas ho homogeneïtzarem segons la nomenclatura que utilitza Windows. Així destaquem, dins l'arxiu de configuració client.ovpn[13.8], els camps més destacables per a la nostra implementació.

Valor	Definició
`dev tun`	Canvi del port per defecte com a mesura d'ofuscar el servei.
`proto udp`	Assignació del protocol a utilitzar en les comunicacions.
`remote tfmjcr.tk 11194`	Adreçament per nom de domini i port designat per establir el túnel.
`ca ca.crt`	Referència a la ubicació de l'arxiu que esdevé l'entitat certificadora pròpia que hem establert.
`cert tfmjcr.tk.crt`	Referència a la ubicació de l'arxiu de certificat de servidor.
`key tfmjcr.tk.key`	Referència a la ubicació que conté la clau privada del client.
`ns-cert-type server`	Indica que s'ha generat un certificat de servidor.
`tls-auth ta.key 1`	Exigeix la utilització, i possessió, d'un certificat addicional d'autenticació TLS en referència al servidor.
`auth-user-pass`	Indica que per l'autenticació per establir el túnel hi haurà d'haver una validació d'usuari local donat d'alta.

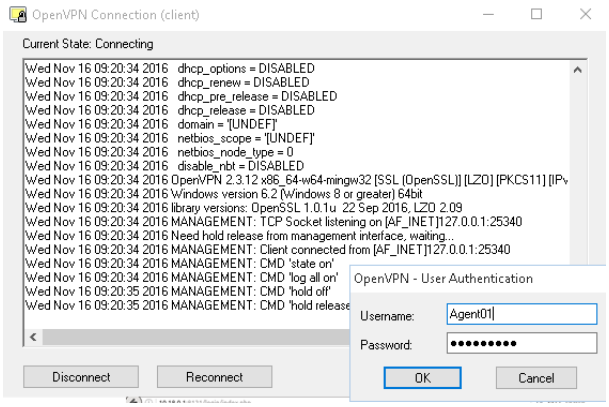
9.5. Moodle

Un cop establert el túnel segur, via OpenVPN, l'aplicació web Moodel, allotjada al Server51 s'encarregarà de presentar la interfície que permetrà la validació dels usuaris en l'entorn. Abans de res doncs, caldrà que l'usuari estableixi dit túnel:

- Opció intèrpret de comandes

```
root@Ubuntu1401Base:/etc/openvpn# openvpn --config client.ovpn
```

- Opció agent



IL·LUSTRACIÓ 15 - EXEMPLE DE CONNEXIÓ CLIENT A LA VPN

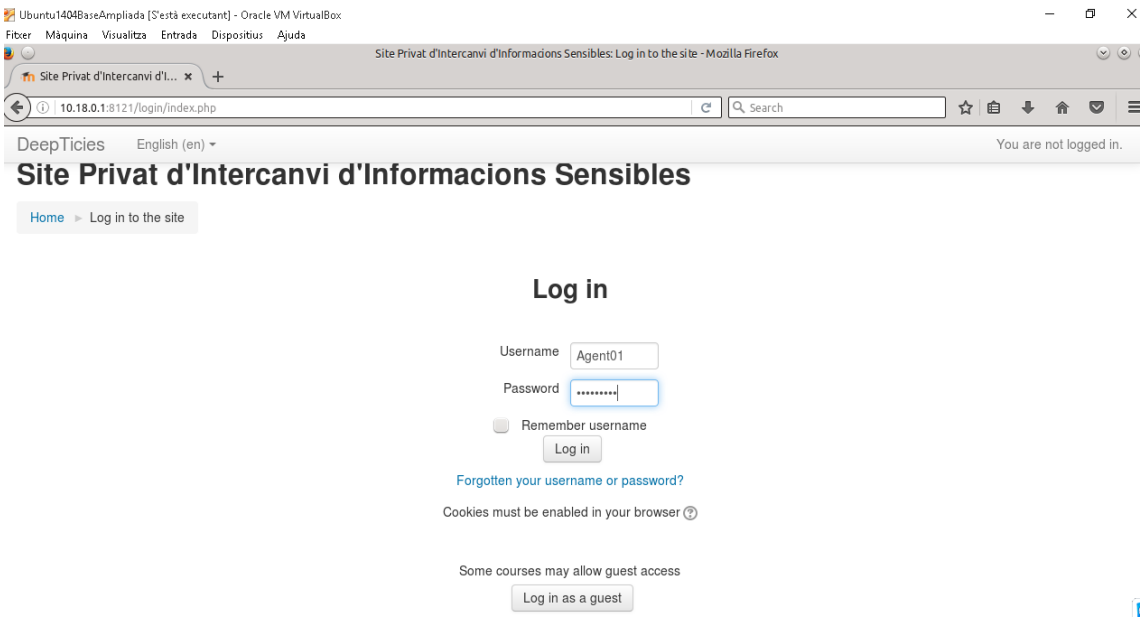
Sigui quina sigui l'opció escollida, s'inicia un protocol de connexió[13.10] fins l'acabament exitós de la seqüencia.

```
Wed Nov 16 09:10:56 2016 us=15079 /sbin/ip addr add dev tun0 local 10.18.0.6 peer 10.18.0.5
```

```
Wed Nov 16 09:10:56 2016 us=280494 /sbin/ip route add 10.18.0.1/32 via 10.18.0.5
```

```
Wed Nov 16 09:10:56 2016 us=782344 Initialization Sequence Completed
```

Que ens permet l'esmentada validació.

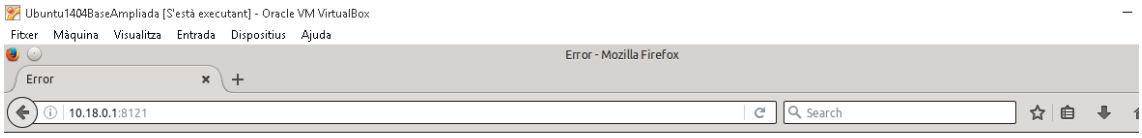


IL·LUSTRACIÓ 16 - PANTALLA DE LOGIN AL SITE DEEPTICIES PER A USUARIS

Així, depenent de les rols assignats a cada usuari, seran presentats els recursos als quals hagi de tenir accés. Aquesta presentació es basa en els anomenats menús contextuals que acoblen l'entorn a l'especificitat de cada usuari. En el nostre cas es basarà en l'assignació del que l'eina anomena aules, que per a nosaltres esdevindran les temàtiques específiques d'informació a protegir, i els xats que permetran la interacció multimèdia en viu d'un grup d'usuaris determinat. Tota aquesta informació tractada serà desada en el Server52, on caldrà establir un túnel diferent [13.11] per tal de poder tenir-hi accés.

```
root@Server51:/etc/openvpn# openvpn --config client.ovpn

Wed Nov 16 08:50:41 2016 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Dec 1 2014

Enter Auth Username:kuse

Enter Auth Password:
```

La prova més evident que la informació és fora del servidor és observar com quan no hi ha túnel establert, la interfície no té accés a la base de dades i ens llença el següent advertiment.



Error: Database connection failed

It is possible that the database is overloaded or otherwise not running properly.

The site administrator should also check that the database details have been correctly specified in config.php

IL·LUSTRACIÓ 17 - ERROR EN NO DISPOSAR DE LA BBDD

La connexió doncs es llençada des del Server51 cap el Server52 i l'arxiu de configuració del Moodle, pel que fa referència a la BBDD queda de la següent manera en els seus punts fonamentals.

Valor	Definició
`port = 33306`	Canvi del port per defecte com a mesura d'ofuscar el servei.
`bind-address = 10.28.0.1`	Tant sols s'atendran peticions des de la interfície creada pel túnel.

L'arxiu encarregat de desar aquesta informació és el `config.php`[13.13], on els principals camps configurats a destacar són:

Valor	Definició
`port = 33306`	Canvi del port per defecte com a mesura d'ofuscar el servei.
`$CFG->dbhost = '10.28.0.1';`	Tant sols s'atendran peticions des de la interfície creada pel túnel.
`$CFG->dbuser = 'modsql';`	Usuari específic destinat a la gestió de les dades de la BBDD.
`$CFG->dbpass = '******';`	Mot de pas, en clar. Perill doncs els usuaris estàndards del Server51 han de poder llegir l'arxiu [Mysql], i per tant aquest camp, per a poder fer qualsevol interacció amb el *site*.
`'dbport' => 33306,`	Port de la BBDD diferent a l'utilitzat per defecte a MySql
`$CFG->wwwroot = 'http://10.18.0.1:8121';`	Adreçament i port específic on es publica el *site*.

Paral·lelament s'ha creat l' usuari remot específic al Mysql del Server52, amb privilegis per accedir a la base de dades de Moodle.

Valor	Definició
`CREATE USER 'modsql'@'10.28.0.6.' IDENTIFIED BY '********';`	Creació de l'usuari referència del Server51 (IP túnel 10.28.0.6)
`GRANT ALL PRIVILEGES ON moodle TO modsql@'10.28.0.6' IDENTIFIED BY '*******';`	Otorgació de privilegis a l'usuari remot sobre la BBDD de Moodle.

Finalment indicar que s'ha realitzat la instal·lació amb el mètode segur `sudo /usr/bin/mysql_secure_installation`.

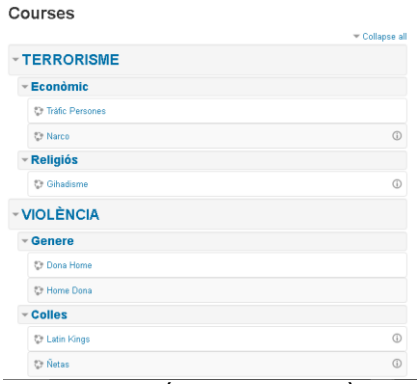
Amb tot això ja es pot accedir al *site*, validar-se i disposar de la infraestructura que Moodle posa al nostre abast. Cal assenyalar que com a norma els usuaris no disposen d'un rol específic, sinó que els rols s'assignen a cada context. Així, hi pot haver un usuari que actuï com administrador d'un tema, el que seria un professor d'un curs, i per tant tingui un seguit de privilegis que no li caldran en un altre temàtica, on només tingui, per exemple, la possibilitat de consultar la informació.

Passem a analitzar una mica en més detall les dues branques desenvolupades per tal de personalitzar el nostre entorn.

9.5.1. Temàtiques

Tal com hem comentat, utilitzarem el que Moodle tracta com a cursos des de la perspectiva temàtica. Així, es podran establir diferents temàtiques i derivades que esdevindran l'entorn de compartició d'aquelles informacions i materials sensibles. Passem a veure, de manera molt esquemàtica, com es gestiona aquest extens entorn, aportant en cada cas alguna mostra exemplificadora.

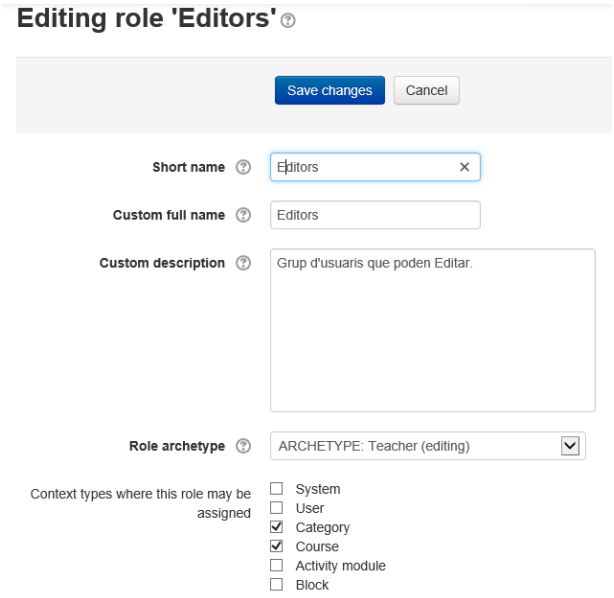
La visualització de l'espai de treball serà mitjançant categories i subcategories, que serviran per a construir un arbre amb les diferents temàtiques, cursos, a tractar. Així, en la imatge contigua podem observar com per exemple el curs Lating Kings pertany a la subcategoria Colles que a l'hora depèn de la categoria principal VIOLÈNCIA.



IL·LUSTRACIÓ 18 - EXEMPLE D'ORGANITZACIÓ SEGONS TEMÀTICA

És bo tenir en compte també en aquesta distribució la utilització d'etiquetes. Això facilitarà la cerca de contingut a mesura que es vagi augmentant la informació encabida en el *site*.

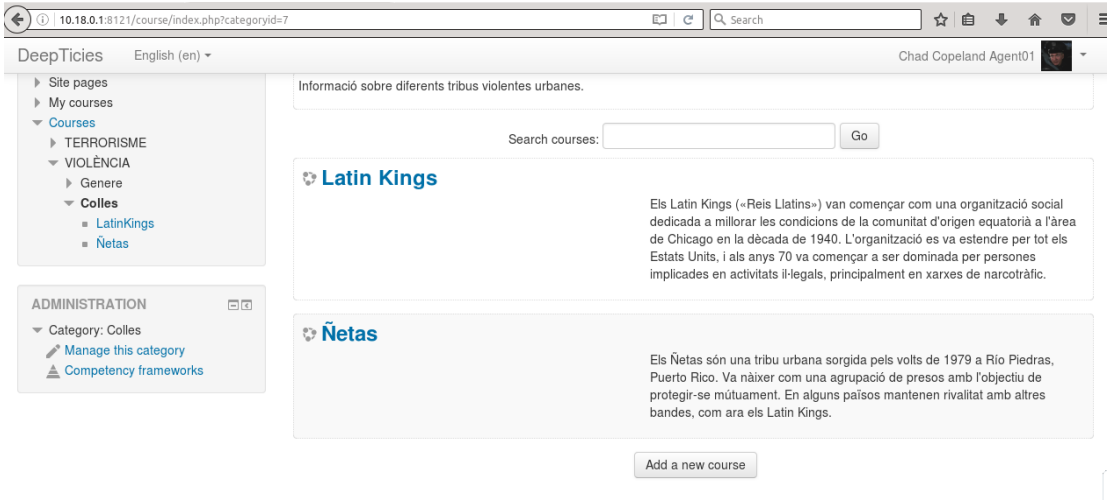
En referència als permisos s'utilitzarà nous rols descriptius amb determinats permisos heretats dels rols inicials que podrem modificar a plaer. Així es manté l'estructura inicial de rols com a base i es modifiquen els grups creats de nou. Aquests grups esdevenen un conjunt d'atributs que disposaran els usuaris que siguin inclosos dins seu. Per exemple, podem veure com s'ha creat un rol d'Editors, còpia del rol *Teacher*, i que es podrà utilitzar per a gestionar els permisos dels usuaris sobre les Categories i Subcategories.



IL·LUSTRACIÓ 19 - PESTANYA CREACIÓ DE NOUS ROLS D'USUARI

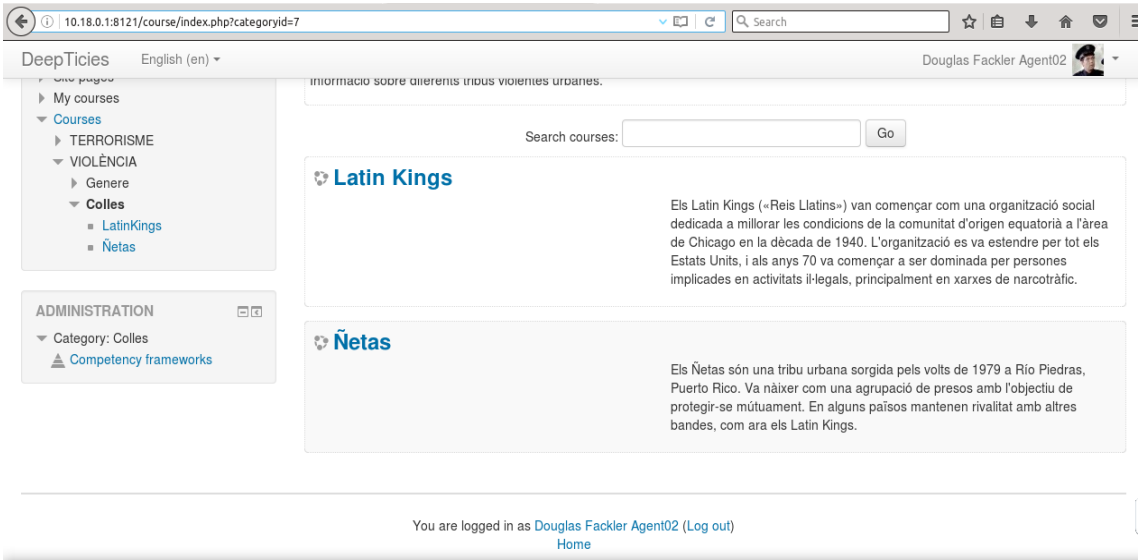
A tall d'exemple, podem observar com en entrar al *Site* els usuaris Agent01 i l'Agent02 tenen la possibilitat de crear, o no, cursos en una determinada subcategoria.

L'Agent01 està ubicat en el rol personalitzat: Creador i se l'ha assignat com membre dins la subcategoria Colles. Per aquets atributs doncs pot crear cursos nous dins l'esmentada subcategoria.



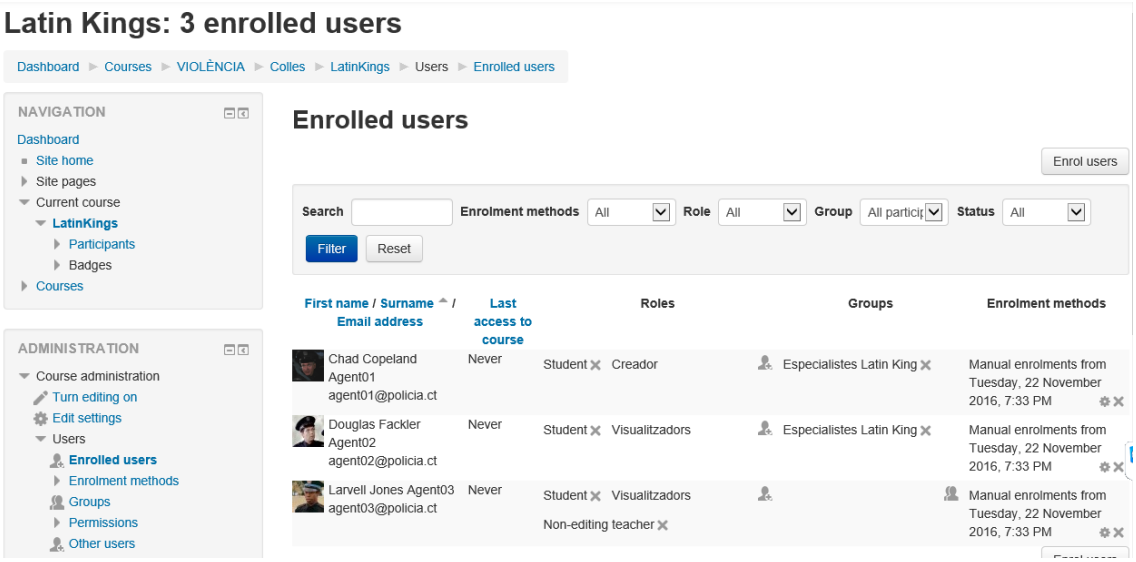
IL·LUSTRACIÓ 20 - USUARI AMB ROL CREADOR POT AFEGIR CURSOS

L'Agent02 forma part del rol personalitzat: Visualitzadors dins la categoria Violència, per tant no podria crear-hi cursos.



IL·LUSTRACIÓ 21 - USUARI AMB ROL VISUALITZADOR NO POT AFEGIR CURSOS

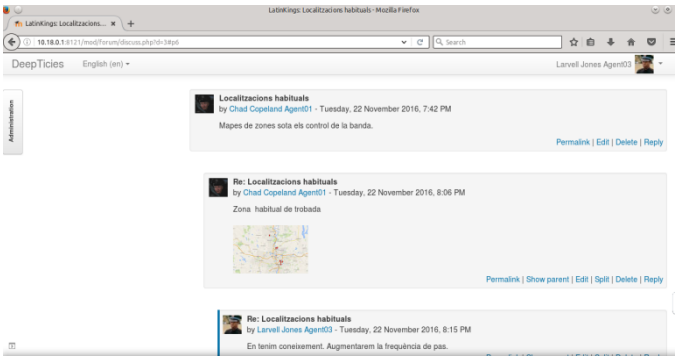
L'assignació d'usuaris participants en cada curs podem fer-la, a grans trets, mitjançant l'assignació individual o bé mitjançant grups preexistents.



IL·LUSTRACIÓ 22 - USUARIS AMB DIFERENTS PERMISOS PER INTERACTUAR EN UNA TEMÀTICA EN CONCRET

Com es pot observar, dins el curs Latin Kings hi consten matriculats el grup d'Especialstes Latin King i un tercer usuari, Agent03 que se li han afegit privilegis de professor sense dret d'edició.

Hi ha una gran quantitat de possibles tipologies d'aules a crear (fòrums, WiKi, blocs...) però totes basades en la compartició segura de la informació basada en privilegis granulars. També cal tenir en compte la possibilitat de temporalitzar el temps en què seran publicades certes notícies, i així gestionar-ne millor la temporalització sobre el seu accés.



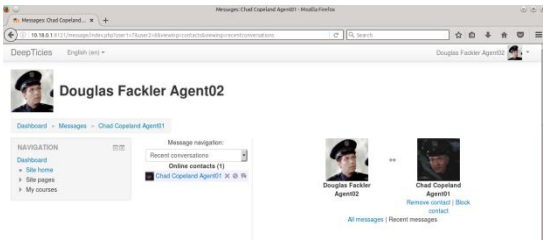
IL·LUSTRACIÓ 23 - EXEMPLE D'INTERCANVI D'INFORMACIÓ ENTRE USUARIS

9.5.2. Xats

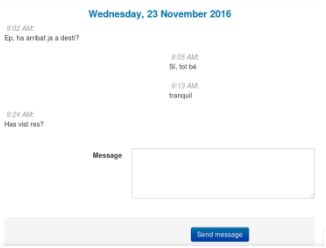
Malgrat la pròpia plataforma disposa d'un sistema de xat propi aquest no té capacitats multimèdia. Es poden doncs iniciar converses en viu, entre diferents tipus de dispositius. El més aconsellable en el cas de dispositius mòbils es descarregar-se l'aplicació gratuïta oficial de Moodle, tant per Android com per iOS. Això s'ha de fer de manera anàloga que en el cas

d'OpenVPN, és a dir cal anar al Play Store o Marketplace respectivament. Cal esmentar però que aquestes no disposen de totes les funcionalitats de la plataforma original, sobretot pel que fa als afegits. Donat això però sempre és possible accedir via web en la seva versió mòbil.

Un possible establiment de conversa seria com el següent:

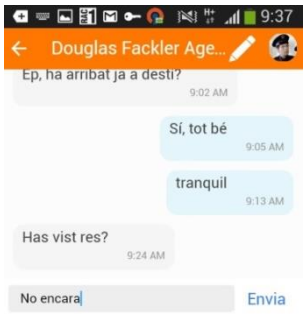


L'Agent02 es troba en un ordinador i envia un missatge de text, tipus SMS, a l'Agent01.



IL·LUSTRACIÓ 24 - MISSATGE ENVIAT PER INTERFÍCIE WEB

L'Agent01, el pot respondre, per exemple des del seu dispositiu mòbil.



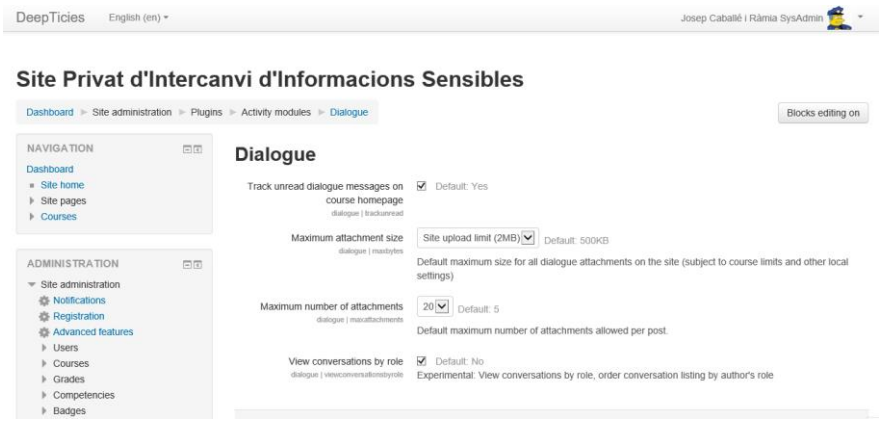
Com veiem però no disposem de cap eina que permeti, per exemple incloure una fotografia o vídeo que pugui ser interessant compartir en el moment. És per això que s'ha inclòs un afegit en la plataforma, el *plugin* anomenat Dialogue que permet incloure adjunts en una conversa entre dos usuaris.

IL·LUSTRACIÓ 25 - MISSATGE DE RESPOSTA MITJANÇANT EL MÒBIL

El procés d'instal·lació sembla senzill, només cal descarregar-se l'afegit corresponent, un arxiu comprimit en zip, des del web de l'autor i afegir-ho a la plataforma mitjançant l'eina d'*install plugins*. Tot i això, per qüestions de permisos d'usuari s'ha realitzat la instal·lació manual en el Server51, fent-ho com a *root*. Només cal descomprimir l'arxiu descarregat a l'espai destinat a als afegits

```
root@Server51:/var/www/html/moodle/mod# zip
mod_dialogue_moodle30_2015111600.zip
```

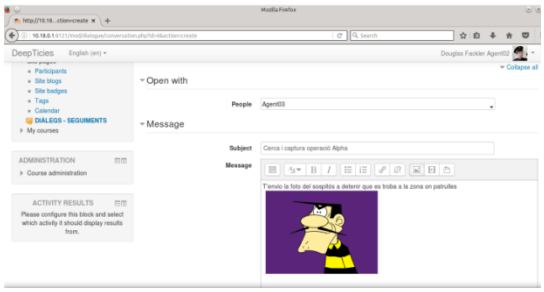
i actualitzar la interfície de administrativa de Moodle.



