Ús de xarxes de Honeypots en la informàtica forense

Treball final de carrera

Enginyeria Tècnica en Informàtica de Sistemes

Autor: Sergi Hernando Terrer

Consultor: José Manuel Castillo Pedrosa

Juny 2016

FITXA DEL TREBALL FINAL

Títol del treball:	Ús de xarxes de Honeypots en la informàtica forense
Nom de l'autor:	Sergi Hernando Terrer
Nom del consultor:	José Manuel Castillo Pedrosa
Data de lliurament (mm/aaaa):	*06/2016*
Àrea del Treball Final:	Administració de Xarxes i Sistemes Operatius
Titulació:	Enginyeria Tècnica en Informàtica de Sistemes (ETIS)

Resum del Treball:

Des de que es va iniciar la comunicació digital s'ha volgut mantenir els sistemes tecnològics i la informació que contenen protegits d'accessos no permesos. Per altra banda, múltiples persones i organitzacions han intentat d'alguna manera accedir a aquests sistemes i informació, per fins personals, econòmics o per simple diversió.

Existeix una lluita constant per mantenir protegits els sistemes i la informació, i la informàtica forense ens ajuda un cop comesa la intrusió, a reunir les proves, analitzar-les i emetre un judici dels delictes comesos a conseqüència d'aquestes intrusions.

Els Honeypots son equips i programes que simulen un sistema real vulnerable amb la intenció d'atraure atacants, i així poder tenir un entorn preparat per després de rebre les intrusions, poder fer aquests anàlisis forenses i ajudar a extreure conclusions. Aquestes conclusions ens serviran per mantenir els sistemes reals millor protegits.

A la primera part d'aquest treball es començarà parlant una mica de l'història dels delictes informàtics i de les lleis existents en referència a aquests delictes. Després s'analitzaran algunes de les eines que serveixen per fer un anàlisis forense de sistemes compromesos. També s'estudiarà els tipus de Honeypots existents.

El nucli del treball consisteix en configurar i implantar una xarxa de Honeypots que estaran actius rebent intrusions als sistemes. Després de que els Honeypots hagin sigut compromesos, es farà un estudi i posterior informe dels atacs rebuts.

Finalment es mostra com gràcies a aquests Honeypots i l'ús de la informàtica forense es poden extreure conclusions que ens ajudaran a millorar la seguretat dels sistemes informàtics.

Abstract (in English, 250 words or less):

Ever since digital communication came into being IT support has wanted to keep systems secure and the information contained therein from unauthorized access. On the other hand, numerous people and organisations have tried somehow or other to access these systems and information either for their own ends, for financial reasons or just for fun.

There is a constant battle to keep systems and information secure, and once an intrusion has occurred forensic computing enables us to gather evidence, examine it and pass judgment as to the crimes committed as a result of such breaches.

Honeypots are mechanisms and programs that simulate a real vulnerable system in order to attract attackers, and thus have an environment already prepared to receive the breaches, and make a forensic analysis of them and help to draw conclusions. These conclusions will enable us to keep the real systems better protected.

In the first part of this Project we shall begin by saying a few words about the history of online crime and the existing legislation regarding this. We shall then examine some of the devices used to make a forensic analysis of systems that have been compromised, as well as looking at existing types of Honeypots.

The very heart of this Paper will consist of configuring and implementing a network of Honeypots that will actively welcome breaches of the system. Research will be carried out on corrupted Honeypots followed by a report on the attacks received.

Ultimately, we can see that thanks to these Honeypots and the use of forensic computing, lessons can be learnt that will help us to improve the security of computer systems.

Paraules clau :

Honeypot, Modern Honey Network, anàlisi forense, delictes informàtics

Índex de continguts

Llista de figures

1.- Introducció

1.1 Justificació del TFC i context en el que es desenvolupa

Aquest projecte correspon al treball final de carrera d'Enginyeria Tècnica en Informàtica de Sistemes i forma part de l'àrea d'administració de xarxes i sistemes operatius.

Cada cop més la comunicació digital té un paper més important a la nostra societat i, cada vegada existeixen més persones i organitzacions que volen interceptar aquestes comunicacions i els sistemes que les produeixen. Els delictes informàtics acaparen titulars a la premsa degut als problemes que causen. Es preveu un futur on la tecnologia estigui cada vegada més integrada en tots els àmbits de la nostra vida i això farà augmentar els objectius i tipus de delictes informàtics que es cometran. La informàtica forense ajuda a identificar, preservar i analitzar dades que puguin ser vàlides dins de un procés legal. Una eina important dins de la informàtica forense son els Honeypots, que simulen ser sistemes reals vulnerables i que permeten ser analitzats posteriorment, generant d'aquesta manera informes que ens ajudaran a protegir els equips reals d'aquests mateixos atacs.

1.2 Objectius del TFC

L'objectiu principal del treball , després d'introduir-nos en els conceptes dels delictes informàtics i de la informàtica forense, és configurar un entorn de proves amb uns Honeypots que formaran part d'aquests entorn i simularan uns equips reals vulnerables que atrauran atacants. D'altra banda es vol demostrar la vulnerabilitat de qualsevol equip mal protegit connectat a la xarxa i com utilitzant la metodologia de la anàlisis forense s'auditaran els sinistres i es trauran conclusions vàlides per poder millorar els sistemes actuals.

1.3 Enfocament i mètode seguit

L'enfocament que li volem donar al treball és un enfocament molt pràctic. Ensenyant com crear una xarxa de Honeypots des de zero i com utilitzar una metodologia forense per analitzar-lo i treure-hi conclusions. L'anàlisi forense segueix una metodologia establerta, però depenent el tipus d'intrusions rebudes es decidirà incorporar uns o altres tipus d'anàlisi.

1.4 Planificació del projecte

El projecte es divideix en dos grans blocs, la primera part més teòrica inclou l'història i defineix amb una mica més de detall els conceptes dels delictes informàtics i la informàtica forense, junt amb un petit anàlisis d'algunes de les eines de la informàtica forense més utilitzades a dia d'avui. La segona part es pràctica i analitza alguns dels Honeypots existents, amb la creació d'una xarxa de Honeypots en un entorn real per al seu posterior anàlisi. Basant-nos en aquests dos grans blocs em fet una planificació respectant les dates proposades.

Hem fet un diagrama de Gantt planificant tot el projecte i que mostrem a continuació:

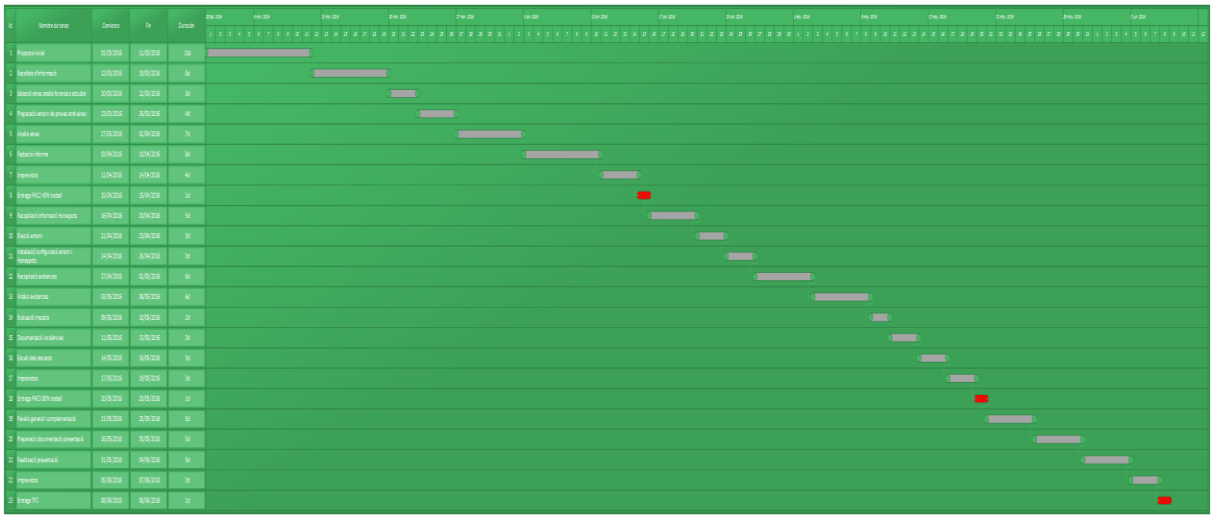


Figura 1 Diagrama de Gantt

I com el gràfic anterior és difícil de llegir, ampliarem la part del text perquè es vegi més clar

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Proposta inicial	01/03/2016	11/03/2016	11d
2	Recollida d'informació	12/03/2016	19/03/2016	8d
3	Selecció eines analisi forense a estudiar	20/03/2016	22/03/2016	3d
4	Preparació entorn de proves amb eines	23/03/2016	26/03/2016	4d
5	Analisi eines	27/03/2016	02/04/2016	7d
6	Redacció informe	03/04/2016	10/04/2016	8d
7	Imprevistos	11/04/2016	14/04/2016	4d
8	Entrega PAC2 40% treball	15/04/2016	15/04/2016	1d
9	Recopilació informació Honeypots	16/04/2016	20/04/2016	5d
10	Elecció entorn	21/04/2016	23/04/2016	3d
11	Instalació/configuració entorn i Honeypots	24/04/2016	26/04/2016	3d
12	Recopilació evidencies	27/04/2016	02/05/2016	6d
13	Anàlisi evidencies	03/05/2016	08/05/2016	6d
14	Evaluació impacte	09/05/2016	10/05/2016	2d
15	Documentació incidències	11/05/2016	13/05/2016	3d
16	Estudi dels atacants	14/05/2016	16/05/2016	3d
17	Imprevistos	17/05/2016	19/05/2016	3d
18	Entrega PAC3 80% treball	20/05/2016	20/05/2016	1d
19	Revisió general i complementació	21/05/2016	25/05/2016	5d
20	Preparació documentació presentació	26/05/2016	30/05/2016	5d
21	Realització presentació	31/05/2016	04/06/2016	5d
22	Imprevistos	05/06/2016	07/06/2016	3d
23	Entrega TFC	08/06/2016	08/06/2016	1d

Figura 2 Diagrama de Gantt ampliació

S'han dividit les entregues basant-se en els dos grans blocs descrits anteriorment. La primera entrega és la proposta, en termes generals, del que conté aquest treball final. Aquesta primera proposta ha servit de base d'aquest primer capítol introductori.

En la segona entrega que pot correspondre a aproximadament el 40% del treball descriurem, partint de la història dels delictes i de la informàtica forense, la vessant més teòrica del projecte. Analitzarem els tipus de delictes informàtics i les diferents eines que també es poden classificar segons per quin tipus de delicte es volen usar. Veurem una clara correspondència de tipus de delictes amb els tipus d'eines usades. Aquesta part integra també el marc legal actual envers tots aquests delictes i un anàlisis de les eines més utilitzades segons la seva classificació.

A la tercera entrega ja inclourem la part pràctica, on veurem els passos a seguir per configurar i instal·lar una sèrie de Honeypots i integrar-los a una xarxa, utilitzant com a eina el projecte Modern Honey Network. Posteriorment veurem les dades obtingudes i farem un informe amb totes elles. Finalment gràcies a aquest informe, podrem extreure conclusions que ens ajudin a millorar la seguretat informàtica d'un sistema.

1.5 Productes obtinguts

En aquest treball final de carrera el producte obtinguts, com ja s'ha descrit anteriorment en aquest primer apartat, serà una xarxa Honeypots fent ús del projecte Modern Honey Network. Configurarem un servidor central que allotjarà la web amb la informació dels Honeypots desplegats. Aquests Honeypots estaran a diferents localitzacions utilitzant diferents VPS, i junt amb aquests, també desplegarem Honeypots en uns servidors locals de la pròpia xarxa local que també estarà connectat al servidor central per poder visualitzar les dades recopilades. Aquesta web d'administració central estarà activa en l'entrega del treball. (http://149.202.48.250/)

1.6 Descripció de la resta de capítols

En el segon capítol, després d'introduir-nos als delictes informàtics amb una mica d'història, es farà una classificació d'ells segons el tipus. Després es parlarà de la legislació aplicable actualment en aquest camp.

El tercer capítol entrarà en el món de la informàtica forense, on després de fer-hi una definició i veure la seva història, es farà una petita classificació de les eines. En el quart capítol s'entrarà en el món dels Honeypots, on es veurà com es poden instal·lar, configurar i publicar per començar a recol·lectar dades que ens serviran més endavant per poder fer un informe.

En el cinquè capítol parlarem de l'anàlisi forense, on descriurem una metodologia genèrica a utilitzar per fer anàlisis forenses. Seguidament veurem com hem recopilat les evidències

gràcies als Honeypots configurats, quin anàlisis podem fer d'elles i veurem l'informe que extraurem mitjançant aquesta recopilació i l'anàlisi.

Finalment acabarem amb una conclusió resultant de tot el treball.

2.- Delictes informàtics

2.1 Que son els delictes informàtics?

Es pot parlar genèricament dels delictes informàtics com a crims electrònics que es realitzen des d'un dispositiu tecnològic amb l'objectiu de destruir, realitzar un frau, robar o falsejar informació. Aquests delictes abasten una gran quantitat d'objectius com poden ser ordinadors, xarxes o qualsevol altre dispositiu electrònic. Amb l'avens de la tecnologia cada cop son més freqüents i sofisticats.

La Organització de Nacions Unides reconeixen els següents tipus de delictes informàtics:

1. Fraus comesos mitjançant la manipulació de computadors
2. Manipulació de dades d'entrada
3. Danys o modificacions de programes o dades computeritzats

Una altra classificació segons el conveni sobre la delinqüència del consell europeu, de Novembre de 2001 signat a Budapest, classifica els delictes en quatre grups:

1. Delictes contra la confidencialitat, la integritat i la disponibilitat de dades i sistemes informàtics: Aquest grup engloba els delictes que afecten al accés il·lícit de sistemes, interpretació il·lícita de dades informàtiques i abusos de dispositius que faciliten la comissió de delictes.
2. Delictes informàtics: Pertanyen al grup els delictes que tenen a veure amb l'esborrat, introducció o supressió de dades informàtiques.
3. Delictes relacionats amb el contingut: Aquí estaran els delictes que produeixen, difonen o oferten continguts delictius per mitjà de sistemes informàtics.
4. Delictes relacionats amb infraccions de la propietat intel·lectual o drets afins, com podria ser la copia o distribució de programes informàtic i tot el que engloba la pirateria informàtica.

2.2 Una mica d'Història dels delictes informàtics

Als anys 60 es crea ARPANET que va ser l'espina dorsal de internet. Aquest fet marca l'inici de les comunicacions.

Al 1981 apareix la primera computadora personal IBM.

Al 1982 neix el primer virus informàtic. Els primers virus per l'ordinador Apple II es propaguen mitjançant els antics disquets, però només a un cercle molt restringit.

El virus "Elk Cloner" és el primer virus en llibertat amb expansió real, programat per Apple /DOS 3.3 i també es propagava en disquets.

Al 1983 gràcies al Dr Fred Cohen, on en un discurs d'agraïment va incloure les pautes per desenvolupar un virus donant-li una definició. Aquest fet i posteriors el van convertir en el primer autor oficial dels virus

Al 1984 Fred Cohen presenta el concepte de virus en un seminari, implementant un virus funcional en UNIX. 2 anys més tard publica els primers articles que s'incorporen a la seva tesis doctoral publicada al 1986. La seva definició de virus, amb orientació mes aviat matemàtica, encara segueix sent reconeguda.

Al 1986 es considera l'inici de la gran epidèmia de virus, on apareixen alguns com el Brain, Virdem, Bouncing Ball i Marihuana, que només afectaven al sector d'arranc del disquet. Més endavant apareixen virus que infectaven els arxius exe i com.

El 2 de Novembre de 1988 Robert Tappan Morris, difon un virus a través de ArpaNet on aconsegueix infectar 6000 servidors.

Al 1987 apareix Lehigh, el primer virus que capta l'interès del públic. Apareixen nVir i Peace, els primers virus per a Macintosh. També apareix Cascade, el primer virus xifrat.

A desembre un estudiant americà fa caure el trànsit de correu i les xarxes a tot el mon amb un cuc informàtic (el Tannenbaum).

Aquell mateix any G DATA comercialitza el primer antivirus del món, es diu G DATA AntiVirusKit i protegia als antics ordinadors Atari ST

Juntament amb la distribució de virus, apareixen molts altres delictes informàtics que seran classificats en el següent apartat.

2.2 Classificació dels tipus de delictes

Segons la classificació dels delictes que ens fa la Organització de les nacions unides que hem descrit en l'apartat 2.1, dins de cada apartat podem trobar diferents tipus de delictes

1. Fraus comesos mitjançant la manipulació de computadors

Aquí trobaríem els delictes comesos a partir de la manipulació de programes, manipulació de les dades de sortida, manipulació de les dades d'entrada, sostracció de dades i els fraus ocasionats per manipulació informàtica

2. Manipulació de dades d'entrada

Aquí trobem els delictes d'alteració de les dades que estan guardades en computadors.

3. Danys o modificacions de programes o dades computeritzats

En aquest punt trobem el sabotatge informàtic que no és més que és l'acte de suprimir, esborrar o modificar funcions d'un sistema amb la intenció d'obstaculitzar el funcionament dels sistemes. Algunes tècniques que permeten produir sabotatges son els virus, els cucs o les bombes lògiques.

2.3 Legislació

Els delictes informàtics no estan contemplats com un tipus especial de delicte a la legislació espanyola, ja que no estan definit ni al codi penal ni a les reformes posteriors que s'han fet

(Llei 15/2003 i Llei 5/2010). Així que no es pot parlar de delicte informàtic pròpiament dit, sinó de delictes fets amb l'ajut de les noves tecnologies. Existeixen però, vàries normes relacionades amb aquest tipus de conductes:

-Llei de Serveis de la societat de la informació i del comerç electrònic

-Llei orgànica de Protecció de dades de caràcter personal.

-Reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal.

-Llei general de Telecomunicacions.

-Llei de signatura electrònica.

-Llei de propietat intel·lectual.

A més d'aquestes normes existeixen en el codi Penal espanyol multitud de conductes il·lícites relacionades amb els delictes informàtics. Existeix un conveni sobre la Ciberdelinqüència[1] que reflexa els següents articles.

Als delictes contra la confidencialitat, la integritat i la disponibilitat de les dades i dels sistemes informàtiques l'article 197 contempla les penes amb les que es castigarà. Al article 278.1 s'exposen las penes amb que es castigarà si l'objectiu es descobrir secrets d'empresa.

Al article 264.2 es tracta de les penes que s'imposaran a qui destrueixi, alteri o inutilitzi les dades, documents electrònics aliens continguts en xarxes, suports o sistemes informàtics.

Els articles 248 i 249 tracten les estafes, mentre que els articles 255 i 256 nombren les penes que s'imposaran a qui cometi fraus utilitzant els mitjans.

L'article 186 cita les penes que s'imposaran a aquells que difonguin, exhibeixin material pornogràfic entre menors d'edat.

[1] Conveni sobre la Ciberdelinqüència, fet a Budapest a novembre de 2001 per els estats membres del consell d'Europa i publicat al BOE núm. 226, de 17 de setembre de 2010, pàgines 78847 a 78896 (50 pàgs.)

Això és una petita pinzellada del marc legal que legisla els delictes informàtics, en cap cas es vol entrar en detalls ja que no és l'objecte d'aquest treball.

3.- Informàtica forense

3.1 Definició

La informàtica forense és l'aplicació de tècniques científiques i analítiques especialitzades que permeten identificar, preservar analitzar i presentar dades que siguin vàlides dins d'un procés legal.

Les diferents metodologies forenses inclouen la captura segura de dades de diferents mitjans digitals i evidències digitals sense alterar la informació d'origen. Les evidències digital obtingudes permeten elaborar un dictamen fonamentat a partir de les probes recollides. Gràcies a aquest procés la informàtica forense apareix com una disciplina auxiliar de la justícia moderna.

3.2 Una mica d'Història de la informàtica forense

Al 1978 Florida reconeix els crims de sistemes informàtics en casos de sabotatge, copyright modificació de dades i casos similars.

Al 1981 neix Copy II PC de central Points software que s'usa per la còpia exacta de disquets, que generalment estan protegits per evitar còpies pirates, la companyia és un exit i es comprada per Symantec al 1994.

Al 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versió del conjunt d'eines "Norton utilities".

Al 1984 el FBI forma el Magnetic Media Program que més tard, al 1991 passarà a ser el Computer Analysis and Response Team (CART).

Al 1986 Clifford Stoll col·labora en la detecció del Hacker Markus Hess. Al 1988 publica el document explicant tot el que va passar, i aquest document es transforma al 1989 en un llibre que anticipa una metodologia forense.

Al 1987 neix la companyia AccessData, pionera en el desenvolupament de productes orientats a la recuperació de contrasenyes i l'anàlisi forense amb eines com la actual Forensic Toolkit (FTK).

Al 1988 se crea la International Association of Computer Investigative Specialists (IACIS), que certificarà a professionals de agencies governamentals en el Certified Forensic Computer Examiner (CFCE), una de les certificacions mes prestigioses en el àmbit forense.

Aquell mateix any es desenvolupa el programa Seized Computer Evidence Recovery Specialists o SCERS, amb l'objectiu de formar a professionals en computer forensics.

El llibre "A forensic methodology for countering computer crime", de P. A. Collier i B. J. Spaul implanta al 1992 el terme "computer forensics". Altres llibres posteriors continuaran desenvolupant el terme i la metodologia.

Al 1995 es funda "International Organization on Computer Evidence" (IOCE), amb l'objectiu de ser punt de trobada entre especialistes en la evidència electrònica i l'intercanvi d' informació.

A partir de 1996 la Interpol organitza els International Forensic Science Symposium, com un fòrum per debatre els avenços forenses.

A l'agost de 2001 neix la Digital Forensic Research Workshop (DFRWS), nou grup de debat i discussió internacional per compartir informació.

3.3 Evidència Digital

En un anàlisis forense digital una de les tasques més importants en l'investigació és la captura de les evidències digitals també anomenades evidències electròniques. Segons la RAE es

defineix evidència com : ”certesa clara i manifesta de la que no es pot dubtar”. En la informàtica una evidència digital es qualsevol informació electrònica trobada en un sistema informàtic que pugui ser contrastable, com una transacció, document o qualsevol tipus d’informació registrable digitalment.

Les evidències digitals son l’element principal per als investigadors i tenen una sèrie de característiques úniques. D’aquestes característiques podem destacar que són volàtils anònimes i modificables.

Un dels desafiaments de la informàtica forense no és si pot existir una evidència digital, sinó a on està guardada aquesta evidència. La meitat de la lluita està en saber on son aquestes evidències i l’altre meitat saber recollir-les i gestionar-les.

3.4 Classificació d’eines d’informàtica forense

Podem fer una classificació genèrica de les eines d’informàtica forense a partir del producte que volem analitzar. Aquesta classificació contempla el següent tipus d’eines:

-Eines per anàlisis de discs

-Eines per anàlisis de dispositius mòbils

-Eines per anàlisis de correus electrònics

-Eines per anàlisis de xarxes

-Eines per filtrar i monitoritzar el transit d’una xarxa tant interna com externa

3.5 Algunes eines utilitzades en la informàtica forense

Existeixen multitud d’eines d’anàlisis forense per als múltiples dispositius electrònics existents al mercant. En aquest treball veurem per sobre algunes de les més utilitzades avui en dia per els pèrits informàtics.

Primer de tot comentarem dos distribucions Linux creades exclusivament per ser utilitzades en anàlisis forenses. Després del nostre anàlisis de totes les existents, s'ha considerat que son les dos més importants i completes.

DEFT

És una distribució Linux per l'anàlisi forense informàtic basat en Ubuntu que inclou eines per anàlisis forense de mòbils i dispositius amb iOs o Android. A DEFT Linux podem trobar moltes eines[2] relacionades amb la informàtica forense, classificades per temes.

Deft està molt ben documentat, ja que es va crear inicialment per ensenyar anàlisis forense a la universitat de Bolonya, i aquest és un dels punts mes rellevants dels que parteix.

CAINE

[2]Eines DEFT
Network Information Gathering

- Host
- Nslookup
- Dig
- Nmap
- Zenmap
- Netcat
- Snmpcheck
- Nbtscan
- Cadaver
- Traceroute
- Hping3
- Xprobe
- Scapy
- Netdiscover

Wireless Information Gathering
- Kismet

Web Application Information Gathering
- Whatweb
- Cmsident
- Dirbuster
- Burpsuite
- Customized Chrome Browser (at least 1gb ram required)

Social Information Gathering
- Creepy
- Snmpcheck
- PieSpy
- Irssi

Identity Protection Tools
- TOR-Browser
- Anonymouse (http://anonymouse.org/anonwww.html)

OSINT Global Framework
- Maltego

Caine és una altra distribució Linux molt famosa, que ofereix un entorn Linux complet integrant moltes eines de software existents amb una interfície gràfica molt amigable.

Algunes de les eines més importants que conté aquesta distribució son les següents:

- Grissom Analyzer
- Automated Image & Restore (AIR)
- Guymager
- Foremost and Scalpel
- Autopsy 2.20 and TSK 3.0
- SFDumper
- Fundl
- Stegdetect
- Ophcrack

Autopsy

Es segurament la millor eina lliure que existeix per l'anàlisi d'evidències digitals. La seva interfície gràfica és un *browser* que basat en les eines en línia de comandaments del Sleuth Kit permet un anàlisis de diferents tipus d'evidències mitjançant la captura d'una imatge de discs. Autopsy i Sleuth kit son Open Source i poden ser executats en plataformes unix. Com autopsy es basa en HTML es pot connectar al servidor Autopsy des de qualsevol plataforma utilitzant un navegador HTML. Autopsy proporciona una interfície tipus "gestió d'arxius" i mostra detalls sobre dades esborrades i estructures del sistema d'arxius

X-Ways Forensics

Aquesta a diferencia de les anteriors, és una eina de pagament i és una plataforma avançada per als analistes forenses digitals. Té múltiples eines per l'anàlisi forense i és compatible amb la majoria de sistemes existents.

A més a més del seu potencial, el consum de recursos de l'aplicació és molt lleuger, amb el que deixa utilitzar-se en equips poc potents. És impossible llistar la gran quantitat de funcionalitats que té però es poden nomenar algunes d'elles com la gestió completa de casos, anàlisis de memòria, anàlisis de discs, anàlisis de registre, múltiples informes sobre les dades etc. Cal destacar que la eina es portable i es pot executar des de un dispositiu extern.

EnCase

Eina desenvolupada per Guidance software, que permet assistir a l'especialista forense durant tot l'anàlisi d'un crim real. Actualment és el software líder del mercat i és el producte de major ús en el camp de l'anàlisi forense. És tota una plataforma d'investigació que recol·lecta dades digitals, realitza anàlisis, informa sobre descobriments i ho presenta en un format vàlid a efectes legals i validat per els tribunals.
Permet obtenir adquisicions vàlides a efectes legals, té funcions de productivitat avançades, és personalitzable amb programació EnScript[3], proporciona dades processables i genera informes. També existeix l'edició portable que pot ser executada des d'un dispositiu USB. Aquesta eina es de pagament i és necessària la compra d'una llicència per al seu ús.

4.- Honeypots

Els atacs a servidor d'internet augmenten any rere any al igual que la seva complexitat. Els Honeypots ens ajuden a investigar aquests atacs i gràcies a aquesta informació, millorar la seguretat dels equips.

4.1 Definició de Honeypot

Un Honeypot és una eina de seguretat que consisteix en la simulació d'un equip real (o un conjunt d'equips) vulnerable per ser atacat, amb la finalitat de recollir dades sobre els atacants i les tècniques usades per comprometre els sistemes. Gràcies l'aprenentatge de les eines i tècniques usades per els atacants, es pot llavors protegir millor els sistemes.

En la seva forma més bàsica son servidors d'informació falsos, posicionats estratègicament en una xarxa de prova. A aquests servidors se'ls hi habiliten eines de monitorització i rastreig de

[3] Llenguatge de programació orientada a objectes i similar a Java o C++, que permet als usuaris crear programes personalitzats que ajudin a automatitzar les tasques de investigació que demanden molt de temps

la informació, de manera que cada rastre d'activitat d'un atacant pugui ser registrat d'una manera detallada.

Les funcions principals d'un Honeypot son:

-**Desviar l'atacant de la xarxa principal del sistema, de manera que no es comprometin els recursos principals**.

En un sistema com el nostre, la solució és posar els Honeypots a la DMZ, d'aquesta manera evitem que es comprometin els recursos principals. També en aquests equips hauríem de limitar les connexions de sortida.

Una altra solució seria col·locar el/s Honeypot/s en una cèl·lula d'aïllament[4]. Per fer-ho es poden utilitzar equips Bait and switch [5]que encaminen el trànsit hostil cap a cel·les d'aïllament.

-**Conèixer noves vulnerabilitats i riscs dels diferents sistemes operatius, entorns i programes.**

Una bona manera de conèixer noves vulnerabilitats es precisament mitjançant els Honeypots, que es posen com una "prova" per als atacants per descobrir quines son les vulnerabilitats del sistema i dels seus programes, on mitjançant les seves deficiències, els atacants accedeixen a recursos concrets, o executen accions que no haurien de poder. Analitzar aquests atacs amb els Honeypots ens poden ajudar a veure on estan aquestes vulnerabilitats o quins son els riscos dels SO en concret.

-**Crear perfils d'atacants i mètodes d'atacs preferits**.

Els Honeypots recopilen una gran quantitat d'informació d'atacants de tot tipus i d'atacs a tot tipus de servei. Aquesta informació estadística, ben analitzada, ens pot ajudar a crear perfils d'atacants i analitzar quins son els mètodes preferits que utilitzen.

[4] En aquest cas no cal que siguin Honeypots els que es col·loquin a una cèl·lula d'aïllament, poden ser equips que siguin còpies exactes dels sistemes de producció real
[5] Equip amb 3 interfícies de xarxa que encamina tot el trànsit hostil a cel·les d'aïllament

4.2 Classificació de Honeypots

Podem classificar els Honeypots, segons el seu nivell d'interacció, en els següents tipus:

Honeypots de baix nivell d'interacció: En aquests Honeypots no existeix sistema operatiu sobre el qual l'atacant pugui interactuar. Son fàcils d'instal·lar i de mantenir però tenen la desavantatge de que la informació obtinguda sol ser limitada. Aquests Honeypots simulen serveis que permeten a l'atacant interactuar sense afectar al sistema on estan implementats

Honeypots de nivell mig d'interacció: Aquests Honeypots permeten major interacció que els de baix nivell però sense arribar a proveir un sistema operatiu amb el que interactuar. Aquests Honeypots son capaços de generar respostes en la interacció d'un atacant a un servei en concret. A més de simular serveis també poden emular el comportament d'un software. La implementació d'aquests sistemes és més complexa que els de baixa interacció i com a contrapartida la informació obtinguda per aquests tipus de Honeypots es bastant superior a la obtinguda amb els anteriors.

Honeypots d'alt nivell d'interacció: Aquest tipus de Honeypots son els que proporcionen més informació dels atacants i els seus mètodes. Tenen un sistema operatiu real on l'atacant pot interactuar, i que presenten un major risc i complexitat. El fet de tenir un sistema operatiu real fa que siguin objectius mes atractius per ser atacats i la seva instal·lació requereix molt més temps, al igual que el seu manteniment. Per contra, son els que proporciones més informació i més valuosa.

4.3 Ubicació dels Honeypots

Podem ubicar el Honeypot dins de la xarxa en localitzacions diferents. Segons aquesta ubicació els podem classificar de la següent manera:

Front of Firewall (abans del Firewall): Aquesta configuració permet una major seguretat per la xarxa i evita l'increment del risc que hi ha en la instal·lació d'un Honeypot. Aquest es troba fora de la protecció del Firewall i pot ser atacat sense perill per a la resta de la xarxa. Al no

estar sota la protecció del Firewall és molt més fàcil d'atacar i això pot comportar un augment no desitjable del trànsit.

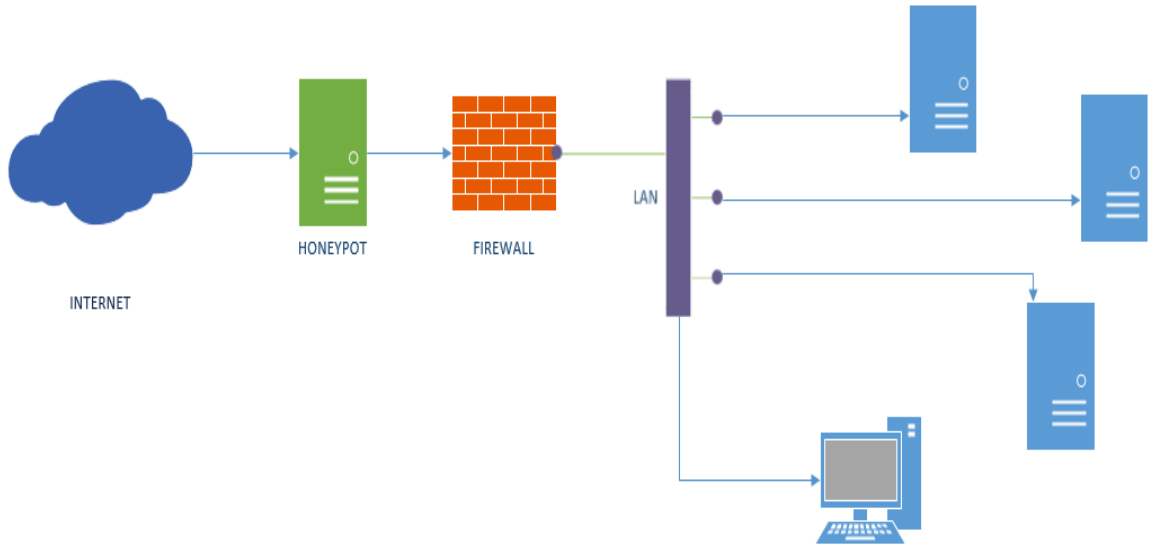


Figura 3 Front of Firewall

Behind the Firewall (darrera del Firewall): En aquesta posició el Honeypot queda afectat per les regles de filtrat del mateix Firewall. S'hauran de modificar algunes regles per permetin algun tipus d'accés al Honeypot per possibles atacants externs. Per altra banda la seguretat està molt més compromesa, ja que un atacant que aconseguís l'accés al Honeypot, podria arribar a accedir a la resta d'elements de la xarxa posant-los en compromís. A més amb aquesta configuració es generaran gran quantitat d'alertes que generaran els sistemes de seguretat de la xarxa. Hi ha vàries circumstàncies que obliguen a utilitzar aquest tipus de configuració com la impossibilitat d'utilitzar una direcció IP externa per al Honeypot. El principal problema que presenta aquest mètode es que requereix una configuració específica per deixar accés al Honeypot però no a la nostra xarxa. No és recomanable a no ser que es sàpiga configurar bé tots els accessos o podem posar en perill la nostra xarxa.

