UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

Grado en Ingeniería Informática

TRABAJO FIN DE GRADO

Detectando honeypots: Estudio, análisis y mejora de la ofuscación de honeypots.

Autor: D. Carlos Javier González Cortés
Tutor: D. Francisco de Borja Rodríguez Ortiz

Julio 2018

Detectando honeypots: Estudio, análisis y mejora de la ofuscación de honeypots.

AUTOR: D. Carlos Javier González Cortés
TUTOR: D. Francisco de Borja Rodríguez Ortiz

Grupo de Neurocomputación Biológica (GNB)
Dpto. Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Julio de 2018

Resumen

Cada día las Tecnologías de la Información y la Comunicación (TIC) avanzan de manera exponencial. Internet se ha introducido en la población hasta el punto de que hoy en día existen cerca de diez mil millones de dispositivos conectados a la red. Y a su vez, aumenta el número de criminales que emplean estas tecnologías para delinquir. El hecho de que Internet sea una red insegura por naturaleza implica ponérselo en bandeja a estos cibercriminales.

Por este motivo, una de las ramas más importantes de la Informática es la seguridad. La protección en la red es tan importante como la protección física, y para obtenerla es necesario alcanzar dos metas: concienciar a los usuarios de la red a dar un uso correcto de la misma y crear dispositivos que nos permitan alcanzar un "estado de seguridad". Uno de los dispositivos más utilizados para este fin son los honeypots, que permiten emular un sistema para hacer de cebo ante los cibercriminales, obtener nuevas metodologías de ataque y distraerlos del objetivo real.

Pero al igual que cualquier otro cebo, un honeypot no será de utilidad si la presa no cae en él. Para ello, debe estar bien oculto. En la actualidad una gran cantidad de los honeypots del mundo utilizan sistemas por defecto, que cualquier cibercriminal detectará y evitará fácilmente, y por tanto se pierden ataques para ser analizados.

Con la intención de evitarlo, en este trabajo de fin de grado se presenta una herramienta capaz de analizar, detectar y ofrecer mejoras a los honeypots. Con este sistema se puede consultar si una dirección IP alberga un honeypot o no. La herramienta cotejará distintos parámetros que los honeypots suelen emplear por defecto y dictaminará las probabilidades que hay de que esa dirección albergue en realidad a un honeypot.

El fin último de esta herramienta es poder servir al administrador de un honeypot para detectar fallos de ocultación en los honeypots, de forma que se hagan indistinguibles de los sistemas reales y que cumplan así la función para la que fueron creados.

Para terminar, se muestran varios análisis de los resultados recogidos por los honeypots durante los periodos de captación de ataque, mostrando una ocultación satisfactoria en la honeypot exterior al haber incrementado su número de ataques.

Palabras clave

Honeypot, Honeynet, Detección, Ocultación, Seguridad Informática, Análisis Forense, Auditoría, Tecnologías de la Información y la Comunicación, Ataques Informáticos, Informática Forense, Test de Penetración.

Abstract

Information and Comunication Technology (ICT) are quickly evolving day by day. Internet has been incorporated into the human population to the extent that nowadays there are approximately ten billion dispositives connected to the network.
At the same time, the number of criminals who use these technologies to commit a crime increases too.
The fact that Internet is an unsafe network by deffault, means it gives all kind of advantages to this cibercriminals.

That is the reason why Security is one of the most important branches in computer Science. Network protection is as important as physical protection, and to obtain it there are two goals necessary to complete it: aware network users to use it correctly and create tools which allow us to earn a "security status". One of the most used tools for this goal is honeypots which allows to emulate a system to use it as a bait and therefore catch the cybercriminals.

But, as well as any other bait, a honeypot will not be useful if a victim does not attack it. And for it, the honeypot must be very well hidden. Today a big percentage of honeypots in network use default system, that every criminal detects and avoid easily.

This is the reason why this final degree consists of a tool that can analyze, detect and improve the honeypot's obfuscation. This system allows to query if an IP has a honeypot or not. The tool analyzes considerable parameters that honeypots usually have by default, and shows the probability of a IP to be a honeypot.

The final aim of this tool is to allow the honeypot administrator to detect vulnerabilities in honeypot's obfuscation, because in this way it can be indistinguisable from a real system.

At the end, several analyses are shown of the results registered during the periods of attack capture. This analyses show a satisfactory obfuscation in the external honeypot having increased its number of attacks.

Keywords

Honeypot, Honeynet, Detection, Hiding, Computer Security, Forensic analysis, Audit, Computer Science, Computer Science Attacks, Forensic Computer Science, Pentesting.

Agradecimientos

A mi madre y a mi padre.
A mi tutor Francisco de Borja Rodríguez.

A esa persona que dijo "vale".
Y a todas las que dijeron "no vales".

A mi tío José Antonio. Gracias Huesitos.
A Dios, Buda, Alá, Gaia o como el lector desee llamarle.

A todos, gracias.

INDICE DE CONTENIDOS

1 Introducción 1
1.1 Contexto 1
1.2 Motivación 1
1.3 Objetivos 2
1.4 Organización de la memoria y etapas del proyecto 2
2 Estado del arte 3
2.1 Honeypots 3
2.2 Tipos de honeypots 3
2.2.1 Honeypots servidor 3
2.2.2 Honeypots cliente 4
2.2.3 Honeytokens 4
2.2.4 Honeypages 4
2.2.5 Honeynets 4
2.2.6 Honeyfarms 4
2.3 Honeypots escogidos para el proyecto 5
2.3.1 ConPot 6
2.3.2 Cowrie 6
2.3.3 Dionaea 6
2.3.4 ElasticPot 7
2.3.5 Glastopf 7
2.3.6 Honeytrap 7
2.3.7 Mailoney 7
2.3.8 Rdpy 8
2.3.9 Suricata 8
2.3.10 Vnclowpot 8
2.3.11 eMobility 8
2.4 Herramientas de detección de honeypots 8
2.4.1 Shodan Honeyscore 9
2.4.2 NMAP 9
2.4.3 FOCA 10
3 Análisis y Diseño 11
3.1 Ámbito del sistema 11
3.1.1 Definición del Problema 11
3.1.2 Planteamiento de la solución 11
3.2 Alcance 11
3.3 Requisitos 12
3.3.1 Requisitos funcionales principales 12
3.3.2 Restricciones de Diseño 12
3.4 Diagrama completo de la herramienta de detección 13
3.5 Etapas del proyecto 14
3.5.1 Estudio de los honeypots actuales para su detección: 14
3.5.2 Instalación de la infraestructura 14
3.5.3 Recogida de datos: 14
3.5.4 Desarrollo de herramienta de detección: 14
3.5.5 Ocultación y aumento de la seguridad de las honeynets: 15
3.5.6 Recogida de datos después de la ocultación: 15
4 Desarrollo e integración 17

4.1 Herramienta de detección de honeypots 17
4.1.1 Descripción General 17
4.2 Ocultación de los honeypots 21
5 Pruebas y resultados 25
5.1 Herramienta de detección 25
5.1.1 IP que alberga una honeynet t-Pot: 25
5.1.2 IP que no alberga una honeynet t-Pot: 27
5.2 Comprobación de herramienta 28
5.3 Recogida de datos 30
5.3.1 Honeynet A (Fuera del firewall de la UAM) 31
5.3.2 Honeynet B (Dentro de UAM) 34
6 Conclusiones y trabajo futuro 39
6.1 Conclusiones 39
6.2 Trabajo futuro 40
Referencias 41
Glosario 43
Anexos I
A Manuales de la honeynet T-Pot I
A.1 Manual de instalación I
A.2 Manual de configuración I
A.3 Manual de utilización II
A.4 Actualizaciones VII
B Información relacionada sobre honeypots y Sistemas de Seguridad IX
B.1 Sistemas de seguridad IX
(1) Intrusion Detection Systems (IDS) IX
(2) Firewalls X
(3) Honeypots X
B.2 Estructura de los honeypots X
B.3 Funcionalidad de los honeypots XI
B.4 Ubicación de los honeypots XI
(1) Antes del Firewall XI
(2) Después del Firewall XII
(3) En una zona desmilitarizada XII
B.5 Clasificación de los honeypots XIII
(1) Clasificación por nivel de interacción XIII
(2) Clasificación por medio XIV
(3) Clasificación por propósito XV
(4) Clasificación por tipo de ocultación. XV
C Programación de la herramienta XVII
C.1 Estructura del proyecto XVII
C.2 Pseudocódigo y diagramas de flujo XVIII
(1) Main XVIII
(2) Modo manual XIX
(3) Modo automático XX
(4) Comprobación de puertos XXI
(5) Comprobación profunda XXII
D Formas de detectar un honeypot XXV
E Análisis detallado de cada honeypot XXXI
E.1 Honeynet A XXXI
(1) ConPot XXXI