IL·LUSTRACIÓ 26 - INSTAL·LACIÓ DEL MÒDUL DIALOGUE

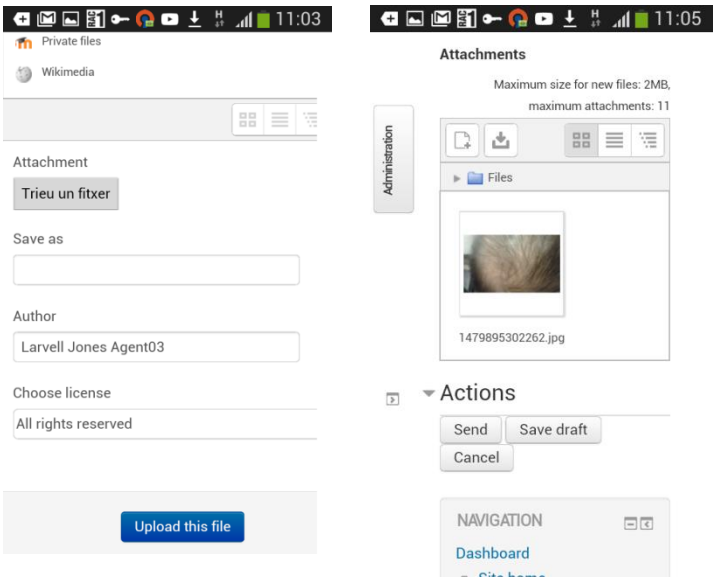
Amb aquest, és possible realitzar transferències d'arxius multimèdia, com per exemple fotografies fetes en l'acte. Com en el cas del xat, per tal d'il·lustrar-ho, passem a simular una situació

Tal com podem observar, l'Agent02 des d'un ordinador de sobretaula, envia una fotografia d'arxiu d'un sospitós a l'Agent03 mitjançat l'obertura d'un diàleg. Per tant s'estableix el que s'esdevé un xat MMS.



IL·LUSTRACIÓ 27 - ENVIAMENT DE CONTINGUT MULTIMÈDIA DES DE LA INTERFÍCIE WEB

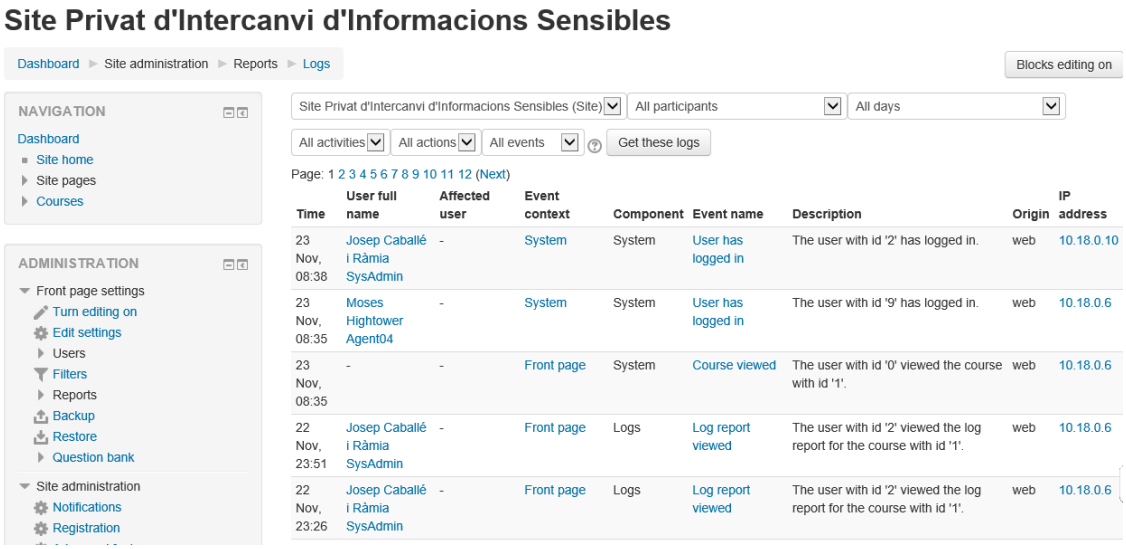
L'Agent03 respon afegint una fotografia, el clatell del sospitós, feta en aquells instant amb la càmera del seu dispositiu mòbil. Aquest procés però implica esmerçar dos salts, el d'escollir afegir un adjunt i el d'establir mitjançant quin dispositiu, en aquest cas la càmera fotogràfica.



IL·LUSTRACIÓ 28 - RESPOSTA EN VIU, AMB CONTINGUT MULTIMÈDIA, DES DEL DISPOSITIU MÒBIL

9.5.3. Gestió de Logs

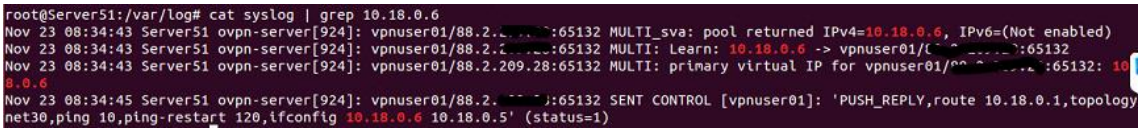
Tota la informació referent a les activitats, recollides en l'*event list,* portades a terme per qualsevol usuari són registrades. A partir d'aquestes és possible utilitzar filtres per tal de cercar una determinada acció feta en el sistema. Serà doncs en l'apartat de *logs* on es podran utilitzar filtres basats en: participants, dies, activitats, accions o esdeveniments.



IL·LUSTRACIÓ 29 - VISUALITZACIÓ DE LES ACTIVITATS DELS USUARIS

D'aquesta manera s'obtenen les dates, l'usuari causant, l'afectat, el tipus d'esdeveniment, la part del sistema afectada, el nom de l'esdeveniment, la descripció, el client d'origen i la IP del client.

És important remarcar, que l'adreça mostrada correspon a la IP interna del túnel client i que si volem saber la seva equivalència amb l'adreçament públic cal consultar l'arxiu `/var/log/syslog`. Així, per exemple ens trobem que filtrant l'esmentat arxiu per IP: `cat /var/log/syslog | grep 10.18.0.6` i coincidint amb l'hora de validació al sistema, obtenim el següent resultat:



IL·LUSTRACIÓ 30 - ARXIU ON ES REGISTRA L'ADREÇAMENT IP DEL COMUNICANT

És a dir que a les 08:34:43 s'ha validat des de la IP 88.2.xxx.xxx s'ha validat l'usuari corresponent al certificat vpnuser01, que s'atansa al registre de validació en la plataforma fet per l'Agent04 a les 08:35.

En el cas de voler traspassar aquestes dades a un altre gestor, tipus Splunk, per a treballar sobre els resultats és possible exportar-les. Disposem doncs, de quatre formats possibles: .csv, .xlsx, .html, .json i .ods.

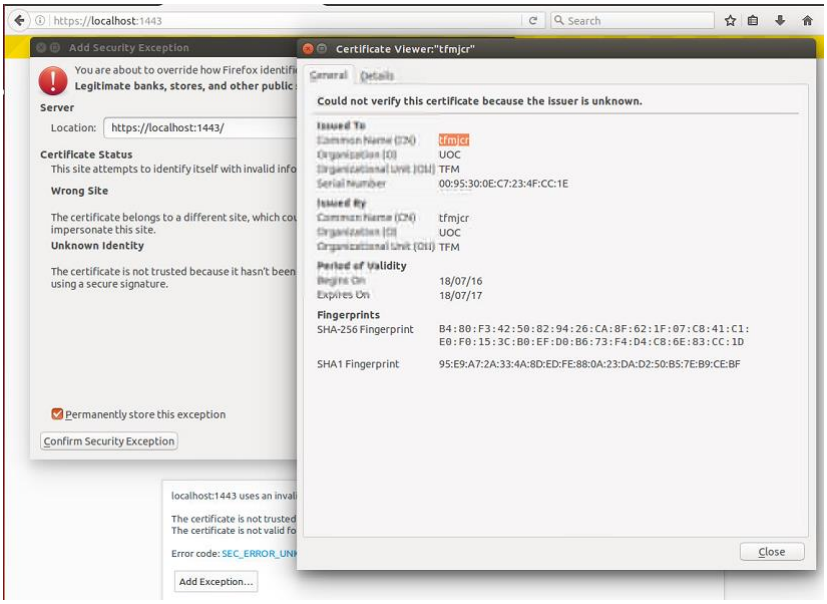
9.6. MODERN HONEY NETWORK

Aquesta distribució ens permet disposar d'un entorn centralitzat de recollida de registres, el *host*, dels *honeypots*, màquines que actuen com a sensors. Cadascun d'aquests espais, s'ha configurat de tal manera que permeti una transmissió segura de les dades recollides i una personalització que faciliti l'interès d'aquells possibles atacants conscients de l'objectiu, és a dir, que vulguin realitzar un atac discrecional. El valor de les dades recollides vindrà donat per una banda, del rastre que l'atacant pugui deixar i de l'altra banda, de les accions que pugui fer sobre l'emulació d'una part de l'entorn de producció. El fet d'esmerçar un clon de la plataforma actual, limitat i sense dades reals, per a ser atacada ens permetrà veure quins mecanismes són els utilitzats pels ciberdelinqüents. D'aquesta manera es podran aplicar les mesures correctives adients en l'entorn real d'explotació per tal de protegir-lo de manera més adient.

9.6.1. Host

La configuració del host, que es troba al servidor físic SRV10, s'ha modificat en referència a la instal·lació estàndard per tal de que les comunicacions siguin amb un port diferent a l'estàndard i que el protocol sia *https*. L'objectiu d'utilitzar aquesta configuració és doble ja que per un costat ens permet que els sensors enviïn les dades xifrades en paquets segurs, cosa podria ser d'utilitat si mai cap atacant pogués arribar a ensumar la xarxa *honeynet*, sense ser-ne conscient de la seva naturalesa. Per un altre costat, obre la possibilitat de poder consultar la informació des de fora el nostre entorn d'una manera segura. Seria possible doncs, configurant l'encaminador adequadament, fer consultes des d'Internet a aquest servei.

Com es pot veure en la figura adjacent, la barra d'eines i l'advertiment sobre el certificat de servidor donen fe d'aquesta metodologia. Malgrat aquesta implementació es rebrà un avis sobre la seguretat ja que, per motius econòmics, s'ha esmerçat un autocertificat.



IL·LUSTRACIÓ 31 - AUTOCERTIFICAT DEL SERVIDOR MHN

Per tal d'assolir-ho, s'han personalitzat les següents entrades dels arxius[13.16] de configuració:

- `/etc/nginx/sites-available/mhn-https`

Valor	Definició
`listen 1443 ssl spdy;`	Establiment del port d'escolta 1443, mitjançant SSL basat en el protocol de transport propi de Google spdy.
`server_name tfmjcr.tk;`	Nom amb que ens referim al servidor MHN.
`ssl_certificate /etc/ssl/private/tfmjcr.tk.crt;`	Ruta d'ubicació del certificat autosignat del servidor.
`ssl_certificate_key /etc/ssl/private/tfmjcr.tk.key;`	Ruta d'ubicació del certificat privat del servidor.

- `/etc/nginx/sites-available/honeymap-https`

Valor	Definició
`listen 1443 ssl spdy;`	Establiment del port d'escolta 1443, mitjançant SSL basat en el protocol de transport propi de Google spdy.
`server_name tfmjcr.tk;`	Nom amb que ens referim al servidor MHN.
`ssl_certificate /etc/ssl/private/tfmjcr.tk.crt;`	Ruta d'ubicació del certificat autosignat del servidor.
`ssl_certificate_key /etc/ssl/private/tfmjcr.tk.key;`	Ruta d'ubicació del certificat privat del servidor.
`proxy_pass http://localhost:13000`	Port on presentar gràficament les dades sobre un mapamundi.

- `/opt/mhn/server/config.py`

Valor	Definició
`SECRET_KEY = 'Ih9VCrSVMRjicOxnQ40ZP9XxBPmANAWK'`	Clau identificativa única del servidor que s'utilitza en cas d'esmerçar funció resum amb salt.
`SUPERUSER_EMAIL = 'kuse@uoc.edu'`	Usuari de validació a l'
`SUPERUSER_PASSWORD = '*****'`	Mot de pas en clar!!!! Cal tenir en compte però que en el sistema només hi ha un usuari habilitat per accedir-hi. Per tant, no cal tenir cura amb els permisos d'aquest arxiu. Si mai s'assolissin

	aquestes credencials per part d'un ciberdelincuent el sistema en la seva totalitat ja estaria compromès.
`SERVER_BASE_URL = 'https://tfmjcr.tk'`	Adreçament del servidor.
`HONEYMAP_URL = 'https://tfmjcr.tk:13000'`	Adreçament del servei de visualització sobre mapa mundial.
`DEPLOY_KEY = 'HnpdhcuM'`	Clau que utilitzaran els sensors per a comunicar-se amb el host.

Comprovem que la configuració sigui correcte mirant que tots els dimonis siguin aixecats.

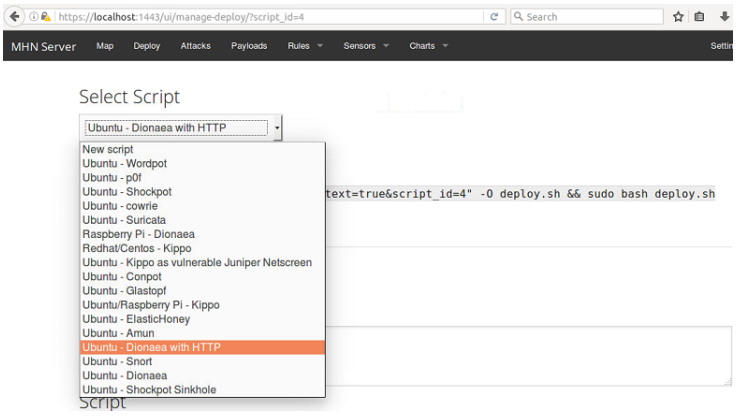
```
root@SRV10:/var/log/mhn# sudo supervisorctl status
geoloc                           RUNNING    pid 12197, uptime 0:05:10
honeymap                         RUNNING    pid 12224, uptime 0:05:08
hpfeeds-broker                   RUNNING    pid 12183, uptime 0:05:11
hpfeeds-logger-splunk            RUNNING    pid 12178, uptime 0:05:12
mhn-celery-beat                  RUNNING    pid 12177, uptime 0:05:12
mhn-celery-worker                RUNNING    pid 12206, uptime 0:05:09
mhn-collector                    RUNNING    pid 12220, uptime 0:05:08
mhn-uwsgi                        RUNNING    pid 12201, uptime 0:05:09
mnemosyne                        RUNNING    pid 12188, uptime 0:05:10
root@SRV10:/var/log/mhn#
```

IL·LUSTRACIÓ 32 - SUPERVISIÓ DEL CORRECTE FUNCIONAMENT DELS DIMONIS MHN

A nivell de configuració del Host només resta finalment establir la connexió amb el dimoni Splunk[9.7], resident al propi servidor, que ens servirà per a realitzar l'explotació de les dades recollides. Per a fer-ho només cal llançar la utilitat `/opt/mhn/scripts/install_hpfeeds-logger-splunk.sh` que permetrà configurar el reenviador.

Valor	Definició
`+ SPLUNK_HOST= 127.0.0.1` `+ SPLUNK_PORT=38000`	Definició de l'adreçament i port on l'Splunk recol·lectarà la informació rebuda pels sensors de l'MHN.

Un cop validats a la interfície, en el nostre cas el que ens interessa és el desplegament del sensor Dianoaea, ja que disposa, entre d'altres, d'un servei que emula la publicació d'un website i un servei Mysql. D'aquesta manera es podrà posar a l'abast dels possibles atacants els serveis que simularan



IL·LUSTRACIÓ 33 - SELECCIÓ D'SCRIPT A IMPLEMENTAR EN SENSOR MHN

l'entorn real.

Un cop obtingut l'*script*, s'ha de llançar en els servidors que faran la funció de honeypot: Server13 i Server14.

9.6.2. Sensors

Abans de res cal assegurar-se que en els mateixos hi ha ubicat el certificat públic[13.16] `tfmjcr.tk.crt` del SRV10 a la ruta `/usr/local/share/ca-certificates`.

També cal tenir en compte que s'ha d'incloure una entrada en l'arxiu hosts on faci referència al domini `tfmjcr.tk` ja que al ser gratuït expira i necessitem que el sistema resolgui la petició del nom sense la intervenció de serveis DNS externs.

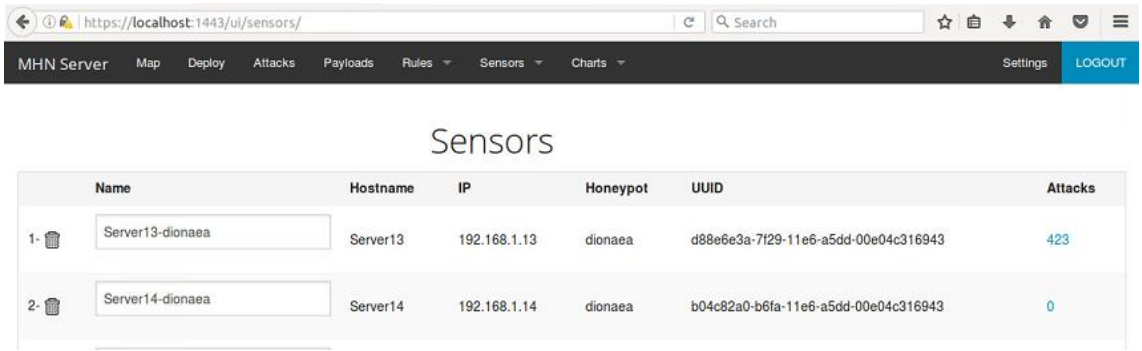
```
kuse@Server14:/etc$ cat hosts
127.0.0.1       localhost
192.168.1.14    Server14
192.168.1.1     tfmjcr.tk
192.168.1.1     tfmjcr
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
kuse@Server14:/etc$
```

IL·LUSTRACIÓ 34 - INCLUSIÓ DE L'ADREÇAMENT A TFMJCR EN SENSOR MHN

Un cop configurat el *host* tenim al nostre abast l'script que ens permetrà instal·lar en cada *honeypot* aquells serveis que desitgem.

```
wget "https://tfmjcr.tk/api/script/?text=true&script_id=4" -O deploy.sh && sudo bash deploy.sh https://tfmjcr.tk HnpdhcuM
```

Amb aquesta comanda s'ha descarregat en el honeypot l'script corresponent, en aquest cas el que es refereix als serveis oferts per Dionaea, i s'ha desplegat mitjançant la tasca `desploy.sh`. En darrera instància es comprova la seva recol·lecció visualitzant-ne el resum de l'activitat en el *host*.



IL·LUSTRACIÓ 35 - LLISTAT DE SENSORS IMPLEMENTATS

Malgrat disposar de tots els serveis que ofereix Dionaea, només es posaran a l'abast dels atacants els referents als ports 80, 443 per a l'emulació web i el 3306 per al Mysql.

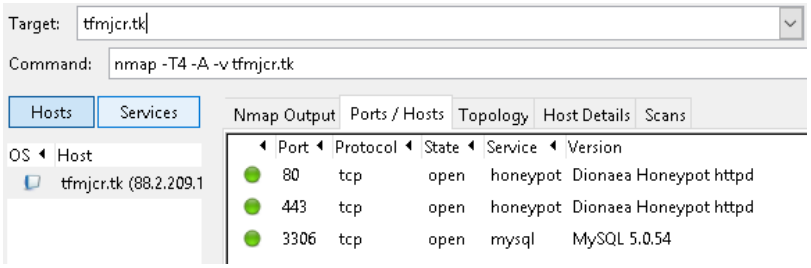
```
kuse@Server14:/etc$ sudo netstat -pntl | grep dionaea
tcp6       0      0 :::443                  :::*                    LISTEN      937/dionaea
tcp6       0      0 :::445                  :::*                    LISTEN      937/dionaea
tcp6       0      0 :::5060                 :::*                    LISTEN      937/dionaea
tcp6       0      0 :::5061                 :::*                    LISTEN      937/dionaea
tcp6       0      0 :::135                  :::*                    LISTEN      937/dionaea
tcp6       0      0 :::3306                 :::*                    LISTEN      937/dionaea
tcp6       0      0 :::42                   :::*                    LISTEN      937/dionaea
tcp6       0      0 :::80                   :::*                    LISTEN      937/dionaea
tcp6       0      0 :::21                   :::*                    LISTEN      937/dionaea
tcp6       0      0 :::1433                 :::*                    LISTEN      937/dionaea
kuse@Server14:/etc$
```

IL·LUSTRACIÓ 36 - PORTS OBERTS PER DIONAEA

Així el tallafocs del Server02[9.8.3] que actua com encaminador i el router físic[9.2] només deixaran pas a aquestes peticions.

IL·LUSTRACIÓ 37 - ESCANEIG EXTERN SOBRE L'OBERTURA DE PORTS

S'ha de tenir en compte que si un atacant fa servir una eina d'escaneig tipus nmap, aquesta podrà detectar l'esquer de forma molt evident. Això és així doncs, utilitza uns patrons[xxiii] que segons la resposta del nostre servidor delatarà el sentit del mateix. Així en una senzilla cerca pot quedar al descobert l'esquer. Caldrà doncs personalitzar l'entorn per a impossibilitar en la mesura del possible la detecció. Per a fer-ho és necessari cercar dins els esmentats patrons que utilitza l'nmap, https://svn.nmap.org/nmap/nmap-service-probes, les referències als serveis que oferim del producte Dionaea



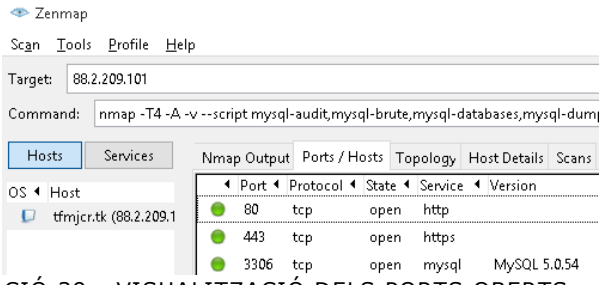
IL·LUSTRACIÓ 38 - INFORMACIÓ DELS SERVEIS OBERTS DES DE L'EXTERIOR

```
match http m|^HTTP/1\.0 200 OK\r\nContent-type: text/html; charset=utf-8\r\nContent-Length: 204\r\n\r\n<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 3\.2
Final//EN\"><html>\n<title>Directory listing for /</title>\n<body>\n<h2>Directory listing for /</h2>\n<hr>\n<ul>\n<li><a
href=\"\.\./\">\.\./</a>\n</ul>\n<hr>\n</body>\n</html>\n$| p/Dionaea honeypot httpd/

match honeypot m|^HTTP/1\.0 200 OK\r\nAllow: OPTIONS, GET, HEAD, POST\r\nContent-Length: 0\r\nConnection: close\r\n\r\n| p/Dionaea Honeypot httpd/
```

Un cop localitzats caldrà modificar el seu enviament mitjançant l'edició, en el nostre cas, de l'arxiu `/usr/lib/dionaea/python/dionaea/http.py`.

Valor	Definició
""" r.append('<!DOCTYPE html PUBLIC >')""" r.append("<html>\n<title>Llistat de l'arbre </title>\n" % displaypath) r.append("<body>\n Llistat de l'arbre \n" % displaypath) r.append("<hr>\n \n")	Eliminació i modificació dels valors que fan *match* en una cerca nmap.
"""self.send_header("Allow", "OPTIONS, GET, HEAD, POST")"""	Eliminació de la cadena que permet a nmap identificar el servei com a Dionaea.

Així doncs, en una cerca avançada ja no apareix cap informació referent a l'esquer present.



IL·LUSTRACIÓ 39 - VISUALITZACIÓ DELS PORTS OBERTS UN COP MODIFICATS ELS VALORS PER DEFECTE

En cada *honeypot* però, caldrà fer modificacions específiques per a personalitzar de millor manera l'entorn.

Finalment caldrà assegurar-nos que el sensor apunta correctament al Host amb les credencials correctes de cada servidor.

```
hpfeeds = {
        hp1 = {
                server = "192.168.1.1"
                port = "10000"
                ident = "907e4918-b94d-11e6-a5dd-00e04c316943"
                secret = "xFLw4DP6GpWFMw10"
                // dynip_resolve: enable to lookup the sensor ip through a webservice
                dynip_resolve = "http://queryip.net/ip/"
        }
```

IL·LUSTRACIÓ 40 - CONFIGURACIÓ DE LES CREDENCIALS PER A QUE EL SENSOR MHN ES COMUNIQUI AMB EL HOST

- Server13

Aquest *honeypot* farà d'esquer del servei web i s'hi han fet les modificacions pertinents per tal d'emular el front-end d'entrada al sistema legítim. Així, per defecte, ens trobem amb que existeix una única entrada, index.html, a la ruta `/var/dionaea/wwwroot/`. En el nostre cas, serà substituïda per un codi font modificat sobre el de producció.

```
kuse@Server13:/var/dionaea/wwwroot$ ls
calendar                                                  index.html?time=1477954800
course                                                    index.html?time=1480546800
help.php?component=moodle&identifier=cookiesenabled&lang=ca  index.html?time=1483225200
help.php?component=moodle&identifier=cookiesenabled&lang=en  index.html?time=1485903600
index.html                                                index.html?time=1488322800
index.html.save                                           index.html?time=1490997600
index.html?lang=ca                                        lib
index.html?lang=en                                        login
index.html?time=1464732000                                mod
index.html?time=1467324000                                robots.txt
index.html?time=1470002400                                theme
index.html?time=1472680800                                user
index.html?time=1475272800
kuse@Server13:/var/dionaea/wwwroot$
```

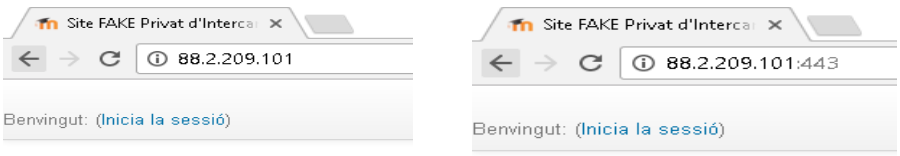
IL·LUSTRACIÓ 41 - DIRECTORI ON RESIDEIX EL "FAKE WEB"

A més, haurem afegit algun arxiu per tal d'atraure l'atenció de l'atacant.

