Honeypots. L'art de la Guerra

Miriam Traver Codina

Resum **- En el present projecte es pretén implementar i configurar diversos Honeypots per tal de poder analitzar els atacs que esperem rebre i així observar com es reacciona davant d'aquests. Basant-nos en els resultats obtinguts comprovarem si els Honeypots realment ens ajuden en la detecció i prevenció d'atacs i, per tant, si són una eina amb la qual podem mantenir de forma continua la seguretat del nostre sistema.**
Arran dels resultats que obtindrem de la realització dels atacs, es realitzarà un anàlisi per determinar si realment és òptim per una empresa dedicar el seu temps i els seus recursos en la implementació d'un Honeypot.

Paraules clau **- Honeypots, HoneyDrive, SQL, Malware, Kippo, Dionaea, seguretat, ciberatacs, detecció, anàlisi, nmap.**

Resum **- En el presente proyecto se pretende implementar y configurar varios Honeypots para poder analizar los ataques que esperamos recibir y así observar cómo se reacciona ante estos. Basándonos en los resultados obtenidos comprobaremos si los Honeypots realmente nos ayudan en la detección y prevención de ataques y, por tanto, si son una herramienta con la que podemos mantener la seguridad de nuestro sistema.**
A raíz de los resultados que obtengamos de la realización de los ataques, se realizará un análisis para determinar si es óptimo para una empresa dedicar su tiempo y sus recursos en la implementación de un Honeypot.

Palabras clave **- Honeypots, HoneyDrive, SQL, Malware, Kippo, Dionaea, seguridad, ciberataques, detección, análisis, nmap.**

Resum **- The present project seeks to implement and configure various Honeypots in order to analyze the attacks we expect to receive and to see how they react to them. Based on the results obtained we will check if the Honeypots really help us in the detection and prevention of attacks and, therefore, if it's a tool with which we can maintain the security of our system.**
Based on the results obtained from the attacks, an analysis will be performed to determine if it's really optimal for a company to spend their time and resources on implementing a Honeypot.

Index Terms **- Honeypots, HoneyDrive, SQL, Malware, Kippo, Dionaea, security, ciber attacks, detection, analysis, nmap.**

1. Introducció

LA tecnologia està avançant a gran velocitat i cada cop hi ha més empreses que incorporen eines tecnològiques per poder progressar i adaptar-se al canvi que estem vivint. Això dóna pas a què totes les dades que les institucions gestionen estiguin localitzades a Internet, pel qual s'han d'augmentar les mesures de seguretat d'aquestes.

El camp de la seguretat està molt fragmentat. A mesura que creixen les amenaces, creixen les capes de seguretat que han d'utilitzar les empreses.

Noves formes d'afrontar els ciberatacs o ciberatacs cada cop més sofisticats i més habituals, fa que, per les companyies, sigui imprescindible que assumeixin que la seguretat no només és un tema tecnològic sinó que té un impacte d'econòmic i de reputació. Podem afirmar sense por a equivocar-nos que es tracta d'una responsabilitat de tota l'organització.

Les dades no estan completament protegides, ja que sempre hi ha alguna manera d'accedir a elles. Per això, el que s'ha d'aconseguir és augmentar al màxim la implementació de tots els mitjans possibles per dificultar l'accés de tercers.

Un Honeypot és una eina la qual es defineix com a "pot de mel" pel fet que és una rèplica d'un sistema que s'utilitza per atraure a l'atacant cap a ell i així evitar que s'ataqui al sistema real. El paper dels Honeypots és purament passiu: La seva funció no és la de protegir, sinó la de distreure. Però alhora és actiu quant a la recol·lecció d'informació.

El fi d'utilitzar-los és recopilar informació dels atacs, la qual ens permeti aprendre i millorar les mesures de seguretat. És a dir, gràcies als Honeypots podem observar els punts on se centren els atacs, els patrons i els programes que s'utilitzen per dur-los a terme.

Resulta una eina molt atractiva doncs desvia l'atenció cap a un altre sistema o permet atrapar als atacants en acció. Això, però, també té una part negativa. En ser una eina de recopilació d'informació requereix que l'informàtic que la gestiona tingui coneixements –i sempre actualitzats- de la seguretat de la xarxa, perquè requereix un manteniment constant, ja que és extremadament fàcil que aquest sistema sigui compromès per un tercer.

- *E-mail de contacte: Miriam.Traver@e-campus.uab.cat*
- *Menció realitzada: Tecnologies de la Informació.*
- *Treball tutoritzat per: Ramón Grau Sala (CAOS)*
- *Curs 2019/20*

2. OBJECTIUS

Tal com afirma Mar López Gil[1] del departament de Seguretat Nacional, la ciberseguretat és ja una qüestió de cultura que ha de ser quotidiana.

Quan parlem d'atacs en el món digital, i com hem pogut constatar amb l'enquesta realitzada, la societat encara no ha pres consciència de la realitat en què ens trobem.

La transformació digital ens ha evocat a una hiperconnectivitat i ha donat lloc a nous riscos, totalment desconeguts i inimaginables per a tothom. Estem doncs davant d'una nova necessitat: en primer lloc, ens cal crear consciència de la nostra vulnerabilitat; en segon lloc, posar els mitjans per assegurar la nostra forma de vida i en tercer lloc veure que és responsabilitat de tots, que no ho hem de fer sols sinó que és una tasca de governs, empreses i ciutadans.

L'objectiu principal d'aquest projecte és implementar un sistema de seguretat basat en els Honeypots per tal de poder rebre atacs, monitoritzar-los i així extreure la informació necessària per a realitzar un anàlisi exhaustiu dels tipus d'atacs que rebem.

Gràcies a aquest monitoratge també es poden prendre mesures sobre els protocols o basant-nos en les accions que realitzin.

En el nostre cas no farem cap acció, ja que el nostre objectiu és deixar que els atacants interaccionin amb el nostre sistema.

A grans trets, ens interessa recopilar la següent informació:

- Protocols.
- Ports TCP/UDP.
- Comandes empreses.
- Estat de les connexions.
- IP d'origen de l'atacant.
- Temps en què aquest s'ha dut a terme.

Hi ha un rang molt ampli d'atacs. Nosaltres ens centrarem en dos estils: connexions SSH[2] i recepció de Malware. Amb el primer estil pretenem poder recol·lectar les diverses comandes que l'atacant escriu a través de la consola contra el nostre sistema i registrar els arxius que puja en el nostre sistema d'arxius.

Quan parlem de Malware ja entrem en la part de la seguretat en la xarxa. El que ens interessa d'aquest punt és poder observar i conèixer tots els fitxers maliciosos que l'atacant hagi descarregat en el nostre sistema.

Per anar més enllà de la part tecnològica, hem cregut oportú sondejar a professionals en l'àmbit de la informàtica per descobrir quines mesures han implantat davant d'aquests nous riscos i vulnerabilitats. Amb aquest objectiu, s'ha dut a terme una enquesta, on no només els hi hem preguntat pel coneixement que tenen dels Honeypots sinó que també hem volgut saber el grau de sensibilització que tenen sobre aquest assumpte i que ens expliquin, en la mesura que ho desitgin, experiències implantades.

[1] **Congreso Cibertodos**. Isaca Madrid 2019

[2] **Connexió SSH:** es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

3. ESTAT DE L'ART

Si volem guanyar en el combat cal conèixer a l'enemic i les seves armes. Però el que també és molt important és conèixer les nostres fortaleses i per descomptat les nostres debilitats.

En temes de seguretat no hem d'escatimar inversions. Els atacants comptaran segur amb eines sofisticades i amb un alt nivell d'organització. I sobretot hi ha una cosa que no tindran: ètica i honor. Les regles del joc no seran les nostres! Pel que hem d'estar preparats i coneixedors dels mitjans que podem emprar.

Els Honeypots són eines de seguretat que s'utilitzen amb el fi de recol·lectar informació sobre els atacants i les tècniques que utilitzen. D'aquesta manera podem, en els nostres sistemes reals, emfatitzar la seguretat en els punts dèbils que s'han trobat.

3.1. Tipus de honeypots

Per tal d'adaptar-se a les necessitats dels usuaris, hi ha dues classificacions, segons l'ambient i el seu grau d'interactivitat. A continuació procedirem a explicar-les.

3.1.1. Interactivitat

S'ha de tenir present que els Honeypots no tenen per què aplicar-se a sistemes complets ni reals, també es poden aplicar per serveis concrets.

- **Baixa interacció:** Són els Honeypots que s'han escollit per implementar en aquest treball, ja que ens permeten emular tant serveis concrets com sistemes operatius complets. El principal avantatge que tenen és que com són sistemes virtuals no contenen ni usuaris ni processos ni cap altre tipus activitat. Per tant, l'única interacció que trobarem serà la dels atacants.

  A l'hora de monitoritzar-los ens faciliten la feina, ja que la probabilitat què alguns d'aquests logs siguin falsos positius[3] és mínima.
- **Alta interacció:** Són Honeypots que s'implementen en sistemes reals, fent ús de servidors, serveis i aplicacions. Com treballem en un entorn real no tenim cap limitació pel que fa a les funcionalitats i tampoc podem assumir cap mena de comportament. Per tant, a diferència dels anteriors, tindrem molta activitat en el sistema i, fins i tot, podem arribar a descobrir atacs de dia 0[4].