(2) Cowrie XXXV
(3) Dionaea XLI
(4) ElasticPot XLVI
(5) Glastopf XLVII
(6) Honeytrap L
(7) Mailoney LV
(8) Rdpy LIX
(9) Suricata LXIII
(10) Vnclowpot LXVIII
(11) eMobility LXXII
E.2 Honeynet B LXXIII
(1) ConPot LXXIII
(2) Cowrie LXXIII
(3) Dionaea LXXV
(4) ElasticPot LXXVI
(5) Glastopf LXXVI
(6) Honeytrap LXXVIII
(7) Mailoney LXXIX
(8) Rdpy LXXIX
(9) Suricata LXXIX
(10) Vnclowpot LXXXI
(11) eMobility LXXXII
E.3 Conclusiones del análisis LXXXII
F Grados de confianza que asigna la herramienta de detección LXXXV

INDICE DE FIGURAS

FIGURA 2.1 HONEYPOT SERVIDOR – FUENTE: HTTPS://WWW.HONEYNET.ORG 4

FIGURA 2.2 HONEYPOT CLIENTE – FUENTE HTTPS://WWW.RESEARCHGATE.NET 4

FIGURA 2.3 EJEMPLO DE UNA HONEYFARM – FUENTE HTTPS://WWW.SYMANTEC.COM 5

FIGURA 2.4 ARQUITECTURA DE LA HONEYNET T-POT – FUENTE: HTTP://DTAG-DEV-SEC.GITHUB.IO 5

FIGURA 2.5 PRUEBA DE SHODAN HONEYSCORE CONTRA LAS HONEYNETS DE LA UAM – FUENTE: HTTPS://HONEYSCORE.SHODAN.IO 9

FIGURA 2.6 EJEMPLO DE ESCANEO PROFUNDO CON NMAP – FUENTE PROPIA 10

FIGURA 2.7 HERRAMIENTA DE OBTENCIÓN DE METADATOS FOCA – FUENTE:WWW.ELEVENPATHS.COM 10

FIGURA 4.1 INICIO DE HONEYCATCH. 17

FIGURA 4.2 COMPROBACIÓN DE HERRAMIENTAS. 17

FIGURA 4.3 COMPROBACIÓN DE PUERTOS ABIERTOS 18

FIGURA 4.4 INTRODUCCIÓN DE CREDENCIALES. 18

FIGURA 4.5 COMPROBACIÓN CONPOT POSITIVA. 19

FIGURA 4.6 COMPROBACIONES COWRIE. 19

FIGURA 4.7 COMPROBACIONES DE DIONAEA. 19

FIGURA 4.8 COMPROBACIONES GLASTOPF. 20

FIGURA 4.9 RESULTADO FINAL DE HONEYCATCH SOBRE LA RED HONEYNET A. 21

FIGURA 4.10 VOLCADO DE LOGS DE HONEYPOT COWRIE. 21

FIGURA 4.11 ELIMINACIÓN DE USUARIOS POR DEFECTO. 22

FIGURA 4.12 COMANDOS COMUNES INSTALADOS. 22

FIGURA 4.13 DIRECTORIO WWW AÑADIDO. 23

FIGURA 4.14 ARCHIVOS AÑADIDOS AL DIRECTORIO TMP. 23

FIGURA 4.15 ACCESO A PÁGINA DE ADMINISTRACIÓN DE T-POT 23

FIGURA 4.16 IZQUIERDA: CONPOT/TEMPLATES/DEFAULT.XML ORIGINAL. DERECHA: MISMO ARCHIVO MODIFICADO. 23

FIGURA 4.17 PÁGINA WEB GLASTOPF. 24

FIGURA 5.1 MAPA DE ATAQUES HONEYNET A (15/4 – 30/4). 31

FIGURA 5.2 HONEYPOTS MÁS ATACADOS DE LA HONEYNET A (15/4 – 30/4). 31

FIGURA 5.3 HISTOGRAMA DE ATAQUES EN LA HONEYNET A (15/4 – 30/4). 31

FIGURA 5.4 ATAQUES DE LA HONEYNET A SEGÚN EL TIPO DE HONEYPOT. (15/4 – 30/4). 32

FIGURA 5.5 IZQUIERDA: REPUTACIÓN DE LAS IP ATACANTES. DERECHA: TOP 10 PAÍSES ATACANTES. (15/4 – 30/4) 32

FIGURA 5.6 MAPA DE ATAQUES HONEYNET A (1/6 – 15/6). 33

FIGURA 5.7 HONEYPOTS MÁS ATACADOS DE LA HONEYNET A (1/6 – 15/6). 33

FIGURA 5.8 HISTOGRAMA DE ATAQUES EN LA HONEYNET A (1/6 – 15/6). 33

FIGURA 5.9 ATAQUES DE LA HONEYNET A SEGÚN EL TIPO DE HONEYPOT. (1/6 – 15/6) 34

FIGURA 5.10 IZQUIERDA: REPUTACIÓN DE LAS IP ATACANTES. DERECHA: TOP 10 PAÍSES ATACANTES. (1/6 – 15/6). 34

FIGURA 5.11 MAPA DE ATAQUES HONEYNET B (15/4 – 30/4). 34

FIGURA 5.12 HISTOGRAMA DE EVENTOS EN LA HONEYNET B (15/4 – 30/4). 35

FIGURA 5.13 HISTOGRAMA DE EVENTOS EN LA HONEYNET B (15/4 – 30/4). 35

FIGURA 5.14 EVENTOS DE LA HONEYNET B SEGÚN EL TIPO DE HONEYPOT (15/4 – 30/4). 35

FIGURA 5.15 IZQUIERDA: REPUTACIÓN DE LAS IP ATACANTES. DERECHA: TOP 10 PAÍSES ATACANTES (15/4 – 30/4). 36

FIGURA 5.16 MAPA DE ATAQUES HONEYNET B (1/6 – 15/6). 36

FIGURA 5.17 HISTOGRAMA DE EVENTOS EN LA HONEYNET B (1/6 – 15/6). 37

FIGURA 5.18 HISTOGRAMA DE EVENTOS EN LA HONEYNET B (1/6 – 15/6). 37

FIGURA A.0.1 CONEXION INSEGURA A LA PÁGINA DE ADMINISTRACIÓN T-POT II

FIGURA A.0.2 HABILITAR CONEXIÓN INSEGURA. II

FIGURA A.0.3 INTRODUCCIÓN DE CREDENCIALES III

FIGURA A.0.40.4 GESTOR DE HONEYPOTS KIBANNA III

FIGURA A.0.5 PÁGINA WEB DE ADMINISTRACIÓN DE LA HONEYNET IV

FIGURA A.0.6 INFORMACIÓN DEL HONEYPOT COWRIE IV

FIGURA A.0.7 PANEL DE CONTROL DE ELASTICSEARCH V

FIGURA A.0.8 PANEL DE CONTROL DE NETDATA V

FIGURA A.0.9 PANEL DE CONTROL DE SPIDERFOOT VI

FIGURA A.0.10 PANEL DE CONTROL DE PORTAINER VI

FIGURA A.0.11 PANEL DE CONTROL DE WEBTTY VII

FIGURA B.0.12 ESQUEMA DE LA ARQUITECTURA DE UN IDS. – FUENTE: HTTPS://WWW.FWHIBBIT.ES X

FIGURA B.0.13 HONEYPOT UBICADO ANTES DEL FIREWALL – FUENTE: HTTPS://WWW.FWHIBBIT.ES XII

FIGURA B.0.14 HONEYPOT UBICADO DENTRO DEL FIREWALL - FUENTE: HTTPS://WWW.FWHIBBIT.ES XII

FIGURA B.0.15 HONEYPOT EN DMZ - FUENTE: HTTPS://WWW.FWHIBBIT.ES XIII

FIGURA C.0.16 PSEUDOCÓDIGO FUNCIÓN MAIN. XVIII

FIGURA C.0.17 DIAGRAMA DE FLUJO DE FUNCIÓN MAIN XIX

FIGURA C.0.18 PSEUDOCÓDIGO FUNCIÓN MODO_MANUAL XX

FIGURA C.0.19 DIAGRAMA DE FLUJO DE FUNCIÓN MODO_MANUAL XX

FIGURA C.0.20 PSEUDOCÓDIGO DE FUNCIÓN MODO_AUTOMÁTICO XXI

FIGURA C.0.21 DIAGRAMA DE FLUJO DE FUNCIÓN MODO_AUTOMATICO XXI

FIGURA C.0.22 PSEUDOCÓDIGO DE LA FUNCIÓN PORT_COMPROBATION XXII

FIGURA C.0.23 DIAGRAMA DE FLUJO DE FUNCIÓN PORT_COMPROBATION XXII

FIGURA C.0.24 PSEUDOCÓDIGO DE FUNCIÓN DEEP_TEST XXIII

FIGURA C.0.25 DIAGRAMA DE FLUJO DE FUNCIÓN DEEP_TEST XXIII

FIGURA D.0.26 EJEMPLO: PÁGINA DE ADMINISTRACIÓN DEL HONEYPOT KIPPO – FUENTE: HTTPS://BRUTEFORCELAB.COM XXVI

FIGURA D.0.27 EJEMPLO: PÁGINA DE ADMINISTRACIÓN DE LA HONEYNET T-POT XXVI

FIGURA D.0.28 COMPROBACIÓN DE USUARIOS EN T-POT XXVII

FIGURA D.0.29 IZQUIERDA, SALIDA AL EJECUTAR INSTRUCCIÓN SUDO EN SISTEMA UBUNTU REAL. DERECHA, SALIDA AL EJECUTAR INSTRUCCIÓN SUDO EN HONEYPOT. XXVII