- robots.txt: arxiu que s'esmerça bàsicament per a que els cercadors puguin indexar informació i amagar-ne d'altre. En el nostre cas, per tal de donar un toc de veracitat, amaguem tot el contingut per defecte als cercadors `Disallow:/` . A més, de manera explícita marquem un arxiu, que ja es troba ocult `.motdepas.txt`, com a no indexable.
- `.motdepas.txt`: arxiu ocult i que no serà mostrat en cerques estàndards dels cercadors, on apareixeran credencials d'usuari.

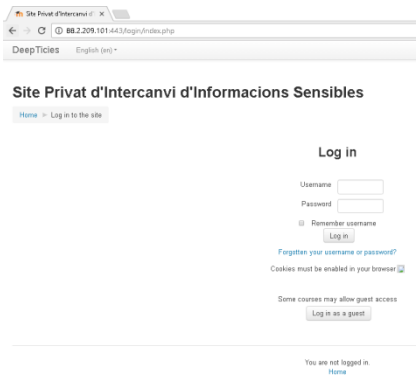
D'altra banda cal indicar que no s'ha fet cap inclusió d'etiquetes <*tags*> per a, tal com esmetavem en l'apartat de dominis, no ser indexats pels cercadors.

Així, el tafaner es trobarà amb una pantalla de benvinguda sòbria, tant pel port 80 com el 443



IL·LUSTRACIÓ 42 - PÀGINA INICIAL DEL "FAKE WEB" DEEPTICIES

que li permetrà derivar al portal d'entrada del *fake site*:



IL·LUSTRACIÓ 43 - PORTAL D'ENTRADA "FAKE"

- Server14

La funció d'aquesta màquina és emular la disponibilitat d'un servei Mysql, tal com succeeix en l'espai de producció. Si bé s'hauria pogut aprofitar aquesta capacitat en el servidor de publicació "fake", això podria despertar sospites. D'aquesta manera també podem veure com es poden anar afegint servidors i serveis en la estructura de la *honeynet*.

Finalment indicar com en l'apartat del test de penetració[10] es podrà observar quines conseqüències tenen totes aquestes modificacions.

9.7. Splunk

Tal com és el cas de les comunicacions en el Modern Honey Network[9.6], s'ha activat el canal segur per a establir l'enviament i recepció d'informació. Aquesta informació però no serà recollida de cada sensor de manera independent, sinó que s'aprofitaran les capacitat del *MHN host* com a repositori dels registres per esmerçar-lo com a font de subministrament.

Així es especificitats en el nostre sistema ens porten a realitzar les següents modificacions respecte a una instal·lació estàndard:

i) Canviar el port de gestió segur a: `http://localhost/en-US/manager/mhn-splunk/server/settings/settings?action=edit`

Valor	Definició
`Management port: 8090`	Port en que es comunica el servei web amb el procés *splunkd*.
`Run Splunk Web: Yes`	Permet la utilització de la interfície web.
`Enable SSL (HTTPS) in Splunk Web: Yes`	Aquí s'activen les comunicacions sobre el canal segur.
`Web port: 38000`	Establiment del port de comunicacions segur.

ii) Habilitem el receptor de dades per a rebre les comunicacions `https://localhost:38000/en-US/manager/system/data/inputs/tcp/cooked`

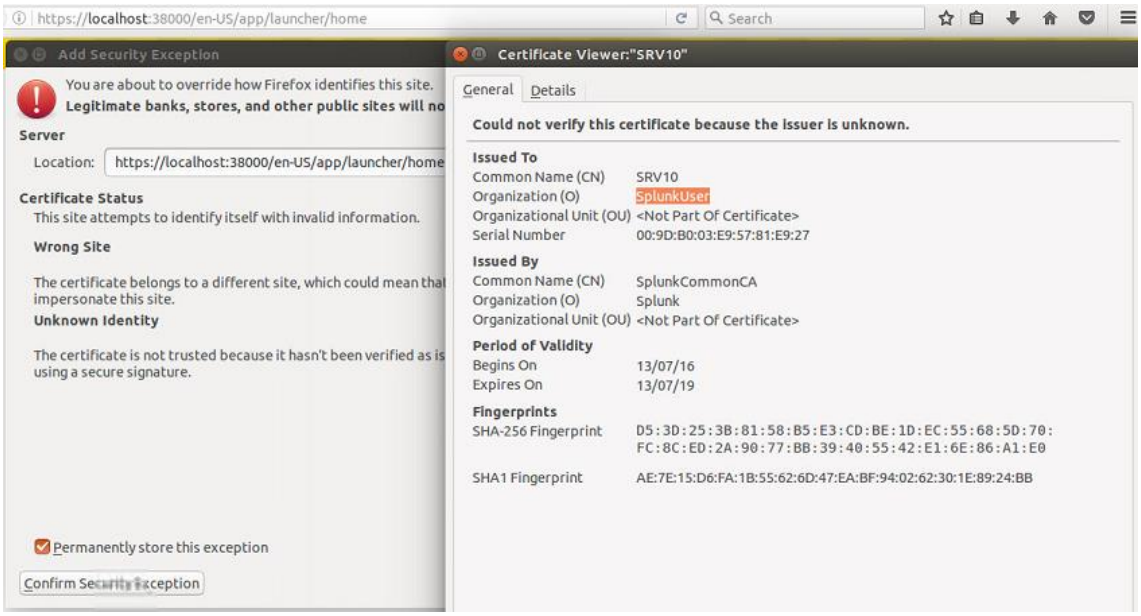
Valor	Definició
`Listen on this port: 9997`	Port que resta a l'espera de rebre les dades dels registres recollits, en el nostre cas de part del MHN.

iii) Preparar l'entorn per a operar en *https* generant un certificat autosignat (malgrat seria preferible adquirir-ne un de compra) a `/etc/ssl/certs`

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:4096 -keyout /etc/apache2/ssl/certs/tfmjcr.tk.key -out /etc/ssl/certs/tfmjcr.tk.crt
```

iv) Copiar el `/tfmjcr.tk.crt` de la ubicació `/usr/local/share/ca-certificates` a `/etc/ssl/certs`, ja que la pròpia màquina fa de client de l'Splunk.

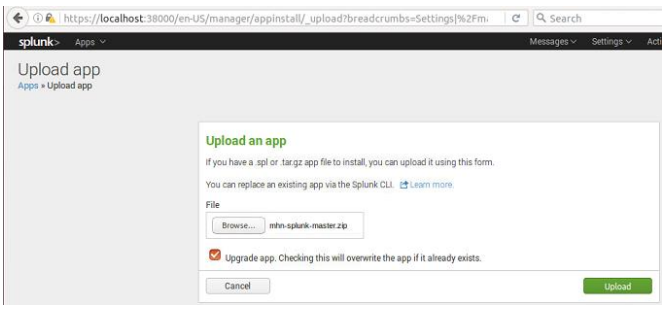
Així ja es pot treballar en la interfície en un canal segur:



IL·LUSTRACIÓ 44 - IMPLEMENTACIÓ HTTPS A SPLUNK

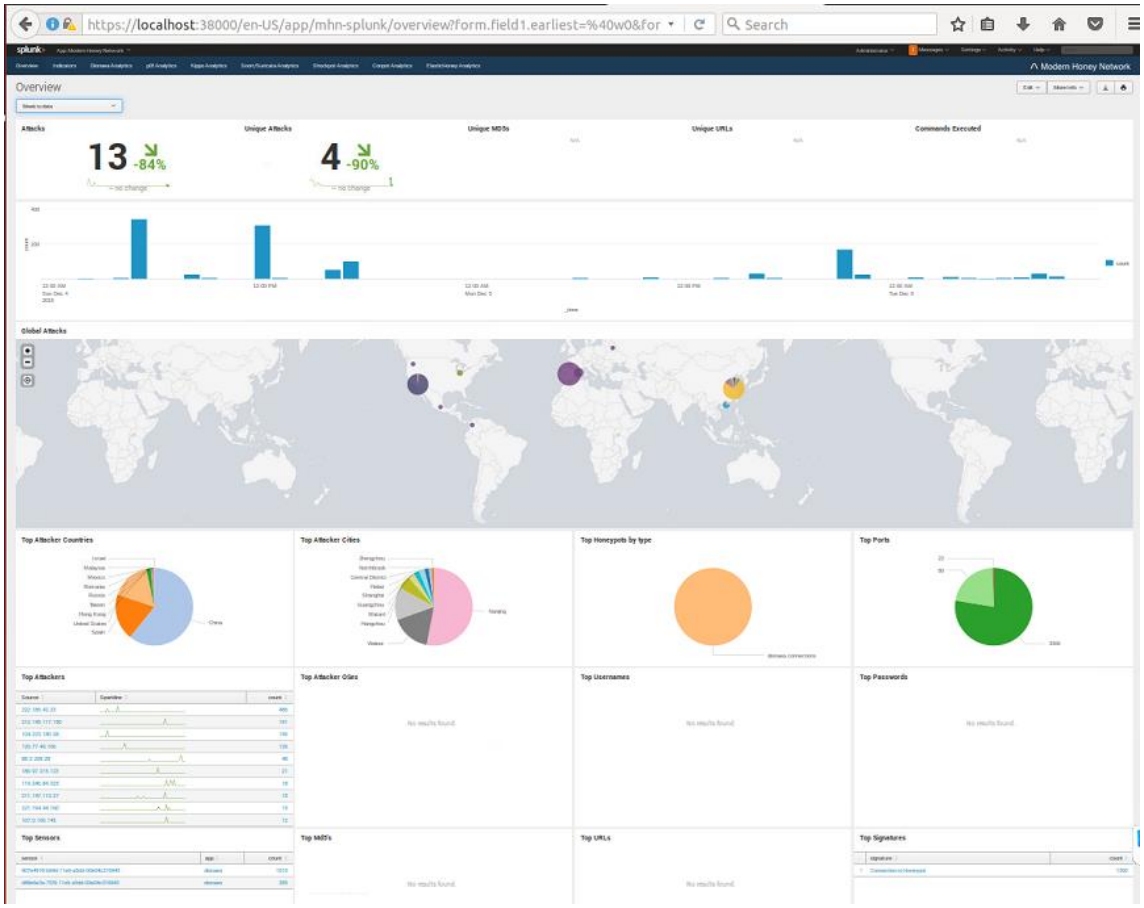
tant pel que fa en la interfície web com en les comunicacions entre MHN[9.6.1] i SPLUNK.

Amb l'eina en marxa ja es pot treballar amb un entorn predefinit per a l'explotació de dades de l'MHN. Només cal fer una importació de l'app per a obtenir un entorn que es pot modificar segons les necessitats de cada moment.



IL·LUSTRACIÓ 45 - IMPORTACIÓ A L'SPLUNK DE L'APP DE L'MHN

D'aquesta manera es disposa d'un entorn amigable on visualitzar les dades que posteriorment seran analitzades.

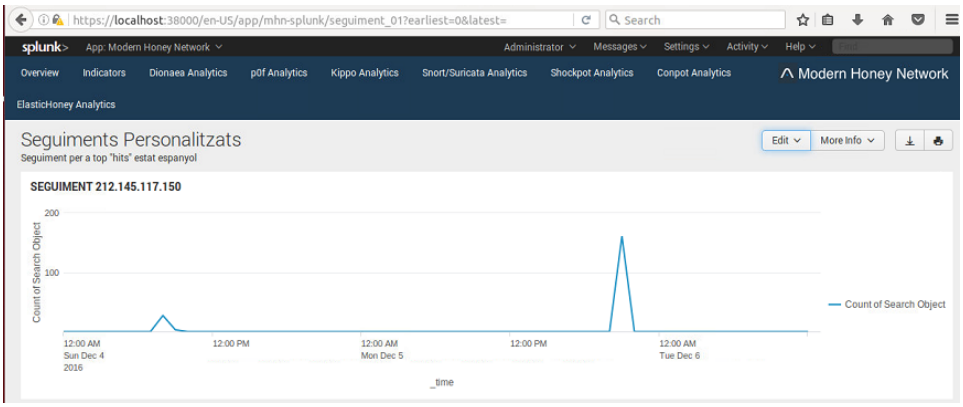


IL·LUSTRACIÓ 46- VISIÓ GENERAL DE L'APP MHN APLICADA AL NOSTRE ENTORN

També es poden generar filtres propis i crear un entorn personalitzat que permeti treballar únicament amb aquells paràmetres que es considerin per a l'anàlisi. En aquest cas hem creat un espai on visualitzar els períodes temporals on les activitats d'un determinat atacant es duen a terme:

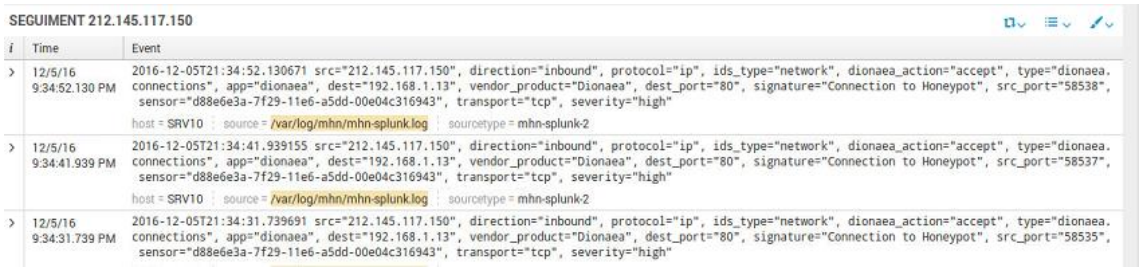
```
(index=* OR index=_*) (source="*mhn-splunk.log*" src="212.145.117.150" date_hour="*") | rename date_hour AS EventObject.date_hour | search
```

Que a mode d'exemple es pot visualitzar així:



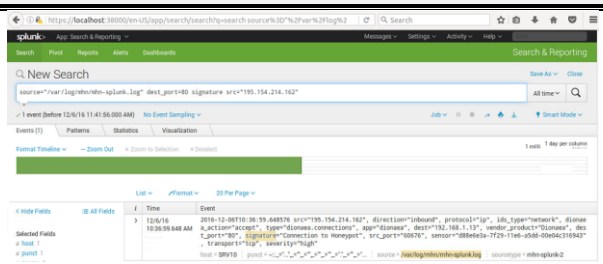
IL·LUSTRACIÓ 47 - SPLUNK, GRÀFICA PERSONALITZADA D'EXEMPLE

Amb concordança de les dades importades.



IL·LUSTRACIÓ 48 - SPLUNK, DADES RECOL·LECTADES

Això només és un exemple de com es poden explotar les dades, vaga la pena dir que el nivell de detall sempre podrà augmentar proporcionalment a les dades adquirides des dels *honeypot*. Tot i això, centrant-nos exclusivament en el cas que ocupa aquesta memòria, ja es pot veure el tractament tancat i minso que fa la interfície de l'MHN de les dades recol·lectades versus el detall de l'Splunk.

MHN	Splunk
	

9.8. Sistemes Operatius

Tota l'estructura es basa en l'instal·lació de programari en diverses màquines, una de física i la resta de virtuals, on s'han desplegat els serveis necessaris. Per tal de garantir la seguretat integral no hi ha prou amb els propis recursos del diferent programari, sinó que s'ha de tenir en compte les configuracions i permisos dels components que són integrats en aquests SO. Per aquesta raó passem a descriure, en cada màquina, quines especificitats té segons la implementació que hem realitzat

9.8.1. Arxius de configuració generalista

A cada servidor s'han modificat certes parts dels seus arxius de configuració amb l'objectiu d'assolir una quota més alta de fortificació pel que fa a la seguretat.

- Server51

Pel que fa al *site* de Moodle aquest es publicada mitjançant el servei d'apache2. Seguint la línia d'ofuscació i de cenyir-se només a l'obertura de serveis imprescindibles, en aquest cas, s'ha modificat el port estàndard d'entrada i les interfícies que en donen accés.

Així s'ha hagut de modificar per una banda l'arxiu `/etc/apache2/sites-enabled/000-default.conf` [13.14]

Valor	Definició
`VirtualHost 10.18.0.1:8121`	Indica que la pàgina serà publicada únicament per la interfície on es munta el túnel sobre un port diferent a l'estàndard.

I per l'altra l'arxiu `/etc/apache2/ports.conf` [13.14]

Valor	Definició
`Listen 10.18.0.1:8121`	Obre el port personalitzat sobre la interfície de xarxa que composa el túnel.

Pel que fa als arxius de registre cal destacar-ne el `/var/log/syslog` aquest conté, entre altres, la informació de les connexions externes que enllacen el certificat que esmerça l'usuari amb el seu adreçament IP. A més de proporcionar-nos altres informacions al respecte com són les hores de connexió. Aquesta informació ens permetrà, tal com esmentàvem anteriorment [9.5.3], associar IP externa amb usuari de Moodle, a part de controlar les connexions realitza el nostre servidor.

9.8.2. Permisos arxius compromesos d'usuari

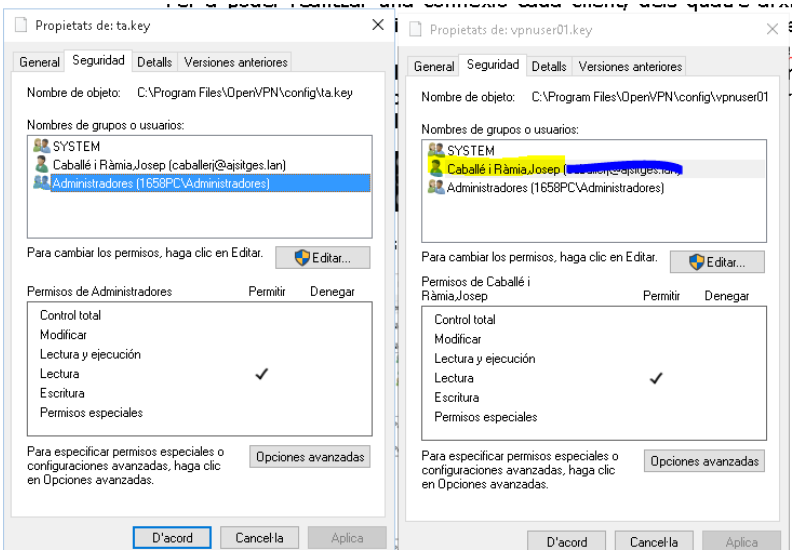
- OpenVPN

Per a poder realitzar una connexió cada client, dels quatre arxius[9.4.2] que ha de disposar el client n'hi ha dos que s'han de garantir que només siguin accessibles a qui estableix el túnel, el ta.key i el vpnuserxx.key. Aquests esdevenen la clau privada i veiem con en el cas d'una màquina Linux només és accessible al root en mode lectura la clau del servidor i a l'usuari la de la sessió del client.

```
kuse@Ubuntu1401Base:/etc/openvpn$ ls -la ta.key vpnuser01.key
-r-------- 1 root root  636 nov 16 09:08 ta.key
-r-------- 1 kuse kuse 1704 jul 29 10:54 vpnuser01.key
```

IL·LUSTRACIÓ 49 - VISUALITZACIÓ DELS PERMISOS SOBRE LA CLAU PRIVADA A UBUNTU

i en una Windows a l'usuari en particular



IL·LUSTRACIÓ 50 - VISUALITZACIÓ DE PERMISOS SOBRE LA CALU PRIVADA A WINDOWS

- Mysql

Per tal de fer la connexió amb el *site*, cada usuari ha de poder llegir l'arxiu `/var/www/html/moodle/config.php`. Això és perillós doncs sense caldre cap elevació de privilegis, qualsevol validació amb un usuari pertanyent a l'equip, serà capaç de llegir l'usuari i mot de pas per accedir a la BBDD de Moodle.

```
kuse@Server51:/var/www/html/moodle$ ls -la config.php
-r--r--r-- 1 root root 717 Aug 14 21:38 config.php
kuse@Server51:/var/www/html/moodle$
```

IL·LUSTRACIÓ 51 - VISUALITZACIÓ DE PERMISOS SOBRE L'ARXIU DE CONFIGURACIÓ DEL MYSQL

Tots els usuaris de l'equip tenen dret de lectura.

Cal doncs assegurar-nos, tancant tots els serveis innecessaris i mitjançant els tallafocs, de no deixar cap oportunitat per a poder fer *login* en aquest equip. Recordem que és l'únic equip de la xarxa a qui, amb les credencials correctes, permetem obrir la BBDD.

9.8.3. Configuració iptables

Aquesta utilitat, pròpia del nucli del sistema operatiu, ens permet establir un sistema de tallafocs a nivell de paquet de xarxa. De fet, esdevé el garant bàsic de que només transitin aquells paquets imprescindibles per assolir la comunicació, i els objectius marcats, entre els dispositius del nostre entorn. D'aquesta manera, encara que per diferents motius, els servidors pugin oferir serveis no controlats, aquests limitaran el seu servei a tal com estigui configurat el *firewall*. Això, ens dotarà d'una seguretat extraordinària a part

del correcte planejament de la xarxa i de l'oferta del programari mínim i imprescindible en cada servidor.

Per tal de veure quines polítiques són actives en el tallafocs de cada Server esmerçarem la comanda `iptables -L -n -v` on els modificadors ens indiquen:

- -L: llista totes les regles actives.
- -n: mostra adreçament i port IP de manera numèrica.
- -v: dóna informació complerta de cada sortida per pantalla.

Un cop obtinguda la sortida detallarem els aspectes més destacables de cada configuració. No es farà esment a la línia que faci referència a: `eth0 tcp 0.0.0.0/0 NEW tcp dpt:17xx` ja que es tracta d'una situació provisional per permetre la gestió via *ssh* del servidor. En llançar l'entorn de producció aquesta serà eliminada per tal d'evitar possibles febleses en el sistema i que per tant pugi ser atacable.

Sobre la configuració[13.9] del tallafoc de cada màquina, passem a destacar-ne aquells aspectes més importants de cara a la nostra instal·lació.

- Server02

Donada la funció de *proxy* que realitzarà aquest servidor cal activar en primer lloc aquesta característica.

```
sudo echo "1" > /proc/sys/net/ipv4/ip_forward
```

Un cop fet ja es pot passar a la configuració de l'iptables.