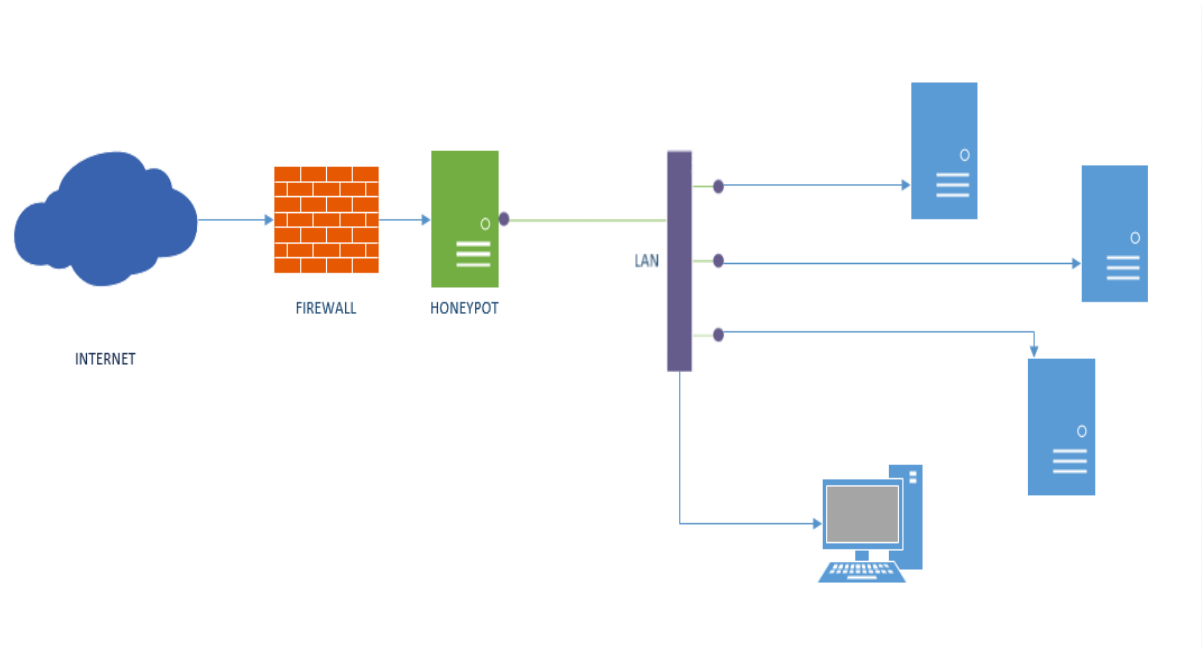


Figura 4 Behind the Firewall

A la DMZ (zona desmilitaritzada): En aquest cas la ubicació del Honeypot serà a la zona desmilitaritzada (DMZ). La zona desmilitaritzada és una zona segura que s'ubica entre la xarxa interna i la xarxa externa. El Firewall aïlla aquesta zona de la resta de la xarxa. Aquesta arquitectura ens permet detectar atacs externs i interns amb una simple reconfiguració del Firewall. Amb aquesta configuració també eliminem les alarmes del sistema i el perill que suposa tenir un Honeypot a la xarxa local ja que no està en contacte amb ella.

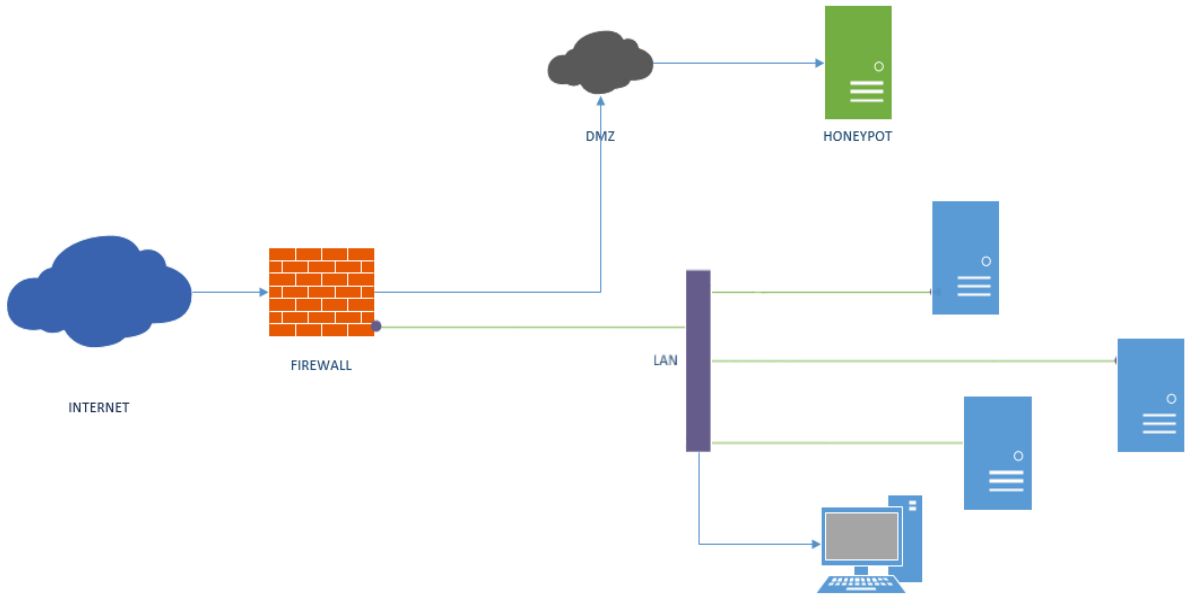


Figura 5 DMZ

Des del meu punt de vista el millor lloc per connectar un Honeypot es dins de la zona desmilitaritzada DMZ, ja que tots els accessos que arriben aquí ja han passat per el Firewall, i per tant, qualsevol trànsit anòmal que arribi aquí s'ha de considerar hostil. Per altra banda, al estar en la DMZ no estarà en contacte directe amb la xarxa interna on estan situats la resta d'equips, i ens evitem així que si l'atacant aconsegueix fer-se amb aquesta màquina, no pugui accedir als equips finals.

4.4 Modern Honey Network

El nucli central del nostre treball consisteix a crear una xarxa de Honeypots amb la que recopilarem tot tipus d'intrusions per al seu posterior anàlisi. Per fer-ho, utilitzarem el projecte Modern Honey Network. Aquest projecte es basa en un Multi-gestor de sensors Honeypot, que utilitza una xarxa virtual de Honeypots on des d'un servidor centralitzat, podrem gestionar tant les dades recopilades com gestionar els sensors que formaran part d'aquesta xarxa de Honeypots. Per poder crear aquesta xarxa, necessitarem crear un servidor principal que allotjarà la web gestora de tots els sensors, junt amb múltiples Honeypots

virtuals, situats a diferents països. Aquestes màquines virtuals les crearem amb varis VPS[6] (Virtual Private Server) ubicats a OVH[7] i a Amazon, junt amb màquines virtuals creades a la xarxa interna, que també formaran part de la Honey Network i estaran incloses en la gestió que es farà des del servidor principal de MHN, ubicat també a una altre VPS. Tots aquests servers virtuals contindran tota mena de Honeypots diferents que enviaran les dades recopilades a aquest servidor "central" on estarà allotjat aquest MHN.

4.5 Preparació de l'entorn

El nostre entorn estarà format per el següent:

- 3 VPS del proveïdor OVH, situats a Gravelines (França), Estrasburg (França) i a Beauharnois (Canadà). Cadascun té instal·lat Ubuntu 14.04 Server 64bits i un d'ells, el situat a Gravelines, farà de servidor central amb la web gestora del Projecte. Tots ells tenen 10Gb de disc i 2Gb de RAM exceptuant el servidor central, que disposa de 20Gb de disc i 4Gb de RAM
- 1 VPS del proveïdor Amazon situat a Irlanda amb 2 instàncies, cadascuna amb 14.04 Server 64bits amb 1Gb de RAM per cada.
- 2 màquines virtuals, situades a Barcelona, a la nostre xarxa interna particular, amb 8Gb d'espai de disc i 1 Gb de RAM cadascuna. Una amb Ubuntu 14.04 Server 64bits i l'altre amb la distro de Linux Honeydrive de la que es parlarà una mica més endavant, les dues executades des de Virtualbox.

Primer de tot s'haurà de crear els VPS a OVH, per això ens registrarem al proveïdor i crearem els 3 VPS mencionats anteriorment. Cadascun d'ells el situarem en una ubicació diferent per poder recopilar informació del diferents llocs.

[6] VPS (Servidor Virtual Privat) Mètode que consisteix en particionar un servidor físic en varis servidors virtuals. Cada servidor virtual pot executar el seu SO i es pot reiniciar de forma independent. Els clients tenen nivell d'accés de root o superusuari i per tant poden instal·lar qualsevol tipus de software, que posteriorment pot ser executat sota el Sistema Operatiu.
[7] Proveïdor d'allotjament web Francès

En aquesta captura veurem els 3 VPS creats amb aquest proveïdor (el que es mostra és el Servidor principal i a l'esquerra podem veure els altres 2 creats):

Figura 6 VPS de OVH

Seguidament crearem el VPS a Amazon, amb les 2 instàncies, de tipus t2.micro amb els següents característiques:

Modelo	CPU virtual	Créditos por hora de la CPU	Memoria (GiB)	Almacenamiento
t2.micro	1	6	1	Solo EBS

Es pot observar les 2 instàncies creades a la mateixa VPS, dins del EC2 management de Amazon:

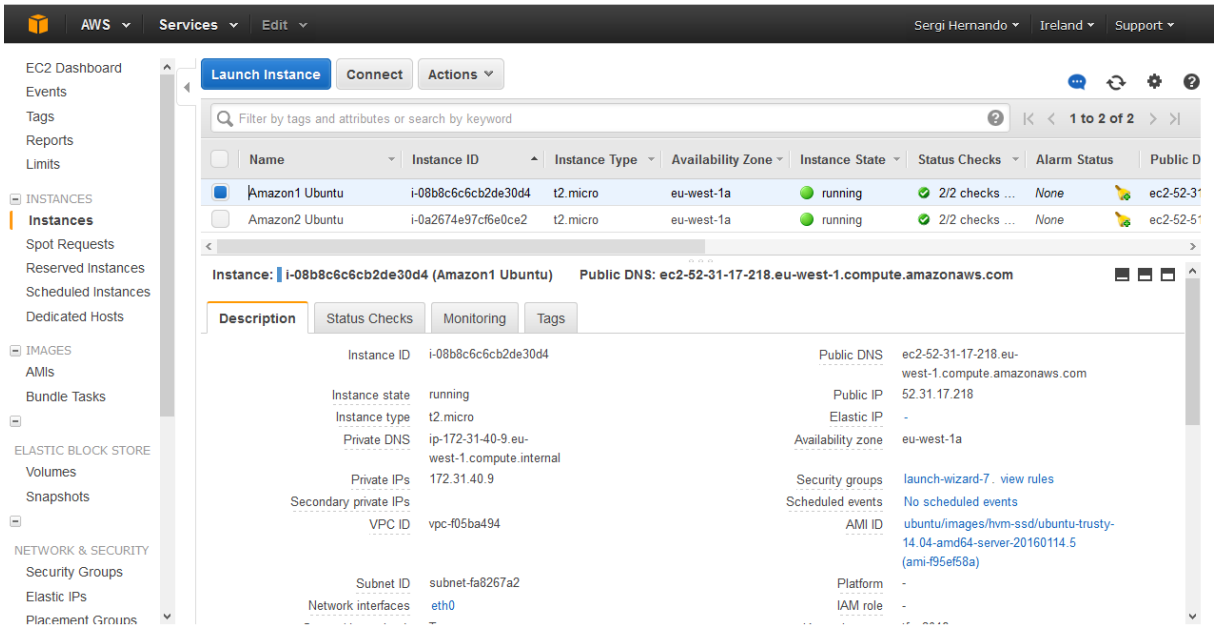


Figura 7 VPS a Amazon

Per completar la nostra xarxa de servidors que formaran part de la nostra Honeynet Network crearem les 2 màquines virtuals a la xarxa interna. Aquestes màquines correran sobre Virtualbox. La primera serà una instal·lació neta de Ubuntu Server 64 bits i a la segona màquina instal·larem la distro Honeydrive[8]. Aquestes 2 màquines de la xarxa interna estaran instal·lades a la DMZ de la pròpia xarxa, evitant així que atacants que es fessin amb elles poguessin accedir a la resta de sistemes de la xarxa (tal com s'explica al apartat 4.3)

A totes les màquines ens connectarem via SSH. Cal remarcar que a diferència de les que hi ha al proveïdor OVH o a la xarxa interna, a les instàncies de Amazon només ens podem connectar utilitzant una clau privada. Aquesta clau que ens dona Amazon amb extensió .pem l'haurem de transformar a .ppk per poder utilitzar el client de SSH Putty. Per fer-ho, hem utilitzat la eina Puttygen que generarà aquest .pkk a partir de la clau .pem. A més a més, en les instàncies de Amazon hem obert ports necessaris per fer funcionar els Honeypots que contindran.

[8] Veure subapartat 4.5.6

Per fer-ho, entrarem a Network&Security, dins de Security Grups, i afegirem els ports que necessitem per aquella màquina en concret. Exemple d'una configuració d'una de les instàncies a Amazon:

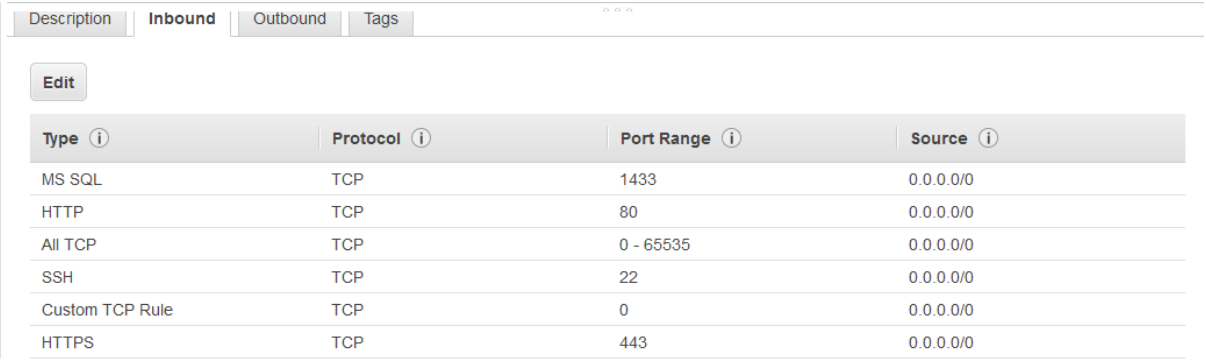


Figura 8 Ports oberts a Instància de VPS a Amazon

Un cop tenim les màquines virtuals, començarem instal·lant i configurant el servidor central de MHN (Modern Honey Network)

Per fer-ho ens connectem al server principal, situat a Estrasburg i instal·larem els paquets necessaris amb la següent comanda:

apt-get install sudo git python gcc automake –y

Ara necessitarem descarregar-nos una còpia del MHN que està a GitHub, ho farem amb la següent comanda:

git clone https://github.com/threatstream/mhn.git

Entrarem a la carpeta mhn que s'ha descarregat i a dins trobarem una carpeta amb scripts. Aquests ens ajudaran a fer la instal·lació. Executarem els següents:

sudo ./install_hpfeeds.sh

sudo ./install_mnemosyne.sh

sudo ./install_honeymap.sh

Un cop acabat, executarem l'script que ens instal·larà el mhn i ens ajudarà a configurar-lo:

sudo ./install_mhnserver.sh

Abans d'acabar ens farà varies preguntes sobre la configuració del servidor, entre elles el correu i password amb el que podrem accedir a la gestió web o la seva pròpia URL.

```
+ '[' -f /etc/redhat-release ']'
+ echo 'DONE installing python virtualenv'
DONE installing python virtualenv
+ mkdir -p /var/log/mhn
+ cd /root/mhn/server/
+ echo ============================================================
============================================================
+ echo '  MHN Configuration'
  MHN Configuration
+ echo ============================================================
============================================================
+ python generateconfig.py
Do you wish to run in Debug mode?: y/n n
Superuser email: shernandot@uoc.edu
Superuser password:
Superuser password: (again):
Server base url ["http://149.202.48.250"]:
Honeymap url [":3000"]:
Mail server address ["localhost"]:
Mail server port [25]:
Use TLS for email?: y/n n
Use SSL for email?: y/n n
Mail server username [""]:
Mail server password [""]:
```

Un cop acabada la configuració es posarà a inserta totes les regles d'Snort que contindrà el propi servidor:

```
Imported 500 rules so far...
Imported 1000 rules so far...
Imported 1500 rules so far...
Imported 2000 rules so far...
Imported 2500 rules so far...
Imported 3000 rules so far...
Imported 3500 rules so far...
Imported 4000 rules so far...
Imported 4500 rules so far...
Imported 5000 rules so far...
Imported 5500 rules so far...
Imported 6000 rules so far...
Imported 6500 rules so far...
Imported 7000 rules so far...
Imported 7500 rules so far...
Imported 8000 rules so far...
Imported 8500 rules so far...
Imported 9000 rules so far...
Imported 9500 rules so far...
Imported 10000 rules so far...
Imported 10500 rules so far...
Imported 11000 rules so far...
Imported 11500 rules so far...
Imported 12000 rules so far...
Imported 12500 rules so far...
Imported 13000 rules so far...
Imported 13500 rules so far...
Imported 14000 rules so far...
Imported 14500 rules so far...
Imported 15000 rules so far...
Imported 15500 rules so far...
Imported 16000 rules so far...
Imported 16500 rules so far...
Imported 17000 rules so far...
Imported 17500 rules so far...
Imported 18000 rules so far...
Imported 18500 rules so far...
Imported 19000 rules so far...
Finished Importing 19419 rules.  Committing data
```