Com a punt negatiu és que en rebre una intrusió, si no es té cura, l'atacant pot sortir de l'entorn controlat i pot acabar posant en perill tots els equips connectats a la xarxa.

3.1.2. AMBIENT

Abans de fer ús dels Honeypots, un s'ha de plantejar quines són les funcionalitats que es volen obtenir de la implantació d'aquests, i arran de les necessitats que es tinguin podem trobar dos ambients, els d'investigació o els de producció.

[3] **Fals positiu:** En aquest cas, quan es detecta una intrusió com sospitosa quan no ho és.

[4] **Atacs de dia 0:** Són atacs produits contra vulnerabilitats, no descobertes, en el software del sistema o d'una aplicació.

- **Investigació:** L'objectiu principal és la investigació i la recol·lecció d'informació per tal de poder fer estudis sobre els comportaments, les tècniques, i els patrons utilitzats. Així mateix, ens permeten conèixer els atacants i obtenir la informació necessària per analitzar-la. Són els més utilitzats per persones que pretenen fer estudis de seguretat i, com el propòsit final és la investigació, tranquil·lament podem deixar que els atacants s'apoderin de la màquina sencera sense que ens suposi un problema.

  L'objectiu és realitzar una recerca amb les dades resultants dels atacs, no s'espera que el sistema realitzi cap acció tan bon punt detecti les intrusions. El sistema ha de mantenir-se passiu emmagatzemant tota la informació dels atacs en els logs pertinents.

- **Producció:** A diferència dels anteriors, estan enfocats a disminuir el risc que pot tenir una empresa o institució respecte als atacs informàtics.

  El seu objectiu no és un altre que el de rebre atacs i així poder protegir els serveis i sistemes de la xarxa. S'espera que el sistema actuï de forma activa i prengui les mesures adequades per evitar d'anys, com podrien ser les denegacions d'accés d'un determinat punt, l'aturada de serveis de forma temporal o la limitació de les capacitats d'un servei.

3.2. Protecció de dades

En tots els àmbits s'ha de tenir present el que les lleis estableixen, però donat la temàtica d'aquest projecte, cal fer un incís en la protecció de dades.

En l'article 18 de la Constitució Espanyola observar que "s'ha de garantir la intimitat [...] i el secret de les comunicacions". Per tant, dependent de la configuració del Honeypot podem estar espiant a un tercer. Això pot suposar un problema, ja que estem recol·lectant la seva informació personal.

Encara que costi de creure, un atacant pot arribar a denunciar a la persona responsable del Honeypot al·legant que està envaint la seva intimitat.

Segons Lance Spitzner[5] hi ha diverses responsabilitats legals en l'ús dels Honeypots, però ens centrarem en la més rellevant: la privacitat. L'objectiu és l'obtenció d'informació, però s'ha de tenir present que aquesta pot dividir-se en dos tipus:

- **Transaccional**: Informació general, com capçaleres, adreça IP, data i hora, etc.
- **Contingut**: És la informació pròpia de la comunicació privada i la qual ens pot donar problemes legals.

Per tant, hem de dur molta cura amb quina mena d'informació estem tractant i quin ús fem d'ella.

4. METODOLOGIA I PLANIFICACIÓ

La metodologia i la planificació de les tasques emprades en la realització d'aquest treball s'explicaran tot seguit, així mateix, s'especificaran els recursos que s'han utilitzat i es mostraran els resultats de l'enquesta a professionals del sector.

[5] **Lance Spitzner**: Pare dels Honeypots i escritor del llibre "Honeypots tracking hackers."

4.1. WATERFALL

S'ha hagut de dividir la posada en marxa del projecte en 4 etapes completament dependents entre elles, per tant, es fa ús de la metodologia waterfall. És a dir, realitzarem un desenvolupament seqüencial de les tasques.

1. Cerca de la documentació i els recursos que es requereixen.
2. Implementació del servidor i la base de dades.
3. Implementació i configuració del Honeypot.
4. Anàlisi de la informació dels atacs rebuts.

La metodologia Waterfall és molt utilitzada, ja que no es pot iniciar una etapa sense acabar la següent. Això ens permet tenir un control de tots els passos i ens crea una necessitat de tenir la feina al dia.

4.2. Recursos

Per tal de poder dur a terme el desenvolupament del projecte s'ha fet ús dels següents recursos:

- **Un ordinador físic:** Dedicat exclusivament a la realització d'aquest projecte. Les seves característiques s'esmentaran a continuació:
  - Sistema Operatiu: Windows 10 Pro
  - Versió: 18.03
  - Tipus de sistema: 64 bits

- **Un producte de virtualització:** S'ha fet ús del programa VirtualBox, realitzant la importació d'un servei virtualitzat el qual té les següents especificacions:
  - Sistema Operatiu: Xubuntu
  - Versió: 12.04.4 LTS
  - Tipus de sistema: 32 bits

- **Dos Honeypots:** Per tal d'enfocar-nos en fer una recol·lecció tant de dades mitjançant SSH com de fitxers maliciosos, s'ha decidit implementar 2 Honeypots que es dediquen en això.
  - **Kippo:** és un Honeypot de baixa interacció i la seva funció resideix en fer una simulació d'un servidor SSH i està pensat per rebre atacs de forma bruta.

    Hem decidit fer ús d'aquest perquè ens permet obtenir molta informació sobre els atacants, fins i tot, ens facilita les comandes que ha executat l'atacant, permetent-nos reproduir la sessió.

    Alhora, cal fer menció que el Honeypot Kippo té un propi sistema de visualització, que ens permet accedir mitjançant una IP. D'aquesta manera podem monitoritzar-lo des d'una altra màquina o dispositiu.

  - **Dionaea**: És un Honeypot de baixa interacció i ens ha interessat perquè és capaç de suportar molts protocols. Recordem que és amb aquest Honeypot amb el qual volem recol·lectar els fitxers maliciosos que l'atacant descarregui en el nostre sistema. Per tant, és important fer un control dels serveis que volem mantenir actius i els ports relatius en aquests.
- **Una base de dades.**

4.3. Organització de les tasques

En la taula següent es mostra la planificació que s'ha dut a terme per la realització del present treball, dividint-lo en diverses setmanes, les quals contenen les subtasques.

Juli Cèsar va dir "*Divide et impera*", és a dir, i dividim el projecte en una sèrie de subtasques, ens serà més senzill avançar i tindrem un control òptim dels canvis.

Dades	Tasques	Subtasques
23/09/2019	Primer plantejament	Resum
		Introducció
		Objectius
		Planificació
		Redacció de l'enquesta
		Cerca de contactes
30/09/2019	Plantejament	Cercar sobre l'estat de l'art
		Cerca de recursos
		Veure la possible implementació
		Cerca de les eines idònies
		Redacció del procediment/canvis
07/10/2019	Plantejament	Redacció del procediment/canvis
		Cerca de les eines idònies
14/10/2019	Plantejament	Redacció del procediment/canvis
		Cerca de les eines idònies
21/10/2019	Implementació	Redacció del procediment/canvis
		Cerca dels recursos
		Enquesta: redacció objectiva
28/10/2019	Implementació	Redacció del procediment/canvis
		Cerca dels recursos
		Enviar les enquestes
04/11/2019	Implementació	Redacció del procediment/canvis
		Base de dades i servidor Apache
11/11/2019	Implementació	Redacció del procediment/canvis
		Base de dades i servidor Apache
18/11/2019	Implementació	Redacció del procediment/canvis
		Cerca informació dels scripts
25/11/2019	Implementació	Redacció del procediment/canvis
		Cerca informació dels scripts
02/12/2019	Implementació	Redacció del procediment/canvis
		Redacció dels scripts
09/12/2019	Implementació	Redacció del procediment/canvis
		Redacció dels scripts
16/12/2019	Implementació	Redacció del procediment/canvis
		Implementació Kippo
23/12/2019	Implementació	Redacció del procediment/canvis
		Implementació del Dionesia
30/12/2019	Monitorització	Redacció del procediment/canvis
		Monitoritzar i enmagatzemar
06/01/2020	Monitorització	Monitoritzar i enmagatzemar
		Redacció del procediment/canvis
13/01/2020	Redacció Final	Analitzar respostes enquestes.
20/01/2020	Redacció Final	Redacció de les conclusions
26/01/2020	Redacció Final	Tancament del projecte

Taula 1: Organització del projecte

4.4. Enquestes

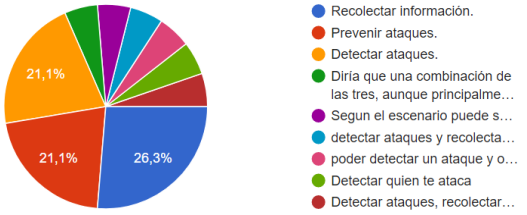
La redacció d'aquesta enquesta consta de 6 preguntes les quals s'han formulat en català, castellà i anglès.

1. Coneix el concepte de Honeypot?

2. Li sembla una eina útil?

A les dues primeres preguntes el 100% dels 27 entrevistats van respondre de forma afirmativa, demostrant que tenien coneixements d'aquests i que creuen que són eficients.