```
root@Server02:/home/kuse# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  eth1   *       0.0.0.0/0            0.0.0.0/0
   36  2520 ACCEPT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:1702
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 4 packets, 552 bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   252 ACCEPT     all  --  eth1   *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 19 packets, 1736 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  *      eth1    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:1702
root@Server02:/home/kuse#
```

IL·LUSTRACIÓ 52 - ESTAT DEL TALLAFOCS A L'ENRUTADOR

Valor	Definició

`:INPUT DROP`
`:FORWARD ACCEPT`
`:OUTPUT ACCEPT`
	Les polítiques per defecte són: Rebuig en els paquets d'entrada. Reenviament i sortida. Acceptació .

Excepcions INPUT ACCEPT	
• `PREROUTING -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.1.13:80`	Permesa l'entrada de tràfic contra serveis als ports 80, 443, 3306 i redirigits als

• `-A PREROUTING -p tcp -m tcp --dport 443 -j DNAT --to-destination 192.168.1.13:443` • `-A PREROUTING -p tcp -m tcp --dport 3306 -j DNAT --to-destination 192.168.1.14:3306`	*honeypot* corresponents.
`POSTROUTING -o eth0 -j MASQUERADE`	S'esmerça com adreçament de sortida el de la pròpia interfície eth0
• `INPUT -i lo -j ACCEPT` • `OUTPUT -o lo -j ACCEPT`	Permès el trànsit en bucle local que necessiten les aplicacions per a les seves comunicacions internes
• `INPUT -i eth1 -j ACCEPT` • `FORWARD -i eth1 -j ACCEPT` • `OUTPUT -o eth1 -j ACCEPT`	Regla d'excepció que no més s'aplicaria en cas d'afegir una nova NIC provisionalment.
`INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT`	No es talla cap comunicació, de cap tipus, ja iniciada prèviament
`INPUT -p tcp -m tcp --dport 1702 -j ACCEPT` `OUTPUT -p udp -m udp --sport 1702 -j ACCEPT`	Regla provisional que permet connectar-se al servidor via SSH per gestionar-lo més còmodament que amb la consola del VirtualBox
`INPUT -j LOG`	Desament de les comunicacions d'entrada en el registre del sistema.

- Server51

```
root@Server51:/etc# iptables -L -n -v
Chain INPUT (policy DROP 8346 packets, 531K bytes)
 pkts bytes target     prot opt in     out     source               destination
   24  1956 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
 201K   28M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    4   280 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:11194
    7   412 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:1751
   42  2544 ACCEPT     all  --  tun0   *       0.0.0.0/0            0.0.0.0/0
    0     0 LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:11194 LOG flags 0 level 4 prefix " AC
CES A VPN NO PERMES "

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  tun0   *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  tun0   eth0    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  eth0   tun0    0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 2161 packets, 91845 bytes)
 pkts bytes target     prot opt in     out     source               destination
 209K   18M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain WHITELIST (0 references)
 pkts bytes target     prot opt in     out     source               destination
```

IL·LUSTRACIÓ 53 - ESTAT DEL TALLAFOCS AL SERVIDOR DE PUBLICACIÓ

Valor	Definició

`:INPUT DROP`
`:FORWARD DROP`
`:OUTPUT ACCEPT`
	Les polítiques per defecte són: Rebuig en els paquets d'entrada i reenviament.

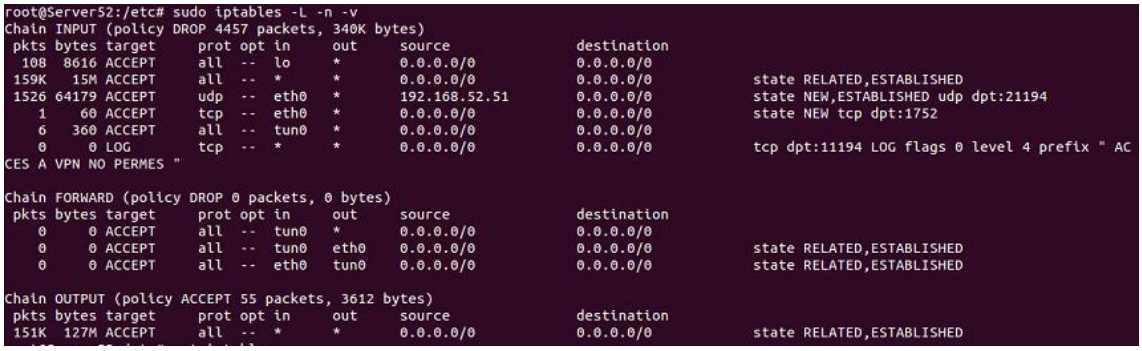
	Acceptació en el tràfic de sortida.
Excepcions INPUT ACCEPT	
`INPUT -i lo -j ACCEPT`	Permès el trànsit en bucle local que necessiten les aplicacions per a les seves comunicacions internes.
`INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT`	No es talla cap comunicació, de cap tipus, ja iniciada prèviament.
`INPUT -p udp -m udp --dport 11194 -j ACCEPT`	Permès el trànsit pel protocol UDP a la interfície pertanyent al túnel per un únic port en l'establiment d'una nova connexió.
`INPUT -i tun0 -j ACCEPT`	S'accepta tot el trànsit per la interfície establerta del túnel.
`INPUT -p tcp -m tcp --dport 11194 -j LOG --log-prefix " ACCES A VPN NO PERMES "`	En cas de detectar un possible intent d'establir un túnel no contemplat, es registre amb un missatge personalitzat.
`FORWARD -i tun0 -j ACCEPT`	S'accepten els paquets reenviats mitjançant la interfície del túnel cap a qualsevol interfície.
`FORWARD -i tun0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT`	S'accepta el reenviament de paquets entre la interfície del túnel i l'ethernet.
`FORWARD -i eth0 -o tun0 -m state --state RELATED,ESTABLISHED -j ACCEPT`	S'accepta el reenviament de paquets entre la interfície de l'ethernet i el túnel.

Cal apuntar que, malgrat no estar activa, hi ha una sentència preparada per tal d'esmerçar una llista blanca (`/usr/local/passi.txt`) on indicar a quins dispositius únicament es permetrà l'entrada des d'internet.

```
### Llistat d'IP a qui permetem la connexió a les DeepTicies
### PASSI=/usr/local/passi.txt
### PASSIMAC=/usr/local/passimac.txt


### Permetem les comunicacions noves a OPENVPN (només en llista blanca)
### for x in `grep -v ^# $PASSI | awk '{print $1}'`; do
### iptables -A INPUT -s $x -p udp --dport 11194  -j ACCEPT
### done
```

IL·LUSTRACIÓ 54 - ARXIU PREPARAT PER LLISTA BLANCA SOBRE EL TALLAFOCS

- Server52



IL·LUSTRACIÓ 55 - ESTAT DEL TALLAFOCS AL SERVIDOR DE BBDD

La configuració del tallafoc és idèntica al Server51 exceptuant la següent entrada:

Valor	Definició
Excepcions INPUT ACCEPT	
`INPUT -p udp -m udp --dport 21194 -j ACCEPT`	Permès el trànsit pel protocol udp a la interfície pertanyent al túnel per un únic port en l'establiment d'una nova connexió.

Cal remarcar que en el cas del servidor de còpies, Server99, no cal afegir cap regla de filtratge per a controlar l'accés. Això és així doncs esmercem una mascara de xarxa de 30 bits, el que significa que només aquestes dues màquines poden formar part de la xarxa.

```
Address:    10.0.0.1
Netmask:    255.255.255.252 = 30
Wildcard:   0.0.0.3
=>
Network:    10.0.0.0/30
HostMin:    10.0.0.1
HostMax:    10.0.0.2
Broadcast:  10.0.0.3
Hosts/Net:  2
```

IL·LUSTRACIÓ 56 - CÀLCUL D'ADREÇAMENT /30

9.8.4. Estat dels ports

És de vital importància deixar únicament els ports oberts imprescindibles per a donar els serveis oferts, i si és possible canviar-ne la seva ubicació per defecte. D'aquesta manera, davant un possible escaneig extern, es disminueix la superfície d'atac i s'emmascara, per ofuscació, la possibilitat de deixar a la en clar serveis coneguts.

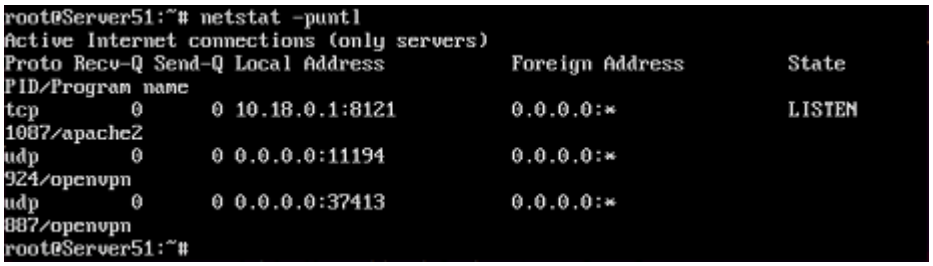
Passem a realitzar un descobriment d'aquests port oberts mitjançant la comanda: `netstat -puntl`. Aquí els paràmetres de l'eina netstat, que ens permet conèixer les connexions actives establertes, són els següents:

- p: indica el protocol a inspeccionar.

- u: per a referir-se a les connexions UDP. Recordem que és el protocol escollit per establir el túnel.
- n: ofereix en nombre de port
- t: per a referir-se a les connexions TCP. Protocol habitual on els serveis descansen els seus processos de comunicació.
- l: permet conèixer quines interfícies intervenen en les comunicacions.

Així en cada servidor trobem els següents ports oberts.

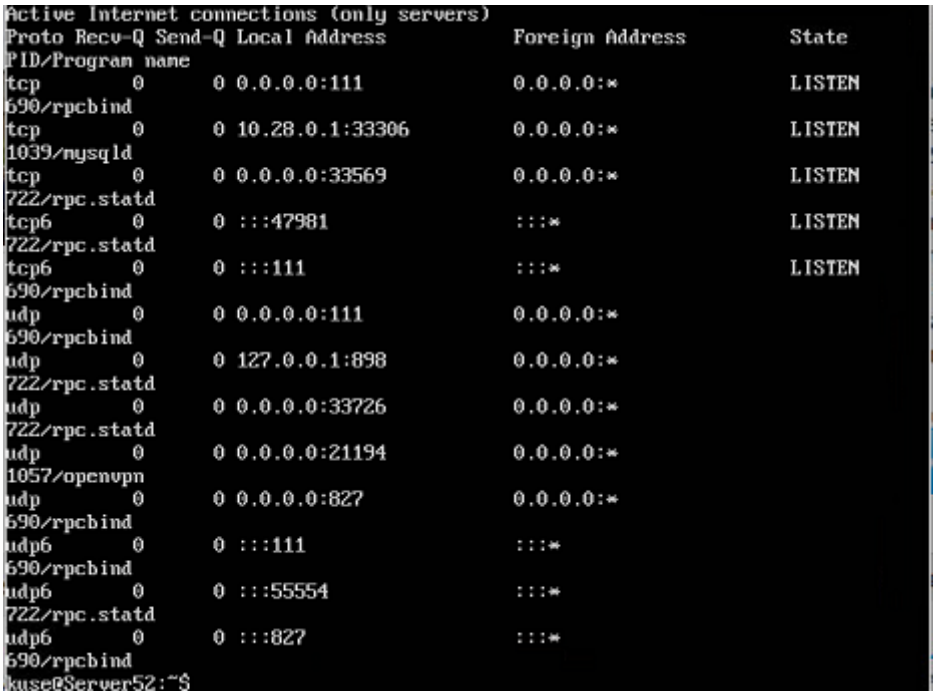
- Server51



IL·LUSTRACIÓ 57 - PORTS OBERTS AL SERVIDOR DE PUBLICACIÓ

  - 8121: motor de publicació del servei web, *site* Moodle, només per la interfície segura del túnel.
  - 11194: servei OpenVPN a l'espera de rebre peticions per a establir túnel.
  - 37413?: ports aleatoris on clients diferents estableixen el canal de comunicació xifrat.

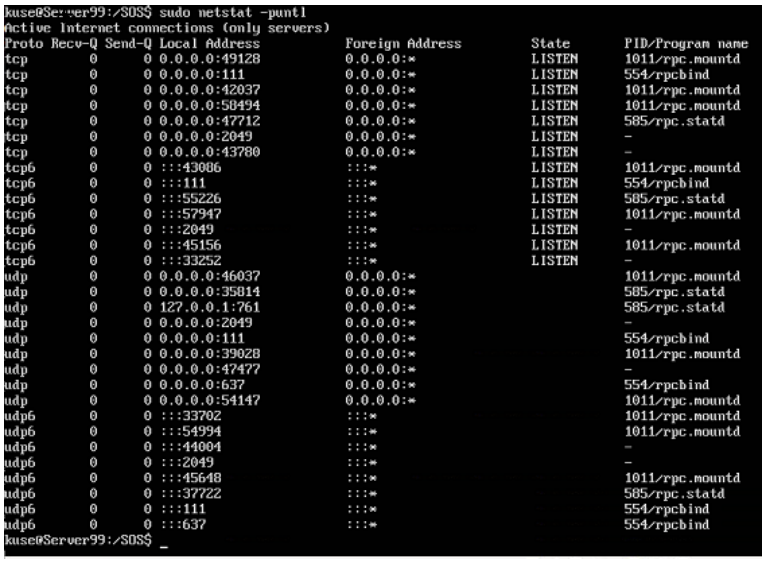
- Server52



IL·LUSTRACIÓ 58 - PORTS OBERTS AL SERVIDOR DE BBDD

- 333306: port obert amb exclusivitat a la interfície 10.28.0.1 que s'estableix en construir el túnel per a que només les màquines que en pertanyin puguin tenir-hi accés. Aquí és on resideix la BBDD del *site* i per tant l'espai a protegir més en el sistema. Cal garantir, amb l'ajuda del tallafocs i aïllant-la d'Internet que només la màquina de publicació hi té accés.
- 111 i resta: port del servei rpcbind, del qual depenen la resta que s'observen oberts, i que és destinat al descobriment de serveis NFS a la xarxa. El motiu de la seva existència és per a poder realitzar la còpia de seguretat de la BBDD de Moodle en el servidor de Backup remot Server99.

- Server99



IL·LUSTRACIÓ 59 - PORTS OBERTS AL SERVIDOR DE CÒPIA DE SEGURETAT

- *: tots els ports oberts corresponen al servei NFS que permet compartir el recurs SOS amb el Server52 i que és el destinatari de l'exportació de la BBDD del *site*.

9.8.5. Còpia de Seguretat

La còpia de seguretat es programa com una tasca llançada pel Server52, i és basada en la exportació complerta de la base de dades del Moodle. Aquest servidor té accés al un recurs compartit NFS del Server99, mitjançant una interfície dedicada, amb adreçament 10.0.0.x/30. Allí és on s'hi bolca l'exportació de la BBDD. La utilitat esmerçada és el mysqldump que és invocat seqüencialment per la utilitat pròpia crontab[13.15]. Així, disposem de la següent comanda:

```
30 4 * * * /usr/bin/mysqldump --defaults-extra-file=/etc/mysqldump.cnf
moodle > /mnt/SOS/moodle_`date +\%Y\%m\%d_\%H\%M`.sql
```

on

Valor	Definició
`30 4 * * *`	Indica la programació temporal: Cada dia (*) de cada mes (*) a les 04 (4) 30 (30) minuts
`/usr/bin/mysqldump`	Comanda a utilitzar
`--defaults-extra-file=/etc/mysqldump.cnf`	Arxiu on són les credencials de l'usuari que pot realitzar l'exportació. Perill!!!! Malgrat tractar-se d'un equip aïllat d'Internet, aquest arxiu disposa de la informació en clar.
`moodle`	Nom de la BBDD a exportar.
`/mnt/SOS/moodle_`date +\%Y\%m\%d_\%H\%M`.sql`	Ubicació del directori compartit i arxiu on s'abocarà la còpia.

10. TEST DE PENETRACIÓ

Un cop muntada tota l'estructura, en revisarem la seguretat des d'un punt de vista d'un atacant extern. L'objectiu es veure com respon el sistema davant la fase d'adquisició d'informació i cerca de vulnerabilitats, no tant en l'explotació i esborrat d'empremtes, ja que el sistema no s'ha dissenyat per tal comesa.

Així, es començaran a realitzar les tasques habituals que un ciberdelinqüent endegaria en cas de voler atacar l'espai de treball que ens ocupa. Tot i això, serà un atac en caixa grisa, és a dir, ens servirem dels nostres coneixements com a creadors de l'entorn per tal de subratllar aquells aspectes interessants referents a la confecció d'aquesta memòria. No sempre es tindran en compte certes mesures de prevenció que un atacant hauria de seguir, com per exemple la utilització de *proxys* anònims o la *torificació* de les eines d'atac. L'objectiu, és localitzar ràpidament en els registres generats pel nostre sistema d'ham, les activitats il·lícites detectades. Els atacants disposen de moltes eines, i coneixements, però el factor humà existeix i pot ocasionar qualsevol descuit. Aquests, a més d'un cert pensament lateral que permeti enllaçar esdeveniments, podria donar-nos la clau per a trobar evidències per a desemmascarar, o protegir-nos, d'un atac.

Passem doncs a realitzar un atac amb les eines més habituals, i gratuïtes, de que es disposen. Totes elles contemplen un munt de possibilitats que són fora de l'abast d'aquest document. En el nostre cas ens servirem únicament d'aquelles especificitats que ajudin a acomplir l'objectiu. Abans de res però visitarem el web DeepTicies, que adjectivarem com a *fake* per assegurar-nos d'on ens trobem, per confirmar que es troba en funcionament[Il·lustració 42 i Il·lustració 43].

- Fase 1: *footprinting*, recol·lecció d'informació genèrica

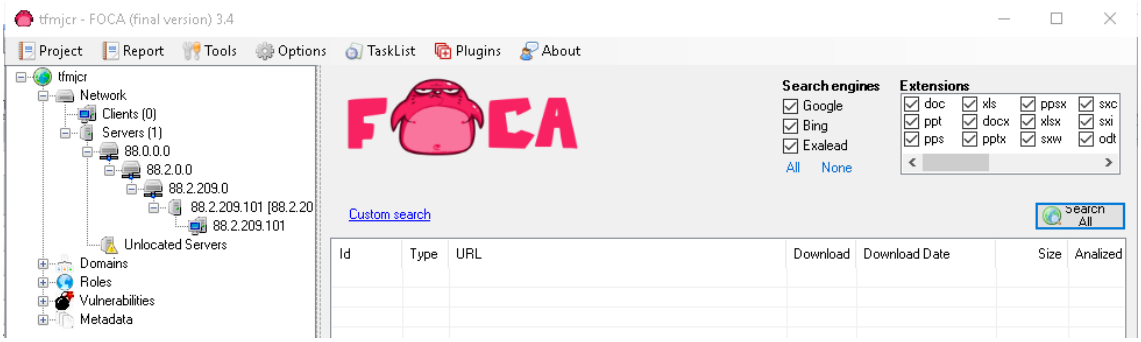
Abans de res, caldrà cercar aquelles dades que són a l'abast de qualsevol persona, ja que es troben publicada en cercadors[Il·lustració 7], fòrums o espais d'intercanvi d'informació. Cal indicar que al no sortir cap referència del domini cercat es poden donar dues situacions. Una que el domini no existeixi, cosa que tampoc vol dir que no hi hagi un servei a atacar, o bé que no s'ha indexat informació, ni deixat els *tag* corresponents, per a que els cercadors puguin incorporar-ne dades. Baixant una mica més el nivell, caldria fer una cerca DNS, per a saber quina IP és associada a domini i així seguir amb la recerca. Aquesta informació[Il·lustració 7 - Resolució dns de google sobre tfmjcr.tk] obtinguda, ens mostra que el domini és lliure. Per tant, en cas de no defallir, caldria que l'atacant trobés la IP a atacar.

  - Enginyeria social

Esmerçant tècniques d'engany, via comunicacions per correu electrònic, telefòniques o de qualsevol tipus, l'atacant miraria d'esbrinar el contingut de l'arxiu host[Il·lustració 5 - Exemples configuració arxiu hostIl·lustració 5 - Exemples configuració arxiu hostIl·lustració 5 - Exemples configuració arxiu hostIl·lustració 5 - Exemples configuració arxiu host d'algun client. Un exemple podria ser, en cas de no tenir ben pautat el servi d'atenció a l'usuari, fer-se passar pel CAU i obtenir aquestes dades. En el supòsit que s'assolís aquesta informació, ja es disposaria d'una IP de referència per a prosseguir l'atac i seguir amb l'adquisició d'informació.

Una tècnica seria fer cerques, més o menys depurades en cercadors sobre la IP descoberta, però ens servirem de programari que automatitza de manera eficient les mateixes.

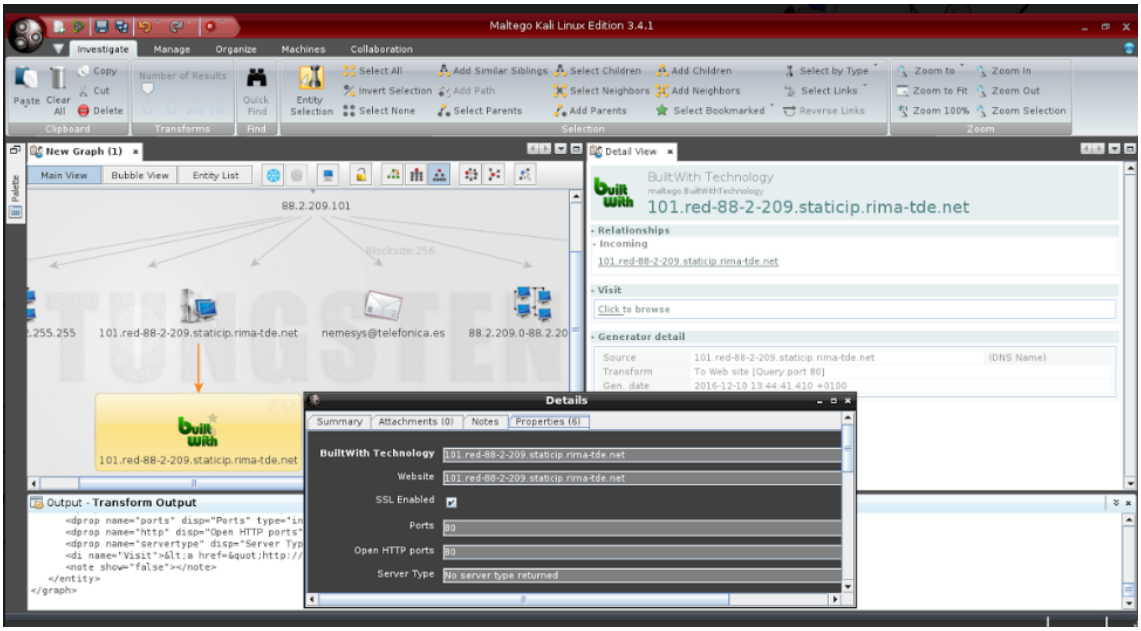
- FOCA PRO 3.4 (Fingerprinting Organizations with Collected Archives)



IL·LUSTRACIÓ 60 - CERCA D'INFORMACIÓ ALS PRINCIPALS CERCADORS VIA FOCA

Tal com era d'esperar no hi ha cap informació indexada en els principals cercadors, això dificulta la tasca de l'atacant però dóna una pàtina de veracitat a l'entorn.

- Maltego Kali Linux Edition 3.4.0



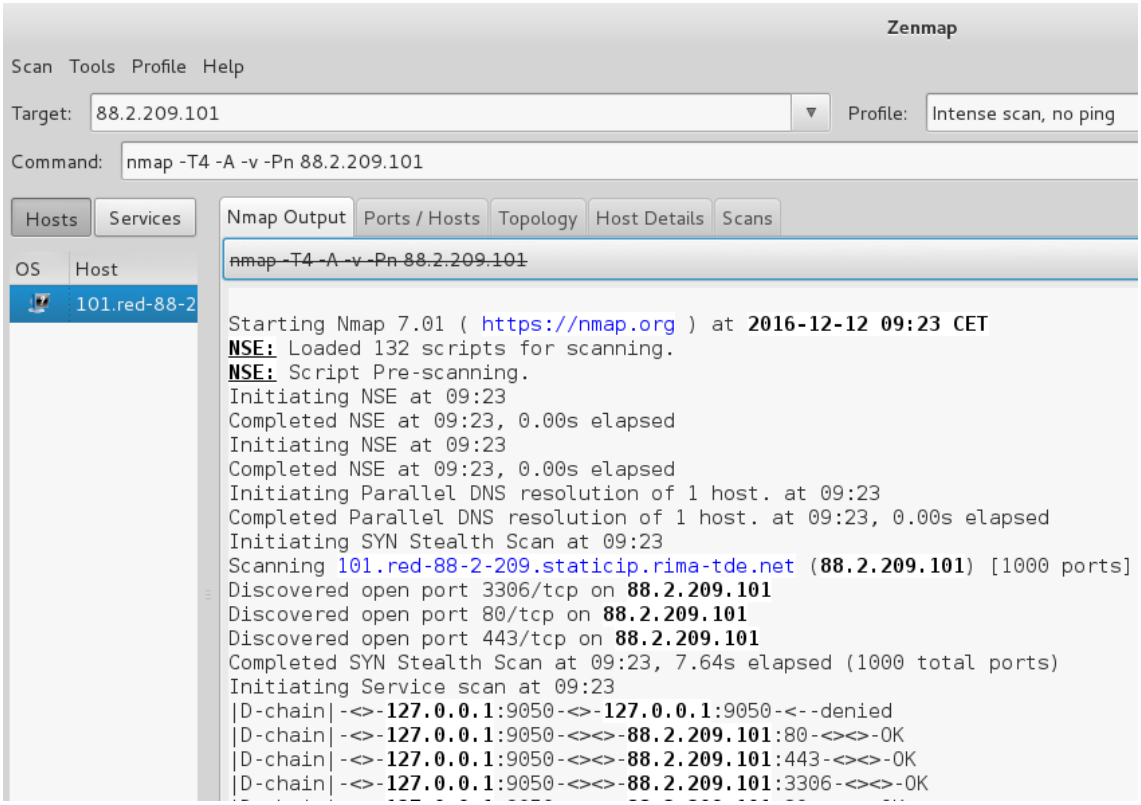
IL·LUSTRACIÓ 61 - INFORMACIÓ OBTINGUDA AMB MALTEGO DETALL FOOTPRINT L3

En aquest cas, ja trobem informació sobre un servei obert al port 80 i que el SSL és activat. És a dir, l'atacant ja té un indici per mirar d'assolir més informació que el pugui ajudar a completar la seva tasca. A més, obté informació sobre l'operador que presta servei[13.17], o de manera més simple mitjançant el correu nemesys@telefonica.net. Cosa que pot servir, per exemple, per a detectar si el sistema disposa d'un router propi de la companyia i així cercar-ne possibles forats de seguretat.

- Fase 2: *fingerprinting*, recol·lecció d'informació específica del sistema.

Un cop obtingudes aquelles dades més generalistes caldria iniciar un anàlisi més profund sobre el sistema que serà atacat. L'atacant mirà d'obtenir informació sobre els serveis oberts, quines vulnerabilitats tenen, quins sistemes operatius hi ha al darrera, de quins dispositius físics disposa i tota aquella informació que el pugui ajudar a fer una intrusió al sistema .

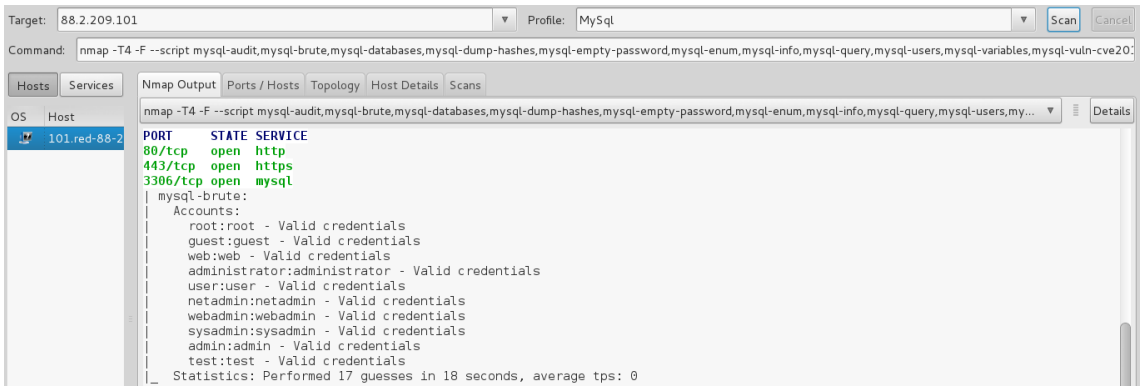
  - NMap 7.0.1, versió visual ZenMap



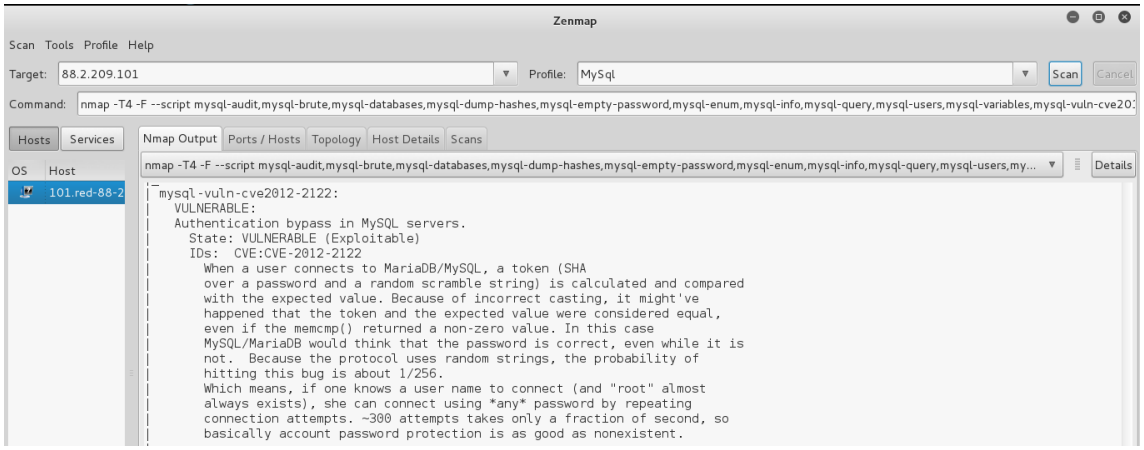
IL·LUSTRACIÓ 62 - RESULTATS NMAP ESCANEIG INTENS

Veiem doncs com els resultats ens mostren que hi ha tres ports coneguts oberts 80, 443 i 3306, fet coherent amb la interfície que veiem[Il·lustració 42 i Il·lustració 43] en visitar el portal *fake*.

Aprofitant les eines que ens aporta el propi programari farem una cerca més avançada i profunda, utilitzant els modificadors adients, contra els servei 3306 trobat que es suposa per defecte un MySql.



IL·LUSTRACIÓ 63 - LLISTAT D'USUARIS I MOTS DE PAS DESCOBERTS PER NMAP



IL·LUSTRACIÓ 64 - VULNERABILITAT DETECTADA PER NMAP

Efectivament s'ha descobert un llistat d'usuaris i mots de pas de la BBDD, a més d'una vulnerabilitat coneguda que podrà ser usada en la següent fase d'explotació.

- Nessus 6.9.1, versió home

88.2.209.101

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	14	14

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10719	MySQL Server Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

IL·LUSTRACIÓ 65 – RESUM ESCANEIG DE VULNERABILITATS CONTRA EL SITE FAKE

Com es pot observar, a priori no sembla que la plataforma tingui cap vulnerabilitat ni mitjana ni greu, tal com correspondria a un *site* segur. Ara, si que hi ha certa informació, segurament deguda a un descuit de l'administrador, que podria ser utilitzada per a atacar l'enton. Resumim aquí els punts destacats.

- `The remote operating system matched the following CPE :`