Al acabar es reiniciaran els serveis instal·lats i haurem de comprovar que tots estan funcionant, per fer-ho executarem aquestes 3 comandes:

sudo /etc/init.d/nginx status

sudo /etc/init.d/supervisor status

sudo supervisorctl status

```
root@vps280399:~# sudo /etc/init.d/nginx status
 * nginx is running
root@vps280399:~# sudo /etc/init.d/supervisor status
 is running
root@vps280399:~# sudo supervisorctl status
geoloc                           RUNNING    pid 32689, uptime 16:13:49
honeymap                         RUNNING    pid 32690, uptime 16:13:49
hpfeeds-broker                   RUNNING    pid 13096, uptime 16:16:13
kippo                            RUNNING    pid 2628, uptime 15:47:04
mhn-celery-beat                  RUNNING    pid 1739, uptime 16:02:33
mhn-celery-worker                RUNNING    pid 1806, uptime 16:01:11
mhn-collector                    RUNNING    pid 1743, uptime 16:02:33
mhn-uwsgi                        RUNNING    pid 3256, uptime 4:29:21
mnemosyne                        RUNNING    pid 30948, uptime 16:14:31
root@vps280399:~#
```

Ja tenim el server principal funcionant. Podem accedir al navegador amb la IP pública del servidor:

http://149.202.48.250

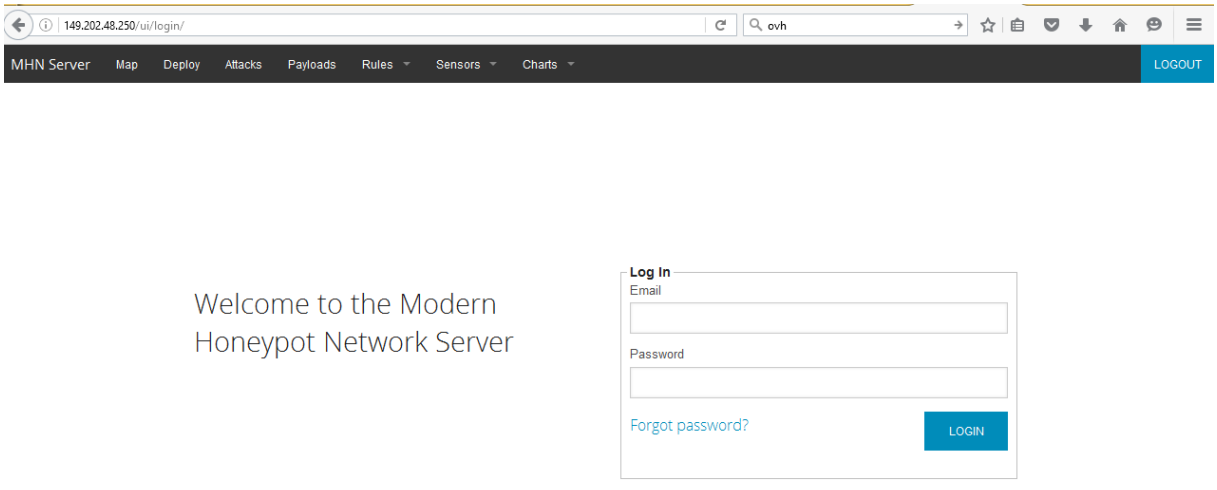


Figura 9 Web principal del nostre Modern Honey Network

Per entrar hem d'iniciar amb el correu i el password introduïts a la configuració. Ara que ja es té el servidor muntat i funcionant, es tractarà d'afegir tots els Honeypots possibles a la resta de servidor

que hem preparat, i connectar-los a aquest servidor "central" per poder-los gestionar. Més endavant i un cop afegim els Honeypots, analitzarem amb detall les opcions que ens oferirà la web del servidor.

També s'haurà d'instal·lar el SO de les 6 màquines Virtuals que junt amb el servidor formaran part d'aquesta Honeynet. Les màquines que estan en les VPS dels proveïdors s'instal·laran automàticament després de que escollim el SO i els paràmetres, després el mateix distribuïdor ens les oferirà ja instal·lades al cap d'una estona. Les 2 màquines virtuals que estan a la xarxa interna, les hem instal·lat descarregant-nos la distribució que volíem i fent una instal·lació des de 0 amb el virtualbox.

4.5.1 Distribució HoneyDrive

Una de les màquines virtuals que formaran part de la xarxa de Honeypots, concretament una de les que hem preparat a la xarxa local, conté la distribució Honeydrive (tal com s'ha comentat al apartat anterior). En aquest apartat comentarem mica les característiques d'aquesta distribució ja que després d'analitzar-ne vàries, creiem que és la més interessant de totes i la més complerta.

Aquesta distribució està basada en Xubuntu 12.04 Desktop. És una distribució clarament enfocada a muntar Honeypots, ja que conté software que serveix per crear molts dels tipus de Honeypots existents. A més d'aquest software també conté moltes eines per poder extreure tot el partit a aquest software. Algunes de les eines que trobarem en aquesta distribució de Linux son:

- Kippo SSH Honeypot,
- Dionaea malware Honeypot
- Amun malware Honeypot
- Glastopf web Honeypot,
- Conpot SCADA/ICS Honeypot.
- Honeyd Honeypot de baixa interacció,
- LaBrea sticky Honeypot,
- Thug and PhoneyC honeyclients
- Eines de seguretat forense i eines anti-malware per monitorització de xarxa, malicious shellcode maliciós i anàlisis de PDF com ntop, p0f, EtherApe, nmap, DFF, Wireshark,

Recon-ng, ClamAV, ettercap, MASTIFF, Automater, UPX, pdftk, Flasm, Yara, Viper, pdf-parser, Pyew, Radare2, dex2jar i més.

4.6 Elecció de Honeypots

Existeixen múltiples opcions de Honeypots, que analitzen múltiples serveis i realitzen infinitat de tasques diferents. Per a la nostre Honeynet, s'han escollit els que ens han semblat més útils i complerts. Els analitzarem amb una mica més de detall en aquest apartat.

-KIPPO

Kippo és un Honeypot que s'encarrega d'aixecar un servei SSH al port que li indiquem que registra tots els intents d'autenticació realitzats contra aquest servei. És àmpliament configurable i personalitzable. Es pot usar per localitzar un atacant, al que inclús deixa iniciar sessió al sistema i li permet interactuar amb un sistema de fitxers fictici, que també és configurable

- **Glastopf**

Aquest Honeypot és capaç d'emular milers de vulnerabilitats web amb l'objectiu de recopilar informació d'aquests atacs, com la injecció SQL i la inserció remota d'arxius, entre molts altres

- **Dionaea**

El principal objectiu és la captura i anàlisis de mostres de malware. És capaç d'aixecar varis serveis i espera que els atacants intentin fer-se amb el control d'aquests serveis per mitja de

peticions malicioses, intentant que l'atacant enviï una mostra de malware per al seu posterior anàlisis. Dedicarem un apartat sencer a analitzar aquest Honeypot

DionaeaFR

-Snort

Snort és un sniffer de paquets i un detector d'intrusos basat en xarxa. Permet registrar, alertar i respondre contra qualsevol anomalia prèviament definida. Pot funcionar com sniffer o com a IDS. Te una base de dades d'atacs que s'actualitza constantment i que es pot afegir utilitzant internet. Aquesta base de dades d'atacs s'actualitza constantment amb les definicions d'atacs que aporten els propis usuaris. Te la opció de incloure regles, creades per defecte per els propis usuaris, modificar aquestes regles o crear-ne de noves. Aquestes regles son les que utilitzarà (estarà atent) Snort un cop estigui actiu. Aquest programa es pot configurar per treballar com un Honeypot més dins de la nostre Honeypot Network.

P0f

Honeypot que captura la finguerprint del atacant, com el SO, la seva versió i el tipus de connexió utilitzada. Això ho aconsegueix analitzant les estructures dels paquets TCP/IP.

Cowrie

És un Honeypot SSH de mitjana interacció dissenyat per registrar atacs de força bruta i la intereacció amb el shell del atacant. Conté opcions interessants com deixar al atacant la possibilitat d'afegir i eliminar arxius, ja que conté un sistema d'arxius complert fals. L'atacant pot veure arxius com el /etc/passwd. Cowrie a més emmagatzema dades en un format

compatible amb UML, i també guarda els arxius descarregats amb Wget per a una posterior inspecció.

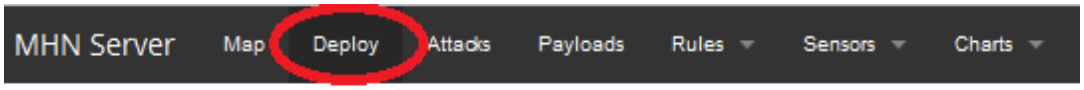
Wordpot

Wordpot és un Honeypot Wordpress que detecta sondes per als plugins , themes, TimThumb i altres arxius comuns utilitzats per les empremtes digitals d'una instal·lació de WordPress.

4.7 Instal·lació de Honeypots i connexió al servidor central

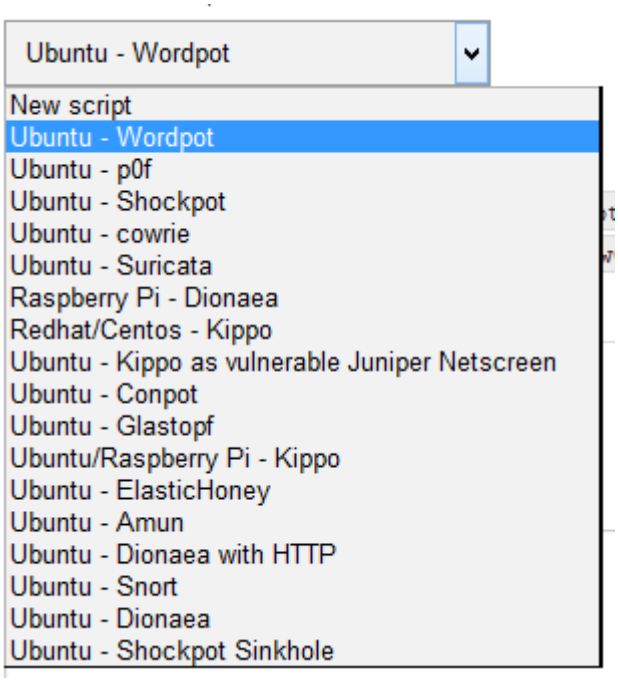
Ara ja disposem del servidor central que ens servirà per gestionar tota la xarxa de Honeypots. El següent pas serà instal·lar tots els Honeypots escollits en la xarxa de servidors que hem preparat al llarg del mapa.

Des del mateix servidor central haurem d'entrar al apartat "Deploy"



Allà tenim una llista dels Honeypots que podem manar afegint a la nostra xarxa, o també tenim la opció d'afegir de nous que no estiguin a la llista, introduint un nou script i generant una nova comanda que posteriorment haurem d'executar a la màquina on volem desplegar el Honeypot en concret. Per al nostre treball mostrarem les passes per instal·lar un dels Honeypots en una de les màquines, ja que no es l'objecte del treball ensenyar com instal·lar tots i cadascun d'ells.

Anem a instal·lar un Honeypot Wordpot a la VPS del proveïdor OVH que tenim situada a Canadà. Dins del apartat Deploy escollirem aquest Honeypot de la llista:



Al escollir ens generarà la comanda que haurem d'executar en el Servidor on volem instal·lar aquest Honeypot:

wget "http://149.202.48.250/api/script/?text=true&script_id=17" -O deploy.sh && sudo bash deploy.sh http://149.202.48.250 qMJQkwGe

Com podem observar, aquesta comanda executarà un script que tenim situat al nostre servidor central (amb ip 149.202.48.250). El script instal·larà el Honeypot, el configurarà i el connectarà al servidor central. Als annexes del treball mostrarem que fa exactament aquest script.

Un cop s'ha revisat tot el que hem comentat anteriorment, anem a fer la instal·lació esmentada. Ens connectem amb PuTTY al Servidor de Canadà que té la IP pública 158.69.204.68

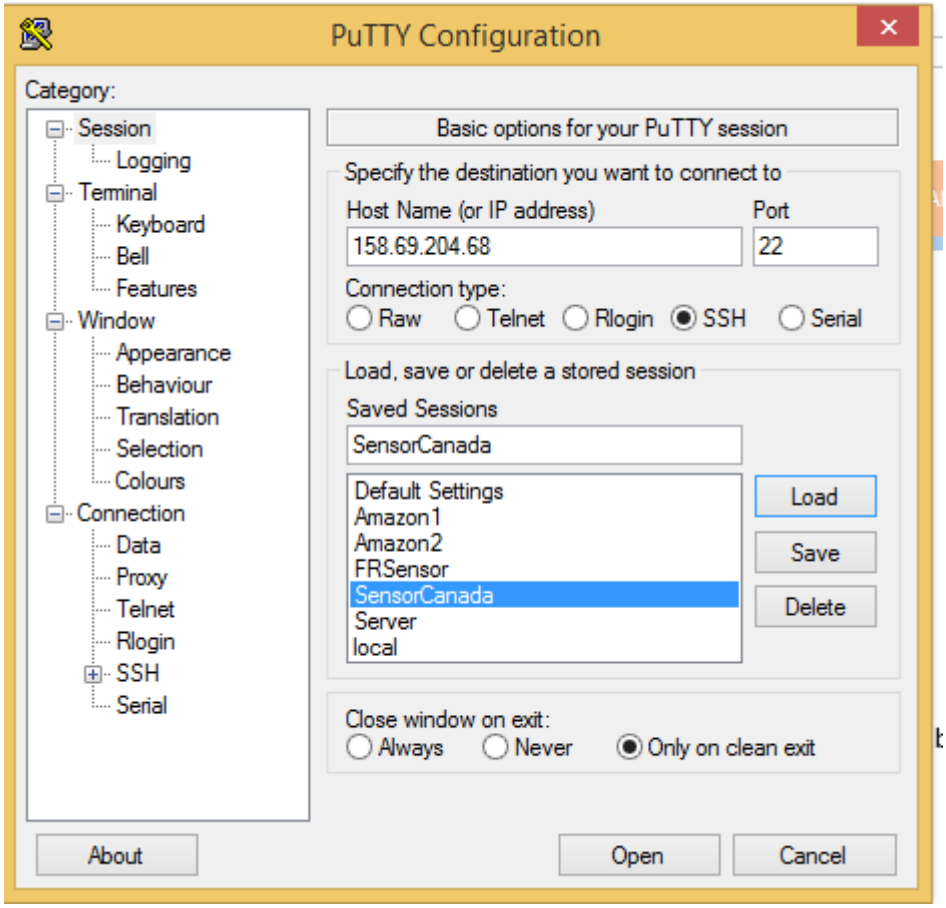


Figura 10 PuTTY

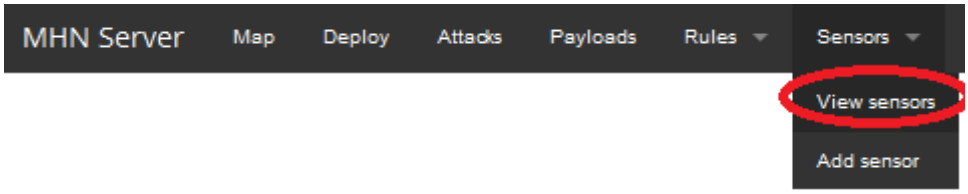
Accedim amb l'usuari root i la password que es va configurar en el seu moment. Aquest servidor prèviament ha sigut instal·lat i configurat i està preparat per poder instal·lar el Honeypot en concret. S'executa la comanda descrita anteriorment:

```
root@vps80943:~# wget "http://149.202.48.250/api/script/?text=true&script_id=17"
 -O deploy.sh && sudo bash deploy.sh http://149.202.48.250 qMJQkwGe
```

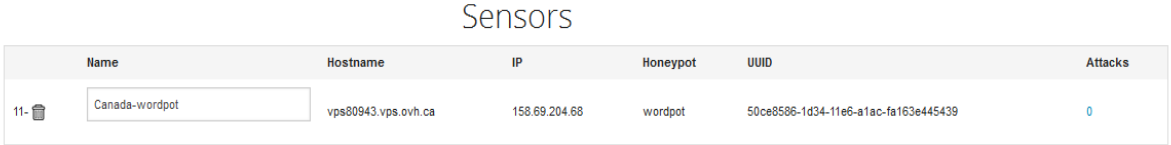
Un cop descarregats els paquets necessaris (els que defineix el script), instal·lat el software, configurat i iniciat el servei, tindrem el Honeypot Wordpot instal·lat la màquina:

```
69e291c41883862fe0dc7c1430
  Running setup.py bdist_wheel for itsdangerous ... done
  Stored in directory: /root/.cache/pip/wheels/fc/a8/66/24d655233c757e178d45dea2
de22a04c6d92766abfb741129a
  Running setup.py bdist_wheel for MarkupSafe ... done
  Stored in directory: /root/.cache/pip/wheels/a3/fa/dc/0198eed9ad95489b8a4f45d1
4dd5d2aee3f8984e46862c5748
Successfully built Flask itsdangerous MarkupSafe
Installing collected packages: Werkzeug, MarkupSafe, Jinja2, itsdangerous, Flask
, hpfeeds-threatstream
  Running setup.py develop for hpfeeds-threatstream
Successfully installed Flask-0.10.1 Jinja2-2.8 MarkupSafe-0.23 Werkzeug-0.11.9 h
pfeeds-threatstream itsdangerous-0.24
+ cp wordpot.conf wordpot.conf.bak
+ sed -i '/HPFEEDS_.*/d' wordpot.conf
+ sed -i 's/^HOST\s.*/HOST = '\''0.0.0.0'\''/' wordpot.conf
+ cat
+ cat
+ supervisorctl update
wordpot: added process group
root@vps80943:~#
```

Ara tornarem a la web d'administració central de la nostra xarxa de Honeypots, anem a comprovar que efectivament s'ha afegit a la nostra xarxa. Per fer-ho accedim al apartat "View Sensors" que hi ha dins de Sensors:



Aquí observarem que el Honeypot Wordpot ha sigut afegit correctament. Ens apareix la IP del servidor on s'ha instal·lat, el tipus de sensor i el nom que li hem posat (En aquest cas Canadà al ser el servidor allotjat allà).