FIGURA D.0.30 IZQUIERDA: COMANDO "MAN LS" EN UN SISTEMA REAL. DERECHA: COMANDO "MAN LS" EN UN HONEYPOT. XXVII

FIGURA D.0.31 COMPROBACIÓN DE COMANDO "USERADD" EN HONEYPOT. XXVIII

FIGURA D.0.32 EJEMPLO DE USO HERRAMIENTA WIRESHARK – FUENTE: WWW.LIFEWIRE.COM XXIX

FIGURA D.0.33 EJEMPLO DE EJECUCIÓN FOCA – FUENTE: HTTP://P01N7L355.BLOGSPOT.COM XXX

FIGURA E.0.34 MAPA DE ATAQUE DE HONEYPOT CONPOT. XXXI

FIGURA E.0.35 HISTOGRAMA DE ATAQUES DE HONEYPOT CONPOT. XXXI

FIGURA E.0.36 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT CONPOT. XXXII

FIGURA E.0.37 REPUTACIÓN DE LAS IPS ATACANTES DE HONEYPOT CONPOT. XXXII

FIGURA E.0.38 MAPA DE ATAQUE DE HONEYPOT CONPOT. XXXIII

FIGURA 0.39 HISTOGRAMA DE ATAQUES DE HONEYPOT CONPOT. XXXIV

FIGURA 0.40 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT CONPOT. XXXIV

FIGURA E.0.41 REPUTACIÓN DE LAS IPS ATACANTES DE HONEYPOT CONPOT. XXXIV

FIGURA E.0.42 MAPA DE ATAQUE DE HONEYPOT COWRIE XXXV

FIGURA E.0.43 HISTOGRAMA DE ATAQUES DE HONEYPOT COWRIE. XXXVI

FIGURA E.0.44 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT COWRIE. XXXVI

FIGURA E.0.45 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT COWRIE. XXXVI

FIGURA E.0.46 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE COWRIE. DERECHA: TOP 10 PAÍSES ATACANTES HONEYPOT COWRIE. XXXVII

FIGURA E.0.47 TAGCLOUD DE USUARIOS Y CONTRASEÑAS MÁS PROBADOS POR LOS ATACANTES DE COWRIE. XXXVII

FIGURA E.0.48 MAPA DE ATAQUE DE HONEYPOT COWRIE XXXIX

FIGURA E.0.49 HISTOGRAMA DE ATAQUES DE HONEYPOT COWRIE. XXXIX

FIGURA E.0.50 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT COWRIE. XXXIX

FIGURA E.0.51 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT COWRIE. XL

FIGURA E.0.52 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE COWRIE. DERECHA: TOP 10 PAÍSES ATACANTES HONEYPOT COWRIE. XL

FIGURA E.0.53 TAGCLOUD DE USUARIOS Y CONTRASEÑAS MÁS PROBADOS POR LOS ATACANTES DE COWRIE. XL

FIGURA E.0.54 MAPA DE ATAQUE DE HONEYPOT DIONAEA. XLII

FIGURA E.0.55 HISTOGRAMA DE ATAQUES DE HONEYPOT DIONAEA. XLII

FIGURA E.0.56 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT DIONAEA. XLII

FIGURA E.0.57 IZQUIERDA: REPUTACIÓN DE LAS IPS ATACANTES DE DIONAEA. DERECHA: TOP 10 PAÍSES ATACANTES DE DIONAEA. XLIII

FIGURA E.0.58 HISTOGRAMA DE PUERTOS ATACADOS EN HONEYPOT DIONAEA. XLIII

FIGURA E.0.59 TAGCLOUD DE USUARIOS Y CONTRASEÑAS MÁS UTILIZADOS AL ATACAR EL HONEYPOT DIONAEA. XLIV

FIGURA E.0.60 MAPA DE ATAQUE DE HONEYPOT DIONAEA. XLIV

FIGURA E.0.61 HISTOGRAMA DE ATAQUES DE HONEYPOT DIONAEA. XLV

FIGURA E.0.62 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT DIONAEA. XLV

FIGURA E.0.63 IZQUIERDA: REPUTACIÓN DE LAS IPS ATACANTES DE DIONAEA. DERECHA: TOP 10 PAÍSES ATACANTES DE DIONAEA. XLV

FIGURA E.0.64 HISTOGRAMA DE PUERTOS ATACADOS EN HONEYPOT DIONAEA. XLVI

FIGURA E.0.65 TAGCLOUD DE USUARIOS Y CONTRASEÑAS MÁS UTILIZADOS AL ATACAR EL HONEYPOT DIONAEA. XLVI

FIGURA E.0.66 MAPA DE ATAQUES DE HONEYPOT GLASTOPF. XLVII

FIGURA E.0.67 HISTOGRAMA DE ATAQUES DE HONEYPOT GLASTOPF. XLVII

FIGURA E.0.68HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT GLASTOPF. XLVIII

FIGURA E.0.69 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE GLASTOPF. DERECHA: TOP 10 PAÍSES ATACANTES DE GLASTOPF. XLVIII

FIGURA E.0.70 MAPA DE ATAQUES DE HONEYPOT GLASTOPF. XLIX

FIGURA E.0.71 HISTOGRAMA DE ATAQUES DE HONEYPOT GLASTOPF. XLIX

FIGURA E.0.72HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT GLASTOPF. XLIX

FIGURA E.0.73 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE GLASTOPF. DERECHA: TOP 10 PAÍSES ATACANTES DE GLASTOPF. L

FIGURA E.0.74 MAPA DE ATAQUE DE HONEYPOT HONEYTRAP. LI

FIGURA E.0.75 HISTOGRAMA DE ATAQUES DE HONEYPOT HONEYTRAP. LI

FIGURA E.0.76 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT HONEYTRAP. LI

FIGURA E.0.77 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT HONEYTRAP. LII

FIGURA E.0.78 MAPA DE CALOR DE PUERTOS DE HONEYPOT HONEYTRAP. LII

FIGURA E.0.79 MAPA DE CALOR DE PUERTOS (EXCLUYENDO EL PUERTO 4899) DE HONEYPOT HONEYTRAP. LII

FIGURA E.0.80 MAPA DE ATAQUE DE HONEYPOT HONEYTRAP. LIII

FIGURA E.0.81 HISTOGRAMA DE ATAQUES DE HONEYPOT HONEYTRAP. LIII

FIGURA E.0.82 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT HONEYTRAP. LIV

FIGURA E.0.83 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT HONEYTRAP. LIV

FIGURA E.0.84 MAPA DE CALOR DE PUERTOS DE HONEYPOT HONEYTRAP. LIV

FIGURA E.0.85 MAPA DE ATAQUES DE HONEYPOT MAILONEY. LV

FIGURA E.0.86 HISTOGRAMA DE ATAQUES DE HONEYPOT MAILONEY. LVI

FIGURA E.0.87 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT MAILONEY. LVI

FIGURA E.0.88 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE MAILONEY. DERECHA: TOP 10 PAÍSES ATACANTES DE MAILONEY. LVI

FIGURA E.0.89 MAPA DE ATAQUES DE HONEYPOT MAILONEY. LVII

FIGURA E.0.90 HISTOGRAMA DE ATAQUES DE HONEYPOT MAILONEY. LVIII

FIGURA E.0.91 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT MAILONEY. LVIII

FIGURA E.0.92 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE MAILONEY. DERECHA: TOP 10 PAÍSES ATACANTES DE MAILONEY. LVIII