```
  cpe:/o:linux:linux_kernel:2.6
```

- `Following application CPE matched on the remote system :`

```
  cpe:/a:mysql:mysql:5.0.54 -> MySQL5.0.54
```

- `Contents of robots.txt :`

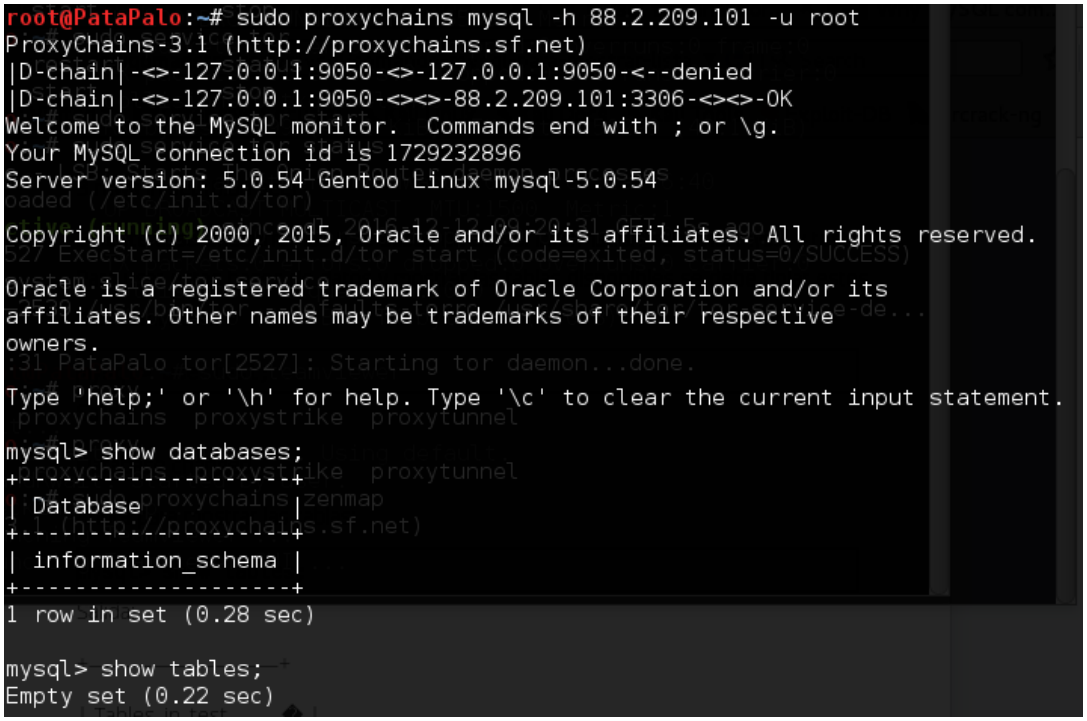
```
User-agent: *
```

```
Disallow:/
Disallow:.motdepas.txt
```

- Fase 3: explotació de les vulnerabilitats.

Amb aquestes dades obtingudes l'atacant pot començar un seguit d'accions contra la plataforma. A tall d'exemple pot intentar:

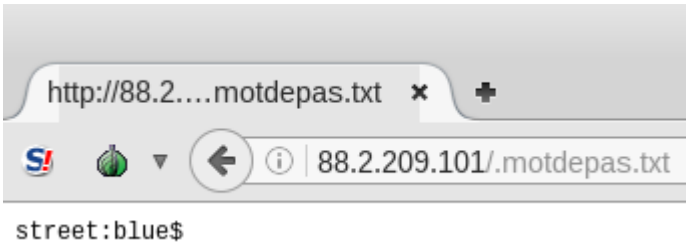
  - Accedir al servei MySql amb les credencials obtingudes:



IL·LUSTRACIÓ 66 - ACCÉS NO AUTORITZAT A LA BBDD SERVER52

El cibercriminal hauria aconseguit entrar en el sistema i executar comandes MySql. Aquest fet seria anàleg a explotar la vulnerabilitat trobada CVE-2012-2122 mitjançant una eina tipus msfconsole (msf auxiliary(mysql_authbypass_hashdump)

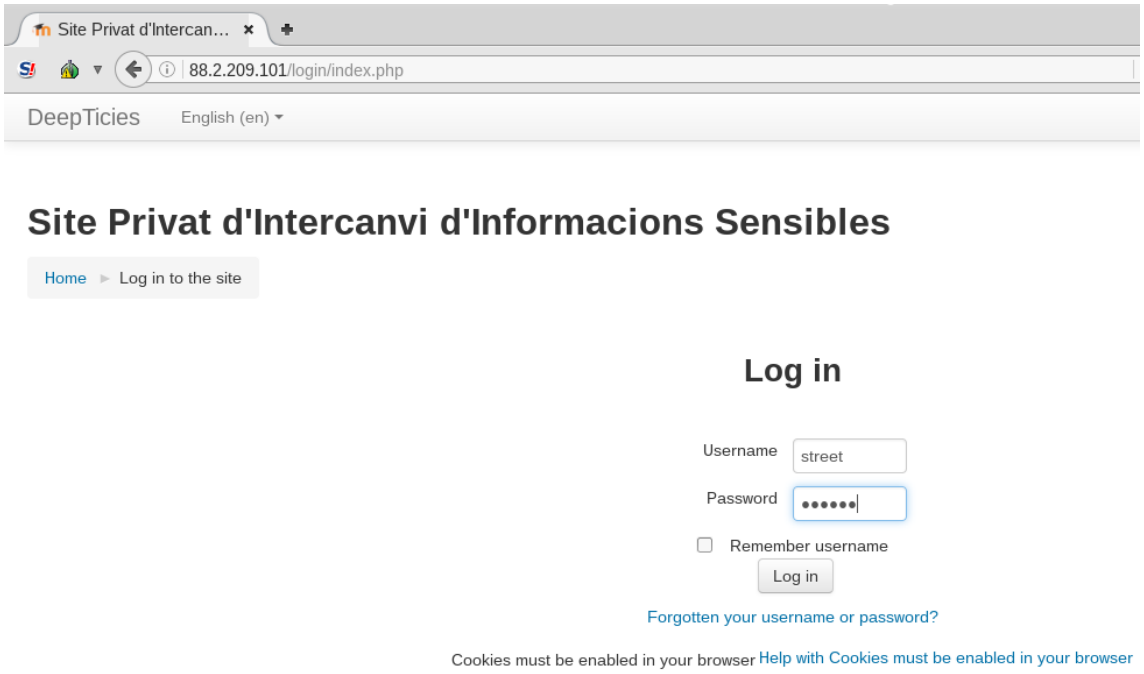
  - Visualitzar l'arxiu ocult .motdepas.txt apuntat en el robots.txt



IL·LUSTRACIÓ 67 - VISUALITZACIÓ DE L'ARXIU OCULT ESQUER

En aquesta ocasió, aprofitant les dades recol·lectades en l'arxiu robots.txt, accedeix a un nom d'usuari i mot de pas ocults. Aquests no tenen cap altra abast que servir de distracció mentre l'atacant mira d'esbrinar on pot ser utilitzat.

- Utilització de les credencials trobades

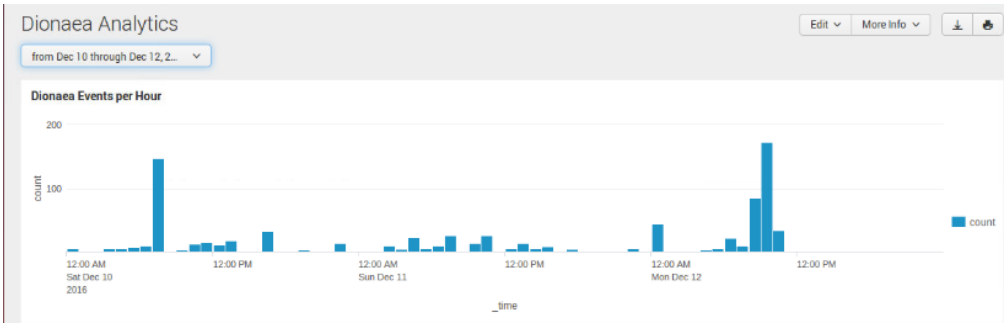


IL·LUSTRACIÓ 68 - INTENT D'ACCÉS NO LEGITIM AMB CREDENCIALS DESCOBERTES

Un exemple possible d'on utilitzar les credencials seria en l'accés al portal que es creu legítim.

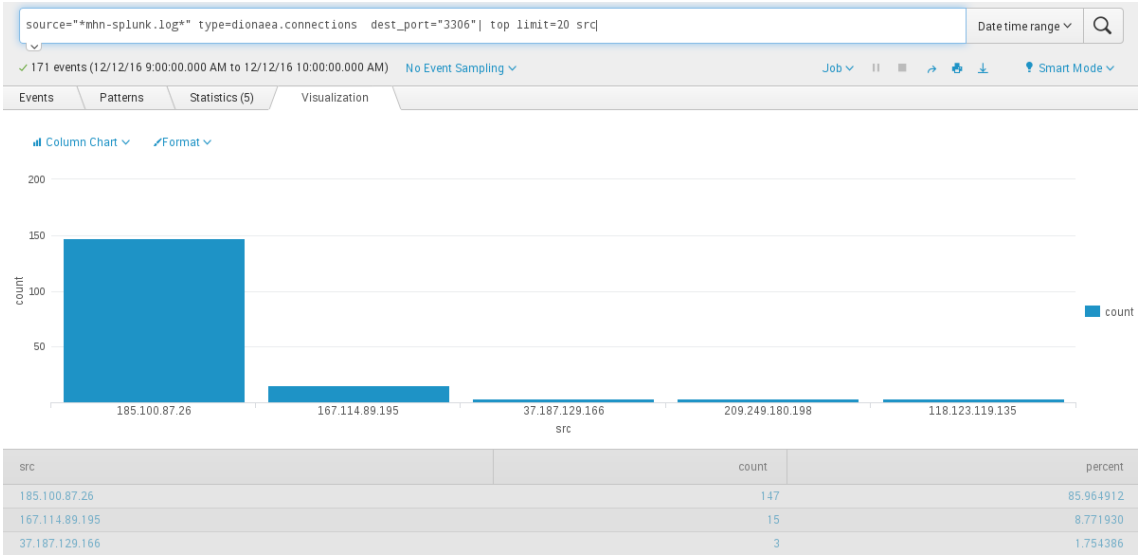
Aquestes serien algunes des les accions que l'atacant podria intentar i en cas de tenir èxit caldria que n'esborrés els registres. Altres possibles actuacions serien atacs de denegació de servei. Això podria portar a col·lapsar l'entrada al sistema, no el servei legítim en sí. Esdevindria una molèstia però no pas una pèrdua de control sobre la seguretat de les dades. El que és important per a l'entorn de producció és que en cap moment s'ha vist amenaçat pel que fa a les dades contingudes.

Pel que fa a la recol·lecció de dades, fent un filtre de les dates en que s'han fet aquest tests es pot veure com hi ha un augment significatiu de l'activitat. Els matins de dissabte 10 de desembre i dilluns 12 de desembre del 2016, hi ha una punta d'activitat que es correspon amb les proves d'intrusió controlades.



IL·LUSTRACIÓ 69 - SPLUNK, RECULL D'ACTIVITAT FILTRADA PER DATA

I com per exemple en aquesta franja hi ha hagut una IP: 185.100.87.26 que connectat amb el servei MySql significativament, amb un rati de 9'8 punts per sobre de la segona classificada, més vegades que cap altre.



src	count	percent
185.100.87.26	147	85.964912
167.114.89.195	15	8.771930
37.187.129.166	3	1.754386

IL·LUSTRACIÓ 70 - LLISTAT ORDENAT D'IP MÉS INTRUSSIVA EN UN PERÍODE

Malgrat procedir d'un proxy anònim[13.20], cosa que no ajuda a desemmascarar l'autor, si que ens permetria per exemple incloure la IP en una llista negra per a *bannejar-ne* el seu accés.

Durant tot aquest procés, cal destacar que en cap cas s'ha identificat cap servei honeypot i per tant l'atacant ha seguit endavant mentre pensava que era en un entorn real. També cal destacar, que el *router* ha actuat de manera transparent, cosa realment important ja que un atac sobre el mateix podria corrompre la seguretat, o si més no la continuïtat del servei.

El resultats de tot plegat podria dir-se que corresponen a un entorn de *deception Technology*. El que s'ha aconseguit, des del punt de vista de protecció, ha estat desviar l'atenció i recopilar informació sobre atacants, que en un futur, o de manera paral·lela, podrien mirar d'assaltar l'entorn legal.

11. MILLORES FUTURES

Un cop definida tota l'arquitectura d'aquest projecte i desplegat el prototipus cal una mirada crítica del mateix. Sí bé aquest prototip ja podria entrar en funcionament en el mateix instant que s'ha acabat amb l'elaboració d'aquesta memòria, caldria una nova implementació que tingués en compte determinats aspectes.

Pel que fa al maquinari, seria convenient disposar d'un hardware robust, que permetés assignar els recursos necessaris a cada màquina virtual, que disposes de mètodes de contingència avançats amb una rèplica segura, periòdica i remota, de les dades. Aquests equipaments haurien d'estar distribuïts en dos centres, equipats convenientment i amb totes les mesures de seguretat previstes per a clústers de CPDs. L'enllaç entre aquests espais s'hauria de garantir, amb duplicitat de canals de comunicació ràpids via diferents fibres òptiques. Així mateix, la sortida a Internet s'hauria de realitzar sobre un canal d'alta gamma i capacitat, que fos replicat per una altra companyia i ubicat en el segon centre de processament de dades. Vaga dir doncs, que l'electrònica a implementar no només hauria de ser d'alta gamma sinó que caldria poder-la configurar per a commutés automàticament en cas de caiguda o atac cibernètic.

En l'apartat de programari caldria dotar la infraestructura de noves funcionalitats que garantissin una millor experiència d'usuari i afegissin un extra de seguretat. Caldria, per exemple, implementar el codi adient per a no permetre l'acció de copiar els contingut de la pantalla i a més afegir una marca d'aigua en tot l'espai on hi figuressin les credencials de l'agent validat. La metodologia de la còpia de seguretat s'hauria de millorar ajudant-se d'un maquinari especialitzat, tal com s'apuntava en el paràgraf anterior. La configuració dels tallafocs s'haurien de depurar més per a millorar-ne el filtratge i el registre d'esdeveniments. En el cas de l'apartat *honeynet* caldria escalar-lo a màquines d'alta interacció sota el concepte actual . És a dir, fer que el portal replicat actués de forma similar, no només en aparença, al real, Així, en cas d'aconseguir unes credencials, l'atacant hauria de ser capaç de fer una validació a l'entorn i poder-hi interactuar. De la mateixa manera que si s'ataqués directament a la base de dades.

Per últim, caldria estudiar la metodologia per a dotar a tota la informació recol·lectada d'una validés legal irrefutable. És a dir, caldria dissenyar el procediment per afegir un *timestamp* a la documentació recollida, així com signar-la digitalment. L'objectiu seria evitar el repudi en un judici, de certes proves i evidències, degut a la impossibilitat de garantir-ne la veracitat.

Aquests paràgrafs, només pretenen donar la visó que per establir un entorn d'aquestes característiques en l'àmbit real, requeriria no només d'una inversió inicial, sinó caldria disposar d'un equip de manteniment quotidià.

12. CONCLUSIONS

La realització d'aquesta memòria ha servit per a deixar constància que l'àmbit que s'ha volgut abastar era prou extens. Només cal entrar en el detall de cada producte a implementar per entendre l'abast del mateix. Així s'han tocat els punts més rellevants de cadascun però quedaria molta feina a polir en cada implementació. Així, entrar a fons en la gestió de la plataforma Moodle o implementar *honeypots* d'alta interacció personalitzats, a tall d'exemple, ja esdevindrien en si mateix un àmbit prou extens.

Aquest treball ha servit doncs, per a veure de a prop la problemàtica, no només de muntar una arquitectura nova, sinó de a mantenir-la i donar-li coherència. La manca d'experiència prèvia en gairebé la totalitat del productes desplegats n'ha sobrecarregat l'esforç d'implementació i explotació dels mateixos.

També ha permés acostar-se a procediments i eines que actualment s'utilitzen sobre dades sensibles i que es creuen més segures del que realment són. La utilització del correu electrònic sense xifrar, el Whatsapp o altres mètodes de missatgeria exposen la informació a poder ser revelada, i tot sovint no es té en compte.

Ha resultat un treball molt enriquidor tant a nivell personal com ho podria arribar a ser a nivell laboral. Posar-se en una situació d'una demanda real i mirar d'aportar una solució dóna un al·licient extra a l'hora de confeccionar una memòria com la present.

L'èxit, finalment ha estat poder desplegar satisfactòriament, l'arquitectura enginyada a nivell de laboratori, però amb funcionalitats reals, sota un entorn auster i limitat. Tal com es mencionava en l'apartat anterior, seria totalment factible posar-la en marxa, sempre i quan es disposessin dels recursos necessaris.

13. ANNEXOS

Donada l'extensió dels arxius de configuració s'ha optat per a fer captures de pantalla que faciliten la lectura i ocupen menor espai en la memòria.

13.1. Arxiu de configuració variables per a generació de claus

```
root@Server51:/usr/share/easy-rsa# cat vars
# easy-rsa parameter settings

# NOTE: If you installed from an RPM,
# don't edit this file in place in
# /usr/share/openvpn/easy-rsa --
# instead, you should copy the whole
# easy-rsa directory to another location
# (such as /etc/openvpn) so that your
# edits will not be wiped out by a future
# OpenVPN package upgrade.

# This variable should point to
# the top level of the easy-rsa
# tree.
export EASY_RSA="`pwd`"

#
# This variable should point to
# the requested executables
#
export OPENSSL="openssl"
export PKCS11TOOL="pkcs11-tool"
export GREP="grep"


# This variable should point to
# the openssl.cnf file included
# with easy-rsa.
export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA`

# Edit this variable to point to
# your soon-to-be-created key
# directory.
#
# WARNING: clean-all will do
# a rm -rf on this directory
# so make sure you define
# it correctly!
export KEY_DIR="$EASY_RSA/keys"

# Issue rm -rf warning
```

```
echo NOTE: If you run ./clean-all, I will be doing a rm -rf on $KEY_DIR

# PKCS11 fixes
export PKCS11_MODULE_PATH="dummy"
export PKCS11_PIN="dummy"

# Increase this to 2048 if you
# are paranoid.  This will slow
# down TLS negotiation performance
# as well as the one-time DH parms
# generation process.
export KEY_SIZE=2048

# In how many days should the root CA key expire?
export CA_EXPIRE=3650

# In how many days should certificates expire?
export KEY_EXPIRE=3650

# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="CT"
export KEY_PROVINCE="BA"
export KEY_CITY="Barcelona"
export KEY_ORG="UOC"
export KEY_EMAIL="kuse@uoc.edu"
export KEY_OU="Treball Final de Master"

# X509 Subject Field
export KEY_NAME="tfmjcr"

# PKCS11 Smart Card
# export PKCS11_MODULE_PATH="/usr/lib/changeme.so"
# export PKCS11_PIN=1234

# If you'd like to sign all keys with the same Common Name, uncomment the KEY_CN
 export below
# You will also need to make sure your OpenVPN server config has the duplicate-c
n option set
# export KEY_CN="CommonName"
"
```

13.2. Arxiu d'entitat de certificació local, clau privada

```
root@Server51:/etc/openvpn/easy-rsa/keys# cat ca.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggS1AgEAAoIBAQDbKRssW2c+UWgY
Vbre+aUOJZTaHaYSefOPJTUQO+l2kaYUcPnTrixlMONd/krTURYGnODwCJ9K56tY
cvQCtNngOag46JuQmu1EYnBwkM/r54hwW1tHGsROOmKgyi6iiv9w6nhWWHeoRzku
aljNhD4jboI3CBTDTCPKty49V/8u8SivUG6JnLLoxpB9RViFgmvoQumoKW6aZWTd
4xabZf/NHu+HSVNDVWmrcy14agi4jFS1cSYrXWgiirl+fhfWSHb5LF8ka43OtBPH
ZzmtRNC9YHYg+KZo4Ot+CNkrmu6NfXkzF97eiYKNGus6d34EmkmOchOUzIFUtwW1
p6DWsPz1AgMBAAECggEBAJtyKIfpvOOCqKa6B/WndHnsPgwHA4gPZmKbrWt6Uz16
TSYqi8iMvYh6N8ovV7tSxCCknRcjxnhGoc32mwRgajl/+6WBtvV2LdxXRhFRZWiZ
rLikHiHs5lfmKZaKUVGQ7WWVqQz1asm82t4FKD99EOXouAt4e+GZ27ko/G8ePy13
J7PCUuya7LK8JkvCjysyHHKommqnDk9SDUTVV5mCLtE4e2oOdSYfPSPoCH366gFt
Za67izZc6ZJEtpkNZD5SwucUxgZyLIt3p+GWZU5hgnkfkms/Wd3CmFYEjctEKoi8
GOBSnsFigw2NlqmG1VkZ5QY+7cCzGPtjTS2QJdvpZ/ECgYEA7kP55kLH94jLUCaR
U/sGp5lEKAlYPucRCzk7r2Sp/Tz2BXFLo84qYUEcEcibgyaEw2CPhwEzSjx5P5v7
pM5RV7XGAySaZ+YbozHJknOj6A16YqMbtNNUkRfnlnJ2xKoad7RxzOlvA4s4iDRR
GfpxgDDPVvKSJxxx5OkquShVOcCgYEA63kYVFaHDNnzqup4NvSzXsWOP3+o7xN8
BXRDf7drI7K6MVYE6lDzPLO6sD1kE8nPfH6zcCTmHQWlOGO6Dfw6s1rL6EjojJJD
H+3aEBu2z+lzEJce5IPMrzRtao2DTB3QvvFKdM1KOxG94iijp4PfywiPQZYO1fzP
2tsW87tNB8MCgYEArIbeSkRrBauxBK2YqAXp8KwDdTYnBw1MAyODO2KZOHw27QP3
sHoVp+x8hcgMC3B1y/98j1ZpLEUTyuKI2fJnZiqCYj477CXsNORS4FbrDBnOV+Qh
qNMpthJoKEFkDM3bcnhfuvAA6cECw2WWoEf/rcIqMJxfBiELvVz2ebbdt1sCgYA1
Usngp2uTzHNynAA3KbjI2GqWCpm98iKetZJnhKi9f8bMT1dznHtIoO1+ZZiZJpVW
8vY9ig2WOuYMXifMbPb6ELCmXIRU+PY8b8d26F/Au3POKNS1GOesMWopu/wkq4fP
BaM/yhFqSP1ADsXotGNkff668oHqh4KmZADRlvO9swKBgQC2xmYftWmr+HcJH6e5
n5R4uOvh1TxwYgFTXCPZGM477imNhZU1p8w+b+jllapWRl1z/6xU4x7KeYe9+4AR
Dwq6tQ7NV/LqrJMC/VgIhJf3JRroPcuA2VXKSQa7EerEiKtHTBpAsuW3jCarm/uW
PT3gzfcyA+cds7uO/O8vK+L24w==
-----END PRIVATE KEY-----
```

13.3. Xifratge Diffie Hellman per a les connexions