Òbviament en aquest moment els atacs rebuts son 0 ja que fa pocs minuts que hem començat a recol·lectar dades. El deixarem varis dies perquè el número d'atacs creixi suficient com per poder fer un bon anàlisi d'ells.

Aquest mateix procés el repetirem tantes vegades com Honeypots vulguem afegir a la nostra xarxa, i cadascun instal·lant-lo a la màquina escollida. La nostra xarxa ha arribat a tenir 20 Honeypots captant informació a la vegada, però finalment s'ha optat per deixar-los en els 10 que més dades interessants ens podien aportar, mes 3 Honeypots més de prova que no ens aporten resultats.

Després de configurar una a un tots els Honeypots de la nostra xarxa, cadascun al servidor escollit prèviament, podem veure una imatge de tots els sensors actius connectats al nostre servidor central. En el nom he posat la ubicació de cadascun i el Honeypot que contenen. A més es pot veure un resum del número d'atacs rebuts per cadascun en el moment de fer la captura. Podem observar també que apareixen els Honeypots que tenim a la nostra xarxa local, i que tenen el nom de "CASA", i que també formen part de la nostra xarxa de Honeypots "global".

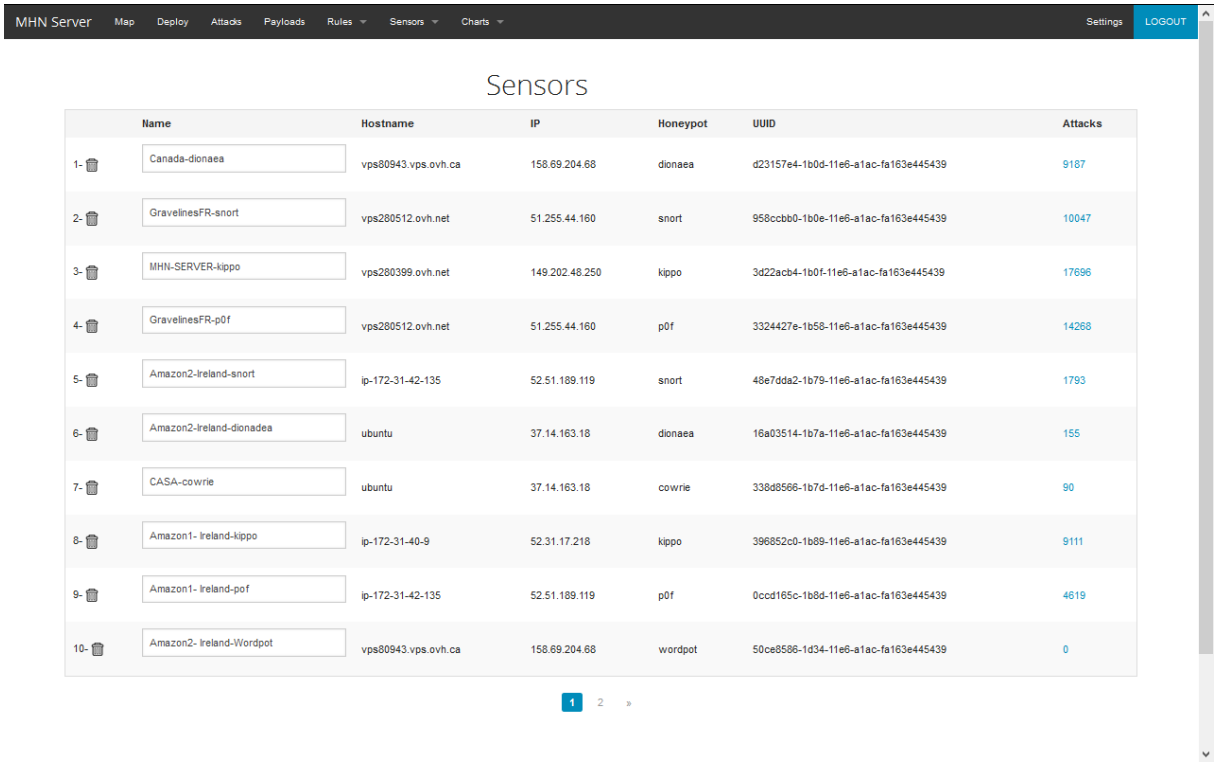


Figura 11 Sensors (Honeypots) del projecte

Un altre apartat del nostre servidor que podem configurar son les regles Snort que contindrà el server per monitoritzar els atacs. Aquestes regles les hem afegit a la instal·lació, però també en podem afegir

manuals. Hi ha més de 20mil regles instal·lades i actives funcionant al nostre servidor, totes elles activades. Si fos necessari es poden desactivar individualment les que no ens interessen.

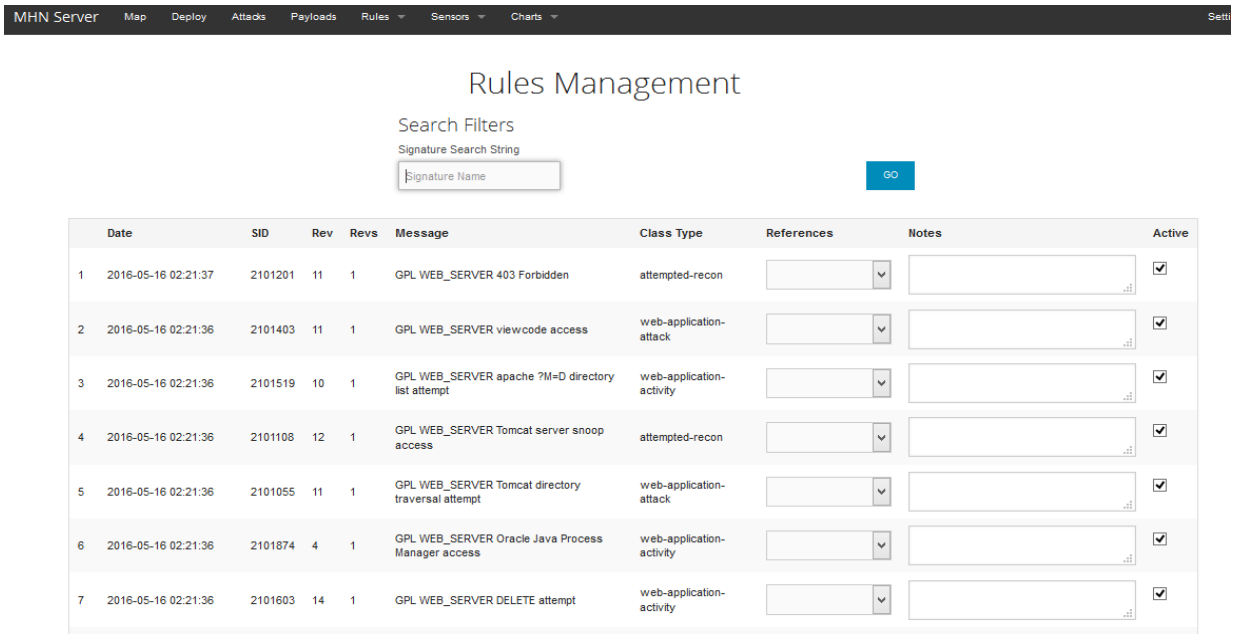


Figura 12 Regles Snort

Totes aquestes regles seran configurades als servidors en els que despleguem Snort i que afegim a la nostra xarxa de Honeypots.

5.- Anàlisis forense

5.1 Metodologia d'anàlisis forense

Anteriorment hem definit l'anàlisi forense com la utilització de tècniques analítiques a una infraestructura tecnològica, tant de hardware com de software, que permeten trobar evidències que col·laborin a portar endavant una causa judicial. Aquesta anàlisis forense necessita seguir una metodologia clara que ens permeti trobar les evidencies, i aquesta metodologia no existeix. Existeixen però bones directrius i indicacions que ens ajuden a fer un

anàlisis forense amb un cert ordre que , aplicades correctament, col·laboren a realitzar un anàlisis forense amb èxit.

Un anàlisis forense es fonamenta en els següents passos:

Identificació

En aquesta fase realitzarem una avaluació dels recursos i els objectius principals per realitzar una investigació interna. També és el moment de documentar-se de tots els antecedents i accions precedents a la investigació. En aquest primer moment s'haurà d'obtenir per escrit l'autorització per començar a realitzar l'anàlisi forense i haurem de signar algun acord de confidencialitat.

Després d'aquests passos preliminars haurem de començar a identificar les evidències, i haurem d'identificar els dispositius implicats com també haurem de descartar els que no es portaran a terme cap anàlisis. És important identificar els discs durs ja que en la majoria de casos, seran els pilars fonamentals de la investigació. Un cop identificades les evidències haurem de recol·lectar-les.

Preservació

Aquest cas és molt important ja que una mala preservació de les evidències pot invalidar tota la investigació davant d'un tribunal. És important mantenir una cadena de custodia de les evidencies per evitar qualsevol tipus de manipulació, al igual que també el lloc on s'emmagatzemin ha de tenir unes condicions de seguretat, sempre mantenint la cadena de custodia.

Anàlisis

Aquest és el pas més extens de un anàlisi forense ja que aquí serà on s'haurà d'esbrinar qui ha causat la evidència, com s'ha causat aquesta evidència o quina és l'afectació que ha tingut en el sistema. Tot això serà investigat de tal manera que s'aconsegueixi reunir la màxima informació possible per, en el següent pas, poder redactar un informe concís. ÉS important

remarcar que aquesta investigació mai s'ha de fer sobre les dades originals sinó amb les dades recol·lectades en la fase anterior. Igualment tots els resultats obtinguts en el procés ha de poder ser verificable i reproduïble en qualsevol moment.

Presentació

En aquesta última fase serà on , amb tota la informació obtinguda a les fases anteriors, es redactarà l'informe i es farà la presentació dels resultats obtinguts. Es pot diferenciar si es farà un informe tècnic o executiu. En l'informe tècnic el públic també serà tècnic i amb coneixements de la matèria, així que es detallarà exactament tots els passos realitzats. Si aquesta presentació es presenta en una causa judicial en canvi, no es farà us de tecnicismes i haurà de ser molt més clara i concisa

5.2 Recopilació d'evidències

En el nostre cas, l'anàlisi forense no te com a objecte ser presentat en un procés legal, per tant la metodologia genèrica que hem definit en l'apartat anterior no serà aplicada exactament. A més a més un dels punts forts dels Honeypots es que no només fan la funció de simular equips reals per ser atacats, sinó que el mateix software incorpora moltes eines que ens ajudaran a preservar i analitzar les evidències, per posteriorment, ajudar-nos a realitzar un informe detallat per poder extreure-hi conclusions.

5.3 Anàlisis d'evidències

Aquest apartat el dividirem en 2 subapartats. Primerament analitzarem les evidencies rebudes a la nostra xarxa de Honeypots. En la nostra web principal del projecte tenim una recopilació de totes les evidències recollides per tots els Honeypots que formen part de la nostra xarxa. Veurem tots els apartats interessants de la web del nostre servidor i les dades recopilades. En

el segon subapartat entrarem en un dels servidors que formen part de la nostra xarxa local (concretament el que té instal·lada la distro Honeydrive[9] i analitzarem un dels Honeypots en concret, mostrant les dades recopilades per aquest Honeypot).

5.3.1 Anàlisis d'evidències de la Xarxa de Honeypots

Un cop tenim muntada tota la xarxa de Honeypots i els hem deixat recopilant dades uns dies, procedirem a analitzar les evidències rebudes a la nostra xarxa. En el nostre servidor tenim múltiples opcions per visualitzar totes les dades recopilades, començarem per veure la pàgina principal (després de loguejar-nos en ella amb el nostre usuari i password. En aquesta pàgina podem observar la llista de les 5 IPs de les que més atacs hem rebut, junt amb els 5 Honeypots i màquines que més evidències han recopilat, les 5 ports més atacats i les 5 signatures d'atacs més usades, tot això en les últimes 24 hores:

[9] Veure subapartat 4.5.6

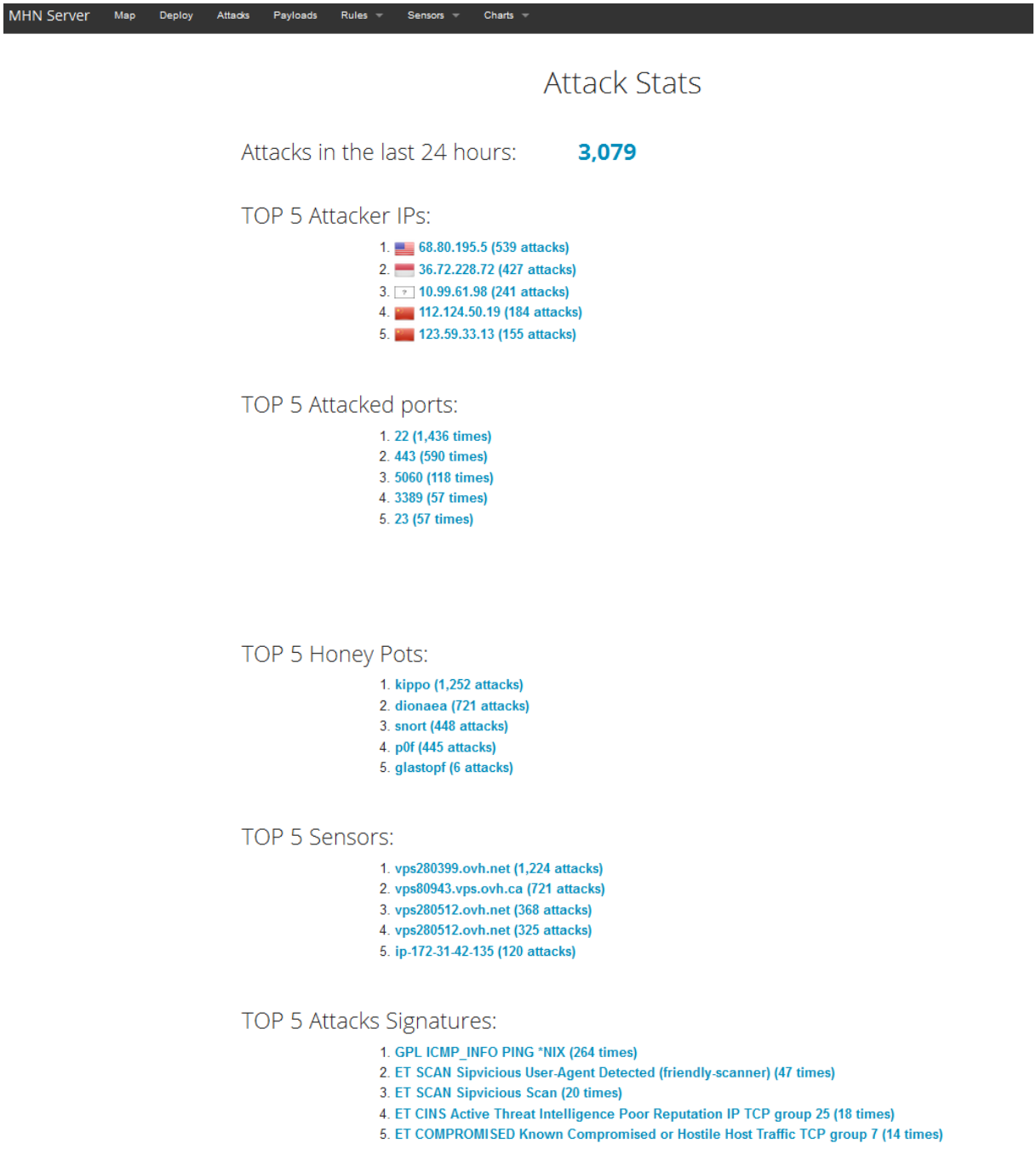


Figura 13 Web principal del MHN

Això ens pot donar una idea Global de la nostra xarxa de captura.

Aquesta informació, però ara si que completa la trobarem al apartat “Atacks” del nostre server. Aquí si que trobarem tots els atacs rebuts per la nostra xarxa. Podem filtrar per Honeypot, per màquina, per dies o inclús per ports. També veurem el país de procedència del atac. Aquesta eina és molt interessant

ja que podem fer un estudi detallat gràcies a les múltiples estadístiques recopilades i als múltiples filtres que podem aplicar.

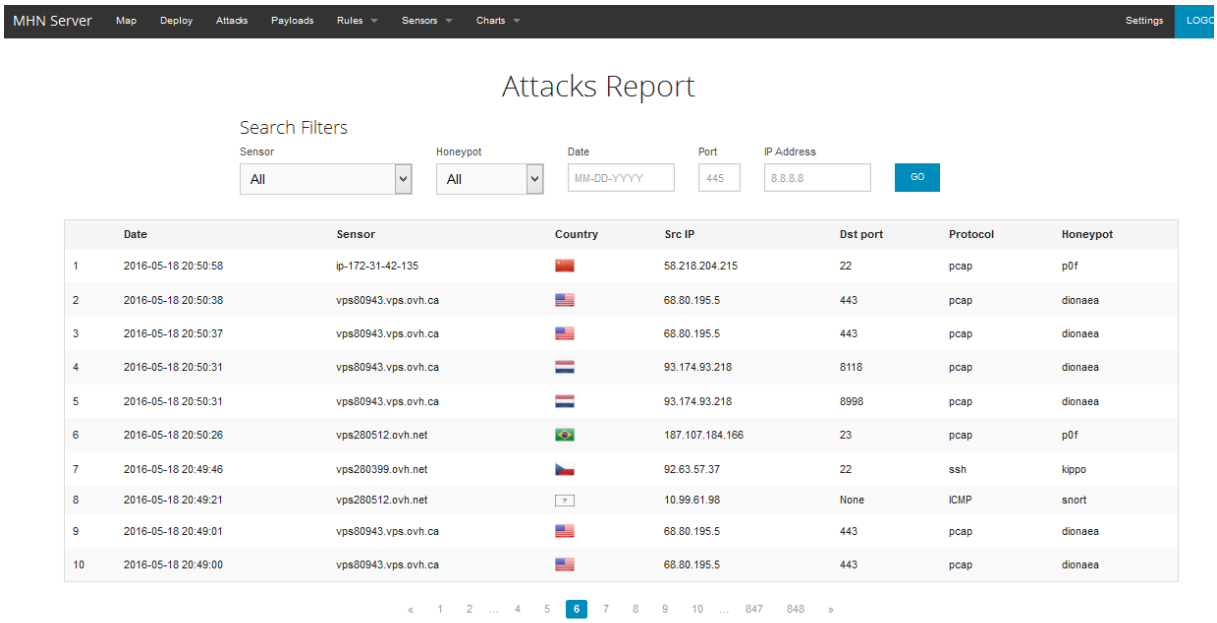


Figura 14 Report d'atacs

Molt interessant també la informació que trobem a Payloads. En aquest apartat ens mostra les alarmes Snort que han saltat a partir de les regles que hem configurat al final d el apartat 4.7. dins dels servidors en els que hem instal·lat Snort, que en el nostre cas son 2, el situat a Gravelines (França) i un dels 2 d'Amazon situats a Irlanda.