FIGURA E.0.93 MAPA DE ATAQUES DE HONEYPOT RDPY. LX

FIGURA E.0.94 HISTOGRAMA DE ATAQUES DE HONEYPOT RDPY. LX

FIGURA E.0.95 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT RDPY. LX

FIGURA E.0.96 IZQUIERDA: REPUTACIÓN DE LAS IPS ATACANTES DE RDPY. DERECHA: TOP 10 PAÍSES ATACANTES DE RDPY. LXI

FIGURA E.0.97 MAPA DE ATAQUES DE HONEYPOT RDPY. LXII

FIGURA E.0.98 HISTOGRAMA DE ATAQUES DE HONEYPOT RDPY. LXII

FIGURA E.0.99 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT RDPY. LXII

FIGURA E.0.100 IZQUIERDA: REPUTACIÓN DE LAS IPS ATACANTES DE RDPY. DERECHA: TOP 10 PAÍSES ATACANTES DE RDPY. LXIII

FIGURA E.0.101 MAPA DE ATAQUES DE HONEYPOT SURICATA. LXIV

FIGURA E.0.102 HISTOGRAMA DE ATAQUES DE HONEYPOT SURICATA. LXIV

FIGURA E.0.103 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT SURICATA. LXIV

FIGURA E.0.104 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT SURICATA. LXV

FIGURA E.0.105 TOP 10 DE DATOS DE ATACANTES RECOGIDOS POR HONEYPOT SURICATA. LXV

FIGURA E.0.106 MAPA DE ATAQUES DE HONEYPOT SURICATA. LXVI

FIGURA E.0.107 HISTOGRAMA DE ATAQUES DE HONEYPOT SURICATA. LXVI

FIGURA E.0.108 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT SURICATA. LXVII

FIGURA E.0.109 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT SURICATA. LXVII

FIGURA E.0.110 TOP 10 DE DATOS DE ATACANTES RECOGIDOS POR HONEYPOT SURICATA. LXVII

FIGURA E.0.111 MAPA DE ATAQUES DE HONEYPOT VNCLOWPOT. LXVIII

FIGURA E.0.112 HISTOGRAMA DE HONEYPOT VNCLOWPOT. LXIX

FIGURA E.0.113 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT VNCLOWPOT. LXIX

FIGURA E.0.114 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE HONEYPOT VNCLOWPOT. DERECHA: TOP 10 PAÍSES ATACANTES DE VNCLOWPOT. LXIX

FIGURA E.0.115 MAPA DE ATAQUES DE HONEYPOT VNCLOWPOT. LXXI

FIGURA E.0.116 HISTOGRAMA DE HONEYPOT VNCLOWPOT. LXXI

FIGURA E.0.117 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT VNCLOWPOT. LXXI

FIGURA E.0.118 MAPA DE ATAQUES DE COWRIE. LXXIII

FIGURA E.0.119 HISTOGRAMA DE ATAQUES DE HONEYPOT COWRIE. LXXIV

FIGURA E.0.120 HISTOGRAMA DE ATAQUES POR PAÍS DE HONEYPOT COWRIE. LXXIV

FIGURA E.0.121 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT COWRIE. LXXIV

FIGURA E.0.122 MAPA DE ATAQUES DE HONEYPOT DIONAEA. LXXV

FIGURA E.0.123 MAPA DE ATAQUE DE HONEYPOT GLASTOPF. LXXVI

FIGURA E.0.124 HISTOGRAMA DE ATAQUES DE HONEYPOT GLASTOPF. LXXVI

FIGURA E.0.125 HISTOGRAMA DE ATAQUES DE HONEYPOT GLASTOPF. LXXVII

FIGURA E.0.126 IZQUIERDA: REPUTACIÓN DE IPS ATACANTES DE HONEYPOT GLASTOPF. DERECHA: TOP 10 PAÍSES DE HONEYPOT GLASTOPF.....LXXVII