```
root@Server51:/etc/openvpn# cat dh2048.pem
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAlm6F8GaRaAyEPbvAbkFlYAd8rOhn5KJoeCsDzIxEE45CsKx+kkbA
ZBiO3ZJyp3DkpGhYKnOyLHcOX4QMceuDWgAk6V2hR2x4/Tjr+sRgTntDj147qTFI
4SpHBL/j/OdSzC4zmVCYy+e2Ok5/GEHbkq7s5FkTKsZ/7dpR/mNLcQ/FUbJMSHnY
5fZOZ8jMGmrTRYctmo8FfAw24zpIm7FBc4ltaNa8BfRL6JXlTjRRSHE7I3FBrrfQ
jUJN/Zm6YzIMK5zeVn7UCnzIrTUaOZa/eRTAafHuUfOZDZfON81q/QHodXXXfkhd
FSX6PkE5NLbujpacSbhPK6cVd3ndoz8a4wIBAg==
-----END DH PARAMETERS-----
```

13.4. Certificats de servidor Server51

```
-----BEGIN CERTIFICATE-----
MIIFQDCCBCigAwIBAgIBATANBgkqhkiG9w0BAQsFADCBnTELMAkGA1UEBhMCQ1Qx
CzAJBgNVBAgTAkJBMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNVBAoTA1VPQzEg
MB4GA1UECxMXVHJlYmFsbCBGaW5hbCBkZSBNYXN0ZXIxDzANBgNVBAMTBlVPQyBD
QTEPMA0GA1UEKRMGdGZtamNyMRswGQYJKoZIhvcNAQkBFgxrdXNlQHVvYy51ZHUw
HhcNMTYwNzI5MDgzMzI1WhcNMjYwNzI3MDgzMzI1WjCBoDELMAkGA1UEBhMCQ1Qx
CzAJBgNVBAgTAkJBMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNVBAoTA1VPQzEg
MB4GA1UECxMXVHJlYmFsbCBGaW5hbCBkZSBNYXN0ZXIxEjAQBgNVBAMTCXRmbWpj
ci50azEPMA0GA1UEKRMGdGZtamNyMRswGQYJKoZIhvcNAQkBFgxrdXNlQHVvYy51
ZHUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8N+BnNrdaCiEbaXrE
uTuxUuOeB5Iqr297udrRoYx3PK2zhp563F18/3WSGzlEfk6eal20WgtVp31OTvi2
x4cOIdWiDjBBNKNS118aWctuQz7PvLFwOmMtlV5jaNqPmaXMHHy+Pme14SkvBpm3
IuRa1MtZthNPKLSuS+i/iCOJ2LzJ43vRQA/gGNOOckmvhIiTn5KWYqS4LF1q4LaY
UwZAoKsNOMQGkBURp2Gs+eItDP1erDH3uQny5T96+IR+WWvioEn04/19tPJuK2rp
Lb08xNOlsnYylFmyU5wcIjwWN5s1jX9KL5W23E+9EIUY6d/k15+olR1M4NEtNGtQ
curPAgMBAAGjggGEMIIBgDAJBgNVHRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDAO
BglghkgBhvhCAQOEJxYlRWFzeS1SUOEgR2VuZXJhdGVkIFNlcnZlciBDZXJOaWZp
Y2FOZTAdBgNVHQ4EFgQUHEuahWNegHkJoxRgnmH9LgPlofQwgdIGA1UdIwSByjCB
x4AURS/Iu1SZb5u5UypYLpX3ISso54mhgaOkgaAwgZOxCzAJBgNVBAYTAkNUMQsw
CQYDVQQIEwJCQTESMBAGA1UEBxMJQmFyY2Vsb25hMQwwCgYDVQQKEwNVT0MxIDAe
BgNVBAsTF1RyZWJhbGwgRmluYWwgZGUgTWFzdGVyMQ8wDQYDVQQDEwZVT0MgQOEx
DzANBgNVBCkTBnRmbWpjcjEbMBkGCSqGSIb3DQEJARYMa3VzZUB1b2MuZWR1ggkA
yqSdLOOevXswEwYDVR0lBAwwCgYIKwYBBQUHAwEwCwYDVROPBAQDAgWgMBQGA1Ud
EQQNMAuCCXRmbWpjci50azANBgkqhkiG9w0BAQsFAAOCAQEAT65DjhWC4BZc67S4
2KEKxeb5qWtX+uOyPxnxWxbv2FQqKx7CVyCvak+IsZT1KnzQhWw1XLS7pmnusmRk
qwcS+cDWKztUJVyRI7A9Xcy2yTwORTa3Q3HS5Xn/XBQkxivGdMLV+C5jQT6RIljW
mXGHAZPUuDAUL2s1kU3fg1H7gvFeDWup1Adp1b2GIZhgiZXBrNhcL+H55hOYOolj
wJHFVnQlEfPCIpgp6WcC9vSxRDnun8vUTfutqsWvrb+K5aOrM1spnYsSsusEuTlt
kpbsRv4hGtc11zEFyLPOWb1KFkyZgIynOz6kV2c7rQfTJbpLTX1n8cqOUQj7HVe8
h/zgKQ==
-----END CERTIFICATE-----
root@Server51:/etc/openvpn# cat tfmjcr.tk.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=UOC CA/name=tfmjcr/emailAddress=kuse@uoc.edu
        Validity
            Not Before: Jul 29 08:33:25 2016 GMT
            Not After : Jul 27 08:33:25 2026 GMT
        Subject: C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=tfmjcr.tk/name=tfmjcr/emailAddress=kuse@uoc.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bc:37:e0:67:36:b7:5a:0a:21:1b:69:7a:c4:b9:
                    3b:b1:52:e3:9e:07:92:2a:af:6f:7b:b9:da:d1:a1:
                    8c:77:3c:ad:b3:86:9e:7a:dc:5d:7c:ff:75:92:1b:
                    39:44:7e:4e:9e:6a:5d:b4:5a:0b:55:a7:7d:74:4e:
                    f8:b6:c7:87:0e:21:d5:a2:0e:30:41:34:a3:52:d7:
                    5f:1a:59:cb:6e:43:3e:cf:bc:b1:70:d2:63:2d:95:
                    5e:63:68:da:8f:99:a5:cc:1c:7c:be:3e:67:b5:e1:
                    29:2f:06:99:b7:22:e4:5a:d4:cb:59:b6:13:4f:28:
                    b4:ae:4b:e8:bf:88:2d:09:d8:bc:c9:e3:7b:d1:40:
                    0f:e0:18:d3:8e:72:49:af:84:88:93:9f:92:96:62:
                    a4:b8:2c:5d:6a:e0:b6:98:53:06:40:a0:ab:0d:38:
                    c4:06:90:15:11:a7:61:ac:f9:e2:2d:0c:fd:5e:ac:
                    31:f7:b9:09:f2:e5:3f:7a:f8:84:7e:59:6b:e2:a0:
                    49:f4:e3:f9:7d:b4:f2:6e:2b:6a:e9:2d:b3:bc:c4:
                    d3:a5:b2:76:32:94:59:b2:53:9c:1c:22:3c:16:37:
                    9b:35:8d:7f:4a:2f:95:b6:dc:4f:bd:10:85:18:e9:
                    df:e4:97:9f:a8:95:1d:4c:e0:d1:2d:34:6b:50:72:
                    ea:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
```

```
            SSL Server
        Netscape Comment:
            Easy-RSA Generated Server Certificate
        X509v3 Subject Key Identifier:
            1C:4B:9A:85:63:5E:80:79:09:A3:14:60:9E:61:FD:2E:03:E5:A1:F4
        X509v3 Authority Key Identifier:
            keyid:45:2F:C8:BB:54:99:6F:9B:B9:53:2A:58:2E:95:F7:21:2B:28:E7:89
            DirName:/C=CT/ST=BA/L=Barcelona/O=UOC/OU=Treball Final de Master/CN=UOC CA/name=tfmjcr/emailAddress=kuse@uoc.edu
            serial:CA:A4:9D:2F:43:9E:BD:7B

        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Key Usage:
            Digital Signature, Key Encipherment
        X509v3 Subject Alternative Name:
            DNS:tfmjcr.tk
Signature Algorithm: sha256WithRSAEncryption
     4f:ae:43:8e:15:82:e0:16:5c:eb:b4:b8:d8:a1:0a:c5:e6:f9:
     a9:6b:57:fa:e3:b2:3f:19:f1:5b:16:ef:d8:54:2a:2b:1e:c2:
     57:20:af:6a:4f:88:b1:94:f5:2a:7c:d0:85:6c:35:5c:b4:bb:
     a6:69:ee:b2:64:64:ab:07:12:f9:c0:d6:2b:3b:54:25:5c:91:
     23:b0:3d:5d:cc:b6:c9:3c:34:45:36:b7:43:71:d2:e5:79:ff:
     5c:14:24:c6:2b:c6:74:c2:d5:f8:2e:63:41:3e:91:22:58:d6:
     99:71:87:01:93:d4:b8:30:14:2f:6b:35:91:4d:df:82:51:fb:
     82:f1:5e:0d:6b:a9:94:07:69:95:bd:86:21:98:60:89:95:c1:
     ac:d8:5c:2f:e1:f9:e6:13:98:d2:89:63:c0:91:c5:56:74:25:
     11:f3:c2:22:98:29:e9:67:02:f6:f4:b1:44:39:ee:9f:cb:d4:
     4d:fb:ad:aa:c5:af:ad:bf:8a:e5:a3:ab:33:5b:29:9d:8b:12:
     b2:eb:04:b9:39:6d:92:96:ec:46:fe:21:1a:d7:35:d7:31:05:
     c8:b3:ce:59:b9:4a:16:4c:99:80:8c:a7:3b:3e:a4:57:67:3b:
     ad:07:d3:25:ba:4b:4d:7d:67:f1:ca:8e:51:08:fb:1d:57:bc:
     87:fc:e0:29
```

```
root@Server51:/etc/openvpn# cat tfmjcr.tk.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwgaAxCzAJBgNVBAYTAkNUMQswCQYDVQQIEwJCQTESMBAGA1UE
BxMJQmFyY2Vsb25hMQwwCgYDVQQKEwNVTOMxIDAeBgNVBAsTF1RyZWJhbGwgRmlu
YWwgZGUgTWFzdGVyMRIwEAYDVQQDEwlOZm1qY3IudGsxDzANBgNVBCkTBnRmbWpj
cjEbMBkGCSqGSIb3DQEJARYMa3VzZUB1b2MuZWR1MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAvDfgZza3WgohG2l6xLk7sVLjngeSKq9ve7naOaGMdzyt
s4aeetxdfP91khs5RH5OnmpdtFoLVad9dE74tseHDiHVog4wQTSjUtdfGlnLbkM+
z7yxcNJjLZVeY2jaj5mlzBx8vj5nteEpLwaZtyLkWtTLWbYTTyiOrkvov4gtCdi8
yeN7OUAP4BjTjnJJr4SIk5+SlmKkuCxdauC2mFMGQKCrDTjEBpAVEadhrPniLQz9
Xqwx97kJ8uU/eviEfllr4qBJ9OP5fbTybitq6S2zvMTTpbJ2MpRZslOcHCI8Fjeb
NY1/Si+VttxPvRCFGOnf5JefqJUdTODRLTRrUHLqzwIDAQABoBgwFgYJKoZIhvcN
AQkHMQkTB3RmbTIwMTYwDQYJKoZIhvcNAQELBQADggEBAKUub8XGtMYVoZ32rwKu
1Tb6S8Dv8dkrrj6Od4a4QsO9fz8pZjTsRe8yGloc5T7bSZ/D5MM7nR6JiXNERtvX
Vf4Em6QSAMQD6Ad54dxs/PDFKXq3FgCQ5aH7yhVJAA83x/OUnow5rDX12OVru/wx
4eCYJ8ibXh6XOykEDH9tu1F5vcgWneBYjrUj/2OvlvmOA3c728JNuZHZhKzPDjzi
Oii2+larTqeW34RgVDGs3cOr4+nXwLbrRFwa7vXax8kMrmSyReYJW9ERoeJt/y+o
oiAOcykHoXVW2bwzZhVxSohT1vKg8U5u2fqkOOsldkG7G4gy6LfQ8lusSz4zShkx
tb8=
-----END CERTIFICATE REQUEST-----
```

```
root@Server51:/etc/openvpn# cat tfmjcr.tk.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC8N+BnNrdaCiEb
aXrEuTuxUuOeB5Iqr297udrRoYx3PK2zhp563F18/3WSGzlEfk6eal2OWgtVp31O
Tvi2x4cOIdWiDjBBNKNS118aWctuQz7PvLFwOmMtlV5jaNqPmaXMHHy+Pme14Skv
Bpm3IuRa1MtZthNPKLSuS+i/iCOJ2LzJ43vRQA/gGNOOckmvhIiTn5KWYqS4LF1q
4LaYUwZAoKsNOMQGkBURp2Gs+eItDP1erDH3uQny5T96+IR+WWvioEnO4/l9tPJu
K2rpLbO8xNOlsnYylFmyU5wcIjwWN5s1jX9KL5W23E+9EIUY6d/kl5+olR1M4NEt
NGtQcurPAgMBAAECggEAEjvjjHw7hQiILoyobRh41PPvwyZ+nY4DYdwee8KHxiF1
voejIMnqcKqa7D2g7abC3Qv26frzMCgaukLQS3zG87KJbLqtKBP+Yo8kOnuyfosb
MarZEdH/87GNxFmrGtBKxJxZ5WBMUc1vXPPpvlkuADKvRJCkDD4oSt5lvPBnVJWO
y7V6XgU7j18vPE7BjxEN19m1Alorr6NvgvFXMXisRJNlkA587rYOmiMFM85/zAj8
MjoyQUVGCSwuBNKyiyedDggIcn1y3KaARkayveOo7NmPdLOsCpztOGPjzmXLF1g1
1yh2unnf+omcAiST/s6zRigFd8IG7Fg28F/TbW+5OQKBgQD5YR65PcN/LnxfQ1/b
UfTRPqb21cKVhl5POZBMntp/LrkZTNhYiIOgyDoa/tFxFvYYSC4vAsSBGdq/mbnh
tZ+J+WzBqOaCEbbaGkOR/oVYQ2o7LxM9336BeohzKvvwOzZFmRMNEv+HloictUD1
giEix657XdV8ODf83eYFSDsVOwKBgQDBNxTqbw1gPlfDOPfTDhA5SpYb7nabhTmL
LzwWJ3FHwWV8uc1eVu5xSgwB5iOijySN8eesnC/LZnq/EDCrf9vyDcTpZoeZIGAe
gYKZjFROxngO3/8c6iukJnelhfOMOZG3srkwORwy4fdsEzLElqKXaxTyJCQfbsW1
y6qpZf/XfQKBgQDC2PVueymyx5l5vWS6MnD8xNOj46Uju1cZOn5qv3us/86OS+yG
UDO4fnmX+h2fJPenxU4AgUMUNCVMqOonZwd+gJpPQAnZOwoJo5fEDIAXlKT+FSwN
ngBOHk9a3Oz5H6459v6BqqRpRl77Qkuwh1pomGhmD8zsP+jO9HnzCprPXQKBgQCX
cr94SvfnGrbcFUlcK8fXwHkNB8v8d171lF661svafOM58sHhUq6wKmRjELMMRbtX
b+gyynJEMt2/6cbchuo2POi7OlwzUMdG4ikmhnKk3fS5ZCap2Xu/vU9HdUnEdXiM
zxCODTrXP3wbQKkooxJrMcpHSsDtynwuSwhIo+T4WQKBgCKw7XOMcqJzbPAL8fCw
WEXalEV/RGAn1PAds4ZznpL8XScsfLii3tTUZ//GYnkwWwnFGqQ5vsaF3zk3uOOL
nTtOqmYl5jp8PDMh4RYagRhXYmv+OODnTOyx8gLcLO81KOvEdAojS4CeM/EsxiRB
nJsvUlQSbXOL22ar4pbRZKGP
-----END PRIVATE KEY-----
root@Server51:/etc/openvpn#
```

13.5. Clau estàtica Server51

```
root@Server51:/etc/openvpn# cat ta.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
bf98b73cbc5777620e454974fea16465
2db3711c9ae82fd3aa60f311d2109f29
366dc62ebc0e71c70178acaf76c8410c
eb6278f4a0e7844a88e57aa894347810
53a20213bf1ed97b2dba5d76055bb44f
1578a185aa80be9fc475e95fe7faaba1
1f1262c45be99427c1feee3d7b6b0a5f
91eb4b44c6603acb782ec7a41fc1e2d8
9db10929946c7a45a4afb189bd2769aa
1d572a60ab27a723366179031c487eb0
a76785ecb09c36ea6e3df7473b0ba73e
b45f5aff3a21f82ec1230c2e9d6798f1
d0c29bc5202e7bdad87a7998aa4bd19c
1f080a98b83f9cfd60618edd8a35a530
c002f7682b9f955a5b73cf6944dac7da
f17c735b7fc923783813 0c5adcbabee6
-----END OpenVPN Static key V1-----
```

13.6. Certificats de Client

```
root@Server51:/usr/share/easy-rsa/keys# cat vpnuser01.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=UOC CA/name=tfmjcr/emailAddress=kuse@uoc.edu
        Validity
            Not Before: Jul 29 08:37:01 2016 GMT
            Not After : Jul 27 08:37:01 2026 GMT
        Subject: C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=vpnuser01/name=tfmjcr/emailAddress=kuse@uoc.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c2:16:31:4e:2c:47:d4:16:a4:9b:24:7d:84:7c:
                    7a:c3:18:59:44:e1:07:14:ad:db:38:14:48:49:69:
                    93:0a:33:dd:a0:3f:86:db:44:37:d6:f1:2c:1b:cd:
                    e6:0a:fd:d1:bf:cd:04:0c:d6:c9:49:9b:a6:58:44:
                    37:59:0f:cf:40:a2:c4:eb:2f:c5:d0:a8:12:c9:63:
                    63:e4:39:f0:19:f2:99:c1:f7:9c:d9:05:e4:c1:01:
                    09:a4:45:77:3b:85:e9:26:6c:a6:7a:bf:5a:b0:68:
                    7d:98:1e:90:4e:45:b7:75:ae:1f:1d:05:7a:a2:8b:
                    e3:b5:be:27:9c:74:fe:d8:ab:5a:e5:f1:7f:c0:27:
                    f9:50:a2:0f:12:fc:a9:bf:0a:5d:5d:4e:7b:07:e3:
                    71:8c:94:61:c4:62:b1:0a:4c:38:ca:a2:a2:a7:fb:
                    43:84:0c:79:6f:a1:50:98:b5:a5:66:47:71:f9:24:
                    45:c6:bb:1c:cb:2e:71:c1:a1:ce:96:2b:0b:77:66:
                    6c:1d:9d:ee:8e:ab:c9:50:09:8f:ce:90:be:d0:31:
                    0c:64:b2:b3:86:2c:36:a5:01:be:00:05:01:28:b9:
                    f8:24:a3:fd:40:29:40:02:2e:ad:2b:a4:d7:de:26:
                    82:1c:db:51:79:07:ed:a5:b2:bf:0a:c2:de:da:6b:
                    40:c1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                Easy-RSA Generated Certificate
            X509v3 Subject Key Identifier:
                3F:15:A7:CF:DE:8C:78:1A:19:0D:3C:1B:32:C3:C1:C6:2B:09:1E:74
            X509v3 Authority Key Identifier:
                keyid:45:2F:C8:BB:54:99:6F:9B:B9:53:2A:58:2E:95:F7:21:2B:28:E7:89
                DirName:/C=CT/ST=BA/L=Barcelona/O=UOC/OU=Treball Final de Master/CN=UOC CA/name=tfmjcr/emailAddress=kuse@uoc.edu
                serial:CA:A4:9D:2F:43:9E:BD:7B

            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Alternative Name:
                DNS:vpnuser01
    Signature Algorithm: sha256WithRSAEncryption
         6e:f2:b2:c6:d8:99:30:1e:86:81:35:75:7f:d2:fb:97:a5:19:
         46:d3:c0:84:27:3e:bf:9b:98:92:8c:c6:58:51:46:ee:05:80:
         1e:77:77:aa:36:c8:3b:6e:36:83:d2:76:1b:c6:03:bc:cc:91:
         bb:f0:cd:d9:73:a8:3c:20:70:da:bd:14:04:e2:e4:66:8b:f0:
         f8:f9:33:d3:05:24:58:58:45:51:65:2f:55:dd:7e:f0:36:12:
         3e:1b:ef:45:72:5b:a8:40:68:fe:15:9c:4f:dc:9b:1f:0e:8e:
         89:b7:75:54:22:d2:ce:04:df:7c:11:53:77:07:06:e4:c6:53:
         93:3e:eb:4b:d9:1f:80:78:ce:10:43:76:e1:c2:50:c6:35:23:
         61:92:86:7e:45:cc:93:e5:e0:7b:6e:72:e7:4e:1f:29:8a:e7:
         9a:03:bd:b8:78:9f:ad:3a:b3:21:3f:99:2a:09:90:6e:75:64:
         10:e4:40:57:92:fd:74:a3:d0:f3:c1:6c:c8:55:ec:7e:17:fc:
         a5:fc:02:ba:a9:dc:ee:1e:d5:16:98:17:8a:d9:e1:8c:8d:8c:
         56:f0:c1:66:22:50:4a:79:b0:8e:61:2f:04:66:53:3d:dd:15:
         e8:a1:24:93:70:24:ca:ce:98:d8:2a:93:1d:c1:28:9e:af:7e:
         fe:2c:54:83
-----BEGIN CERTIFICATE-----
MIIFjCCBA6gAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBnTELMAkGA1UEBhMCQ1Qx
CzAJBgNVBAgTAkJBMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNVBAoTA1VPQzEg
MB4GA1UECxMXVHJlYmFsbCBGaW5hbCBkZSBNYXNOZXIxDzANBgNVBANTB1VPQyBD
QTEPMA0GA1UEKRMGdGZtamNyMRswGQYJKoZIhvcNAQkBFgxrdXNlQHVvYy51ZHUw
HhcNMTYwNzI5MDgzNzAxWhcNMjYwNzI3MDgzNzAxWjCBoDELMAkGA1UEBhMCQ1Qx
CzAJBgNVBAgTAkJBMRIwEAYDVQQHEwlCYXJjZWxvbmExDDAKBgNVBAoTA1VPQzEg
MB4GA1UECxMXVHJlYmFsbCBGaW5hbCBkZSBNYXNOZXIxEjAQBgNVBANTCXZwbnVz
ZXIwNTEPMA0GA1UEKRMGdGZtamNyMRswGQYJKoZIhvcNAQkBFgxrdXNlQHVvYy51
ZHUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDCFjFOLEfUFqSbJH2E
fHrDGFlE4QcUrds4FEhJaZMKM92gP4bbRDfW8SubzeYK/dG/zQQM1slJm6ZYRDdZ
D89AosTrL8XQqBLJY2PkOfAZ8pnB95zZBeTBAQmkRXc7hekmbKZ6v1qwaH2YHpBO
Rbd1rh8dBXqii+O1viecdP7Yq1rl8X/AJ/1Qog8S/Km/C11dTnsH43GM1GHEYrEK
TDjKoqKn+OOEDH1voVCYtaVmR3H5JEXGuxzLLnHBoc6WKwt3Zmwdne6Oq81QCY/O
kL7QMQxksrOGLDa1Ab4ABQEoufgko/1AKUACLqOrpNfeJoIc21F5B+2lsr8Kwt7a
aODBAgMBAAGjggFqMIIBZjAJBgNVHRMEAjAAMC0GCWCGSAGG+EIBDQQgFh5FYXN5
LVJTQSBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFD8Vp8/ejHgaGQ08
GzLDwcYrCR5OMIHSBgNVHSMEgcowgceAFEUvyLtUmW+buVMqWC6V9yErKOeJoYGj
pIGgMIGdMQswCQYDVQQGEwJDVDELMAkGA1UECBMCQkExEjAQBgNVBAcTCUJhcmNl
bG9uYTEMMAoGA1UEChMDVU5DMSAwHgYDVQQLExdUcmViYWxsIEZpbmFsIGR1IE1h
c3RlcjEPMA0GA1UEAxMGVU5DIENBMQ8wDQYDVQQpEwZOZm1qY3IxGzAZBgkqhkiG
9w0BCQEWDGt1c2VAdW9jLmVkdYIJAMqknS9Dnr17MBMGA1UdJQQMMAoGCCsGAQUF
BwMCMAsGA1UdDwQEAwIHgDAUBgNVHREEDTALggl2cG51c2VyMDEwDQYJKoZIhvcN
AQELBQADggEBAG7yssbYwTAehoE1dX/S+5elGUbTwIQnPr+bmJKMxlhRRu4FgB53
d6o2yDtuNoPSdhvGA7zMkbvwzdlzqDwgcNq9FATi5GaL8Pj5M9MFJFhYRVF1L1Xd
fvA2Ej4b7OVyW6hAaP4VnE/cmx8Ojom3dVQiOs4E33wRU3cHBuTGU5M+6OvZH4B4
zhBDduHCUMYiI2GShn5FzJP14HtucudOHymK55oDvbh4n606syE/mSoJkG51ZBDk
QFeS/XSjOPPBbMhV7H4X/KX8Arqp3O4e1RaYF4r24YyNjFbwwWY1UEp5sI5hLwRm
Uz3dFeihJJNwJMrOmNgqkx3BKJ6vfv4sVIM=
-----END CERTIFICATE-----
```