El servidor no només té aquesta integració amb Snort, sinó que també la té amb els Honeypots Kippo i cowrie, i al apartat "charts" podem veure diferents gràfiques que ens mostren informació recopilada en els atacs. Mostrarem una d'elles com exemple, en aquest cas ens mostra els passwords amb els que més nombres de vegades han intentat accedir.

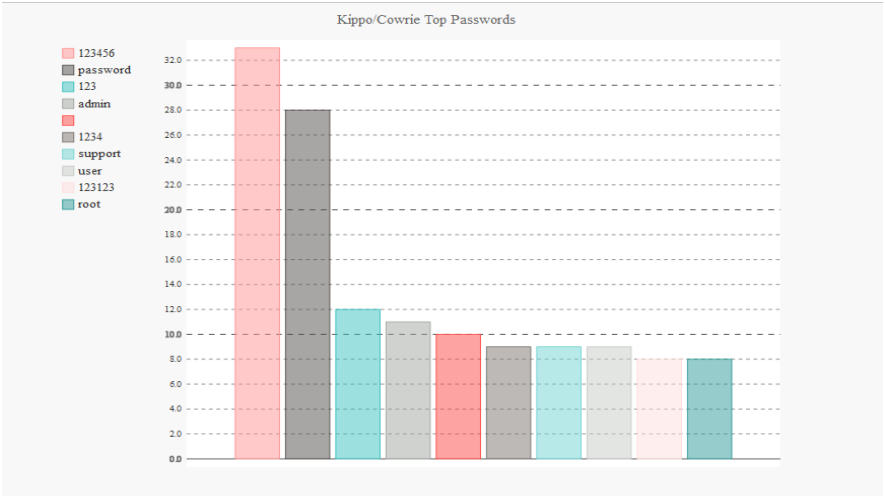


Figura 15 Top Passwords usats

Una altra funcionalitat que ens aporta el nostre servidor és la visualització del mapa del món en temps real, on ens mostra en cada moment els atacs que estan rebent alguns dels nostres Honeypots desplegats arreu del món. En temps real podem observar l'origen del atac i el Honeypot que l'ha detectat, tot en un entorn gràfic molt treballat. La següent captura ens mostra un exemple d'un moment concret amb els atacs que estem rebent en temps real. A la part de sota apareix un log que ens indica l'origen exacte del atac junt amb el Honeypot que el detecta.

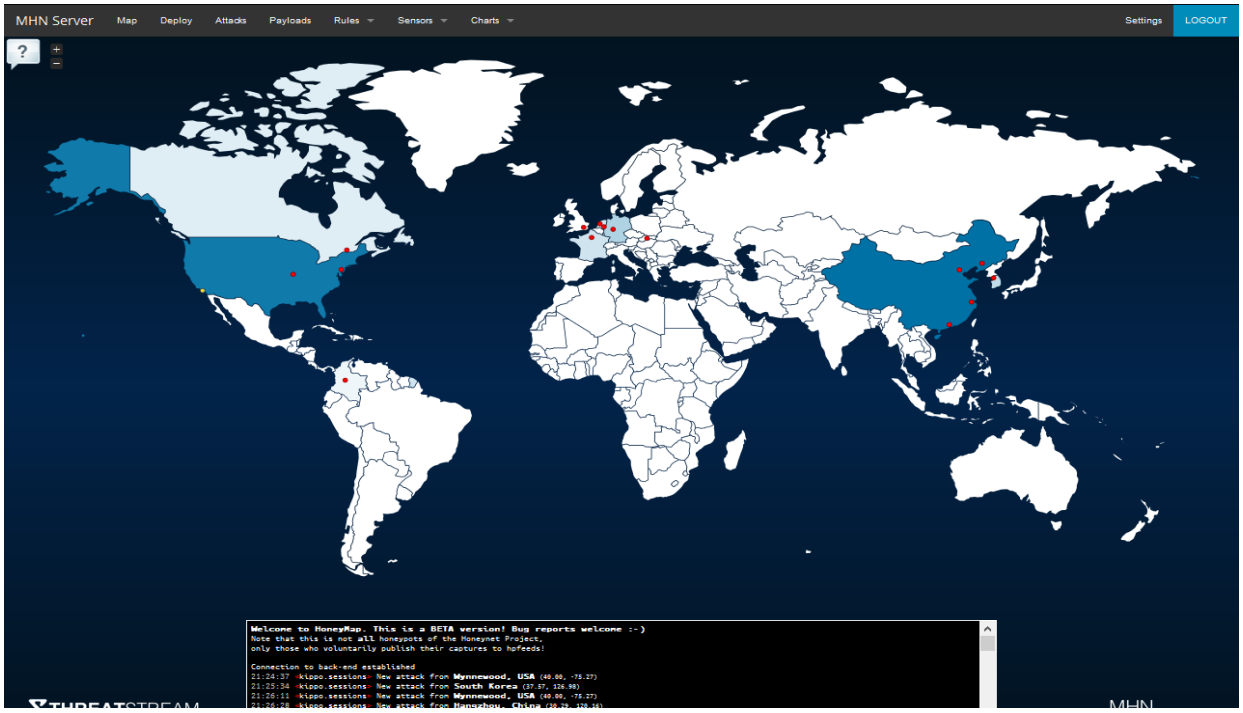


Figura 16 Mapa del món d'atacs en temps real

5.3.2 Anàlisis d'evidències del Honeypot Dionaea

A part del que hem vist en l'apartat anterior, amb la recopilació de dades que ens mostra el nostre servidor central de Honeypots, en aquest apartat volem endinsar-nos una mica més en l'anàlisi d'un dels Honeypots que formen part de la nostra xarxa. De tots els que disposem desplegats, el que més interessant i més dades de valor ens ha aportat és el Honeypot Dionaea. A més de ser el que més dades de valor ens ha aportat, té un entorn gràfic molt treballat i una alta usabilitat.

La màquina en la que realitzarem l'anàlisi és la màquina local que conté la distro Honeydrive[10], que com hem comentat anteriorment, forma part també de la nostra xarxa de Honeypots connectada al servidor central. En l'apartat 4.6 s'ha explicat per sobre quina era la funció exacte d'aquest Honeypot Dionaea, ara hi entrarem una mica més en detall.

El Honeypot Dionaea està desenvolupat en python és capaç de detectar payloads maliciosos i recol·lectar mostres de malware per al seu posterior anàlisis. Els serveis actius d'aquest Honeypot son els següents:

- SMB (Server Message Block): 445
- HTTP (Hypertext Transfer Protocol): 80
- HTTPS (Hypertext Transfer Protocol Secure): 443
- FTP (File Transfer Protocol): 21
- TFTP (Trivial File Transfer Protocol): 69
- MySQL (Structured Query Language): 3306
- MSSQL (Microsoft Structured Query Language Server): 1433
- EPMAP (Endpoint Mapper): 135
- SIP (Session Initiation Protocol): 5060/5061
- Nameserver (Host Name Server): 42

[10] Veure subapartat 4.5.6

Quan un atacant comprova que un d'aquests serveis és vulnerable, el més probable és que intenti a atacar-lo mitjançant peticions malicioses i l'enviament de payloads. En aquest cas el procés de perfilat es fet per Libemu registrant totes les invocacions a les funcions del sistema amb els seus corresponents arguments, és a dir, fent un "hooking"[11] de cadascuna de les funcions definides pel programa. Dionaea també permet l'execució de Shellcode per determinar quin és l'objectiu del programa. Quan el Shellcode ha sigut perfilat després del registre de les funcions invocades i les connexions de xarxa que s'han establert després de la execució del programa maliciós, Dionaea es capaç de determinar la intenció del programa i categoritzar-lo.

Per analitzar els resultats utilitzarem DiadoneaFR, que no és més que un Framework que ens mostrarà els resultats obtinguts amb el Honeypot Dionaea mitjançant una pàgina web.

Per poder executar aquest Framework i iniciar el servei que ens permetrà entrar a la web només haurem d'executar la següent comanda (òbviament, dins el servidor on el tenim instal·lat):

sudo python manage.py runserver 192.168.1.138:600

(la ip 192.168.1.138 és la ip local del servidor on tenim Dionaea)

Ara accedirem a la web, des de la xarxa local, amb qualsevol navegador entrant a l'adreça 192.168.1.138:600

La plana principal ens mostra la següent informació

[11] El terme Hooking engloba una sèrie de tècniques que s'utilitzen per alterar o augmentar el comportament de un SO, les plicacions o altres components de software mitjançant la intercepció de crides a funcions o missatges o events passats entre els components de software. El codi que s'encarrega d'aquest tipus de funció interceptant crides, events o missatges s'anomena Hook (ganxo)

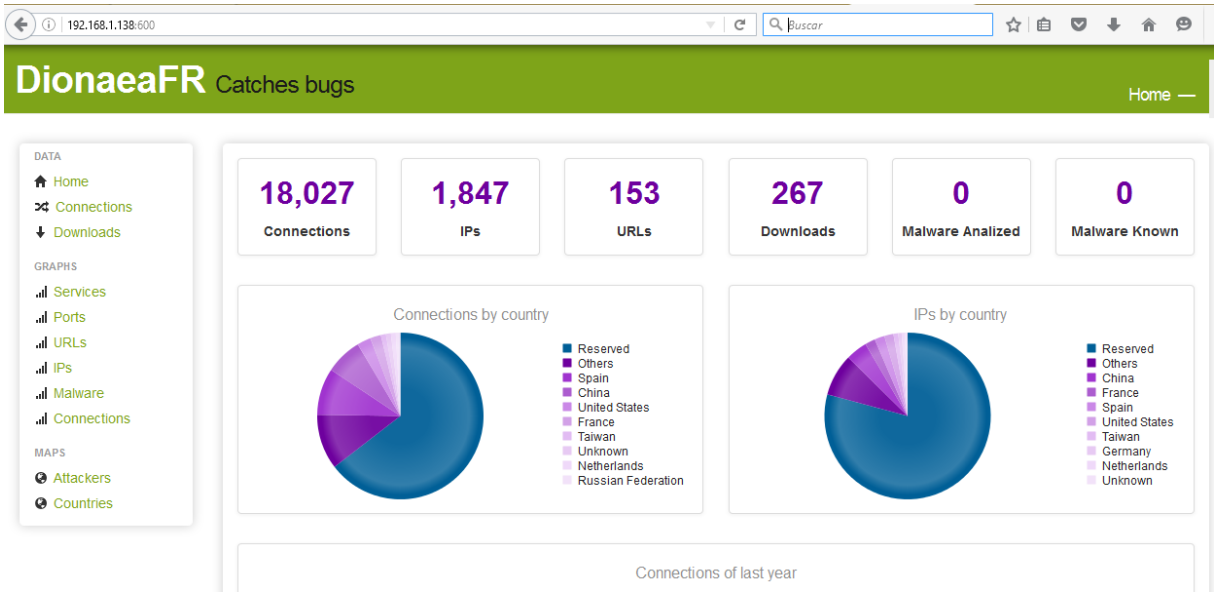


Figura 17 Evidències Dionaea

Com es pot observar al menú de l'esquerra, disposem de múltiples opcions per visualitzar els intents d'intrusió al nostre Honeypot, analitzarem les més importants.

Al apartat "connections" hi trobarem un llistat de totes les connexions rebudes. Aquí podem aplicar filtres de tot tipus per veure només les que ens interessin en aquell moment.

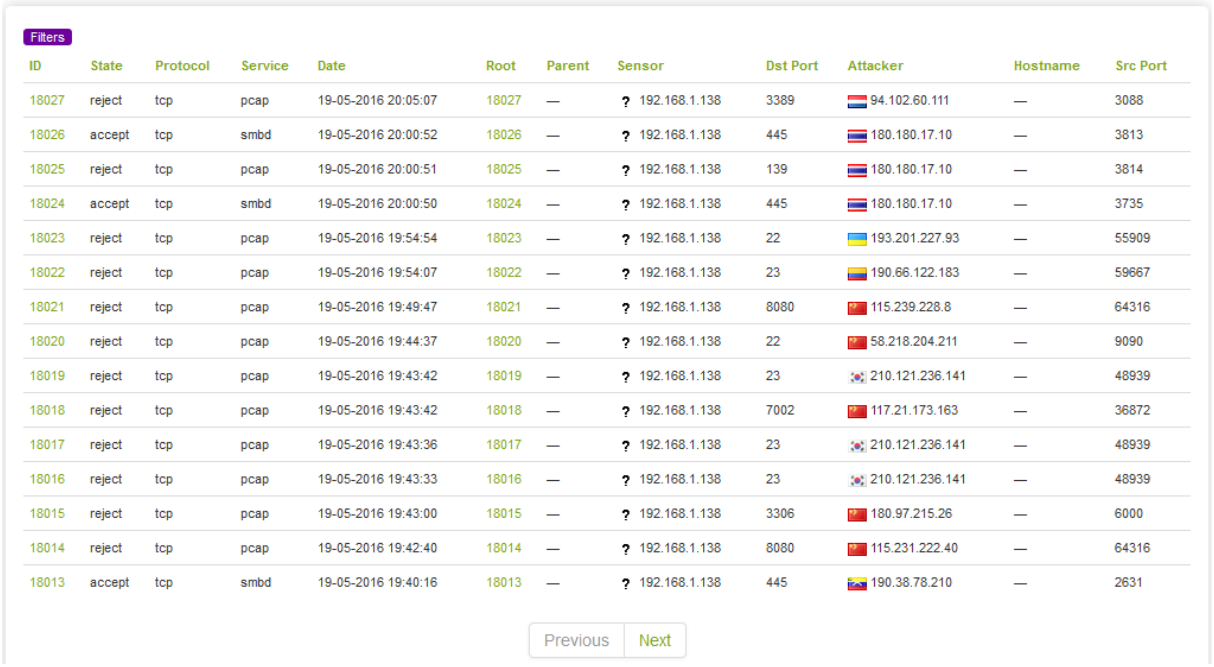


Figura 18 Connexions Dionaea

Al apartat de GRAPHS hi trobarem gràfiques de serveis, ports, url's, IP's, Malware i connexions rebudes. De tots els gràfics disponibles, en les següents captures podem observar el gràfic dels ports més utilitzats i les IPs que més han atacat a aquest Honeypot:

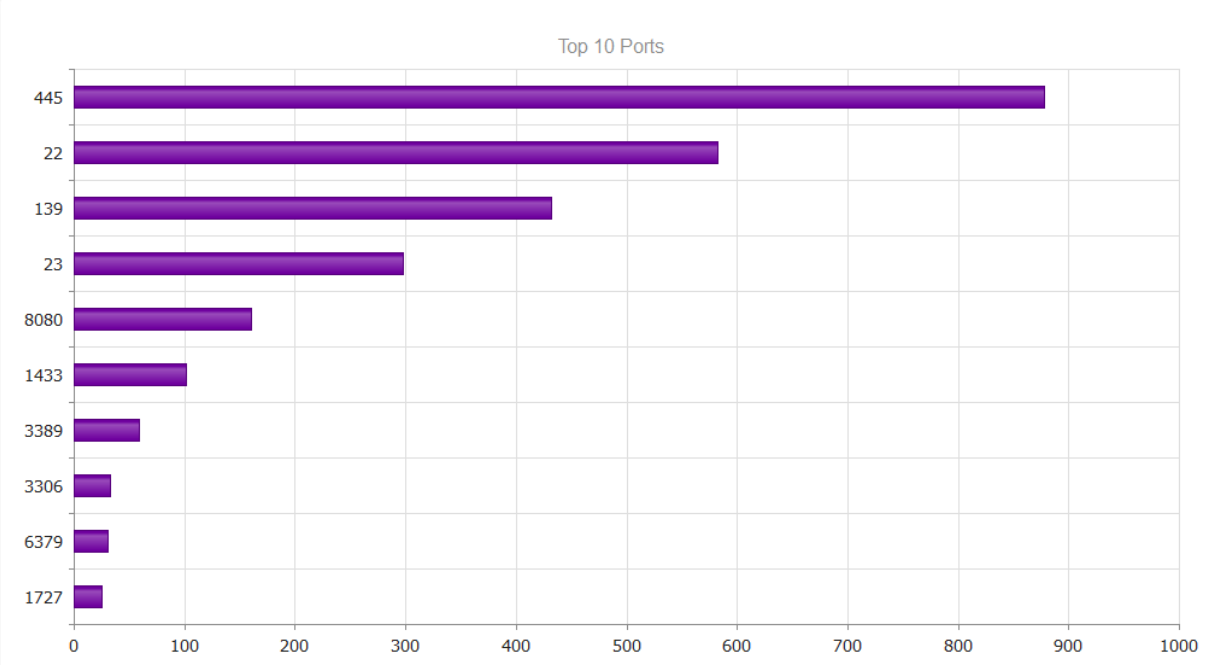


Figura 19 Top 10 ports Dionaea

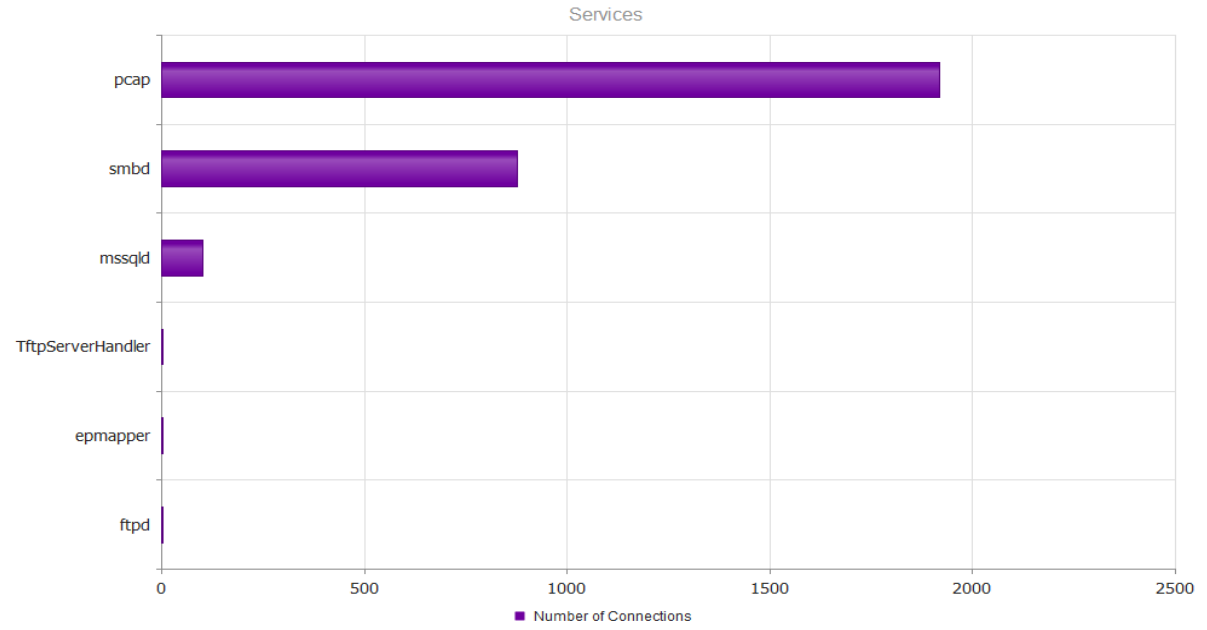


Figura 20 Serveis atacats Dionaea

Finalment a mapes ens mostrarà, en un mapà del món, els punts exactes des d'on s'han realitzat els atacs i amb una classificació de colors (de més clar a més fort segons els atacs rebuts) els països des d'on s'han rebut els atacs

Figura 21 Mapa món d'atacs rebuts

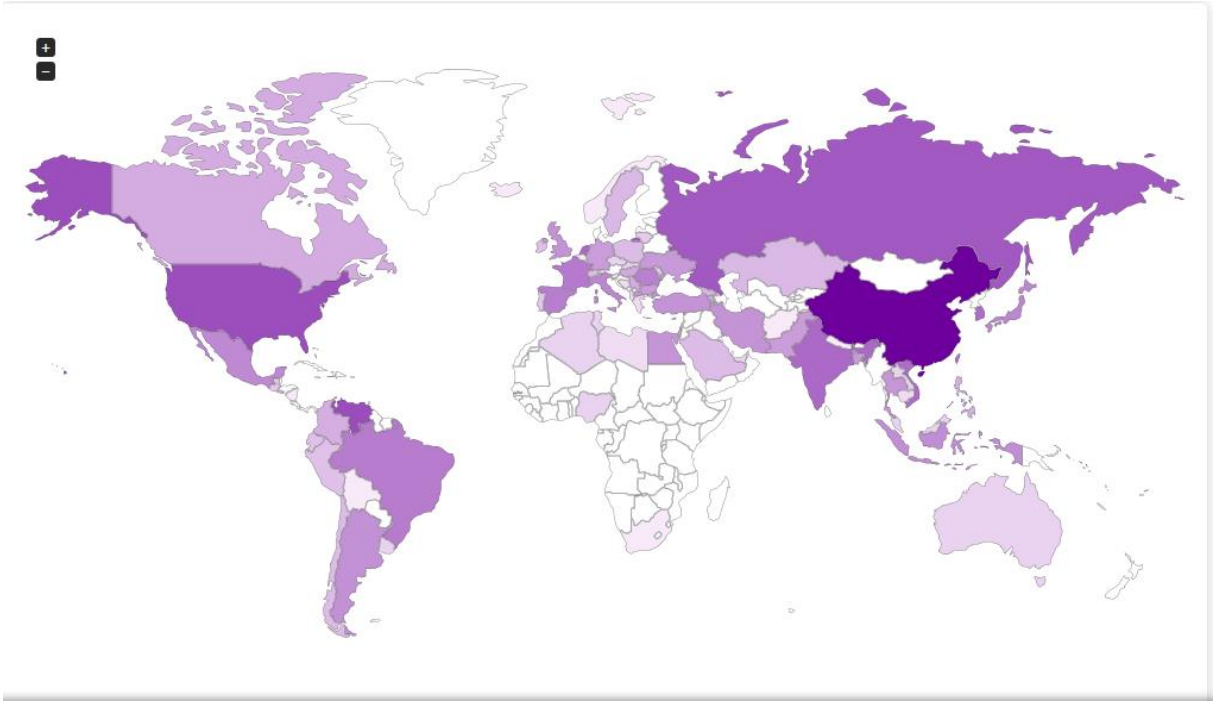


Figura 22 Països amb més atacs (més fosc, més atacs)

5.4 Resum d'evidències

La nostra xarxa de Honeypots segueix activa rebent intrusions, i ho estarà fins a dies posteriors a la presentació del treball, però en el següent apartat farem un resum de les evidències rebudes en les últimes 3 setmanes que és el temps que porta activa la nostra xarxa de Honeypots.

Honeypot	Deteccions
Pof	18905 deteccions
Cowrie	90 deteccions
Kippo	26882 deteccions
Glastopf	142 deteccions
Dionaea	9367 deteccions
Snort	11875 deteccions
Wordpot	0 deteccions

Classificació de ports més utilitzats per els atacants a la nostra xarxa de Honeypots:

Nº de port	Deteccions	Servei
Port 22	41075	SSH
Port 443	6892	Https
Port 5060	2632	SIP
Port 23	2618	Telnet
Port 80	1280	Http
Port 3389	1064	RDP
Port 53	720	DNS
Port 25	683	SMTP
Port 1433	472	SQL Server
Port 445	310	Microsoft-ds

Port 8080	**243**	**Https Tomcat**

Hem rebut atacs a altres múltiples ports, però amb menys de 200 deteccions a cadascun i per tant no els hem considerat com a dades suficientment destacables per afegir a la taula

6.- Conclusions

Avui en dia és habitual veure als mitjans de comunicació notícies relacionades amb atacs informàtics rebuts a institucions, governs, empreses i persones individuals. En un món cada cop més globalitzat i connectat tecnològicament entre si, la seguretat informàtica s'ha convertit en un camp primordial a l'hora de mantenir qualsevol servei informàtic. La informàtica forense s'ha convertit en un camp essencial a l'hora de detectar atacs i atacants, i els Honeypots son una eina més que ens pot ajudar a prevenir aquests atacs. Amb aquest treball hem estudiat com crear una xarxa de Honeypots repartits arreu del món, i com aquesta xarxa de Honeypots creats amb uns recursos al abast de tothom, ens poden generar dades molt vàlides per planificar millor com s'han de protegir els nostres sistemes reals.

Hem demostrat com els sistemes connectats a la xarxa, que són la majoria actualment, estan constantment intentant ser atacats per altres persones arreu del món. I això ens obliga a estudiar més a fons com protegir aquests sistemes per prevenir qualsevol tipus d'intrusió. També hem pogut estudiar com hi ha uns serveis crítics als que s'ha de prestar una major atenció, ja que son víctimes en un tant per cent molt elevats dels intents d'intrusió.
Si s'ha d'instal·lar un sistema informàtic real amb uns serveis concrets, muntar uns Honeypots que simulin plenament aquests serveis ens pot ajudar a prevenir futurs atacs als nostres sistemes reals a partir d'estudiar els atacs rebuts als Honeypots. En el nostre cas hem creat una xarxa de Honeypots per estudiar els atacs rebuts en general en múltiples serveis, però en un sistema informàtic concret podríem crear-los dins del propi sistema, simulant un o varis serveis vulnerables concrets que ens interessin per ser atacats. Això no només ens aporta dades importants per aprendre més del nostre sistema sinó que "distreu" als atacants, que poden pensar que estan atacant a un sistema real, donant-nos més temps de reacció a l'hora de protegir els nostres sistemes.

Inicialment el nostre objectiu del treball consistia en crear un parell de Honeypots de forma local per analitzar les dades obtingudes, però gràcies a l'ajuda del consultor i la investigació trobada sobre els Honeypots, es va decidir que la millor manera de generar suficients dades que ens servissin per poder extreure conclusions més valuoses, consistia en crear una xarxa de Honeypots a nivell global. Aquesta xarxa ha sigut suficientment gran com per obtenir moltes més dades de les que haguéssim obtingut localment, i ens ha permès extreure millors conclusions.
Gràcies a aquesta xarxa de Honeypots els nostres objectius, que volien mostrar la utilitat d'aquests sistemes d'una manera pràctica, han sigut complerts.

La planificació i metodologia proposada inicialment ha sigut seguida al llarg de tot el treball, només ha calgut fer algun petit canvi sobre com s'enfocaven alguns dels temes per centrar-los més amb l'objectiu del treball. El canvi més rellevant i no previst inicialment a tant gran escala, com ja s'ha comentat anteriorment, ha sigut la creació de la xarxa de Honeypots, que connectats a un servidor central han estat recopilant dades al llarg de vàries setmanes.

Els delictes informàtics és un camp on cada dia apareixen noves maneres de vulnerar els sistemes i a la vegada cada dia apareixen noves maneres de protegir-los. És un camp que avança dia rere dia i una línia de treball futur no explorada en aquest treball, perquè encara està en fase de investigació i encara no existeix una versió funcional, seria la creació de xarxes de Honeypots "intel·ligents". Actualment varis investigadors estant estudiant en el projecte Honeymix, que consisteix en crear una plataforma dissenyada de tal manera que els atacants no puguin determinar si estan atacant un sistema real o un Honeypot. Un SDN[12] (Software Defined Network) programable escull quins sistemes seran exposats a cada atacant per a fer la interacció el més real i convincent possible per al intrús. Aquesta investigació i altres relacionades amb el perfeccionament dels Honeypots son un tema interessant per explorar en futurs treballs.

[12] Xarxes definides per software: Conjunt de tècniques amb l'objectiu de facilitar la implementació i implantació de serveis de xarxa, i ho haconsegueix separant el pla de control (software) del pla de dades (hardware)

7.- Glossari

Honeypot: Eina de seguretat informàtica consistent en la simulació d'un equip real vulnerable, amb la finalitat de recollir dades sobre els atacants i les tècniques usades per comprometre els sistemes.

Informàtica forense: Aplicació de tècniques científiques i analítiques que permeten identificar, preservar, analitzar i presentar dades vàlides dins d'un procés legal.

Distro: distribució de software basada en el nucli de Linux que inclou determinats paquets de software per satisfer les necessitats d'un grup específic d'usuaris.

Modern Honey Network (MHN): Projecte que consisteix a crear una xarxa de Honeypots connectats a un servidor central que administra i gestiona els resultats de les evidències detectades.

Virus (informàtic): Malware que té per objecte alterar el funcionament de una computadora o xarxa de computadores sense el permís o el coneixement del usuari.

Malware: abreviatura de "Malicious Software", terme que engloba a tot tipus de programa o codi informàtic maliciós que té com a funció danyar un sistema informàtic o causar un mal funcionament.

Ciberdelinqüència: qualsevol tipus d'activitat il·legal en la que s'utilitzi Internet, una xarxa privada o pública o un sistema informàtic domèstic.

Evidència digital: qualsevol informació en format digital que pugui establir una relació entre un delicte i el seu autor

Firewall: Sistema de xarxa expressament encarregat de separar xarxes de computadors efectuant un control de trànsit entre elles

VPS: Mètode que consisteix en particionar un servidor físic en varis servidors virtuals. Cada servidor virtual pot executar el seu SO i es pot reiniciar de forma independent.

Honeydrive: Distro de Linux enfocada a la creació de Honeypots.

Putty: Client SSH, Telnet, rlogin i TCP raw amb llicència lliure.

Sniffer: Analitzador de paquets. Programa que captura les trames de una xarxa de computadores.

SSH: Nom d'un protocol i del programa que l'implementa que serveix per accedir a màquines remotes a través d'una xarxa.

Shellcode: conjunt de subrutines que busquen manipular un sistema, normalment programades en llenguatge ensamblador.

8.- Bibliografia

I. Llibre: **Honeypots: Tracking Hackers**

Autor: Lance Spitzner 2002

II. Llibre: **Análisis forense de sistemes informáticos** (UOC)

Autors: Helena Rifà Pous, Jordi Serra Ruiz i José Luis Rivas López 2009

III. Llibre: **Introducción a la informàtica forense** (editorial RA-MA)

Autor: Franciso Lázaro Domínguez 2013

IV. Llibre: **Honeynet: Recolección y análisis forense de los ataques detectados en una Honeynet** (Editorial Paperback)

Autors: Nayuribe Girado i Natasha Márquez (2012)

Webgrafia

- Conveni sobre la Ciberdelinqüència- Budapest 23-11-2001

https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

- DionaeaFR: Anàlisi de resultats de un honeypot (Raúl Rodríguez 2013)

http://www.securityartwork.es/2013/04/24/dionaeafr-analisis-de-resultados-de-un-honeypot/

- Captura de malware amb el Honeypot Dionadea (Jonathan Banfi Vázquez 2015)

http://revista.seguridad.unam.mx/numero24/poc-captura-de-malware-con-el-honeypot-dionaea-ii

- EnCase® Forensic

https://www.guidancesoftware.com/encase-forensic

- Modern Honey Network

https://threatstream.github.io/mhn/

- Honeydrive: A honeypot Linux distro

https://bruteforce.gr/honeydrive

- Informatica forense: generalidades, aspectos técnicos y herramientas

Autors : Óscar López, Haver Amaya, Ricardo León

http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf

- Dionaea low interaction honeypot

https://github.com/rep/dionaea

- Kippo - SSH Honeypot

https://github.com/desaster/kippo

- Glastopf Profect

http://glastopf.org/

- Snort detection software

https://www.snort.org/

- Cowrie SSH Honeypot

https://github.com/micheloosterhof/cowrie

- Wordpot: A Wordpress Honeypot

https://github.com/gbrindisi/wordpot

- Honeypots with Modern Honey Network (MHN)

https://fischer-its.com/?p=2076

- Modern HoneyPot Network: dejando un tarro de miel en internet (Joan Escorihuela)

https://www.joanesmarti.com/modern-honeypot-network-dejando-un-tarro-de-miel-en-internet/

- Breaking Honeypots for Fun and Profit

Speaker: DeanSysman, Gadi Evron, Itamar Sher. Event: 32th Chaos Communication Congress [32c3] of the Chaos Computer Club [CCC]

https://www.youtube.com/watch?v=tNqn47kEDb8

Annexes

Script que s'executa al executar la comanda per instal·lar el Honeypot Wordpot i que posteriorment es connecta al nostre servidor central de la nostra xarxa de Honeypots

wget "http://149.202.48.250/api/script/?text=true&script_id=17" -O deploy.sh && sudo bash deploy.sh http://149.202.48.250 qMJQkwGe

```
set -e
set -x

if [ $# -ne 2 ]
    then
        echo "Wrong number of arguments supplied."
        echo "Usage: $0 <server_url> <deploy_key>."
        exit 1
fi

server_url=$1
deploy_key=$2

wget $server_url/static/registration.txt -O registration.sh
chmod 755 registration.sh
# Note: this will export the HPF_* variables
. ./registration.sh $server_url $deploy_key "wordpot"

apt-get update
apt-get -y install git python-pip supervisor
pip install virtualenv

# Get the Wordpot source
cd /opt
git clone https://github.com/threatstream/wordpot.git
cd wordpot

virtualenv env
```

```
. env/bin/activate
pip install -r requirements.txt

cp wordpot.conf wordpot.conf.bak
sed -i '/HPFEEDS_.*/d' wordpot.conf
sed -i "s/^HOST\s.*/HOST = '0.0.0.0'/" wordpot.conf

cat >> wordpot.conf <<EOF
HPFEEDS_ENABLED = True
HPFEEDS_HOST = '$HPF_HOST'
HPFEEDS_PORT = $HPF_PORT
HPFEEDS_IDENT = '$HPF_IDENT'
HPFEEDS_SECRET = '$HPF_SECRET'
HPFEEDS_TOPIC = 'wordpot.events'
EOF

# Config for supervisor.
cat > /etc/supervisor/conf.d/wordpot.conf <<EOF
[program:wordpot]
command=/opt/wordpot/env/bin/python /opt/wordpot/wordpot.py
directory=/opt/wordpot
stdout_logfile=/opt/wordpot/wordpot.out
stderr_logfile=/opt/wordpot/wordpot.err
autostart=true
autorestart=true
redirect_stderr=true
stopsignal=QUIT
EOF

supervisorctl Update
```

Cada Honeypot executarà el seu script en concret, crec que mostrant un d'ells és suficient, ja que mostrar-los tots generaria uns annexes de mes de 50 pàgines

Figures generades desde la nostra web central del servidor central de la nostra xarxa de Honeypots