FIGURA E.0.127 MAPA DE ATAQUES DE HONEYPOT HONEYTRAP. LXXVIII

FIGURA E.0.128 PUERTOS ATADOS DE HONEYPOT HONEYTRAP..... LXXVIII

FIGURA E.0.129 MAPA DE ATAQUES DE HONEYPOT SURICATA.....LXXIX

FIGURA E.0.130 HISTOGRAMA DE ATAQUES DE HONEYPOT SURICATA..... LXXX

FIGURA E.0.131 HISTOGRAMA DE ATAQUES DE HONEYPOT SURICATA..... LXXX

FIGURA E.0.132 TOP 10 DE DATOS DE ATACANTES RECOGIDOS POR HONEYPOT SURICATA. ... LXXX

FIGURA E.0.133 HISTOGRAMA DE PUERTOS ATACADOS DE HONEYPOT SURICATA.....LXXXI

FIGURA E.0.134 COMPARATIVA DE ATAQUES EN LA HONEYNET A ANTES Y DESPUÉS DE LA OCULTACIÓN.....LXXXII

FIGURA E.0.135 COMPARATIVA DE ATAQUES EN LA HONEYNET B ANTES Y DESPUÉS DE LA OCULTACIÓN..... LXXXIII

INDICE DE TABLAS

TABLA 2.1 CARACTERÍSTICAS HONEYPOT CONPOT 6

TABLA 2.2 CARACTERÍSTICAS HONEYPOT COWRIE 6

TABLA 2.3 CARACTERÍSTICAS HONEYPOT DIONAEA 6

TABLA 2.4 CARACTERÍSTICAS HONEYPOT GLASTOPF 7

TABLA 2.5 CARACTERÍSTICAS HONEYPOT HONEYTRAP 7

TABLA 2.6 CARACTERÍSTICAS HONEYPOT MAILONEY 7

TABLA 2.7 CARACTERÍSTICAS HONEYPOT RDPY 8

TABLA 2.8 CARACTERÍSTICAS HONEYPOT VNCLOWPOT 8

TABLA 2.9 CARACTERÍSTICAS HONEYPOT EMOBILITY 8

TABLA E.0.1 PROVEEDORES DE LAS IPS ATACANTES EN CONPOT. XXXII

TABLA E.0.2 INPUTS INTRODUCIDOS POR ATACANTES DE HONEYPOT CONPOT. XXXIII

TABLA E.0.3 RESPUESTAS A COMANDOS INTRODUCIDOS EN EL HONEYPOT CONPOT. XXXIII

TABLA E.0.4 PROVEEDORES DE LAS IPS ATACANTES EN CONPOT. XXXV

TABLA E.0.5 PROVEEDORES DE LAS IPS ATACANTES EN COWRIE. XXXVIII

TABLA E.0.6 COMANDOS INTRODUCIDOS EN HONEYPOT COWRIE. XXXVIII

TABLA E.0.7 PROVEEDORES DE LAS IPS ATACANTES EN COWRIE. XLI

TABLA E.0.8 COMANDOS INTRODUCIDOS EN HONEYPOT COWRIE. XLI

TABLA E.0.9 PROVEEDORES DE LAS IPS ATACANTES EN DIONAEA. XLIV

TABLA E.0.10 PROVEEDORES DE LAS IPS ATACANTES EN DIONAEA. XLVI

TABLA E.0.11 PROVEEDORES DE LAS IPS ATACANTES EN GLASTOPF. XLVIII

TABLA E.0.12 PROVEEDORES DE LAS IPS ATACANTES EN GLASTOPF. L

TABLA E.0.13 PROVEEDORES DE LAS IPS ATACANTES EN HONEYTRAP. LIII

TABLA E.0.14 PROVEEDORES DE LAS IPS ATACANTES EN HONEYTRAP. LV

TABLA E.0.15 PROVEEDORES DE LAS IPS ATACANTES EN MAILONEY. LVII

TABLA E.0.16 COMANDOS INTRODUCIDOS POR SMTP EN HONEYPOT MAILONEY. LVII

TABLA E.0.17 PROVEEDORES DE LAS IPS ATACANTES EN MAILONEY. LIX

TABLA E.0.18 COMANDOS INTRODUCIDOS POR SMTP EN HONEYPOT MAILONEY. LIX

TABLA E.0.19 PROVEEDORES DE LAS IPS ATACANTES EN RDPY. LXI

TABLA E.0.20 PROVEEDORES DE LAS IPS ATACANTES EN RDPY. LXIII

TABLA E.0.21 DESCRIPCIÓN DE LOS MENSAJES INTERCAMBIADOS DE HONEYPOT SURICATA. ..LXVI

TABLA E.0.22 DESCRIPCIÓN DE LOS MENSAJES INTERCAMBIADOS DE HONEYPOT SURICATA.LXVIII

TABLA E.0.23 PROVEEDORES DE LAS IPS ATACANTES EN VNCLOWPOT. LXX

TABLA E.0.24 INTERCAMBIO VNC DE HONEYPOT VNCLOWPOT. LXX

TABLA E.0.25 PROVEEDORES DE LAS IPS ATACANTES EN VNCLOWPOT. LXXII

TABLA E.0.26 INTERCAMBIO VNC DE HONEYPOT VNCLOWPOT. LXXII

TABLA E.0.27 COMANDOS MÁS INTRODUCIDOS POR LOS ATACANTES DE HONEYPOT COWRIE. LXXV

TABLA E.0.28 PROVEEDORES DE LAS IPS ATACANTES EN GLASTOPF. LXXVII

TABLA E.0.29 DESCRIPCIÓN DE LOS MENSAJES INTERCAMBIADOS DE HONEYPOT SURICATA LXXXI

TABLA F.0.30 PORCENTAJES DEL GRADO DE CONFIANZA QUE APORTA CADA TEST. LXXXV

1 Introducción

1.1 *Contexto*

Internet se ha ido introduciendo día a día en nuestras vidas de forma asombrosa. Esto ha hecho que cada vez sean más los ataques que los dispositivos reciben por parte de atacantes que desean robar información o dinero utilizando para ello sus computadoras.
Además, cada vez los ataques son más y más refinados, y es muy complicado librarse de ellos una vez han infectado un ordenador.

Es por ello por lo que hoy en día es muy importante la prevención de los ataques informáticos. Si conseguimos evitar que los atacantes entren en nuestro ordenador, conseguiremos alcanzar la seguridad. Dado que es imposible que exista una seguridad perfecta, puesto que una de las primeras leyes de la seguridad informática es que si alguien dispone de tiempo y recursos podrá vulnerar el sistema más seguro (1), debemos tratar de poner la mayor cantidad de trampas que podamos a los atacantes, y estudiar sus movimientos para anteponernos a las adversidades. Hay varias vías para minimizar los ataques: auditorías de seguridad con las que detectar vulnerabilidades del propio sistema, pruebas específicas y protección de infraestructuras críticas como los sistemas SCADA, antivirus, firewalls…

Pero en una rama paralela a estos sistemas tendríamos los honeypots, sistemas activo-pasivos de seguridad, que permiten emular un sistema para confundir a los atacantes y hacerles perder el tiempo a la vez que recopilan información de estos y almacenan datos muy interesantes para su posterior estudio. Estos datos pueden ser las herramientas que utilizan para atacar, si son humanos o bots, el comportamiento de los mismos, e incluso la ubicación desde donde están atacando. Saber qué técnicas emplean los atacantes contra nuestras infraestructuras y sistemas es clave para saber cómo protegernos y para distraerlos y evitar que ataquen a sistemas reales.

Los honeypots adquieren la apariencia del hardware, software, datos e información de servicio de los equipos que queremos proteger. Con la diferencia de que en realidad están vacíos, no poseen ninguna información que el atacante pueda utilizar en nuestra contra. Por tanto, sin el camuflaje preciso y las herramientas adecuadas para ocultar el honeypot la trampa no funcionará y el atacante descubrirá rápidamente que no se encuentra en un sistema real.

Este proyecto es un documento creado a partir del estudio y análisis de las tecnologías de la Seguridad Informática, en concreto de las conocidas redes de honeypots, y está basado en la investigación y creación de una herramienta implementada con el fin de mejorar la oclusión de los honeypot en la red. Para ello se emplearán técnicas de pentesting, auditoría informática e informática forense, descubriendo así cuáles son las principales técnicas que utilizan los atacantes para descubrir a los honeypots, e implementar contramedidas en los honeypots de la Universidad Autónoma de Madrid haciéndolos aún más robustos.

1.2 *Motivación*

El motivo principal que da vida a este proyecto es desarrollar contramedidas que impidan a los atacantes detectar si el sistema que atacan es real o se trata de un honeypot, y de esa forma aumentar el tiempo que pasan en estos sistemas trampa y disminuir el número de sistemas reales que atacan. De esta forma los honeypots serán mejorados para ser

prácticamente indistinguibles con un entorno real y poder realizar su función principal: engañar a los atacantes.

Con este motivo, se creará y empleará una herramienta para auditar y mejorar los honeypots residentes en la Universidad Autónoma de Madrid, con lo que se espera recibir un mayor número de ataques especializados de los que podamos sacar aún más información en un futuro.

1.3 *Objetivos*

El principal objetivo de este proyecto es mejorar la ocultación de los honeypots para aumentar así su efectividad. Este objetivo se distribuye en los siguientes subobjetivos:

- ***Objetivo 0: Implantación de un sistema de honeypots en la Universidad Autónoma de Madrid.***

Se instalarán dos redes de honeypots, que servirán como plataforma de trabajo y estudio. Se configurarán de forma que haya una red de honeypots delante del firewall de la universidad y otra detrás, para así comparar cómo afecta este sistema defensivo a los ataques recogidos.

- ***Objetivo 1: Creación de una herramienta que evalúe la posibilidad de que un determinado sistema sea un señuelo.***

Mediante la realización de una auditoría de seguridad se creará una herramienta basada en técnicas de pentesting en la que se realizarán una serie de comprobaciones en la supuesta máquina honeypot para detectar si realmente lo es. Para ello adquiriré el rol de atacante.

- ***Objetivo 2: Mejora y ofuscación de sistemas señuelo con los datos obtenidos.***

El fin último es mejorar los sistemas honeypot con la información recopilada y volverlos más ocultos ante los atacantes, para que de esa forma muchos más ataques queden registrados y se pueda recopilar aún más información.

- ***Objetivo 3: Estudio y Análisis de los Ataques en una red de honeypots (Honeynet).***

Se comprobarán los ataques realizados a los honeypots de la Universidad Autónoma de Madrid antes y después de mejorar su ocultación con los datos recogidos tras probar la herramienta, para realizar un estudio sobre cómo mejorar el nivel de detección.

1.4 *Organización de la memoria y etapas del proyecto*

La organización de esta memoria consta de los siguientes apartados:

- ***Introducción:*** Presentación del proyecto, motivación del mismo, y objetivos que se cumplirán durante su desarrollo.
- ***Estado del arte.*** Estudio de los distintos tipos de honeypots que se utilizarán y mecanismos de ocultación actuales.
- ***Análisis y Diseño.*** Planificación de cada etapa que conforma este proyecto.
- ***Desarrollo e integración.*** Técnicas y procedimientos ejecutados para el cumplimiento de los objetivos propuestos para desarrollar la herramienta y ocultar los honeypots.
- ***Pruebas y resultados.*** Resultados obtenidos tras el desarrollo y pruebas realizadas para la verificación de estos. Abarca la fase de pentesting, la prueba de la herramienta y el análisis de los resultados.
- ***Conclusiones y trabajo futuro.*** Conclusiones sobre el trabajo realizado y posibles vías a seguir para continuar su desarrollo y evolución.

2 Estado del arte

En este capítulo se explica con detalle los fundamentos de los honeypots, véase: qué son, cómo funcionan, qué tipos hay y para qué sirven. Además, se analizan específicamente los honeypots que conforman las dos honeynets del proyecto. Por último, se describen las herramientas de detección de honeypots que existen actualmente en el mercado y sus puntos fuertes y débiles.

2.1 *Honeypots*

Un honeypot ("tarro de miel" en inglés) es un recurso multidisciplinar de seguridad informática, cuya principal función es ser comprometido, atacado e invadido por usuarios maliciosos, engañándoles con la apariencia de un sistema real. Los honeypots son una fuente de información para el investigador de seguridad informática puesto que monitoriza y analiza dichos ataques en un sistema sin ningún tipo de información sensible que pueda ser comprometida.

Un honeypot no reduce la probabilidad de que ataquen un sistema, de hecho todo lo contrario, un honeypot busca que lo ataquen la mayor cantidad de usuarios maliciosos posible, puesto que su fin último es analizar las técnicas que emplean estos atacantes para mejorar el resto de los sistemas mediante la realización de un análisis forense. Sin embargo, un honeypot puede desviar la atención de los atacantes y hacer que pierdan el tiempo atacándolos en vez de tratar de vulnerar los sistemas reales. De hecho, el problema principal de los honeypots es ser demasiado dulces, es decir, son tan fáciles de penetrar que los atacantes detectan rápidamente que se encuentran dentro de uno al vulnerarlo, y cesan rápidamente sus actividades en los mismos.