```
root@Server51:/usr/share/easy-rsa/keys# cat vpnuser01.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC/jCCAeYCAQAwgaAxCzAJBgNVBAYTAkNUMQswCQYDVQQIEwJCQTESMBAGA1UE
BxMJQmFyY2Vsb25hMQwwCgYDVQQKEwNVTOMxIDAeBgNVBAsTF1RyZWJhbGwgRmlu
YWwgZGUgTWFzdGVyMRIwEAYDVQQDEwl2cG51c2VyMDExDzANBgNVBCkTBnRmbWpj
cjEbMBkGCSqGSIb3DQEJARYMa3VzZUB1b2MuZWR1MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAwhYxTixH1BakmyR9hHx6wxhZROEHFK3bOBRISWmTCjPd
oD+G2OQ31vEsG83mCv3Rv8OEDNbJSZumWEQ3WQ/PQKLE6y/FOKgSyWNj5DnwGfKZ
wfec2QXkwQEJpEV3O4XpJmymer9asGh9mB6QTkW3da4fHQV6oovjtb4nnHT+2Kta
5fF/wCf5UKIPEvypvwpdXU57B+NxjJRhxGKxCkw4yqKip/tDhAx5b6FQmLWlZkdx
+SRFxrscyy5xwaHOlisLd2ZsHZ3ujqvJUAmPzpC+ODEMZLKzhiw2pQG+AAUBKLn4
JKP9QClAAi6tK6TX3iaCHNtReQftpbK/CsLe2mtAwQIDAQABoBgwFgYJKoZIhvcN
AQkHMQkTB3RmbTIwMTYwDQYJKoZIhvcNAQELBQADggEBAAJ4nUwfEBERtDgfiLOQ
BPFpO4Fg+fQ8IymVrwV8gLQjmLTlkhh/JdJlWMIVT1rNPs7JzLNVbTwtxGz8Lxtq
DOgOIGu7jFCHHbW4rKHqzwH823VaQOSYfeZNeOi289DDhhukpZXlVtF7O58OdpRu
tM+MR7XuT6mFTYQN9VOYQ8wgiShQK8B3LNUQ5WM58TQpYbk+cvEMp5iPOeoNlu3d
+tomwWyIyYh79KZtfXdAl+uEYZBQi6yYUY99OVh/qGTkzwwFaKs1+a4jBo1XriTJ
WZWoDDOc3MIkrwjFAzAVGDYYCOq7GWscjl2NW7rURNOP2+zcum25fhv6U+KPVK+p
Q8E=
-----END CERTIFICATE REQUEST-----
```

```
root@Server51:/usr/share/easy-rsa/keys# cat vpnuser01.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDCFjFOLEfUFqSb
JH2EfHrDGFlE4QcUrds4FEhJaZMKM92gP4bbRDfW8SwbzeYK/dG/zQQM1slJm6ZY
RDdZD89AosTrL8XQqBLJY2PkOfAZ8pnB95zZBeTBAQmkRXc7hekmbKZ6v1qwaH2Y
HpBORbd1rh8dBXqii+O1viecdP7Yq1rl8X/AJ/lQog8S/Km/C11dTnsH43GM1GHE
YrEKTDjKoqKn+OOEDHlvoVCYtaVmR3H5JEXGuxzLLnHBoc6WKwt3Zmwdne6Oq8lQ
CY/OkL7QMQxksrOGLDalAb4ABQEoufgko/1AKUACLqOrpNfeJoIc21F5B+2lsr8K
wt7aaODBAgMBAAECggEBAL3nsxS3VQzbnvJCcSI6HnBYmbhAqon8Vvx3NAfI6lvY
RelvXOeaZzzEPBFOlLt6gUo3ktfxLYD9cHT7QmC9jF/FJAKvetHgMomk22/LlPf+
nZ3h5zGeh6almkaGxdSTAX9cXkTKiTUE+KboePBtXMYjukPOQaFcWVFSHzYCb/2V
cFdbH7OWROtHz1d/yyy7cRRbjqBG3ItC66q2yuVwDJiRRk8H3nXDU2kL/dxJjR+5
apa/8gkOT/sg2ijndfO8bqiXvong2UDeucTJAeByEn2ERlbJG/4FtAAkMlSkBw7O
2Jdwps7CeU6oxG2rOMnR4mTyLo/GIWM4wTasoLFaEXUCgYEA51zZiYETSt5hsMZB
t9mfWxmUE3nJqbubeM2KI5q7FC9A9EuvBD7uKVgbaWaKq4Ud/4dG/16gSlOVki+h
SCLN8O4UiIXH6z+ivjwHb9QCTU6kjCA15kz1hrOkGaalXnGfxG4xhUaBcDLc6TUn
cO4qhEUEkAA6+p95hiS2hdtajJ8CgYEA1sEqjZ81fu3KLDdgG419w9TQcQiB9zw1
gQNCg9yQ+KBbOu3D1/YT4GWEYeg9Fkp7ZtfAT/zpqW+17vQIN/YOAVmQZPlS887h
t6/eaHSTBc9eqcQoBzKepeLLftvmtYCrRsY5LfdTsh6KVaskdT7Nv8DJHcmp8/kZ
v/8+YF+/1p8CgYAqJAZXflQmQeUnTqUvuIrHDBylg3xQ1yQVV9K+c3N51LWPCa4C
Jvg4PZOYkJ3XafKx1VEAOJsXkGbabqSAwB4lH+arizqDxd59qe9s1f/pVtav0zoe
DYx3EOJdDbZ3QljobW3Fqbbv2cPVEmJxtl+2IeAX3oLfnWaEIXHBZdfTXwKBgB+O
VtBkmpnCGzkQEgE6c0Z5WP+i/mXz5PDGJ9nOaSD/fyhTk7mCIT2R7TftxjwmSae9
ADdAtJz/Gz63gRWoBDrSjFMqB7Rnq+cv4oB6OLfD1ucfObqFB6bcgoZrjaUR+Rj3
O6OzegrsTetOsHDB/72zeFn2LhD5g3Og5muG5kuFAoGAFXI5PSjMbTkIEVgzEOg+
p75b1Nfa+e3pCtrzQHfG8E4o3t69rX7wS19S5aXV2DUMFutk71CXK7vsCNboRKQj
WY5tz6vxstJOX2292b+3CNgaqTqxJi8hP/DQPOM5EfJnNNoNuiKe4f6+V3JARkDS
FsgOy1ufU2MZW/bxnYPMtWo=
-----END PRIVATE KEY-----
```

13.7. Arxiu de configuració de servidor

```
root@Server51:/etc/openvpn# cat server.conf
#################################################
# Sample OpenVPN 2.0 config file for            #
# multi-client server.                          #
#                                               #
# This file is for the server side              #
# of a many-clients <-> one-server              #
# OpenVPN configuration.                        #
#                                               #
# OpenVPN also supports                         #
# single-machine <-> single-machine             #
# configurations (See the Examples page         #
# on the web site for more info).               #
#                                               #
# This config should work on Windows            #
# or Linux/BSD systems.  Remember on            #
# Windows to quote pathnames and use            #
# double backslashes, e.g.:                     #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
#                                               #
# Comments are preceded with '#' or ';'         #
#################################################

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.  You will need to
# open up this port on your firewall.
###
port 11194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
```

```
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one.  On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt
cert tfmjcr.tk.crt
key tfmjcr.tk.key  # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
dh dh2048.pem
```

```
# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
###
server 10.18.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file.  If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface.  Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0.  Finally we
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients.  Leave this line commented
# out unless you are ethernet bridging.
###
;server-bridge 10.18.0.4 255.255.255.0 10.18.0.50 10.18.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses.  You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge
```

```
# Push routes to the client to allow it
# to reach other private subnets behind
# the server.  Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN.  This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients.  There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
```

```
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients.  See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.  CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
;client-to-client

# Uncomment this directive if multiple clients
```

```
# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120

# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
;cipher AES-128-CBC   # AES
;cipher DES-EDE3-CBC  # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nogroup
```

```
# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "\Program Files\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it.  Use one
# or the other (but not both).
;log         openvpn.log
;log-append  openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 6

# Silence repeating messages.  At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
###

plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so /etc/pam.d/openvpn
```

13.8. Arxiu de configuració de client

```
kuse@Ubuntu1401Base:/etc/openvpn$ cat client.ovpn
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
```

```
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
###
remote tfmjcr.tk 11194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
```

```
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
###
ca ca.crt
###
cert vpnuser01.crt
###
key vpnuser01.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server
```

```
# If a tls-auth key is used on the server
# then every client must also have the key.
tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20

auth-user-pass
# static-challenge "Enter Google Authenticator Code" 1

#Prevent the password file from being cached
auth-nocache
```

13.9. Arxius tallafocs Servers

```
root@Server02:/etc# cat iptables.conf
# Generated by iptables-save v1.4.21 on Thu Dec  1 19:48:27 2016
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.1.13:80
-A PREROUTING -p tcp -m tcp --dport 443 -j DNAT --to-destination 192.168.1.13:443
-A PREROUTING -p tcp -m tcp --dport 3306 -j DNAT --to-destination 192.168.1.14:3306
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Thu Dec  1 19:48:27 2016
# Generated by iptables-save v1.4.21 on Thu Dec  1 19:48:27 2016
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [4:552]
:OUTPUT ACCEPT [39:3576]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1702 -j ACCEPT
-A INPUT -j LOG
-A INPUT -j DROP
-A FORWARD -i eth1 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -o eth1 -j ACCEPT
-A OUTPUT -p udp -m udp --sport 1702 -j ACCEPT
COMMIT
# Completed on Thu Dec  1 19:48:27 2016
root@Server02:/etc#
```

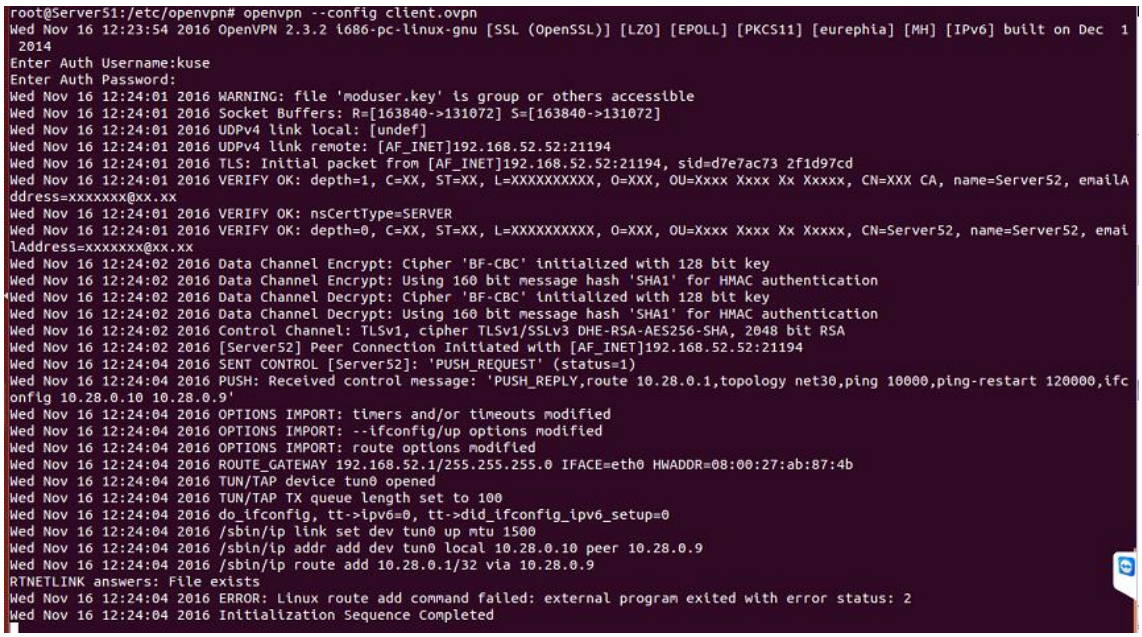
```
root@Server51:/etc# cat iptables.conf
# Generated by iptables-save v1.4.21 on Wed Oct 26 09:59:26 2016
*mangle
:PREROUTING ACCEPT [510:41979]
:INPUT ACCEPT [510:41979]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [374:35358]
:POSTROUTING ACCEPT [374:35358]
COMMIT
# Completed on Wed Oct 26 09:59:26 2016
# Generated by iptables-save v1.4.21 on Wed Oct 26 09:59:26 2016
*nat
:PREROUTING ACCEPT [11:835]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [2:84]
:POSTROUTING ACCEPT [2:84]
COMMIT
# Completed on Wed Oct 26 09:59:26 2016
# Generated by iptables-save v1.4.21 on Wed Oct 26 09:59:26 2016
*filter
:INPUT DROP [11:835]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [2:84]
:WHITELIST - [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m udp --dport 11194 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport 1751 -j ACCEPT
-A INPUT -i tun0 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 11194 -j LOG --log-prefix " ACCES A VPN NO PERMES "
-A FORWARD -i tun0 -j ACCEPT
-A FORWARD -i tun0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -o tun0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Oct 26 09:59:26 2016
```

```
root@Server52:/etc# cat iptables.conf
# Generated by iptables-save v1.4.21 on Thu Aug 18 09:17:33 2016
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.52.51/32 -i eth0 -p udp -m state --state NEW,ESTABLISHED -m udp --dport 21194 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport 1752 -j ACCEPT
-A INPUT -i tun0 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 11194 -j LOG --log-prefix " ACCES A VPN NO PERMES "
-A FORWARD -i tun0 -j ACCEPT
-A FORWARD -i tun0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth0 -o tun0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Thu Aug 18 09:17:33 2016
root@Server52:/etc#
```

13.10. Seqüencia establiment túnel Client-Server51

```
root@Ubuntu1401Base:/etc/openvpn# openvpn --config client.ovpn
Wed Nov 16 09:37:35 2016 OpenVPN 2.3.2 i686-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Dec  1 2014
Enter Auth Username:Agent01
Enter Auth Password:
Wed Nov 16 09:37:51 2016 Control Channel Authentication: using 'ta.key' as a OpenVPN static key file
Wed Nov 16 09:37:51 2016 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Nov 16 09:37:51 2016 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Nov 16 09:37:51 2016 Socket Buffers: R=[163840->131072] S=[163840->131072]
Wed Nov 16 09:37:51 2016 UDPv4 link local: [undef]
Wed Nov 16 09:37:51 2016 UDPv4 link remote: [AF_INET]88.2.209.101:11194
Wed Nov 16 09:37:51 2016 TLS: Initial packet from [AF_INET]88.2.209.101:11194, sid=0e8a1a79 8756c31d
Wed Nov 16 09:37:51 2016 VERIFY OK: depth=1, C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=UOC CA, name=tfmjcr, emailAddress=kuse@uoc.edu
Wed Nov 16 09:37:51 2016 VERIFY OK: nsCertType=SERVER
Wed Nov 16 09:37:51 2016 VERIFY OK: depth=0, C=CT, ST=BA, L=Barcelona, O=UOC, OU=Treball Final de Master, CN=tfmjcr.tk, name=tfmjcr, emailAddress=kuse@uoc.e
du
Wed Nov 16 09:37:53 2016 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Nov 16 09:37:53 2016 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Nov 16 09:37:53 2016 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed Nov 16 09:37:53 2016 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed Nov 16 09:37:53 2016 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Wed Nov 16 09:37:53 2016 [tfmjcr.tk] Peer Connection Initiated with [AF_INET]88.2.209.101:11194
Wed Nov 16 09:37:55 2016 SENT CONTROL [tfmjcr.tk]: 'PUSH_REQUEST' (status=1)
Wed Nov 16 09:37:55 2016 PUSH: Received control message: 'PUSH_REPLY,route 10.18.0.1,topology net30,ping 10,ping-restart 120,ifconfig 10.18.0.14 10.18.0.13'
Wed Nov 16 09:37:55 2016 OPTIONS IMPORT: timers and/or timeouts modified
Wed Nov 16 09:37:55 2016 OPTIONS IMPORT: --ifconfig/up options modified
Wed Nov 16 09:37:55 2016 OPTIONS IMPORT: route options modified
Wed Nov 16 09:37:55 2016 ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:c9:fb:7a
Wed Nov 16 09:37:55 2016 TUN/TAP device tun0 opened
Wed Nov 16 09:37:55 2016 TUN/TAP TX queue length set to 100
Wed Nov 16 09:37:55 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Wed Nov 16 09:37:55 2016 /sbin/ip link set dev tun0 up mtu 1500
Wed Nov 16 09:37:55 2016 /sbin/ip addr add dev tun0 local 10.18.0.14 peer 10.18.0.13
Wed Nov 16 09:37:56 2016 /sbin/ip route add 10.18.0.1/32 via 10.18.0.13
Wed Nov 16 09:37:56 2016 Initialization Sequence Completed
```

13.11. Seqüencia establiment túnel Server51-Server52



13.12. Arxiu configuració Mysql al Server52

```
root@Server52:/etc/mysql# cat my.cnf
#
# The MySQL database server configuration file.
#
# You can copy this to one of:
# - "/etc/mysql/my.cnf" to set global options,
# - "~/.my.cnf" to set user-specific options.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html

# This will be passed to all mysql clients
# It has been reported that passwords should be enclosed with ticks/quotes
# escpecially if they contain "#" chars...
# Remember to edit /etc/mysql/debian.cnf when changing the socket location.
[client]
port            = 33306
socket          = /var/run/mysqld/mysqld.sock

# Here is entries for some specific programs
# The following values assume you have at least 32M ram

# This was formally known as [safe_mysqld]. Both versions are currently parsed.
[mysqld_safe]
socket          = /var/run/mysqld/mysqld.sock
nice            = 0

[mysqld]
#
# * Basic Settings
#
user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 33306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 10.28.0.1
#
# * Fine Tuning
```

```
key_buffer              = 16M
max_allowed_packet      = 16M
thread_stack            = 192K
thread_cache_size       = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
myisam-recover         = BACKUP
#max_connections        = 100
#table_cache            = 64
#thread_concurrency     = 10
#
# * Query Cache Configuration
#
query_cache_limit       = 1M
query_cache_size        = 16M
#
# * Logging and Replication
#
# Both location gets rotated by the cronjob.
# Be aware that this log type is a performance killer.
# As of 5.1 you can enable the log at runtime!
#general_log_file        = /var/log/mysql/mysql.log
#general_log             = 1
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
#
# Here you can see queries with especially long duration
#log_slow_queries       = /var/log/mysql/mysql-slow.log
#long_query_time = 2
#log-queries-not-using-indexes
#
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see README.Debian about
#       other settings you may need to change.
#server-id              = 1
#log_bin                        = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
max_binlog_size         = 100M
#binlog_do_db           = include_database_name
#binlog_ignore_db       = include_database_name
#
# * InnoDB
#
# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
# Read the manual for more InnoDB related options. There are many!
#
```

```
# * Security Features
#
# Read the manual, too, if you want chroot!
# chroot = /var/lib/mysql/
#
# For generating SSL certificates I recommend the OpenSSL GUI "tinyca".
#
# ssl-ca=/etc/mysql/cacert.pem
# ssl-cert=/etc/mysql/server-cert.pem
# ssl-key=/etc/mysql/server-key.pem



[mysqldump]
quick
quote-names
max_allowed_packet      = 16M

[mysql]
#no-auto-rehash # faster start of mysql but no tab completition

[isamchk]
key_buffer              = 16M

#
# * IMPORTANT: Additional settings that can override those from this file!
#   The files must end with '.cnf', otherwise they'll be ignored.
#
!includedir /etc/mysql/conf.d/
```

13.13. Arxiu configuració Moodle al Server51

```
kuse@Server51:/var/www/html/moodle$ cat config.php
<?php  // Moodle configuration file


unset($CFG);

global $CFG;

$CFG = new stdClass();


$CFG->dbtype    = 'mysqli';

$CFG->dblibrary = 'native';

$CFG->dbhost    = '10.28.0.1';

$CFG->dbname    = 'moodle';

$CFG->dbuser    = 'modsql';

$CFG->dbpass    = '[redacted]';

$CFG->prefix    = 'mdl_';

$CFG->dboptions = array (

  'dbpersist' => 0,

  'dbport' => 33306,

  'dbsocket' => '',

);


$CFG->wwwroot   = 'http://10.18.0.1:8121';

$CFG->dataroot  = '/var/moodledata';

$CFG->admin     = 'admin';


$CFG->directorypermissions = 0777;


require_once(dirname(__FILE__) . '/lib/setup.php');


// There is no php closing tag in this file,

// it is intentional because it prevents trailing whitespace problems!
```

13.14. Arxius configuració apache2 al Server51

```
kuse@Server51:/etc/apache2/sites-enabled$ sudo cat 000-default.conf
<VirtualHost 10.18.0.1:8121>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
###
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/moodle/

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
kuse@Server51:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf
### NameVirtualHost 127.0.0.1:52121
Listen 10.18.0.1:8121

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

13.15. Arxius configuració Backup al Server52

```
  GNU nano 2.2.6                File: /tmp/crontab.YHfMzx/crontab

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 2 * * * mount 10.0.0.1:SOS /mnt/SOS
############## * * * * * /usr/bin/mysqldump -uroot -pMysql14 --opt moodle > /mnt/SOS/moodle_`date +\%Y\%m\%d_\%H\%M`.sql
30 4 * * * /usr/bin/mysqldump --defaults-extra-file=/etc/mysqldump.cnf moodle > /mnt/SOS/moodle_`date +\%Y\%m\%d_\%H\%M`.sql
```

```
root@Server52:/etc# cat mysqldump.cnf
[mysqldump]
host = localhost
port = 33306
user = SOSUsr
password = [redacted]
```

13.16. Arxius configuració MHN Host

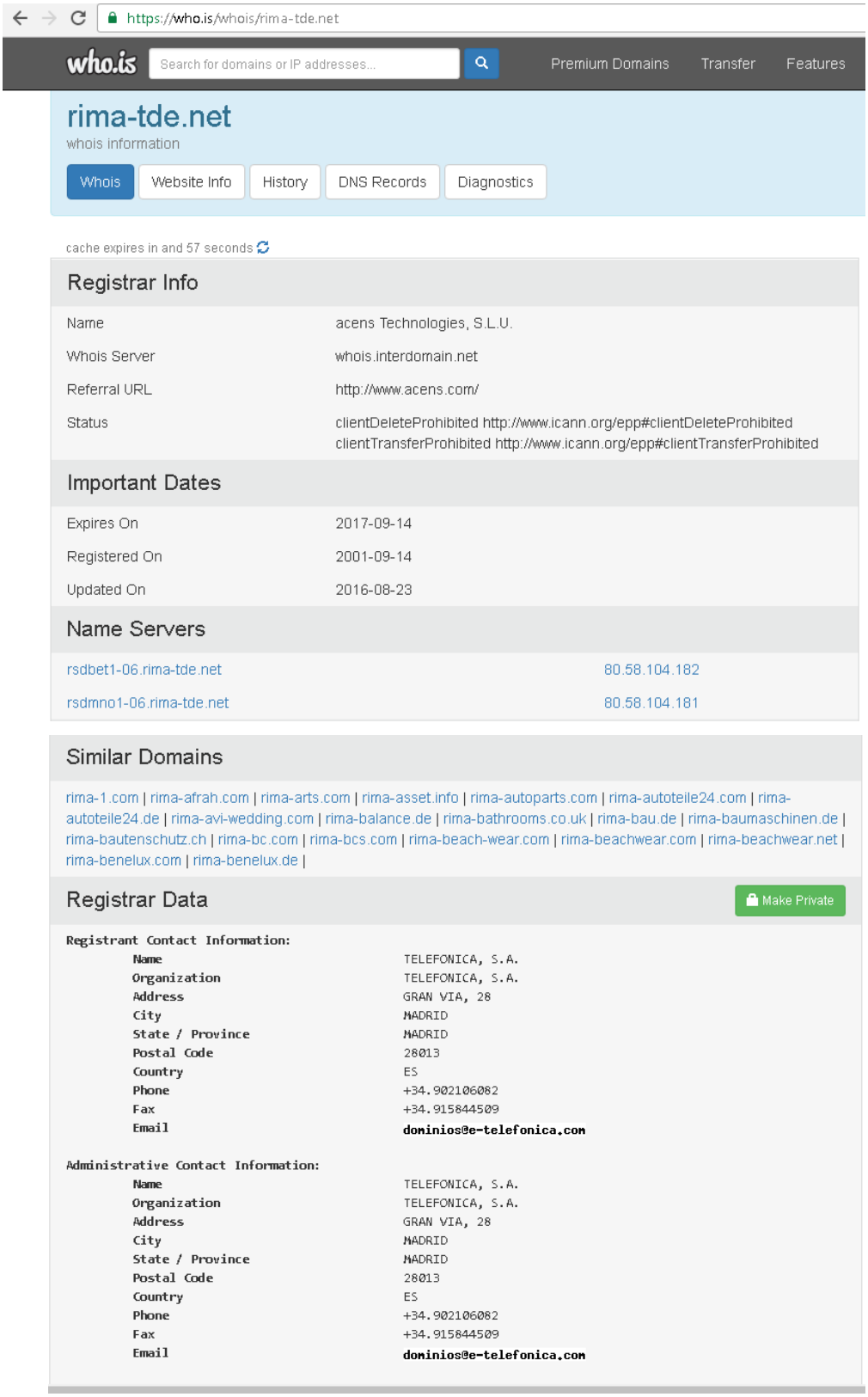
```
root@SRV10:/etc/nginx/sites-available# cat honeymap-https
map $http_upgrade $connection_upgrade {
    default upgrade;
    ''      close;
}

server {
    listen   1443 ssl spdy ;
    ssl_certificate /etc/ssl/private/tfmjcr.tk.crt;
    ssl_certificate_key /etc/ssl/private/tfmjcr.tk.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5;
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    add_header Strict-Transport-Security "max-age=31536000";
    ssl_dhparam /etc/ssl/certs/dhparam.pem;

    root /opt/honeymap/client;
    index index.html index.htm;

    server_name tfmjcr.tk;

    location / {
        try_files $uri $uri/ /index.html;
    }

    location /data/ {
        proxy_pass http://localhost:13000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
    }
}
root@SRV10:/etc/nginx/sites-available#
```

```
root@SRV10:/etc/nginx/sites-available# cat mhn-https
server {
    listen               1443 ssl spdy;
    server_name          tfmjcr.tk;

    ssl_certificate      /etc/ssl/private/tfmjcr.tk.crt;
    ssl_certificate_key /etc/ssl/private/tfmjcr.tk.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5;
    ssl_prefer_server_ciphers on;
    ssl_session_cache shared:SSL:10m;
    add_header Strict-Transport-Security "max-age=31536000";
    ssl_dhparam /etc/ssl/certs/dhparam.pem;

    if ($ssl_protocol = "") {
        rewrite ^ https://$host$request_uri? permanent;
    }

    location / {
        try_files $uri @mhnserver;
    }

    root /opt/www;

    location @mhnserver {
      include uwsgi_params;
      uwsgi_pass unix:/tmp/uwsgi.sock;
    }

    location  /static {
      alias /opt/mhn/server/mhn/static;
    }
}
root@SRV10:/etc/nginx/sites-available#
```

```
root@SRV10:/opt/mhn/server# cat config.py
"""
Template to create config.py file.
Do not add 'config.py' to SCM.
"""

import os
from celery.schedules import crontab


_basedir = os.path.abspath(os.path.dirname(__file__))

MHN_SERVER_HOME = _basedir

# Local settings.
DEBUG = False
SECRET_KEY = 'Ih9VCrSVMRjicOxnQ40ZP9XxBPmANAWK'
SUPERUSER_EMAIL = 'kuse@uoc.edu'
SUPERUSER_PASSWORD = [redacted]
SERVER_BASE_URL = 'https://tfmjcr.tk'
HONEYMAP_URL = 'https://tfmjcr.tk:13000'
DEPLOY_KEY = 'HnpdhcuM'
LOG_FILE_PATH = '/var/log/mhn/mhn.log'

MAIL_SERVER = 'localhost'
MAIL_PORT = 25
MAIL_USE_TLS = True
MAIL_USE_SSL = True
MAIL_USERNAME = 'kuse'
MAIL_PASSWORD = ''
DEFAULT_MAIL_SENDER = ''
MAIL_DEBUG = DEBUG

# Other settings.
FEED_AUTH_REQUIRED = False
SQLALCHEMY_DATABASE_URI = 'sqlite:///' + os.path.join(_basedir, 'mhn.db')
SECURITY_PASSWORD_HASH = 'bcrypt'
SECURITY_PASSWORD_SALT = SECRET_KEY
SECURITY_LOGIN_URL = '/ui/login/'
BROKER_URL = 'redis://localhost:6379'
CELERY_RESULT_BACKEND = BROKER_URL
RENDERED_RULES_PATH = os.path.join(_basedir, 'mhn/static/mhn.rules')
CELERYBEAT_SCHEDULE = {
    'fetch-emerging-rules': {
            'task': 'mhn.tasks.rules.fetch_sources',
            'schedule': crontab(hour=12),
            'args': ()
    }
}
SNORT_RULES_SOURCE = {
    'name': 'Emerging Threats',
    'uri': 'http://rules.emergingthreats.net/open/snort-2.9.0/emerging.rules.tar.gz'
}
HONEYPOT_CHANNELS = {
    'dionaea': [
        'mwbinary.dionaea.sensorunique',
        'dionaea.capture',
        'dionaea.capture.anon',
        'dionaea.caputres',
        'dionaea.connections'
    ],
    'conpot': ['conpot.events'],
    'snort': ['snort.alerts'],
    'kippo': ['kippo.sessions'],
    'cowrie': ['cowrie.sessions'],
    'thug': ['thug.files', 'thug.events'],
    'glastopf': ['glastopf.files', 'glastopf.events'],
    'amun': ['amun.events'],
    'wordpot': ['wordpot.events'],
    'shockpot': ['shockpot.events'],
    'p0f': ['p0f.events'],
    'suricata': ['suricata.events'],
    'elastichoney': ['elastichoney.events'],
}
root@SRV10:/opt/mhn/server#
```