3. Quina creu que és la seva funcionalitat principal?



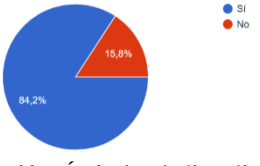
Il·lustració 1: Funcionalitat dels Honeypots.

El 26'3% dels participants diuen que l'objectiu és la recol·lecció de dades, molt seguit tenim les funcionalitats de prevenir o detectar atacs amb un 21'1% ambdues. Podem observar 6 respostes extres les quals els entrevistats ens han indicat, sent la majoria la unificació de les respostes principals.

Totes les respostes podrien considerar-se certes, ja que si bé s'esperava que la majoria fos la recol·lecció de dades, s'ha de fer èmfasi en el fet que, en quant es detecta un atac es genera un log i es recull la informació de l'atac i l'atacant.

Per altra banda, si el nostre Honeypot és passiu, no previndrà cap atac, però si és actiu podem fer que prengui accions contra els atacs. En general, no prevé de forma directa, sinó que mitjançant la informació obtinguda nosaltres prenem mesures per evitar aquest atac en el sistema real.

4. Creu què és òptim dedicar-li el temps d'implementació i de manteniment en comparació als avantatges que ofereix?



Il·lustració 2: És óptim dedicar-li temps?

El 84'2% consideren que són eines útils, però l'altre 15'8% diu que hi ha maneres millors de protegir el sistema sense haver d'implementar un Honeypot.

Després de raonar-ho, podem arribar a la conclusió que es plantegen un Honeypot de caràcter de producció, on es fa una rèplica exacta del sistema real. Si és així, podem entendre que els costos serien molt elevats i es requeriria un manteniment constant.

Però creiem que justament fer ús d'ells ens seria del tot útil, ja que aconseguim augmentar les mesures de seguretat al màxim.

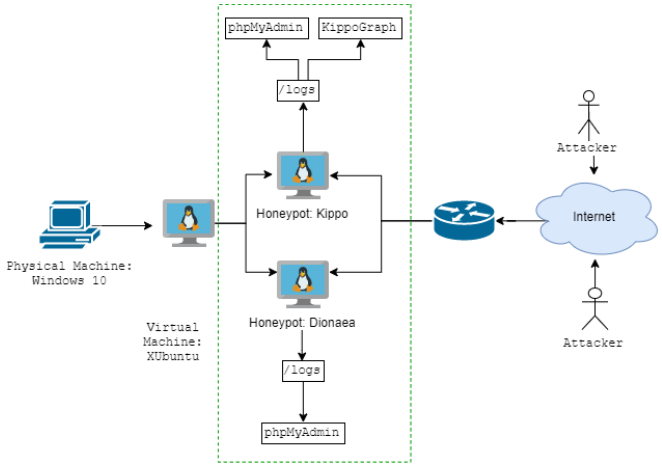
Arran de les dues preguntes restants, les quals eren de resposta oberta, volíem extreure experiències i opinions de caràcter personal. Descobrint que el 90% dels entrevistats no ha tingut cap experiència implementant-los ni són conscients dels recursos necessaris. Mentre que el 10% restant correspon a aquells que han implementat algun fa uns anys i els que han dut una cerca per implementar-ne però sense arribar a fer-ho.

5. DISSENY I IMPLEMENTACIÓ

En aquest apartat farem menció de tot el relacionat amb el disseny i la implementació del sistema i de les eines necessàries per a aconseguir tirar endavant l'actual projecte.

5.1. Fase de disseny

El primer que s'ha de fer en un projecte d'aquest caire és la realització d'un diagrama on es mostrin tots els components i les relacions entre ells.



Il·lustració 3: Disseny del sistema.

L'ordinador físic que tenim és on carregem la màquina virtual que configurarem. En aquesta màquina importarem el sistema de virtualització HoneyDrive, i la nostra funció residirà en configurar-los i posar-los en marxa.

És important tenir present quin és el procés a seguir per trobar possibles fallades en el nostre disseny.

Què volem dir amb això? Quan un atacant va contra la nostra màquina es generen logs, els quals emmagatzemen la informació de l'activitat sospitosa. El problema resideix en què aquests logs estan en el mateix sistema. No té cap lògica mantenir informació sensible en un sistema sabent que el seu destí és rebre atacs.

Per què? Perquè la informació es pot comprometre i perdre així la fiabilitat.

Per poder fiar-nos de les dades ens convé treure-les de la màquina en quant són generades. La manera de fer-ho és connectant la màquina virtual a la nostra base de dades, phpmysql, que emmagatzemarà la informació i quedarà segura i fora de les mans de l'atacant.

En quant s'escriguin els logs, s'iniciarà un procés automàtic que enviarà un mail notificant de la intrusió i enviant les dades. D'aquesta manera aconseguim la informació de dues fonts diferents i, en cas de dubte, podem comparar els valors.

5.2. Fase d'implementació

Un cop s'ha realitzat el disseny i s'ha supervisat diverses vegades per evitar trobar possibles errors més tard, ja podem donar-li el vist-i-plau i seguir amb la implementació dels components que formaran part del nostre sistema.

5.2.1. Plantajament de la xarxa

Abans de dur a terme qualsevol acció s'ha d'analitzar quins serveis i protocols volem analitzar, és a dir, hem de mirar quins ports hem d'obrir per tal de permetre que els atacants puguin entrar en el nostre ordinador.

Port	Servei	Especificació
22	SSH	Servei de Shell.
23	TELNET	Connexió client-servidor.
25	SMTP	Transferència de correu.
42	NameServer	Servei de noms d'Internet.
80	HTTP	Transferència de hipertext .
135	EndPoint Mapper	Assigna endpoints. Sobrecàrrega.
445	Microsoft-ds	Msg de servidor sobre TCP/IP.
1433	Ms-sql-s	Mixrosoft SQL Server.
3389	TerminalServer	Escriptori remot.
5060	SIP	Transmetre/rebre peticions.

Taula 2: Ports i serveis utilitzats

El primer que farà un atacant abans de realitzar qualsevol acció és un escaneig de ports, per tant, a més d'obrir els anteriors ports, s'han oberts alguns altres per tal de mostrar-nos dèbils. Quan fem un escaneig amb nmap[6], per exemple, se'ns mostren els ports, l'estat i els serveis que utilitzen.

Una fallada molt comuna és un cop oberts els ports executar ja els serveis. Cal tenir una visió més ample i, per exemple, fer-nos a nosaltres mateixos un escaneig de ports. Per què? La resposta l'hem mencionat unes línies enrere, però passa desapercebuda fàcilment.

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Dionaea honeypot ftpd
42/tcp   open  nameserver?
80/tcp   open  http          Apache httpd 2.2.22
135/tcp  open  msrpc?
443/tcp  open  ssl/https
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s      Dionaea honeypot MS-SQL server
5060/tcp open  honeypot      Dionaea Honeypot sipd
5061/tcp open  ssl/honeypot  Dionaea Honeypot sipd
```

Il·lustració 4: Resultat d'un nmap al nostre sistema.

L'escaneig mostra a l'atacant el servei utilitzat i aquest especifica tot el nom, com podem observar en la imatge. Per tant, l'atacant podria dedicar-se a fer-nos atacs de denegació de servei i no li treuríem utilitat a la nostra feina.

Això pot solucionar-se de forma tant senzilla com anant al codi del fitxer i canviar-li el nom. D'aquesta manera quan l'atacant realitzi l'escaneig no veurà que és un servei que està sent implementat per un Honeypot.

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp?
42/tcp   open  nameserver?
135/tcp  open  msrpc?
443/tcp  open  https?
445/tcp  open  microsoft-ds?
1433/tcp open  ms-sql-s?
5060/tcp open  sip?
5061/tcp open  sip-tls?
```

Il·lustració 5: Resultat nmap sense versions.

[6] **Nmap:** eina gratuïta de codi obert per a l'exploració de vulnerabilitats i la detecció de xarxes. S'utilitza per identificar quins dispositius s'estan executant en els seus sistemes, descobrir els hosts disponibles i els serveis que ofereixen.

5.2.2. Sistema de visualització

En aquest apartat explicarem el sistema de visualització gràfic que hem implementat. Aquest tipus de sistemes són els que recol·lecten la informació que volem extreure dels Honeypots que tenim instal·lats i ens permeten veure la informació de forma gràfica i pràctica.

El sistema de visualització que hem utilitzat és la base de dades phpMyAdmin, ja que és una plataforma que ens permet accedir a ella des de qualsevol lloc mitjançant un navegador. Abans d'iniciar aquesta instal·lació (annex 2) s'ha de tenir present que per poder dur-la a terme requerim un servidor. En el nostre cas Apache, per tant, hem d'assegurar-nos que tenim tots els paquets i les dependències necessàries per iniciar la base de dades.

En la realització d'aquest apartat vàrem tenir problemes amb el correcte funcionament del servidor i les diferents versions dels paquets, per tal, procedirem a explicar els passos a seguir en l'annex 1.

5.2.3. Sistemes Honeypot

En aquest apartat explicarem la implementació, la configuració i l'execució dels Honeypots en el nostre sistema.

Abans de posar en marxa el nostre sistema hem fet ús d'una pentabox on ja venien un conjunt de Honeypots configurats. D'aquesta manera hem pogut practicar amb ells i obtenir més coneixements d'aquests sense donar a conèixer els nostres.