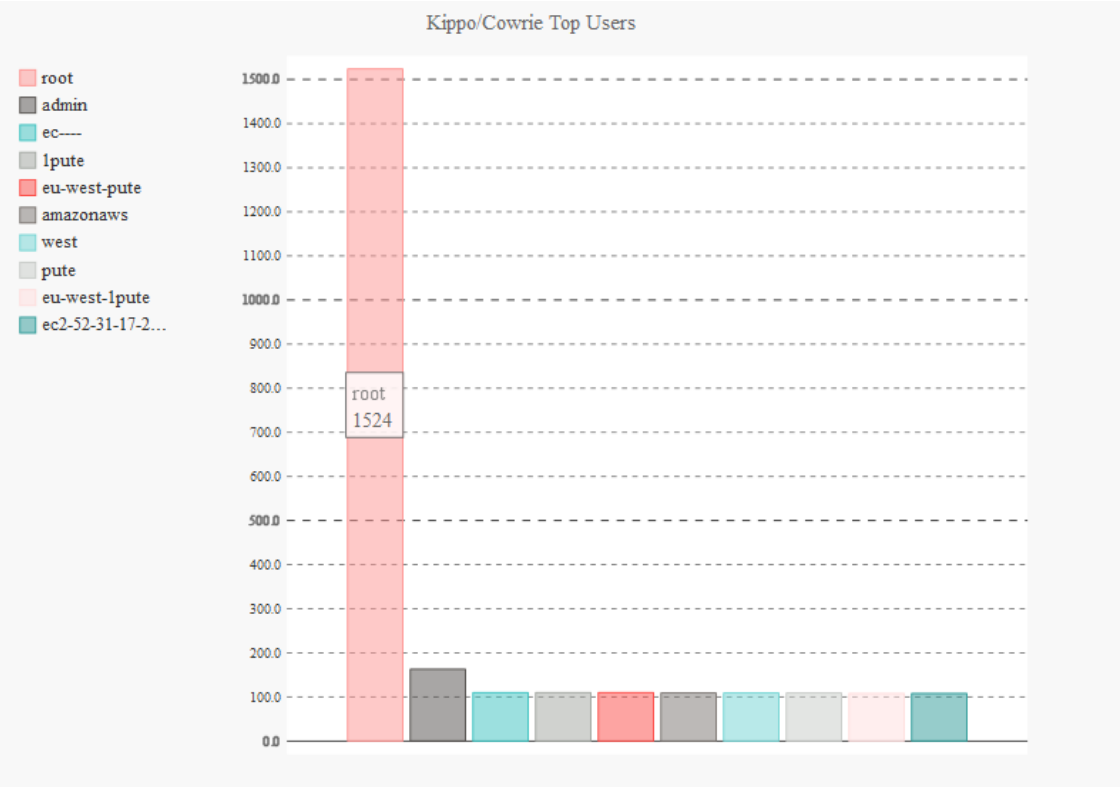


Figura 23 Top Usuaris

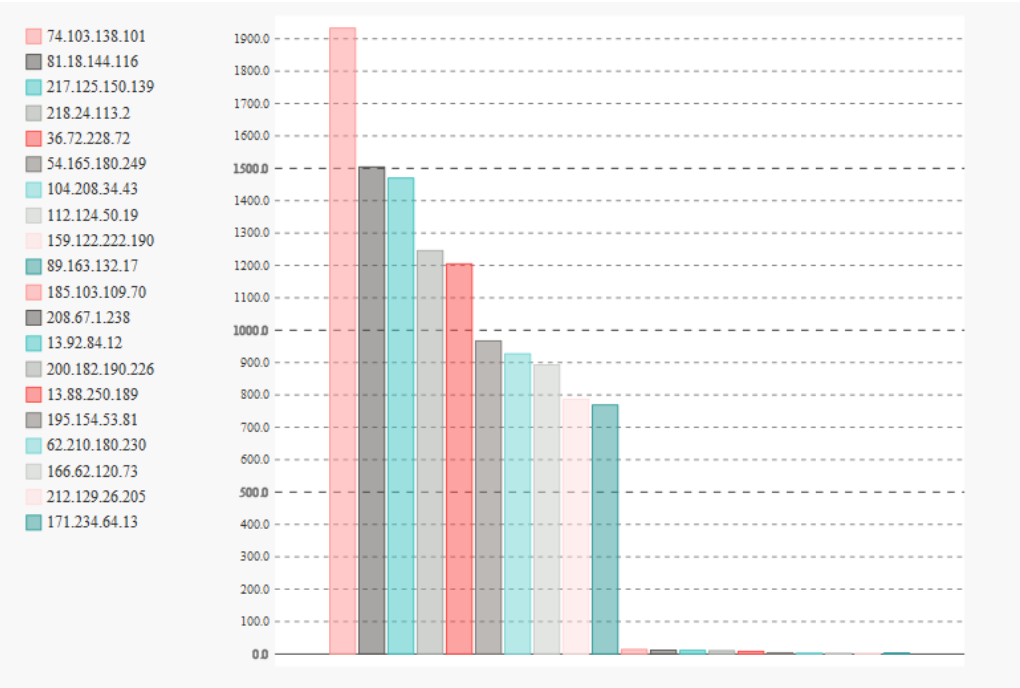
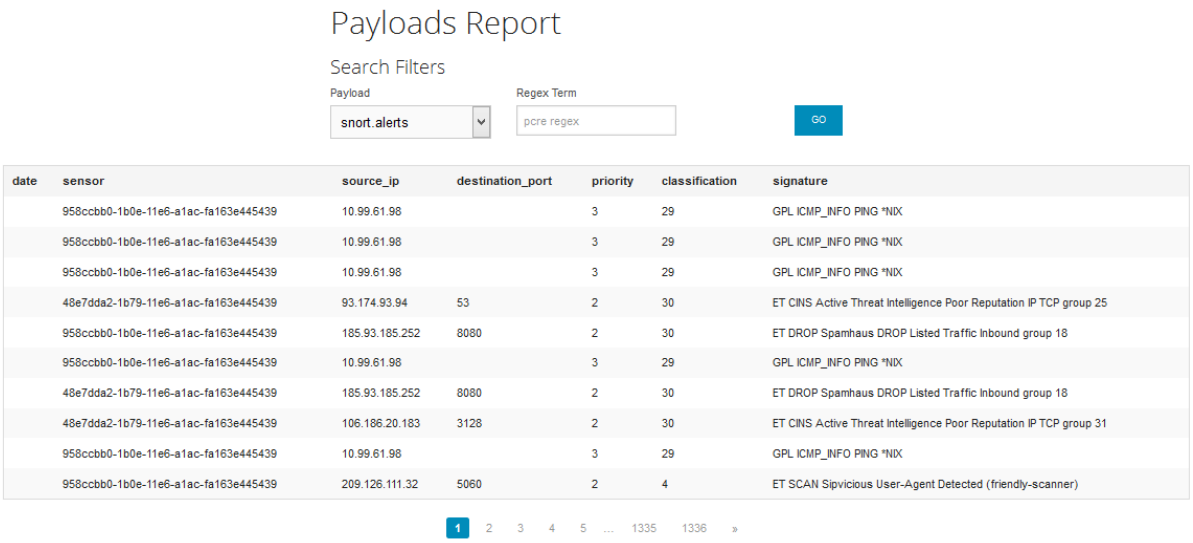


Figura 24 Top Ip d'atacants



Payloads Report

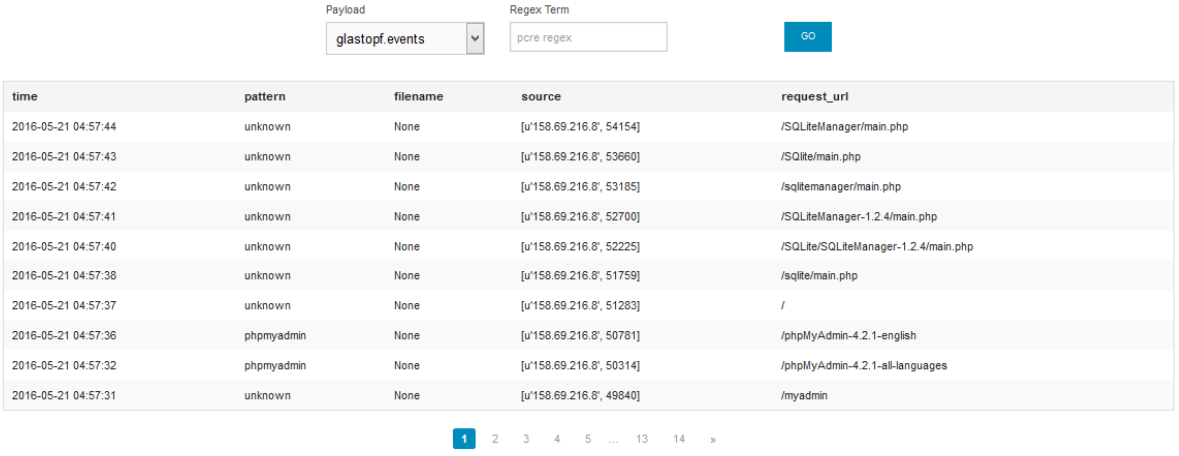
Search Filters

Payload: snort.alerts | Regex Term: pcre regex | GO

date	sensor	source_ip	destination_port	priority	classification	signature
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	10.99.61.98		3	29	GPL ICMP_INFO PING *NIX
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	10.99.61.98		3	29	GPL ICMP_INFO PING *NIX
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	10.99.61.98		3	29	GPL ICMP_INFO PING *NIX
	48e7dda2-1b79-11e6-a1ac-fa163e445439	93.174.93.94	53	2	30	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 25
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	185.93.185.252	8080	2	30	ET DROP Spamhaus DROP Listed Traffic Inbound group 18
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	10.99.61.98		3	29	GPL ICMP_INFO PING *NIX
	48e7dda2-1b79-11e6-a1ac-fa163e445439	185.93.185.252	8080	2	30	ET DROP Spamhaus DROP Listed Traffic Inbound group 18
	48e7dda2-1b79-11e6-a1ac-fa163e445439	106.186.20.183	3128	2	30	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 31
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	10.99.61.98		3	29	GPL ICMP_INFO PING *NIX
	958ccbb0-1b0e-11e6-a1ac-fa163e445439	209.126.111.32	5060	2	4	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)

1 2 3 4 5 ... 1335 1336 »

Figura 25 Alertes Snort



Payload: glastopf.events | Regex Term: pcre regex | GO

time	pattern	filename	source	request_url
2016-05-21 04:57:44	unknown	None	[u'158.69.216.8', 54154]	/SQLiteManager/main.php
2016-05-21 04:57:43	unknown	None	[u'158.69.216.8', 53660]	/SQlite/main.php
2016-05-21 04:57:42	unknown	None	[u'158.69.216.8', 53185]	/sqlitemanager/main.php
2016-05-21 04:57:41	unknown	None	[u'158.69.216.8', 52700]	/SQLiteManager-1.2.4/main.php
2016-05-21 04:57:40	unknown	None	[u'158.69.216.8', 52225]	/SQLite/SQLiteManager-1.2.4/main.php
2016-05-21 04:57:38	unknown	None	[u'158.69.216.8', 51759]	/sqlite/main.php
2016-05-21 04:57:37	unknown	None	[u'158.69.216.8', 51283]	/
2016-05-21 04:57:36	phpmyadmin	None	[u'158.69.216.8', 50781]	/phpMyAdmin-4.2.1-english
2016-05-21 04:57:32	phpmyadmin	None	[u'158.69.216.8', 50314]	/phpMyAdmin-4.2.1-all-languages
2016-05-21 04:57:31	unknown	None	[u'158.69.216.8', 49840]	/myadmin

1 2 3 4 5 ... 13 14 »

Figura 26 Events del Honeypot Glastopf

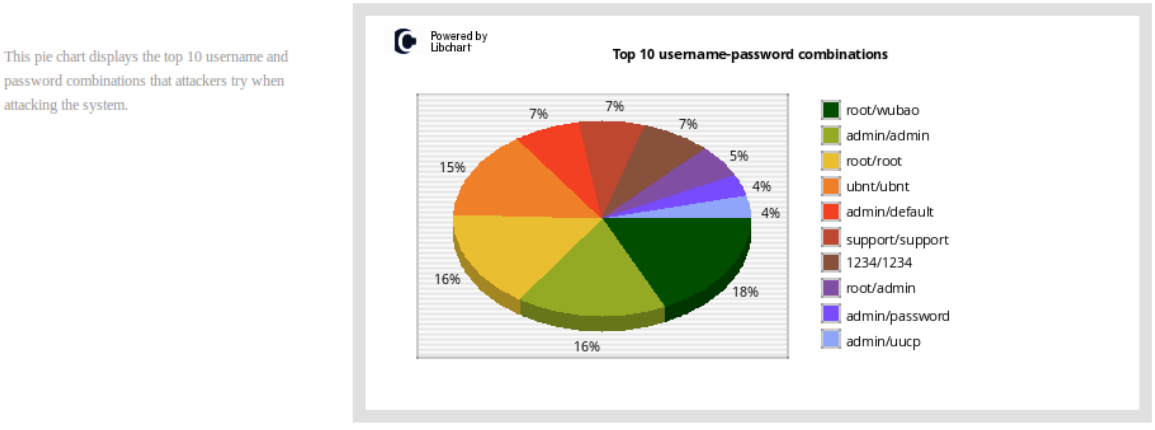


Figura 27 Events Kippo

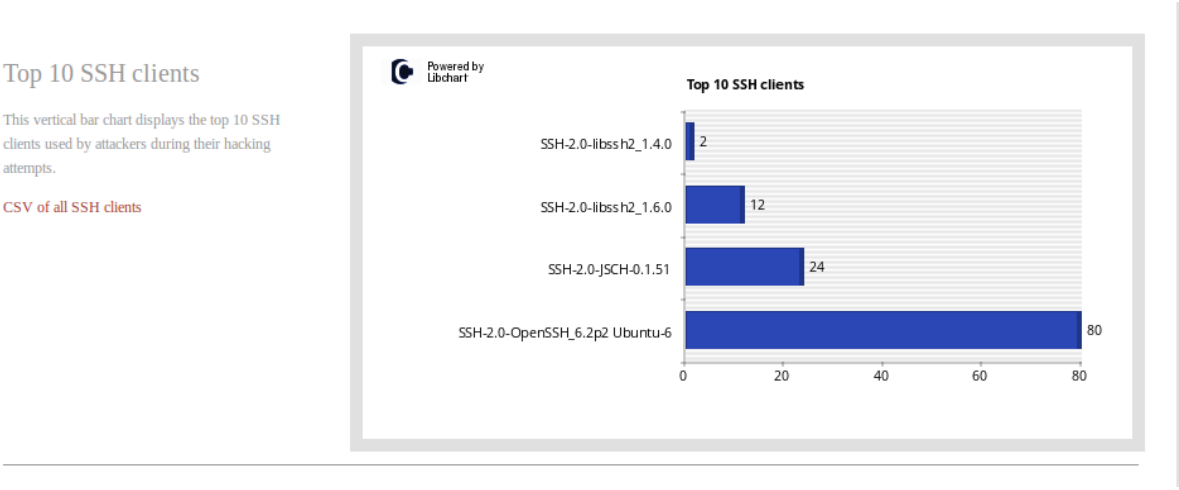


Figura 28 Clients SSH Kippo

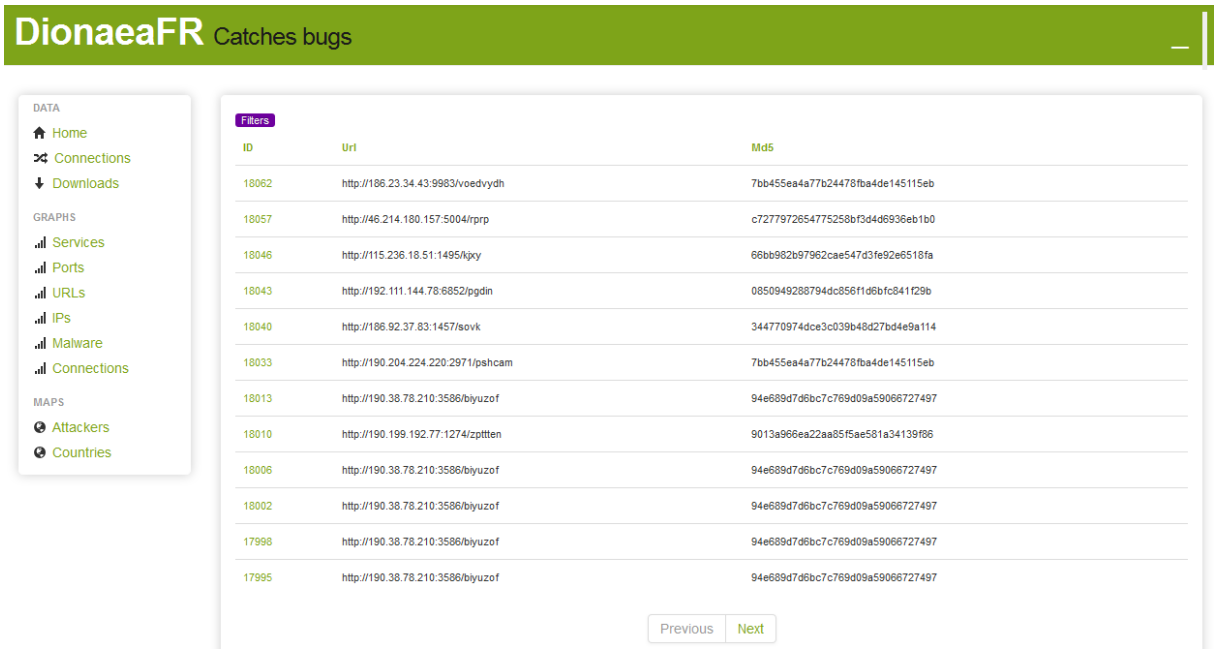


Figura 29 Descàrregues des de Dionaea