kuse@Server14:/usr/local/share/ca-certificates$ cat tfmjcr.tk.crt
-----BEGIN CERTIFICATE-----
MIIFqTCCA5GgAwIBAgIJAJUwDscjT8weMA0GCSqGSIb3DQEBCwUAMGsxCzAJBgNV
BAYTAmN0MRIwEAYDVQQIDAlDYXRhbHVueWExDDAKBgNVBAoMA1VPQzEMMAoGA1UE
CwwDVEZNMQ8wDQYDVQQDDAZ0Zm1qY3IxGzAZBgkqhkiG9w0BCQEWDGt1c2VAdW9j
LmVkdTAeFw0xNjA3MTgxMDQwMTdaFw0xNzA3MTgxMDQwMTdaMGsxCzAJBgNVBAYT
AmN0MRIwEAYDVQQIDAlDYXRhbHVueWExDDAKBgNVBAoMA1VPQzEMMAoGA1UECwwD
VEZNMQ8wDQYDVQQDDAZ0Zm1qY3IxGzAZBgkqhkiG9w0BCQEWDGt1c2VAdW9jLmVk
dTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKoHbNTJMeyQ1PtxHDX8
yrb8M47RxsNswpQLG8yo9DlDFupsA+3ycQhrQjVw+eaIm9wsKSvBs48MX6wHgALQ
VaXPEvwtDBSPSi2KF9UHar9SJsSXr1z4qLcc5EnEkrvl99xsfOSd1LkioFTBmbM+
+5iEvzh5csIUb/pG0CKh93BUmFJ62MA1jG6pZzc0/NYp9piACrV/YVQ2h3133Pye
b/bgz5l+PfbRpC/rVxuGlD533LwWOuXwl7JqeFPLFKZJsLJ2rJEuMB0/4Q+j8MgZ
9GVdV+aMD/5zHYBb9vfhUmqD3xq6mJ4j1DfUj9I+nwkk80R6ZXxIMXGDXoByL4rl
ILX2klQM7EKiijt26UA8tdvsjSgOr1RTG13zYY7PMO1BLUEc3DO7RcSgtnAO9Cos
wg/HRGMPVp2DL0ZFoj9otiKlLeXlbsIbZG/nbp0fD5tTgftWQq4fBf4/sUurT0Jk
VX2kwo1FqZPoz3hzZW3y7DtmF5XULLd5YoV9KSriZHCBrbIHv21dqbYrgrIWMrfV
Y5iN0UzZdDpMM6gyKtfVT0Y4KMxH6Mq3EFSuSbHGafzJWZn/HR1zfMQ2wuNECWRI
lzX9QwLn6aFvNEmOrubWyNBz2VplanfLHB3JLP/b8OwT8oXUtPrFey5ThurTDMsK
zw2JrpMF7+acQps7F7oXlhG1AgMBAAGjUDBOMB0GA1UdDgQWBBSeL2dOKx4toDCZ
S3c6NSrfrku2sTAfBgNVHSMEGDAWgBSeL2dOKx4toDCZS3c6NSrfrku2sTAMBgNV
HRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4ICAQAkFYHBMKVqTI5FBx0Luda2H+Rd
wPoPQrCWTHEORagoVwWwp0qCfU0qhIkbwlgQJDDlU8NziFGCzyB3buE7IBsE0LVC
S6Ju1Umvu9sozb+KyFF9UcB6Mla3dMxg66a2WaGow/xmycyb5ZyYDblYKLwMwZdQ
HkJwBy0mjRNjL8Inx2StPzvGdl048SNhO+0KWu8n/1VzVccVisYKRbW33XcjD0uO
Kw0CpSkpZ1E4C52malpsV52yfLfAVy3rxqq7yMNV/2sX+gZApqnXpmkJ9C8Vz1S3
N/6UHszy4m/bNO6LOovUkLFS73pb7QxpX+cgDToPVXmk1REmrZJ2wWZFXHq2qIRt
o0vPGXgk7jXp9nM2T/5IGMREtDV1WR0rS6SJLx72jt1w8B6kAgTm4eEQtYJC8UYW
gF9gA1MLrQEvLn79V3u5cLeSuUFkb4Xt4k+AhHGzDFx4c26xiCxpxe3Ohc6WQhTC
0aTzfWMXka0/Wm9DjYAM9P3Wi/9dzHMab9Ho4rIfjq8zUEsevUqPqI1whfVNiE2r
1QYo1+lsxKse3cdUCay+9p4rjeNTd6EdUxPvq61BY3hkKt/CmyrcCNWpccWYxX7t
8CJfj5vn+k4pBVll9+VZpp33jFwEUcvLm6iEqvGD9Qn3H9POehvdzpesKHXJytGm
QLmrddHxaDt77nFq0g==
-----END CERTIFICATE-----
kuse@Server14:/usr/local/share/ca-certificates$

13.17. Consulta servei WhoIS per a test de penetració



13.18. Consulta NMap Avançada

Nmap scan report for 101.red-88-2-209.staticip.rima-tde.net (88.2.209.101)

Host is up (0.017s latency).

Not shown: 97 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

3306/tcp open mysql

| mysql-brute:

| Accounts:

| root:root - Valid credentials

| guest:guest - Valid credentials

| web:web - Valid credentials

| administrator:administrator - Valid credentials

| user:user - Valid credentials

| netadmin:netadmin - Valid credentials

| webadmin:webadmin - Valid credentials

| sysadmin:sysadmin - Valid credentials

| admin:admin - Valid credentials

| test:test - Valid credentials

|_ Statistics: Performed 17 guesses in 18 seconds, average tps: 0

| mysql-databases:

|_ information_schema

| mysql-empty-password:

| anonymous account has empty password

|_ root account has empty password

| mysql-enum:

| Valid usernames:

| root:<empty> - Valid credentials

| netadmin:<empty> - Valid credentials

| guest:<empty> - Valid credentials

| user:<empty> - Valid credentials

| web:<empty> - Valid credentials

| sysadmin:<empty> - Valid credentials

| administrator:<empty> - Valid credentials

| webadmin:<empty> - Valid credentials

| admin:<empty> - Valid credentials

| test:<empty> - Valid credentials

|_ Statistics: Performed 10 guesses in 18 seconds, average tps: 0

| mysql-info:

| Protocol: 53

| Version: .0.54

| Thread ID: 1729232896

| Capabilities flags: 41516

| Some Capabilities: LongColumnFlag, Speaks41ProtocolNew, Support41Auth, SupportsCompression, ConnectWithDatabase, SupportsTransactions

| Status: Autocommit

|_ Salt: aaaaaaaa

| mysql-vuln-cve2012-2122:

| VULNERABLE:

| Authentication bypass in MySQL servers.

| State: VULNERABLE (Exploitable)

| IDs: CVE:CVE-2012-2122

| When a user connects to MariaDB/MySQL, a token (SHA

| over a password and a random scramble string) is calculated and compared

| with the expected value. Because of incorrect casting, it might've

| happened that the token and the expected value were considered equal,

| even if the memcmp() returned a non-zero value. In this case

| MySQL/MariaDB would think that the password is correct, even while it is

| not. Because the protocol uses random strings, the probability of

| hitting this bug is about 1/256.

| Which means, if one knows a user name to connect (and "root" almost

| always exists), she can connect using *any* password by repeating

| connection attempts. ~300 attempts takes only a fraction of second, so

| basically account password protection is as good as nonexistent.

|

| Disclosure date: 2012-06-9

| Extra information:

| Server granted access at iteration #1500

|

| References:

| https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql

| http://seclists.org/oss-sec/2012/q2/493

|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122

Nmap done: 1 IP address (1 host up) scanned in 41.76 seconds

13.19. Consulta Nessus estàndard

Plugin ID,CVE,CVSS,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output
10287,"","","None","88.2.209.101","udp","0","Traceroute Information","It was possible to obtain traceroute information.","Makes a traceroute to the remote host.","n/a","","For your information, here is the traceroute from to 88.2.209.101 :

xx.xxx.x.x.xx
172.254.0.102
?

10302","","","None","88.2.209.101","tcp","80","Web Server robots.txt Information Disclosure","The remote web server contains a 'robots.txt' file.","The remote host contains a file named 'robots.txt' that is intended to
prevent web 'robots' from visiting certain directories in a website for
maintenance or indexing purposes. A malicious user may also be able to
use the contents of this file to learn of sensitive documents or
directories on the affected site and either retrieve them directly or
target them for other attacks.","Review the contents of the site's robots.txt file, use Robots META tags
instead of entries in the robots.txt file, and/or adjust the web
server's access controls to limit access to sensitive
material.","http://www.robotstxt.org/wc/exclusion.html","Contents of robots.txt :

User-agent: *
Disallow:/
Disallow:.motdepas.txt

10302","","","None","88.2.209.101","tcp","443","Web Server robots.txt Information Disclosure","The remote web server contains a 'robots.txt' file.","The remote host contains a file named 'robots.txt' that is intended to
prevent web 'robots' from visiting certain directories in a website for
maintenance or indexing purposes. A malicious user may also be able to
use the contents of this file to learn of sensitive documents or
directories on the affected site and either retrieve them directly or
target them for other attacks.","Review the contents of the site's robots.txt file, use Robots META tags
instead of entries in the robots.txt file, and/or adjust the web
server's access controls to limit access to sensitive
material.","http://www.robotstxt.org/wc/exclusion.html","Contents of robots.txt :

User-agent: *
Disallow:/
Disallow:.motdepas.txt

10719","","","None","88.2.209.101","tcp","3306","MySQL Server Detection","A database server is listening on the remote port.","The remote host is running MySQL, an open source database server.","n/a","","
Version : 5.0.54
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT

Server Capabilities :
CLIENT_LONG_FLAG (Get all column flags)
CLIENT_CONNECT_WITH_DB (One can specify db on connect)
CLIENT_COMPRESS (Can use compression protocol)
CLIENT_PROTOCOL_41 (New 4.1 protocol)
CLIENT_TRANSACTIONS (Client knows about transactions)
CLIENT_SECURE_CONNECTION (New 4.1 authentication)

11153","","","None","88.2.209.101","tcp","3306","Service Detection (HELP Request)","The remote service could be identified.","It was possible to identify the remote service by its banner or by
looking at the error message it sends when it receives a 'HELP'
request.","n/a","","A MySQL server is running on this port."
11219,"","","None","88.2.209.101","tcp","443","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans
against broken services, but they might cause problems for less robust
firewalls and also leave unclosed connections on the remote target, if
the network is loaded.","Protect your target with an IP filter.","","Port 443/tcp was found to be open"
11219,"","","None","88.2.209.101","tcp","80","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans
against broken services, but they might cause problems for less robust
firewalls and also leave unclosed connections on the remote target, if
the network is loaded.","Protect your target with an IP filter.","","Port 80/tcp was found to be open"
11219,"","","None","88.2.209.101","tcp","3306","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably
quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans
against broken services, but they might cause problems for less robust
firewalls and also leave unclosed connections on the remote target, if
the network is loaded.","Protect your target with an IP filter.","","Port 3306/tcp was found to be open"
11936,"","","None","88.2.209.101","tcp","0","OS Identification","It is possible to guess the remote operating system.","Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP,
SNMP, etc.), it is possible to guess the name of the remote operating
system in use. It is also possible sometimes to guess the version of
the operating system.","n/a","","

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6"
12053,"","","None","88.2.209.101","tcp","0","Host Fully Qualified Domain Name (FQDN) Resolution","It was possible to resolve the name of the remote host.","Nessus was able to resolve the fully qualified domain name (FQDN) of
the remote host.","n/a","","
88.2.209.101 resolves as tfmjcr.tk.

19506","","","None","88.2.209.101","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","This plugin displays, for each tested host, information about the
scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management
  checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.","n/a","","Information about this scan :

Nessus version : 6.9.1
Plugin feed version : 201612012115
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : x.x.x.x
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None

CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/12/2 13:20 Romance Standard Time
Scan duration : 733 sec

22964","","","None","88.2.209.101","tcp","80","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","A web server is running on this port."
22964,"","","None","88.2.209.101","tcp","443","Service Detection","The remote service could be identified.","Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.","n/a","","A web server is running on this port."
24260,"","","None","88.2.209.101","tcp","80","HyperText Transfer Protocol (HTTP) Information","Some information about the remote HTTP configuration can be extracted.","This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.","n/a","","
Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, GET, HEAD, POST
Headers :

Connection: close
Content-Length: 1472

24260","","","None","88.2.209.101","tcp","443","HyperText Transfer Protocol (HTTP) Information","Some information about the remote HTTP configuration can be extracted.","This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.","n/a","","
Protocol version : HTTP/1.0
SSL : no

Keep-Alive : no
Options allowed : OPTIONS, GET, HEAD, POST
Headers :

Connection: close
Content-Length: 1472

25220","","","None","88.2.209.101","tcp","0","TCP/IP Timestamps Supported","The remote service implements TCP timestamps.","The remote host implements TCP timestamps, as defined by RFC1323. A
side effect of this feature is that the uptime of the remote host can
sometimes be computed.","n/a","http://www.ietf.org/rfc/rfc1323.txt",""
43111","","","None","88.2.209.101","tcp","80","HTTP Methods Allowed (per directory)","This plugin determines which HTTP methods are allowed on various CGI
directories.","By calling the OPTIONS method, it is possible to determine which HTTP
methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough
tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and
considers them as unsupported if it receives a response code of 400,
403, 405, or 501.

Note that the plugin output is only informational and does not
necessarily indicate the presence of any security vulnerabilities.","n/a","","Based on the response to an OPTIONS request :

- HTTP methods GET HEAD POST OPTIONS are allowed on :

/

43111","","","None","88.2.209.101","tcp","443","HTTP Methods Allowed (per directory)","This plugin determines which HTTP methods are allowed on various CGI
directories.","By calling the OPTIONS method, it is possible to determine which HTTP
methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough
tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and
considers them as unsupported if it receives a response code of 400,
403, 405, or 501.

Note that the plugin output is only informational and does not
necessarily indicate the presence of any security vulnerabilities.","n/a","","Based on the response
to an OPTIONS request :

- HTTP methods GET HEAD POST OPTIONS are allowed on :

/

45590","","","None","88.2.209.101","tcp","0","Common Platform Enumeration (CPE)","It is
possible to enumerate CPE names that matched on the remote
system.","By using information obtained from a Nessus scan, this plugin reports
CPE (Common Platform Enumeration) matches for various hardware and
software products found on a host.

Note that if an official CPE is not available for the product, this
plugin computes the best possible CPE based on the information
available from the scan.","n/a","http://cpe.mitre.org/
https://nvd.nist.gov/cpe.cfm","
The remote operating system matched the following CPE :

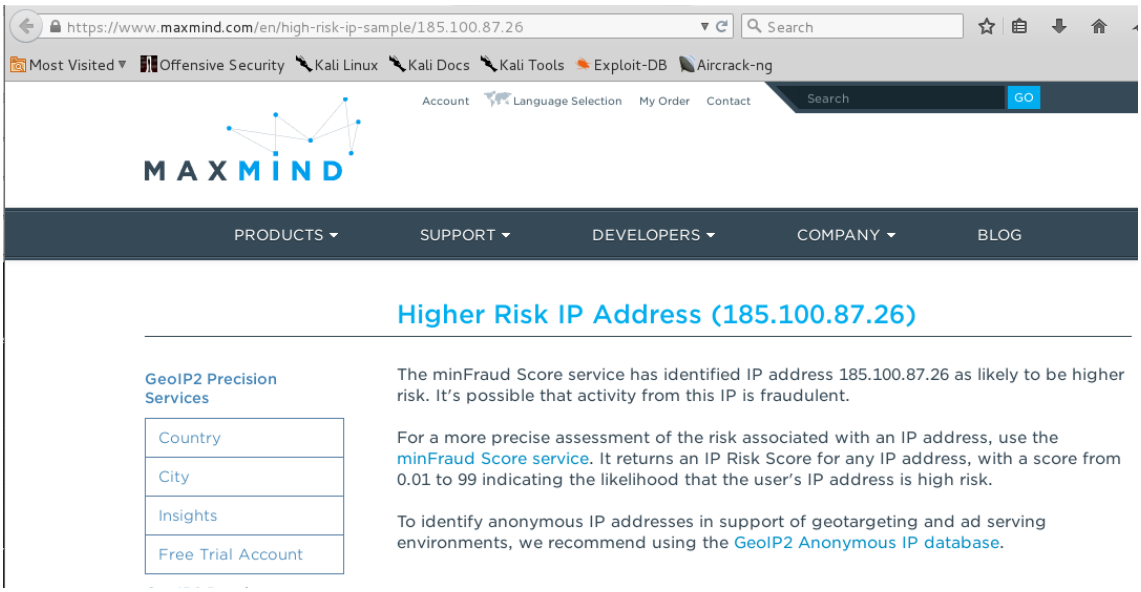
cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:mysql:mysql:5.0.54 -> MySQL5.0.54

54615","","","None","88.2.209.101","tcp","0","Device Type","It is possible to guess the remote
device type.","Based on the remote operating system, it is possible to determine
what the remote system type is (eg: a printer, router, general-purpose
computer, etc).","n/a","","Remote device type : general-purpose
Confidence level : 65

13.20. Control de perillositat segons ip



i Tor and The Dark Net: Remain Anonymous and Evade NSA Spying (01/05/2016). IpSec Tor. [Llibre físic]. Capítol 2 [data de consulta: octubre/novembre 2016].
ii newzzniper.com (28/02/2016). https://newzzniper.com/index.php/2016/02/28/la-verdad-sobre-la-internet-profunda-o-deep-web/. [en línia]. Article [data de consulta: octubre/novembre 2016].
iii OpenVPN (2002-2016). Your private path to access network resources and services securely [en línia] http://openvpn.net [data de consulta: tardor 2016].
iv cisco.com (21/08/2013). SSL Introduction with Sample Transaction and Packet Exchange http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-socket-layer-ssl/116181-technote-product-00.html.[en línia]. Article [data de consulta: octubre/novembre 2016].
v sans.org (2004) OpenVPN and the SSL VPN Revolution https://www.sans.org/reading-room/whitepapers/vpns/openvpn-ssl-vpn-revolution-1459. [en línia]. Article [data de consulta: octubre/novembre 2016].
vi opencms.org (2016).OpenCms 7 server installation http://www.opencms.org/en/development/installation/server.html. [en línia]. Guia [data de consulta: octubre/novembre 2016]
vii mybb.com (2016). Forum software everyone can Love. https://mybb.com/. [en línia] Guia 16 [data de consulta: octubre 2016]
viii CCN-CERT (setembre 2016). Riesgos de uso de whatsapp. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html. [en línia]. Article IA-21/16 [data de consulta: octubre 2016]
ix moodle.org (2016). Acerca de Moodle https://docs.moodle.org/all/es/Acerca_de_Moodle [en línia]. Fitxa de producte [data de consulta: octubre/novembre 2016].
x Mohssen Mohammed, Habib-ur Rehman (01/12/2015). Honeypots and Routers, Collcting Internet Attacks. CRC Press. [llibre físic]. Varis [data de consulta: tardor 2016].
xi LAP Lambert Academic Publishing (13/10/2015). Incorporating Additional Intelligence Into The Client Honeypot, Roza Honarbakhsh. Lambert Publishing. [llibre físic].]. Varis [data de consulta: tardor 2016].
xii redmine.honeynet.org (2006-2013). hpfeeds . https://redmine.honeynet.org/projects/hpfeeds/wiki. [en línia]. Guia [data de consulta: novembre 2016]
xiii splunk.com (2005-2016). What Is Splunk? https://www.splunk.com. [en línia] Fitxa producte [data de consulta: tardor 2016]
xiv Jason Trost (2016). threatstream/mhn-splunk. https://github.com/threatstream/mhn-splunk. [en línia]. Guia [data de consulta: tardor 2016]

xv hussainweb.me (2014). Install Ubuntu Server 14.04+ on VirtualBox. http://hussainweb.me/install-ubuntu-server-14-04-virtualbox/. [en línia] Guia d'instal·lació. [data de consulta: tardor 2016]
xvi movistar.es (-).Wireless ADSL Router RTA01N User´s Manual. http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/modem-router-inalambricos-/. [en línia] Guia d'instal·lació. [data de consulta: tardor 2016]
xvii ubuntu.com (2015). IptablesHowTo. https://help.ubuntu.com/community/IptablesHowTo. -/. [en línia] Guia d'instal·lació. [data de consulta: tardor 2016]
xviii ubuntu.com (16/10/2015). https://help.ubuntu.com/community/VirtualBox/Installation. -/. [en línia] Guia d'instal·lació. [data de consulta: tardor 2016]
xix Sharon Campbell (28/01/2015). How To Set Up an OpenVPN Server on Ubuntu 14.04. https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-14-04. -/. [en línia] Guia d'instal•lació. [data de consulta: tardor 2016]
xx moodle.org. Step-by-step Installation Guide for Ubuntu (20/01/2015) https://docs.moodle.org/26/en/Step-by-step_Installation_Guide_for_Ubuntu. [en línia] Guia d'instal•lació. [data de consulta: tardor 2016]
xxi Paul White (004/12/2013). How To Set Up an Artillery Honeypot on an Ubuntu VPS. https://www.digitalocean.com/community/tutorials/how-to-set-up-an-artillery-honeypot-on-an-ubuntu-vps. Guia d'instal•lació. [data de consulta: tardor 2016]
xxii Splunk.com (2005-2016). Admin Manual. https://docs.splunk.com/Documentation/Splunk/6.5.1/Admin/ConfigureSplunktostartatboottime. Guia d'instal•lació. [data de consulta: tardor 2016]
xxiiiGordon Lyon (2008-2016). Nmap Network Scanning. https://svn.nmap.org/nmap/nmap-service-probes. [en línia]. Guia [data de consulta: tardor 2016]