En l'annex 3 podem observar la instal·lació de pentabox (sobre Kali light) i algunes proves realitzades en diversos ports.

Un cop passada la fase inicial de les proves, per tal de veure com funcionen els honeypots, ens centrarem en la implementació i configuració del sistema que realment volem analitzar.

En un principi volíem treballar sobre l'eina honeyd, la qual ens permetria realitzar la creació de diversos honeypots cadascun amb un sistema operatiu diferent. Mentre l'implementàvem ens vàrem adonar que moltes de les comandes que executàvem estaven depredades o obsoletes. Això ens va obligar a buscar una forma alternativa de dur a terme un escenari com l'anteriorment descrit.

Fent una cerca ens hem trobat amb HoneyDrive, la qual és una distribució de Linux que té una gran varietat de honeypots ja implementats. Entre el conjunt que té podem trobar els que ens interessen: Kippo i Dionaea.

A continuació procedirem a explicar els dos Honeypots que s'han emprat.

5.2.4. Kippo:

Kippo (annex 5) ens permet emular un servei SSH amb el seu propi login i amb una reproducció d'un sistema de fitxers. Inclús podem integrar un SO i posar-hi documents.

Gràcies a això podem aprendre molt perquè se'ns permet reproduir de forma automàtica les sessions (comandes) que han dut a terme els atacants.

A més, Kippo ens permet una sèrie de característiques molt atractives:

- Sistema fals d'arxius.
- Reproducció de sessions.
- Guarda tots els arxius amb els que interactua l'atacant.
- Sobre la consola, simula finalitzar la sessió oberta, i d'aquesta manera ens permet monitoritzar les accions de l'atacant en trobar-se en aquesta situació.

5.2.5. Dionaea:

Fem ús de Dionaea (annex 6) perquè ens dóna molta llibertat quant als protocols a fer servir, alhora, i com bé indica el nom, és una carnívora.

L'objectiu de la nostra "planta carnívora" resideix en què captura una còpia del Malware que l'atacat intenta introduir en el nostre sistema o del que està propagant-se per la xarxa.

Alguns dels serveis que volem implementar justament per aquest Honeypot són els següents:

- MSSQL (1433): Mitjançant comandes poder manipular dades SQL.
- SMB (445): Accepta l'intercanvi de missatges de servidors sobre el protocol TCP/IP.
- HTTP (80): Permet fer transferències en format HTTP mitjançant el servei del World Wide Web (www).
- NameServer (42): Servei que facilita els noms d'Internet.

Abans d'iniciar amb el monitoratge dels Honeypots cal fer menció que s'ha posat en marxa Dionaea dues vegades. La primera vegada vàrem tenir moltíssimes connexions però no teníem cap moviment de fitxers maliciosos, el que ens va estranyar molt. Donat que volíem veure com reaccionava el Honeypot, es va crear una nova màquina virtual i s'ha adaptat per tal de tenir-la en condicions per realitzar atacs. Amb aquesta es va crear un fitxer php i vam provar d'enviar-lo en el nostre sistema.

Il·lustració 6: Creació fitxer PHP.

Il·lustració 7: Connexió i intent d'enviament.

Com vàrem veure que no hi havia manera d'enviar un fitxer, vam realitzar una exhaustiva cerca i vàrem acabar descobrint que havíem de modificar el fitxer de configuració SSL d'Apache per tal d'indicar-li que ens permetis activar el protocol WebDav. Aquest s'encarrega de permetre treballar, editar i guardar arxius des de servidors Web.

6. MONITORITZACIÓ

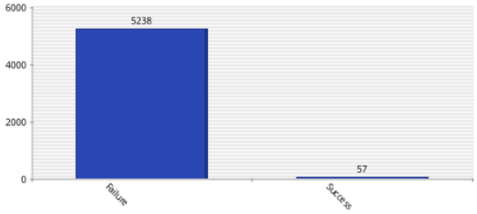
En aquest apartat analitzarem els resultats obtinguts del monitoratge dels dos Honeypots.

Abans d'entrar en detall, cal matisar que els Honeypots han estat actius durant una setmana aproximadament. Ja que, com bé deia fa 25 segles Sun Tzu en el seu llibre "L'Art de la Guerra", que dóna títol en el nostre treball, "*Mai és beneficiós per a un país deixar que una operació militar es prolongui per molt temps.*"

I, en aquesta nova guerra d'Internet amb la qual lluitem cada dia, els seus consells ens són perfectament útils. Tenir aixecat el sistema durant molt de temps fa que s'acabi coneixent aquest i, si els atacants descobreixen la nostra trampa, poden arribar a interactuar falsament per fer caure el nostre sistema.

6.1. KIPPO

Hem rebut un total de 5295 connexions SSH, dels quals únicament 57 han tingut éxit i han entrat en el nostre Honeypot.



Il·lustració 8: Atacs rebuts en Kippo

Quan aquests atacants aconsegueixen inserir en el sistema, de forma automàtica es crea una consola paral·lela la qual no conté cap mena d'informació i alhora s'encarrega de gestionar les comandes que s'utilitzen i fins i tot grava la sessió per més tard poder reproduir-la.

ID	
1	ls
2	cd ..
3	sudo /su
4	sudo -su
5	apt-get sudo
6	nano /var/lib/apt/lists/lock

Il·lustració 10: Comandes emprades.

Il·lustració 9: Shell falsa

ID	Timstamp	Size	Play the log
1	2020-01-09 17:46:55	7.39kb	Play
2	2020-01-09 17:46:51	7.39kb	Play
3	2020-01-09 17:46:47	7.39kb	Play

Il·lustració 11: Regristre de grabacions dels atacs.

Una altra manera de veure les interaccions dels atacants amb el nostre sistema és mitjançant els logs.

```
2019-12-23 17:37:35+0000 [HoneyPotTransport,92,69.158.207.141] starting service ssh-useraith
2019-12-23 17:37:35+0000 [SSHService ssh-useraith on HoneyPotTransport,92,69.158.207.141] root trying auth password
2019-12-23 17:37:35+0000 [SSHService ssh-useraith on HoneyPotTransport,92,69.158.207.141] login attempt [root/123456] succeeded
2019-12-23 17:37:35+0000 [SSHService ssh-useraith on HoneyPotTransport,92,69.158.207.141] root authenticated with password
2019-12-23 17:37:35+0000 [SSHService ssh-useraith on HoneyPotTransport,92,69.158.207.141] starting service ssh-connection
2019-12-23 17:37:36+0000 [SSHService ssh-connection on HoneyPotTransport,92,69.158.207.141] got channel session request
2019-12-23 17:37:36+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,92,69.158.207.141] channel open
2019-12-23 17:37:36+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,92,69.158.207.141] executing command "cat /etc/issue"
2019-12-23 17:37:36+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,92,69.158.207.141] Unhandled Error
```

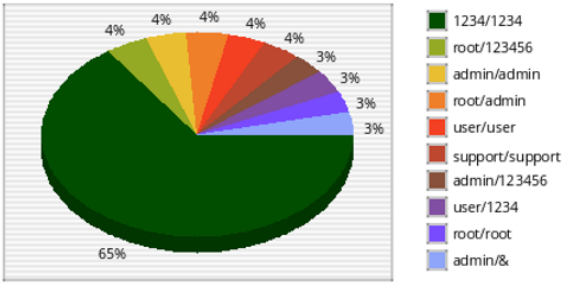
Il·lustració 12: Log d'un atac amb éxit.

En aquest cas podem observar com l'atacant ha provat l'usuari root amb el pwd 123456, i com són els correctes per accedir al nostre sistema, li concedim permís.

Automàticament podem veure la creació d'un nou canal, que correspondrà a la shell anteriorment mencionada.

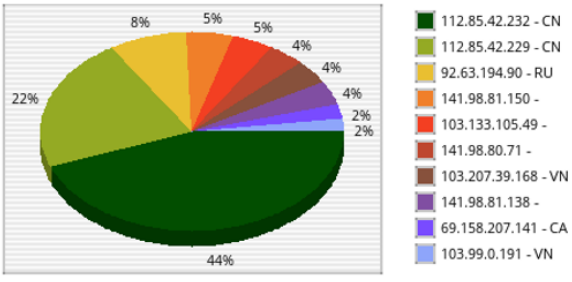
Veiem que l'atacant el primer que ha fet és realitzar una mostra del fitxer i li ha sorgit un error.

Mirant el gràfic pertinent a tots els users i pwd probats, podem veure que la majoria han estat els més bàsics, 1234 per ambdues.



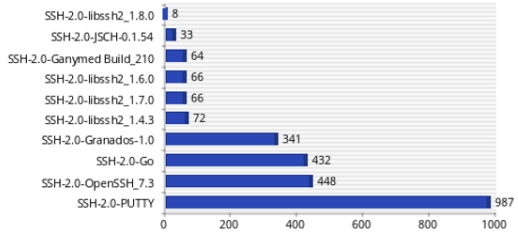
Il·lustració 13: Combinació users i pwd

Podem observar una gran varietat de combinacions que tendeixen a ser bastant comuns, però fora d'aquestes hi ha hagut algunes molt concretes. Com vindria a ser "america"o "spania" que entenem que poden ser realitzats per atacants del mateix país, sinó, és més difícil posar aquestes contrasenyes.



Il·lustració 14: Atacs per països.