Comparado con el resto de las herramientas de seguridad, la principal diferencia es que estas están diseñadas para una tarea específica. Por ejemplo, un IDS (Intrusion Detection System) se emplea para la detección de ataques mediante el monitoreo de actividades, con el fin de detectar accesos no autorizados, un firewall se usa para controlar el tráfico de la red, etc., pero un honeypot sin embargo no busca resolver un solo problema, sino que se puede emplear de distintas formas, según la función que se le quiera dar.

2.2 *Tipos de honeypots*

A continuación, se explica brevemente las distintas variedades de honeypots que podemos encontrar en este proyecto. Se puede localizar más información sobre los diferentes sistemas de seguridad, la estructura, funcionalidad, ubicación y clasificación de los honeypots, así como el diseño de los que se han implantado en la Universidad Autónoma de Madrid, en el anexo B.

2.2.1 Honeypots servidor

Denominados honeypots pasivos, son los más comunes, sobre todo entre los honeypots de baja interacción. Simulan ser servidores con una funcionalidad específica a los que los atacantes se conectan. Su función es obtener las metodologías de ataques (sobre todo las nuevas y poco conocidas, llamadas zero-days) que utilizan los atacantes para vulnerar los servidores a los que se conectan, ya que cualquier cliente que se conecte a este honeypot es considerado una amenaza (2).

Permiten detectar nuevos exploits y malware simulado.
La Figura 2.1 muestra una representación entre un honeypot servidor y un atacante.

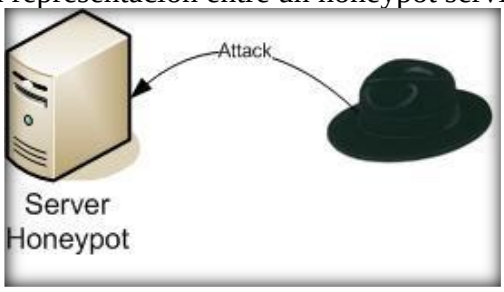


Figura 2.1 Honeypot servidor – Fuente: https://www.honeynet.org

2.2.2 Honeypots cliente

Denominados honeypots pasivos, son menos comunes, se dan sobre todo entre los honeypots de baja interacción. La Figura 2.2 representa la interacción entre un honeypot cliente y un servidor maligno.

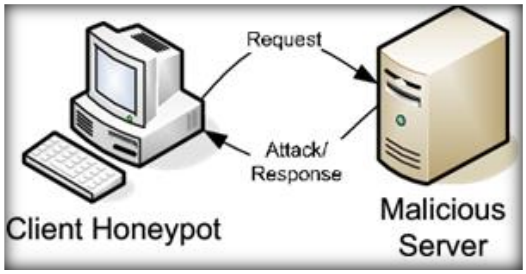


Figura 2.2 Honeypot cliente – Fuente https://www.researchgate.net

2.2.3 Honeytokens

Son técnicas a más bajo nivel que los honeypots. Consisten en marcar ciertos archivos, bases de datos, mails o cualquier otro tipo de recurso de forma que cualquier acceso se considere siempre un ataque, y haciendo que envíen una alerta al administrador en caso de que alguien acceda al mismo (3).

2.2.4 Honeypages

Son páginas dentro de un sitio web que no son referenciadas en ningún lugar de la web y por tanto son inaccesibles a cualquier usuario legítimo. Por ello, la única forma de acceso es mediante escaneos y crawlers. De ese modo cada vez que se intenta acceder a una de estas páginas se informa al administrador del sitio web (4).

2.2.5 Honeynets

Son conjuntos de honeypots desplegados en una misma red. Su primera aparición fue en 1999, por Lance Spitzner, el fundador de "The Honeynet Project" (5). Para este proyecto TFG se han escogido dos honeynets t-Pot formadas por once honeypots cada una.

2.2.6 Honeyfarms

Se despliegan varios honeypots en un punto concreto y se redirige el tráfico de los atacantes de otras redes a esa "granja de honeypots" (Figura 2.3).
El inconveniente de este sistema es que se genera un único punto de ruptura, que, si el atacante detecta, no volverá a caer si es redirigido desde otras redes (6).

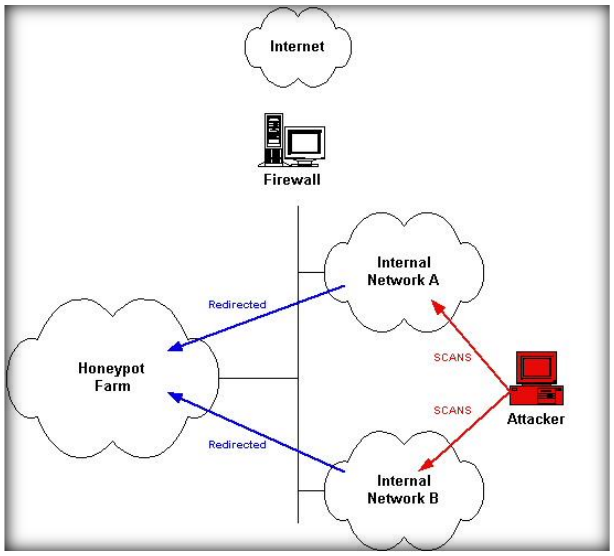


Figura 2.3 Ejemplo de una honeyfarm – Fuente https://www.symantec.com

2.3 *Honeypots escogidos para el proyecto*

A continuación, se describen los distintos tipos de honeypots que se han estudiado y posteriormente instalado en dos servidores de la Universidad Autónoma de Madrid. Estos están recogidos en una honeynet llamada t-Pot (7), que reúne once honeypots en una sola dirección IP, utilizando la arquitectura que se muestra en la Figura 2.4.

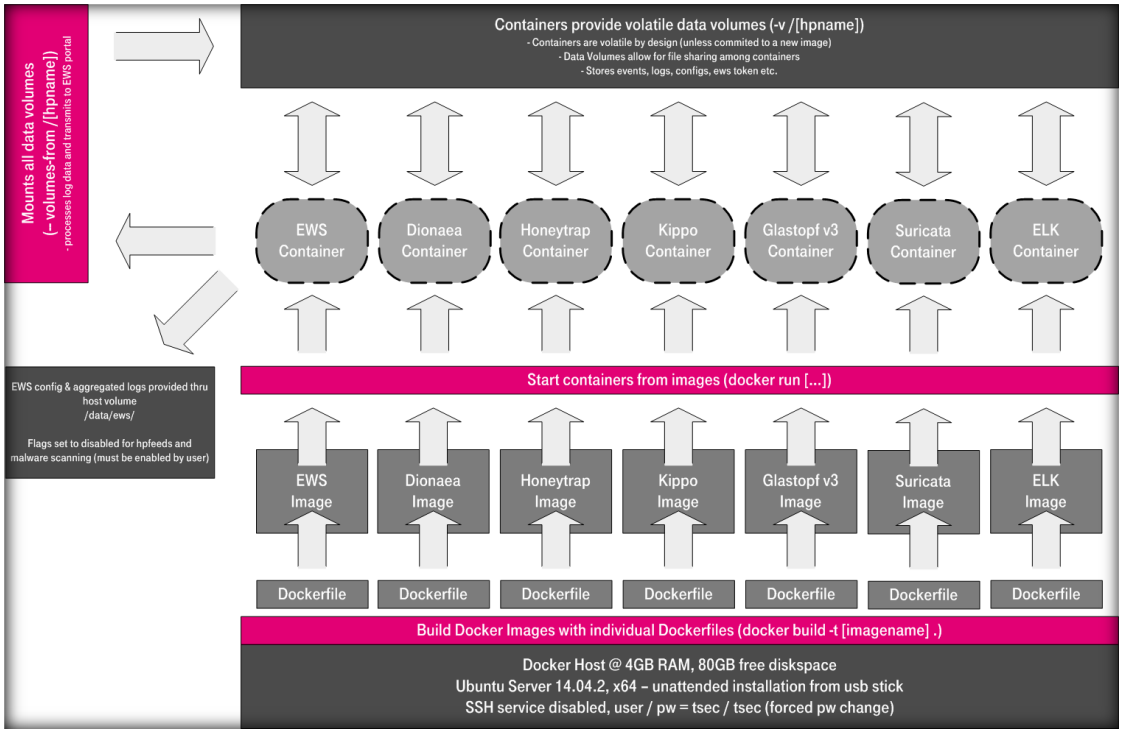


Figura 2.4 Arquitectura de la honeynet t-Pot – Fuente: http://dtag-dev-sec.github.io

2.3.1 ConPot

Nombre:	ConPot	Puertos utilizados:	81
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.1 Características honeypot ConPot

ConPot es un honeypot de Honeynet Project ideado para simular Sistemas de Control Industrial. Es un servidor interactivo diseñado para ser fácilmente lanzable y modificable (Tabla 2.1). Permite construir un entorno prácticamente idéntico al de un complejo sistema industrial, proporcionando una gran cantidad de protocolos, como los protocolos específicos de ICS (Modbus, por ejemplo).
También permite crear una interfaz de usuario personalizable, así como modificar el tiempo de respuesta de los servicios (8).