La major part dels atacs que hem rebut procedeixen de Xina, seguits per Rússia.



Il·lustració 15: Tipus de SSH.

Kippo ens permet identificar de quin tipus de SSH proveeixen els atacs, això ens pot servir en el nostre sistema, impedir connexions corresponents a certes versions.

Per finalitzar, farem menció de la taula inferior. Aquesta ens dóna informació relativa a les IP's, Ciutat, Regió, coordenades i té una columna anomenada lookup.

ID	IP Address	Probes	City	Region	Country Name	Code	Latitude	Longitude	Hostname	Lookup
1	112.85.42.232	1509	Xinpu	Jiangsu	China	CN	34.5997	119.1594	112.85.42.232	
2	112.85.42.229	744	Xinpu	Jiangsu	China	CN	34.5997	119.1594	112.85.42.229	
3	92.63.194.90	278	Izhevsk	Udmurtiya Republic	Russia	RU	56.85	53.2333	92.63.194.90	
4	141.98.81.150	170							141.98.81.150	
5	103.133.105.49	153							103.133.105.49	
6	141.98.80.71	136							141.98.80.71	
7	103.207.39.168	132			Vietnam	VN	16	106	103.207.39.168	
8	141.98.81.138	131							141.98.81.138	
9	69.158.207.141	74			Canada	CA	43.6319	-79.3716	69.158.207.141	
10	103.99.0.191	71	Thanh Pho Ninh Binh	Tinh Ninh Binh	Vietnam	VN	20.2539	105.975	103.99.0.191	

Il·lustració 16: Taula d'informació d'IPs.

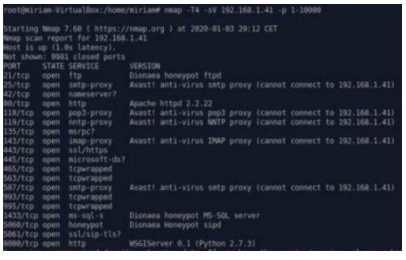
El lookup és un conjunt de criteris que ens permeten analitzar les IP's de forma individual, dient-nos per exemple si pertanyen a una llista negra o propietats concretes d'aquestes.

6.2. DIONAEA

Mitjançant Dionaea volem veure quantes peces de Malware intenten inserir en el nostre ordinador, això ho aconseguim oferint serveis vulnerables a la xarxa amb l'objectiu d'aconseguir una còpia d'aquest Malware.

En posar en marxa Dionaea vàrem rebre un nombre aproximat de 70 connexions i ens va estranyar, però no vam prendre cap mesura. Al segon dia, el nombre no es va moure, el que ja va començar a preocupar-nos, així que es va adaptar una segona màquina i sobre aquesta hem llençat un nmap a la IP pertinent al nostre Honeypot.

La sorpresa ens la vam endur en veure que no érem conscients que els serveis tenen nom i aquests delataven la nostra trampa.



Il·lustració 17: Serveis amb els seus noms i versions.

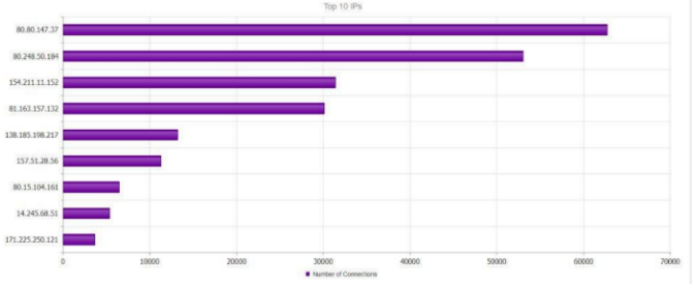
Un cop descoberta la nostra fallada, vam entrar en els fitxers de configuració i vàrem treure els noms.

Alhora, en la il·lustració 18 podem observar que tenim l'Avast activat, doncs el vàrem desactivar per facilitar l'accés a serveis com smtp o mtp.

Al fer aquest canvi, el nombre de connexions va començar a créixer sense cap problema.

Il·lustració 18: Connexions rebudes.

En la setmana que vàrem tenir actiu aquest Honeypot vam rebre 349.054 connexions, totes aquestes les van realitzar 661 IP's diferents. Aquesta xifra ens ajuda a intuir que la gran part d'aquestes eren causades per màquines degut a la diferència d'ambdós valors.



Il·lustració 19: Atacs per IP.

Com podem observar en la imatge superior, veiem que efectivament el nombre de connexions per única IP és desorbitat.

Si entrem a diferenciar les IP's pels països als quals pertanyen ens trobem amb la següent gràfica.

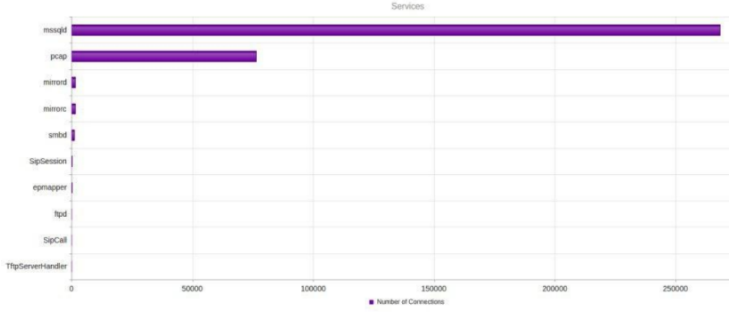
Il·lustració 20: Atacs per països per IP.

Podem observar que la majoria de les IP's pertanyen a Bulgària, el que va ser graciós de veure va ser que depenent de l'hora del dia, coincidint amb les hores de son, els diversos països anaven pujant o baixant. Sempre els mateixos, sempre en les mateixes hores, va haver-hi un punt que ja feia gràcia veure si un superava a l'altre.

Però a part d'aquests països, s'han rebut atacs de molts altres, encara que si bé no tots s'han pogut observar perquè la IP era desconeguda, sí que tenim l'origen d'aquests.

Il·lustració 21: Origen dels atacs.

Alhora, Dionaea ens permet conèixer els serveis a través dels quals s'han realitzat les connexions. I en aquest punt cal fer menció en què es van obrir uns ports més per tal de poder permetre les connexions.



Il·lustració 22: Serveis atacats.

Com podem veure en la imatge, el servei més atacat i amb gran diferència ha estat el de la base de dades, mssqld. Seguidament tenim el servei pcap, el qual pot pertànyer tant a npcac o a Winpcap, i són serveis de Windows els que serveixen per capturar tràfic -en viu- de la xarxa.

Alhora podem veure dos serveis que tenen el mateix nombre de connexions, aquest son els mirrord i mirrorc. Són dimonis i la seva funció resideix en la de controlar i supervisar els mòduls de miralls. Els miralls són els que ens proporcionen rèpliques de la consola

Un altre és smbd, el qual és un dels tres dimonis que componen el servei de Samba. Smbd subministra serveis per poder compartir arxius a clientsWindows mitjançant els ports TCP 139 i 445.

Els serveis sipsession i pmapper són serveis que estan orientats a la identificació de sessions, usuaris i els rols que tenen aquests.

Per finalitzar tenim el servei FTP, que és un protocol a nivell d'aplicació que ens permet fer transferències d'arxius entre sistemes a través de xarxes TCP / IP.

Després de la meitat del periode d'implementació al final vam poder observar com un atacant va aconseguir entrar i perpetra una descàrrega.

La informació que se'ns dona de l'atacant és molt detallada, tal com podem comprovar en la imatge inferior, l'atac s'ha dut a terme a través del port 2794, mitjançant el servei mssqld i el protocol TCP.

Il·lustració 23: Informació de l'atacant que ha descarregat els binaris.

També podem veure que la IP d'origen resideix en l'Índia i que el sistema operatiu utilitzat és el Windows i la versió d'aquest.

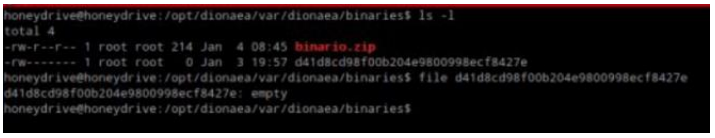
L'atacant ha realitzat una descàrrega introduint una URL en el buscador i mitjançant diverses connexions les quals han produït cada una 1 descàrrega, encara que totes elles pertinents a la mateixa IP: 14.141.10.162.

Il·lustració 24: Binaris descarregats.

Això ens fa pensar en què possiblement les connexions se li tancaven abans que pogués efectuar la descàrrega completa dels fitxers.

Dionaea emmagatzema els fitxers en la carpeta de binaris, allà guarda una còpia del que l'atacant ens ha intentat descarregar en el nostre sistema i també del Malware que s'intenta executar.

Com hem mencionat abans, ens hem trobat amb quatre comandes relatives amb una descàrrega de fitxers, però en cadascuna de les comandes el fitxer era el mateix. Anant a la carpeta pertinent podem observar que únicament tenim un fitxer amb aquest nom i que està completament buit.



Il·lustració 25: Anàlisi del binari descarregat.

Quan Dionaea s'encarrega de generar fitxers temporals i al final guarda una còpia del fitxer anomenant-lo amb el resultant d'aplicar l'algoritme md5. Amb la comanda file se'ns mostra el tipus de fitxer, en el nostre cas, donat que està buit ens diu que és empty.

Després d'analitzar el fitxer hem arribat a la conclusió de què és un fitxer de tipus zip que s'ha validat amb un Hash de tipus MD5 buit.

Si bé aquest fitxer no ens dóna informació, podem comprovar que realment és molt senzill que un cop accedeixin en el nostre sistema, ens puguin atacar amb algun script que sí que ens pot produir un dany impensable.

7. Conclusió

Al llarg del nostre treball, i partint d'uns mitjans materials bastant limitats, hem estat capaços d'instal·lar i configurar dos Honeypots, Kippo i Dionaea, de col·locar aquests esquers en la nostra xarxa, de mantenir-los durant un curt espai de temps i de recol·lectar i classificar els atacs que s'han rebut. I, certament, hem pogut valorar en primera persona que el ràtio cost/benefici de la implementació d'aquests sistemes de defensa resulten clarament positius, corroborant així l'opinió de la majoria dels professionals enquestats.

Seguint amb un fragment del llibre de Sun Tzu: *"la millor victòria és vèncer sense combatre, i aquesta és la distinció entre l'home prudent i l'ignorant"*. Els Honeypots permeten a l'administrador encarregat de la ciberseguretat mantenir la lluita lluny del sistema real, el qual ha de protegir, i fer-ho sense perdre ni el seu temps ni recursos que poden ser emprats en altres tasques. I no sols això; sinó que li permeten també recopilar una informació valuosíssima sobre els atacants.

És positiu per a una empresa dedicar part dels seus recursos de ciberseguretat a la implementació dels Honeypots?

La nostra resposta és un rotund sí. El cost econòmic que comporta la inversió es rendibilitza si pensem que no només protegim el sistema de possibles atacs sinó que alhora estem aprenent i descobrint possibles debilitats que podran ser esmenades abans de rebre un possible nou atac.

8. Treball futur

A continuació indicarem la possible línia de recerca que pot prendre el projecte després de l'estudi realitzat.

Com s'ha vist, els Honeypots són eines útils per a protegir els nostres sistemes, el problema resideix en quant aquests són descoberts per l'atacant, ja que pot realitzar-nos atacs de manera massiva per a falsejar els nostres resultats o simplement fer caure el sistema.

En el transcurs d'aquest projecte ens hem trobat amb un programari, Shodan, el qual analitza les IPs i retorna un nombre el qual representa la probabilitat de què la IP en qüestió pertanyi, o no, a un Honeypot.

El possible treball futur resideix a ser capaços d'eliminar per complet tot rastre del nostre Honeypot i fer una rèplica exacta d'un sistema real.

9. Agraïments

Després de molts mesos de feina i molta matèria apresa, per fi puc redactar els agraïments, donant per finalitzat el treball dut a terme.

M'agradaria iniciar agraint al meu tutor, Ramón Grau, ja que durant tot el transcurs d'aquest projecte ha estat al meu costat. També haig de mencionar a la meva família, que m'ha aguantat en les meves històries del TFG.

Fer una menció especial a Jordi Pons, Remo Suppi, Gemma Codina, Jorge Fatas, Carlos Fernández, Enric Rovira, Manuel Pina, Néstor Pina, Eulalia Formenti, José Luís Rodriguez, Ana Torrell, Xavier Capel, Marc Soriano, Tito Berja, Arnau Canyes, José Manuel López, Susana Moreno, Sergi SanMartí, Raúl Anton, Vicente Casino i Miguel Ángel Otín.

I als meus companys d'Accenture: Andrés Gil, Jaume Marsinyach, Adrià Castany i Albert Gormenzano.

Alhora, agrair a tots els lectors d'aquest projecte. Desitjo que, gràcies en aquest, pugueu haver gaudit d'una bona estona i que, igual que jo, trobeu un incentiu per iniciar a testejar amb els Honeypots.

10. Referències

[1] <L'art de la Guerra> Sun Tzu.

[2] «Deployment of a low interaction honeypot in an organizational private network». En 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 130-35. Udaipur: IEEE, 2011. https://doi.org/10.1109/ETNCC.2011.5958501.

[3] Dowling, S., M. Schukat, y H. Melvin. «Data-centric framework for adaptive smart city honeynets». En 2017 Smart City Symposium Prague (SCSP), 1-7, 2017. https://doi.org/10.1109/SCSP.2017.7973836.

[4] «Experiences with Honeypot Systems: Development, Deployment, and Analysis - IEEE Conference Publication». Accedit el 2 d'octubre de 2019. https://ieeexplore.ieee.org/document/1579742.

[5] Honeypot: a supplemented active defense system for network security - IEEE Conference Publication». Accedit el 2 d'octubre de 2019. https://ieeexplore.ieee.org/abstract/document/1236295.

[6] Huang, Cheng, Jiaxuan Han, Xing Zhang, y Jiayong Liu. «Automatic Identification of Honeypot Server Using Machine Learning Techniques». Security and Communication Networks 2019 (22 de septiembre de 2019): 1-8. https://doi.org/10.1155/2019/2627608.

[7] Karchev_MA_ComputerScience.pdf». Accedit el 2 d'octubre de 2019. https://essay.utwente.nl/79167/1/Karchev_MA_ComputerScience.pdf.

[8] Kilinc, H. Hakan, y Omer Faruk Acar. «Analysis of Attack and Attackers on VoIP Honeypot Environment». En 2018 26th Signal Processing and Communications Applications Conference (SIU), 1-4. Izmir, Turkey: IEEE, 2018. https://doi.org/10.1109/SIU.2018.8404331.

[9] Leonard, A. M., H. Cai, K. K. Venkatasubramanian, M. Ali, y T. Eisenbarth. «A honeypot system for wearable networks». En 2016 IEEE 37th Sarnoff Symposium, 199- 201, 2016. https://doi.org/10.1109/SARNOF.2016.7846755.

[10] Nedeltchev, Plamen, Mani Kesavan, Hugo Latapie, y Enzo Fenoglio. «VIRTUALIZED INTELLIGENT HONEYPOT AGENT», s. f., 8.

[11] International Journal on Future Revolution in Computer Science & Communication Engineering, s. f.

[12] «US20190190951A1.pdf». Accedido 2 d'octubre de 2019. https://patentimages.storage.googleapis.com/aa/d0/37/081e8cd18cdf73/US20190190951A1.pdf.

[13] Yashwant, Pagar Harshali, Pathare Anjali Sanjay, y Shaikh Sameer Shekhanur. «Buckler: Intrusion Detection and Prevention Using Honeypot» 2, n.o 1.

[14] Yewale, Prachi Shantaram, Anup Kumar Maity, Ravindra Sangle, y Prasad Awere. «Web-Based Honeypot Analysis Tool». International Journal of Innovations in Engineering and Technology 13, n.o 1 (2019): 5.

[15] «0x00sec - The Home of the Hacker». 0x00sec - The Home of the Hacker. Accedit el 2 d'octubre de 2019. https://0x00sec.org/.

[16] Alfon. «Entendiendo los HoneyPots y HoneyNets. Una visión práctica. Parte I». Seguridad y Redes (blog), 25 de octubre de 2010. https://seguridadyredes.wordpress.com/2010/10/25/entendiendo-los-honeypots-y-honeynets-una-visian-practica- partei

[17] Cheswick, Bill. «An Evening With Berferd In Which a Cracker Is Lured, Endured, and Studied», s. f., 11.

[18] «DEA-es-4HoneypotsyHoneynets.pdf». Accedit el 2 d'octubre de 2019.ttps://www.cs.upc.edu/~gabriel/files/DEA-es- 4HoneypotsyHoneynets.pdf.

[19] «Honey pots; descubre qué son, monitorízalos y caza al cazador». Pandora FMS - The Monitoring Blog (blog), 9 de octubre de 2017. https://pandorafms.com/blog/es/honey- pots/.

[20] «Honeypot: seguridad informática para detectar amenazas». IONOS Digitalguide. Accedit el 2 d'octubre de 2019. https://www.ionos.es/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/.

[21] «Honeypot, una herramienta para conocer al enemigo». INCIBE-CERT, 14 de junio de 2018. https://www.incibe-cert.es/blog/honeypot-herramienta-conocer-al-enemigo.

[22] «Honeypots : Herramienta de Seguridad de la Informacion». Honeypots : Herramienta de Seguridad de la Informacion. Accedit el 2 d'octubre de 2019. https://honeypots.wordpress.com/.

[23] «p5sd6337.pdf». Accedit el 2 d'octubre de 2019. https://www.feandalucia.ccoo.es/docu/p5sd6337.pdf.

[24] Patiño, José Enrique López. «DESARROLLO DE UN HONEYPOT PARA LA MONITORIZACIÓN Y PREVENCIÓN DE ATAQUES», s. f., 58.

[25] «¿Qué es un honeypot? Una trampa para atrapar a los hackers en el acto». Accedido 2 de octubre de 2019. https://www.cybertechprojects.com/news/que-es-un-honeypot-una-trampa-para-atrapar-a-los-hackers-en-el- acto/.

[26] «Run the Trap! How to Setup Your Own Honeypot to Collect Malware Samples». 0x00sec - The Home of the Hacker, 8 de julio de 2018. https://0x00sec.org/t/run-the- trap-how-to-setup-your-own-honeypot-to-collect- malware-samples/7445.