2.3.2 Cowrie

Nombre:	Cowrie	Puertos utilizados:	22, 23
Interacción:	Media	Configuración:	Media

Tabla 2.2 Características honeypot Cowrie

El honeypot Cowrie fue desarrollado por Michel Oosterhof (9). Es una versión de otro honeypot, el Kippo, que realiza una simulación de un servidor de SSH (Tabla 2.2) con un sistema de gestión de archivos falso, emulando a un Debian 5.0, de forma que el atacante que consiga entrar en este honeypot puede crear, modificar y eliminar archivos (soporta SFTP y SCP), además de reproducir las sesiones registradas en tiempo real.
Es un honeypot muy útil puesto que permite guardar los archivos que el atacante se descarga, para analizarlos posteriormente.
También permite espiar las acciones posteriores del atacante, ya que simula la finalización de la sesión SSH, pero en realidad sigue conectado, monitorizando.
Otras funcionalidades interesantes de este honeypot son:

- Permite ejecutar comandos por SSH, y hacer login mediante TCP con un Proxy SSH.
- Acepta conexiones SMTP para dirigirlas a un honeypot de SMTP.
- Permite guardar registros en formato JSON de todas las entradas e intentos de ataque.

2.3.3 Dionaea

Nombre:	Dionaea	Puertos utilizados:	21, 42, 60, 80, 135, 443, 445, 1433, 1723, 3306, 5060, 5061, 8081
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.3 Características honeypot Dionaea

El honeypot Dionaea es la versión que surgió a partir del Nepenthes, un honeypot de baja interacción (Tabla 2.3). Simula un procesador x86 con detección de shellcode (10). Guarda todos los archivos que el atacante genere. Soporta los siguientes protocolos:

- SMB: protocolo de red para compartir archivos entre nodos en Windows. Tiene muchas vulnerabilidades fácilmente explotables.
- HTTP: Protocolo de comunicación para transferencia de información en WWW. También soporta HTTPS.

- FTP: Protocolo de red para transferencia de archivos entre sistemas conectados por TCP. En este protocolo Dionaea permite crear directorios, y subir y bajar archivos.
- MSSQL: Protocolo utilizado en los servidores SQL de Microsoft. Dionaea permite iniciar sesión y decodificar las queries que se realizan.
- VoIP: Dionaea en realidad no se conecta a un servidor VoIP, sino que registra los mensajes SIP que recibe.

2.3.4 ElasticPot

ElasticPot es la versión simplificada para honeypots de ElasticSearch, un motor de búsqueda de aplicaciones que funcionan en entornos de alto rendimiento (11). Tiene una gran capacidad para generar índices que facilitan cuantiosamente el acceso a los datos que guardan el resto de honeypots. Utiliza el puerto 9200.

2.3.5 Glastopf

Nombre:	Glastopf	Puertos utilizados:	80
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.4 Características honeypot Glastopf

El honeypot Glastopf ofrece una emulación de un servidor web minimalista (12). Está escrito en Python. Sus herramientas recolectan información sobre ataques basados en aplicaciones web como los conocidos "SQL Injection", "Remote File Inclusion" y "Local File Inclusion". Glastopf trata de responder al atacante con una respuesta que parezca realista, para que se produzca el ataque. Es fácil de configurar y de mantener (Tabla 2.4), es capaz de guardar registros en MySQL o en SQLite, permite inyecciones SQL, y contiene una gran cantidad de vulnerabilidades conocidas que muchos servicios web poseen.

2.3.6 Honeytrap

Nombre:	Honeytrap	Puertos utilizados:	25, 110, 139, 3389, 4444, 4899, 5900, 21000…
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.5 Características honeypot Honeytrap

El honeypot Honeytrap fue desarrollado por Tillmann Werner. Se caracteriza porque no ofrece un servicio vulnerable en concreto, sino que permite emular cualquier tipo de servicio (Tabla 2.5). Esto lo consigue continuando con la negociación TCP en cualquier puerto y registrando la petición que realice el atacante para conectarse. De esta forma quedan guardados ataques desconocidos. En algunos servicios en concreto ofrece respuestas prefijadas para mayor realismo (POP3, FTP, HTTP…).

2.3.7 Mailoney

Nombre:	Mailoney	Puertos utilizados:	25, 2525
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.6 Características honeypot Mailoney

Mailoney es un honeypot que implementa un servidor SMTP (Tabla 2.6) y está escrito en Python. Es Open Relay, esto es, permite que cualquier usuario de internet lo use para enviar

correo electrónico a través de él. Permite que se realice el ataque “Credential Harvester Attack Method” (13).

2.3.8 Rdpy

Nombre:	Rdpy	Puertos utilizados:	3389
Interacción:	Baja	Configuración:	Media

Tabla 2.7 Características honeypot Rdpy

Rdpy es un honeypot que usa el Recorded Sesion Scenario para reproducir el escenario a través del protocolo Remote Desktop Protocol de Microsoft (Tabla 2.7). Está escrito en Python (14).

2.3.9 Suricata

Suricata no es un honeypot, sino que es un detector de intrusiones de código abierto. Tiene una arquitectura multi-hilos y fue desarrollado por la comunidad de OISF (15). Gracias a esto es una herramienta escalable que es capaz de identificar los principales protocolos de red y controlar los archivos que viajan por la red.

2.3.10 Vnclowpot

Nombre:	Vnclowpot	Puertos utilizados:	5900
Interacción:	Baja	Configuración:	Sencilla

Tabla 2.8 Características honeypot Vnclowpot

Vnclowpot es un honeypot VNC de baja interacción (Tabla 2.8). Escucha en un puerto y registra las respuestas a un VNC Auth estático (16).

2.3.11 eMobility

Nombre:	eMobility	Puertos utilizados:	80, 8080
Interacción:	Media	Configuración:	Compleja

Tabla 2.9 Características honeypot eMobility

El honeypot eMobility se creó con el fin de recopilar información sobre los motivos y métodos de los atacantes cuyo objetivo es la infraestructura de transporte de nueva generación. Consiste en un sistema central de carga con varios puertos de carga, y transacciones simuladas (Tabla 2.9). Una vez que el atacante obtiene acceso a la interfaz web del sistema central, podrá reconfigurar, controlar y manipular las transacciones de carga en curso e interactuar con otros puntos de carga (17).

2.4 *Herramientas de detección de honeypots*

En esta sección se describen las distintas herramientas que pueden utilizarse para detectar honeypots.

2.4.1 Shodan Honeyscore

Hasta ahora han salido muy pocas herramientas al mercado que permitan la detección de honeypots. La más notoria es sin duda la creada por el equipo de Shodan, un referente en el mundo de la ciberseguridad.
Esta herramienta recibe el nombre de "Honeyscore" y con ella se puede introducir una dirección IP y comprobar si se trata de un honeypot o no (18). Se basa en comprobar ciertas características comunes de los honeypots y tratar de analizar si es un honeypot o no. Cabe destacar que esta herramienta está en desarrollo y aún dista mucho de mostrar unos buenos resultados. Por ejemplo, al pasar esta herramienta en los honeypots que se han colocado en la Universidad Autónoma de Madrid antes de ocultarlos, el resultado ha sido incorrecto: Shodan informa de que las dos IPs parecen sistemas reales (Figura 2.5).
En las posteriores imágenes se ha censurado cualquier tipo de información que pueda vulnerar la privacidad de las máquinas utilizadas.

Figura 2.5 Prueba de Shodan Honeyscore contra las honeynets de la UAM – Fuente: https://honeyscore.shodan.io

El problema principal de esta herramienta, y en parte el motivo por el que he decidido desarrollar una propia, es que Shodan Honeyscore solo realiza comprobaciones de footprinting. En el caso de honeypots como Cowrie, que permite conexión mediante SSH, se necesita usuario y contraseña para acceder a un honeypot. Es por esto por lo que Shodan Honeyscore solo puede utilizarse en honeypots de baja interacción, mientras que mi herramienta está pensada para poder detectar tanto los de baja como los de alta interacción.