[27] «Patiño - DESARROLLO DE UN HONEYPOT PARA LA MONITORIZACIÓN Y.pdf». Accedido 3 de nov de 2019.

[28] Segovia, Alberto. «Honeynets II: Honeypots (Para aprender, perder… o no)». Security Art Work, 30 de abril de 2010. https://www.securityartwork.es/2010/04/30/honeypots-ii-para-aprender-perder%e2%80%a6-o-no/.

[29] Ana González y Pedro Berrocal. <<Seguridad en Sistemas Operativos - HoneyPot.>> Accedit el 29 d'octubre 2019 . https://blog.hackingcodeschool.net/wp-content/uploads/2017/05/Trabajo-de-Fin-de-M%C3%A1ster.pdf

[30] Niels Provos. <<Virtual Honeypot Framework>>Accedit el el 29 d'octubre de 2019. http://www.citi.umich.edu/u/provos/papers/honeyd.pdf

[31] Sergio Espí Luis. <<DESARROLLO DE UN HONEYPOT PARA LA MONITORIZACIÓN Y PREVENCIÓN DE ATAQUES>> Accedit el 30 d'octubre de 2019. https://riunet.upv.es/bitstream/handle/10251/91797/ESP%C3%8D%20%20Desarrollo%20de%20un%20honeypot%20para%20la%20monitorizaci%C3%B3n%20y%20prevenci%C3%B3n%20de%20ataques..pdf?sequence=1

[32] Fernando Vañó García. <<Configuración, Ampliación e Implantación de un Honeypot.>> Accedit el 30 d'octubre de 2019. https://www.fervagar.com/files/projects/hed_report_es.pdf

[33] Carlos Rosado Moral. <<Estudio y análisis de la implantación de un honeypot en una plataforma portátil para informática forense (RASPOT)>> Accedit el 30 d'octubre de 2019. https://repositorio.uam.es/handle/10486/662509

[34] «DEA-es-4HoneypotsyHoneynets.pdf». Accedido 3 de noviembre de 2019. https://www.cs.upc.edu/~gabriel/files/DEA-es- 4HoneypotsyHoneynets.pdf.

[35] «Developments of the Honeyd Virtual Honeypot». Accedit el 3 de novembre de 2019. http://www.honeyd.org/.

[36] «Hack Tutorial and Reference | UltimatePeter.Com». Accedit el 3 de novembre de 2019. https://ultimatepeter.com/category/technology/tutorial s/hack-tutorial-and-reference/.

[37] «hed_report_es.pdf». Accedit el 3 de novembre de 2019.https://www.fervagar.com/files/projects/hed_report_es.pdf.

[38] «Honeyd-CONFIGURACIÓN, EJECUCIÓN Y PRUEBA - ASO». Accedit el 3 de novembre del 2019. http://www.adminso.es/index.php/Honeyd-CONFIGURACI%C3%93N,_EJECUCI%C3%93N_Y_PRUEBA.

[39] The Ethical Hacker Network. «HoneyDrive 0.1 - "Honeypots in a Box!"» Accedit el 3 de novembre del 2019. https://www.ethicalhacker.net/forums/topic/honeydrive-0- 1-honeypots-in-a-box/.

[40] Patiño, José Enrique López. «DESARROLLO DE UN HONEYPOT PARA LA MONITORIZACIÓN Y PREVENCIÓN DE ATAQUES», s. f., 58.

[41] «17111043.pdf». Accedit el 3 de noviembre de 2019. https://security.cse.iitk.ac.in/sites/default/files/17111043.pdf. Chamotra, S., J. S. Bhatia, R. Kamal.

[42]«provos-honeyd.pdf». Accedit el 3 de noviembre de 2019. https://www.fp6-noah.org/events/workshop-1/provos-honeyd.pdf.

[43] «Honeyd (VIII). Tráfico capturado». Tecnoloxía xa (blog), 29 de agosto de 2011. http://tecnoloxiaxa.blogspot.com/2011/08/honeyd-viii- trafico-capturado.html.

[44] <<Captura de Malware con Dionaea>> Accedit el 19 de gener del 2020. https://www.honeynet.unam.mx/es/content/poc-captura-de-malware-con-el-honeypot-dionaea-ii

[45]<<Configuració i anàlisis de malware>> Accedit el 19 de gener del 2020. https://thehackerway.com/2015/04/14/honeypots-parte-3-configuracion-y-analisis-de-malware-con-dionaea/

[46]<<Visualizing Dionaea's>> Accedit el 19 de gener del 2020. https://bruteforce.gr/visualizing-dionaeas-results-with-dionaeafr/

[47]<<Dionaea con interface gráfico>> Accedit el 19 de gener del 2020. http://kinomakino.blogspot.com/2017/03/honeypots-xvii-dionaea-con-interface.html

[48] <<Shodan: Honeypot or not>> Accedit el 20 de gener de 2020. https://honeyscore.shodan.io/

[49] <<Honeypots industriales>> Accedit el 20 de gener de 2020. https://www.incibe-cert.es/blog/honeypots-industriales

[50] <<Monitorización de Honeypots>> Accedit el 20 de gener de 2020. https://pandorafms.com/blog/es/honey-pots/

[51] <<El Arte de la Ciberguerra: Conociendo al Enemigo Para una Mejor Defensa >> Accedit el 20 de gener de 2020. https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp2017-l_arte_de_la_ciberguerra_manuel_camacho.pdf

11. ANNEX

A continuació mostrarem les diverses instal·lacions i configuracions de les eines emprades en aquest projecte.

11.1. A1. Instal·lació LAMP

LAMP són les sigles que defineixen el procés d'instal·lació dels programes necessaris per fer ús de PHP en distribucions basades en Debian, com Ubuntu. LAMP corresponen a la instal·lació d'Apache, MySQL i PHP.

El primer pas és entrar a la consola com a root, així evitem que se'ns pregunti constantment la contrasenya.

```
sudo su
```

Procedirem instal·lant el servidor web Apache2.

```
apt-get install apache2
```

Per comprovar la correcta instal·lació anem al buscador i indiquem l'adreça localhost o la IP (ifconfig) del dispositiu, llavors s'hauria de mostrar la següent imatge:

Il·lustració 26: Correcte funcionament del servidor Apache.

A continuació instal·larem PHP, s'ha de tenir present que hi ha diverses versions i una mala selecció pot fer que els serveis no ens funcionin, per tant, nosaltres hem decidit fer una instal·lació general i que el mateix compilador gestioni les versions.

```
apt-get install libapache2-mod-php
```

A l'acabar la instal·lació dels mòduls, hem de reiniciar el servidor.

```
/etc/init.d/apache2 restart
```

Per tal de comprovar que PHP ens funciona, ens és suficient com crear un fitxer php en el directori

/var/www/html i des del navegador cridar-lo mitjançant localhost o IP/nomFitxer.php. En el nostre fitxer cridàvem la funció "phpinfo()" la qual ens mostra informació dels mòduls del sistema.

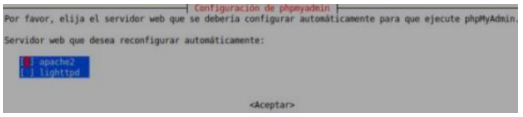
Il·lustració 27: Correcte funcionament de PHP i Apache.

11.2. A2. Instal·lació PHPMyAdmin

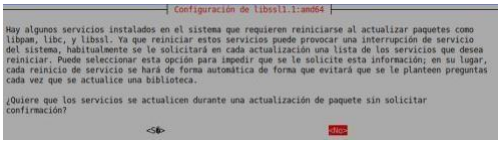
Un com tinguem els serveis anteriors funcionant, procedirem a instal·lar la base de dades.

```
apt-get install phpmyadmin
```

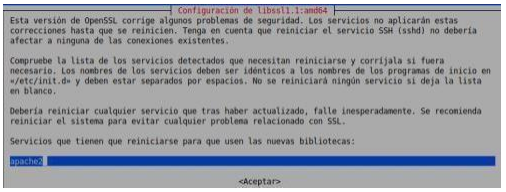
Se'ns mostrarà una taula com la següent i haurem de seleccionar l'opció d'Apache2, alhora sortiran unes pantalles com les següents i s'han de marcar com estan.



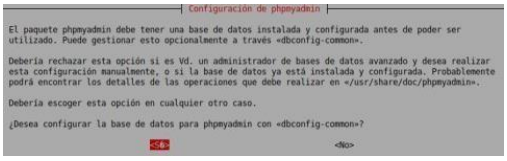
Il·lustració 28: Sel•lecció del servidor enllaçat a la BD.



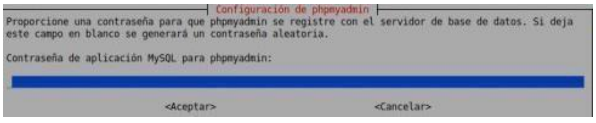
Il·lustració 29: No actualitzar serveis sense consentiment.



Il·lustració 31: Reinici Apache.



Il·lustració 30: Configuració de la BD.



Il·lustració 32: Indiquem un pwd per phpmyadmin.

Un cop feta la instal·lació procedirem a obrir el servei i alhora reiniciem apache.

```
service mysql

start service

apache2 restart
```

Un pas recomenable és la instal·lació de la següent extensió, la qual ens activa un mòdul específic de PHP.

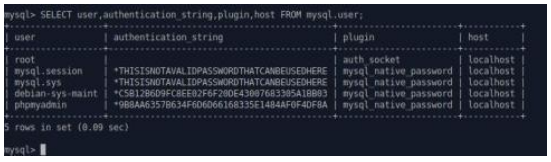
```
sudo phpenmod mbstring
```

Per acabar, ajustarem l'accés root amb contrasenya, que de normal no està actiu.

```
mysql -u root –p
```

Un cop estem dintre, procedirem a sol·licitar que printi els usuaris i els mòdels d'autenticació que utilitzen.

```
SELECT user,authentication_string,plugin,host
FROM mysql.user;
```

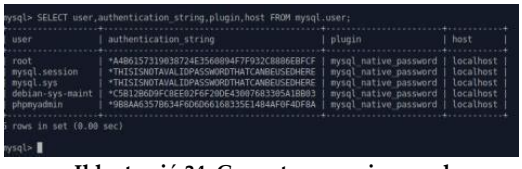


Il·lustració 33: Usuaris mysql

Com podem observar, l'usuari root solament té l'autenticació "auth_socket", el que ens indica que no tindrem accés des de PHPMyAdmin. Procedirem a canviar-ho mitjançant la sentència següent:

```
ALTER USER 'root'@'localhost' IDENTIFIED
WITH mysql_native_password BY 'XXX';
```

On el valor XXX és la contrasenya per accedir a la nostra base de dades i, si tornem a llençar la comanda anterior, observarem que la taula s'ha actualitzat.

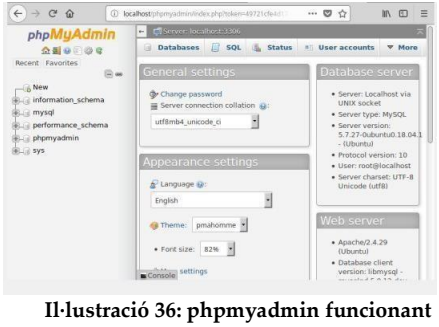


Il·lustració 34: Correctes usuaris mysql

Per finalitzar, reiniciem apache i anem al navegador i li indiquem l'adreça localhost/phpmyadmin.

Il·lustració 35: Pàgina d'inici phpmyadmin

En posar les nostres credencials podrem observar que se'ns ha creat la base de dades correctament i ja està en funcionament.



Il·lustració 36: phpmyadmin funcionant

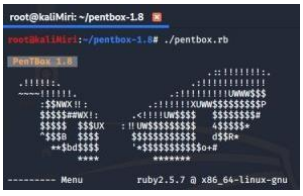
11.3. A3. INSTAL·LACIÓ PENTABOX

Per tal de poder fer proves sobre Honeypots fàcilment instal·lables s'ha realitzat la instal·lació del sistema operatiu Kali per tal de sobre aquest fer córrer Pentabox.

El primer que s'ha de fer és descarregar i extreure el tar de Pentabox i si tot va bé, el posem en marxa i llavors observem la següent imatge.

```
Wgethttp://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
```

```
tar -zxvf pentbox-1.8.tar.gz
./pentbox.rb
```



Il·lustració 37: Pentabox funciona

Potser ens trobem amb l'error de què no reconeix "ruby", això ho podem solucionar amb una última comanda:

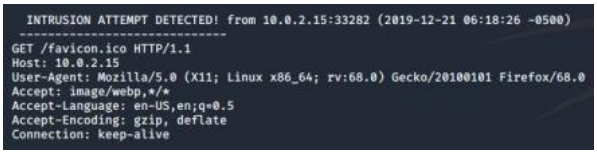
```
apt-get install ruby
```

Un cop instal·lat correctament, marquem el punt 2, ja que ens interesen les eines de xarxa i a continuació anem als honeypots.

Il·lustració 38: Menú i config

Podem observar que ens dóna 2 possibilitats, l'autoconfiguració activa un honeypot per defecte en el port 80. A continuació mostrarem una prova de la seva execució.

Il·lustració 39: Accés HTTP



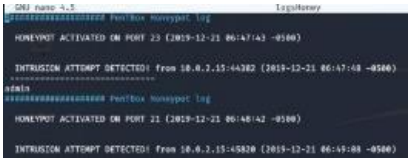
Il·lustració 40: Detecció de l'accés HTTP

Com volem analitzar més serveis, escollim la configuració manual i indicarem el port sobre el qual volem treballar i si volem guardar les intrusions en un log.

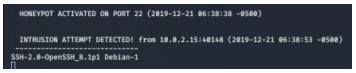
Il·lustració 41: Accessos Telnet i FTP

Il·lustració 42: Accés SSH

Les deteccions dels accessos les podem veure a continuació:



Il·lustració 43: Logs dels ports 21 i 23



Il·lustració 44: Accés SSH

11.4. A4. INSTAL·LACIÓ HONEYDRIVE

HoneyDrive és un servei virtualitzat (.OVA) el qual podem descarregar des de la pàgina de bruteforce. Per fer ús d'ell s'ha d'obrir VirtualBox, anar a arxiu i a l'opció "importar serveis virtualitzats" i seleccionem l'OVA descarregada.

Abans de fer córrer la nova màquina, s'ha de tocar la configuració de xarxa, en el nostre cas hem indicat que sigui un "adaptador pont", ja que així la nostra VM tindrà una direcció privada similar a la de la màquina principal. Si anem a configuració avançada, en l'apartat "modo promiscuo" s'ha li ha indicat que ho permeti a les VM.

Això significa que estem traient el filtre de recepció de paquets, per tant, podem observar tot el tràfic de les connexions. Ens és útil perquè ens permet fer un seguiment de l'activitat de la xarxa, però enfatitzar que sol permetem que ho apliqui a les MV perquè no volem que es pugui visualitzar el trànsit de la màquina amfitriona.

Il·lustració 45: Configuració de la xarxa.

Aquesta configuració l'hem dut a terme perquè és la forma en la qual podem rebre atacs.

Un cop desplegat el servei, en l'escriptori hi ha el fitxer "readme.txt" el qual ens indica els tipus de honeypots que té la màquina i les eines instal·lades.

11.5. A5. CONFIGURACIÓ DE KIPPO

Kippo és un tipus de Honeypot que gestionen els atacs de SSH gestionan un login propi. Per tant, podrem veure les diverses combinacions que fan els atacants en la nostra base de dades.

Per tal de configurar Kippo el primer que hem de fer és anar al fitxer de configuració "kippo.cfg" i indicar-li el port sobre el qual volem que actuï.

Per defecte, treballa sobre el port 2222, però nosaltres volem que treballi sobre el 22, SSH. Aquí cal matitzar que Kippo s'executa com un usuari sense privilegis, per tant, no podem simplement aixecar-lo sobre el port 22.

Tenim dos posibles opcions, llençar una comanda iptables que ens redirigueixi al port 22.

O bé seria fer ús d'authbind, que és un software que ens permet aixecar serveis a usuaris sense privilegis en ports inferiors al 1024.

El primer a fer és l'instal·lació i posteriorment la configuració de l'accès com a usuaris normals al port 22. Per això crearem un fitxer anomenat 22 i li donarem els permisos del nostre usuari:

```
apt-get install authbind
nano /etc/authbind/byport/22
chown honeydrive:honeydrive /etc/authbind/byport/22
chmod 777 /etc/authbind/byport/22
```

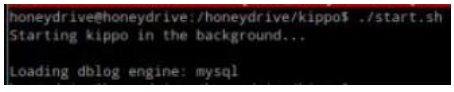
Un cop fet això, hem d'indicar-li al fitxer start.sh que tingui present l'establert en l'authbind. Això ho fem afegint al principi la següent línea:

```
#!/bin/sh

echo -n "Starting kippo in background..."
authbind --deep twistd -y kippo.tac -l log/kippo.log
--pidfile kippo.pid
```

Per finalitzar, en el propi fitxer de la configuració, canviem el port per defecte 2222 al port 22, ara que ja tenim permisos.

Un cop configurat el port, engeguem el Honeypot.



Il·lustració 46: Run Kippo

Per finalitzar, anem al buscador posant la nostra IP: 192.168.1.126/kippo-graph/

Ara que el tenim actiu, solament ens queda estar a l'espera de rebre atacs.

11.6. A6. CONFIGURACIÓ DE DIONAEA

Com ja s'ha mencionat, Dionaea és un tipus de Honeypot de baixa interacció que s'encarrega de capturar càrregues útils i programes maliciosos.

En aquest apartat mostrarem la configuració de DionaeaFR. És tractca d'una interfície web.

El primer que fem és anar a la carpeta /honeydrive/DionaeaFR/ i fer correr les següents comandes.

Il·lustració 47: Inici del servidor web

Aquestes s'encarreguen de iniciar el servidor web per a la nostra IP en el port que li indiquem. Per tant, podrem accedir a l'interfície si en el buscador li indiquem la següent URL: 192.168.1.126:8000

I ja per aixecar-lo anem a la carpeta /honeydrive/dionaea-vagrant/ i iniciem el fitxer runDionaea.sh

Il·lustració 48: Posada en marxa de Dionaea

Il·lustració 49: Posada en marxa de Dionaea com a dimoni.