Dado que el enfoque principal de la herramienta es que la utilicen administradores para comprobar la capacidad que tienen sus honeypots de hacerse pasar por sistemas reales, sin entrar dentro del honeypot en muchos casos no se podrá comprobar esto.
Por ello, como se mostrará en el apartado de desarrollo de este proyecto, se ha decidido que la herramienta reciba un usuario y contraseña para poder realizar pruebas dentro de la máquina, haciéndonos pasar por un atacante que ha conseguido robar unas credenciales y está investigando tras el acceso si se trata de un sistema trampa.

2.4.2 NMAP

Nmap (Network Mapper) es una potente herramienta de código abierto que se utiliza para rastrear puertos, permitiendo evaluar la seguridad de los sistemas informáticos (19).
Utiliza distintos tipos de paquetes de red aleatorios para escanear y detectar los distintos puertos que una máquina tiene, identificando cuales están abiertos y los servicios que corren tras los mismos. Tiene múltiples formas de ser ejecutado, permitiendo realizar tanto escaneos silenciosos y prácticamente indetectables como escaneos rápidos y agresivos que pueden llegar incluso a colapsar la red donde se encuentra la máquina.

Durante este proyecto se emplea esta herramienta con las direcciones IP que la Universidad Autónoma de Madrid ha proporcionado. Cabe destacar que el uso de Nmap está terminantemente prohibido contra direcciones IP que no pertenezcan a la persona que ejecuta la herramienta, excepto si se tiene permiso explícito del dueño de dichas direcciones.
En la Figura 2.6 se muestra la ejecución de Nmap sobre una IP con varios puertos abiertos.

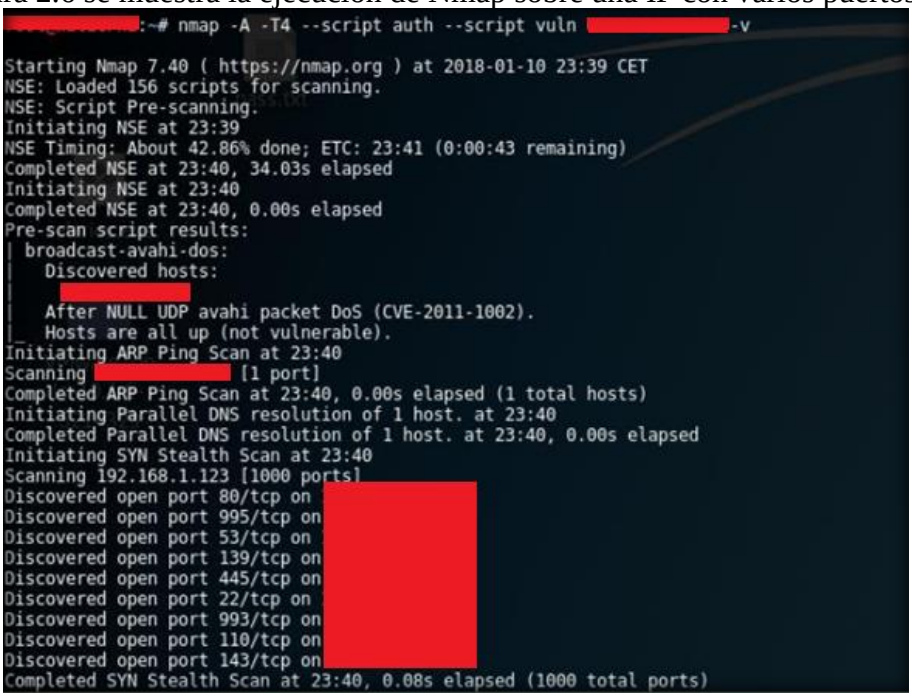


Figura 2.6 Ejemplo de escaneo profundo con nmap – Fuente propia.

2.4.3 FOCA

FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta desarrollada por el equipo de ElevenPaths empleada para obtener metadatos de múltiples documentos (20). La Figura 2.7 muestra el logo de la herramienta.

Figura 2.7 Herramienta de obtención de metadatos FOCA – Fuente:www.elevenpaths.com

Esta herramienta permite analizar honeytokens en documentos. Además, gracias a poseer una funcionalidad con la que puede descargar páginas web y examinarlas, también permite detectar honeypages.

3 Análisis y Diseño

En este punto se explica en detalle el ámbito del sistema, esto es, la introducción al problema que debe ser resuelto mediante el sistema, y la solución que se ha dado al mismo. Además, se muestran los principales requisitos de la aplicación, y las distintas etapas que se han seguido a lo largo de este proyecto TFG.

3.1 *Ámbito del sistema*

3.1.1 Definición del Problema

En la actualidad existen numerosas versiones de honeypots que ofrecen simular distintos servicios. Sin embargo, una gran cantidad de los honeypots que se utilizan hoy en día son configurados por defecto, con lo que es relativamente sencillo identificarlos. Por este motivo un atacante que llegue a un honeypot y detecte rápidamente que se trata de un sistema trampa saldrá inmediatamente de él, pues entenderá que no puede obtener ningún dato útil. El problema reside en que esto provoca que no se alcance el principal objetivo de la existencia de un honeypot: capturar e identificar nuevas formas de ataque.

3.1.2 Planteamiento de la solución

Para solucionar los problemas planteados, se propone la siguiente herramienta a fin de detectar honeypots pobremente configurados. El sistema propuesto se denomina HoneyCatch y está formado por estos componentes:

- Un sistema de detección basado en mapeo de puertos y comparación de estos con los puertos abiertos por defecto en los once sistemas honeypot con los que se ha trabajado.
- Un módulo encargado de las pruebas superficiales que incluirá el punto anterior, así como búsqueda de páginas de administración visibles y otras búsquedas de footprinting.
- Un módulo de detección "inside" que simulará la investigación que realiza un atacante una vez que ha vulnerado el sistema trampa. Este módulo permitirá incluir la funcionalidad de descubrir si la configuración interna del honeypot es correcta.

3.2 *Alcance*

El alcance del sistema es claro, los usuarios a los que va dirigido son los administradores de sistemas de redes que contengan honeypots. Dado que para utilizar la aplicación es necesario proporcionar un usuario y contraseña con los que poder trabajar en el interior de honeypot, personas ajenas no podrán utilizar la herramienta para comprobar si redes que no les pertenecen contienen honeypots. De esa forma nos aseguramos de que no se podrá utilizar con fines delictivos.

En cuanto a la detección de honeypots, la herramienta se centrará en identificar los 11 tipos de honeypots que se han colocado en las dos honeynets de la Universidad Autónoma de Madrid. La descripción de estos está disponible en el apartado "Honeypots escogidos para el proyecto", en el estado del arte de este documento.

3.3 *Requisitos*

A continuación, se describen los requisitos funcionales y no funcionales que se han extraído a partir del análisis del problema, en base a toda la información obtenida.

3.3.1 Requisitos funcionales principales

[R01] Dirección IP

- El usuario indicará la dirección IP que el programa comprobará. Esto se indicará en un momento determinado de la ejecución de este.
- El formato de entrada estará formado por cuatro números enteros entre 0 y 255 separados por puntos [xxx.xxx.xxx.xxx]

[R02] Introducción de usuario válido

- En la segunda fase el sistema pedirá las credenciales de un usuario y contraseña válidos para la dirección IP introducida.
- El sistema aceptará cadenas vacías en caso de que el honeypot auditado no requiera credenciales para entrar.

[R03] Herramientas de terceros

- El sistema utilizará lenguajes de programación y herramientas que deberán estar instaladas en el ordenador donde se ejecute. En caso de no estar las mismas instaladas, la herramienta lo notificará antes de continuar.
- Algunas herramientas (como Nmap) podrán ser sustituidas por métodos manuales que emplee el sistema para hacerse con la información necesaria, pero otras (como Python o algunos módulos de este) se considerarán imprescindibles y la herramienta no se ejecutará si no están instalados.

[R04] Puntuación

- La herramienta calificará la dirección con una puntuación de 0 a 100.
- Esta calificación se estimará según los resultados de las distintas pruebas realizadas.

[R05] Base de entrenamiento

- El sistema se probará y desarrollará utilizando para las pruebas las dos honeynets de la Universidad Autónoma de Madrid. Las pruebas se crearán en función de las configuraciones por defecto que se observen en los mismos.
- También se probará en máquinas que no contengan honeypots para comprobar la diferencia en la salida.

[R06] Modularización

- El diseño del sistema se realizará de forma que esté completamente modularizada.
- De esta forma la modularización facilitará la adición de nuevas pruebas de detección de honeypots no incluidas en la base de entrenamiento inicial.

3.3.2 Restricciones de Diseño

[R07] Interfaz

- El sistema no contará con interfaz gráfica.
- Mostrará toda la información de cada módulo ejecutado por terminal.

[R08] Salida

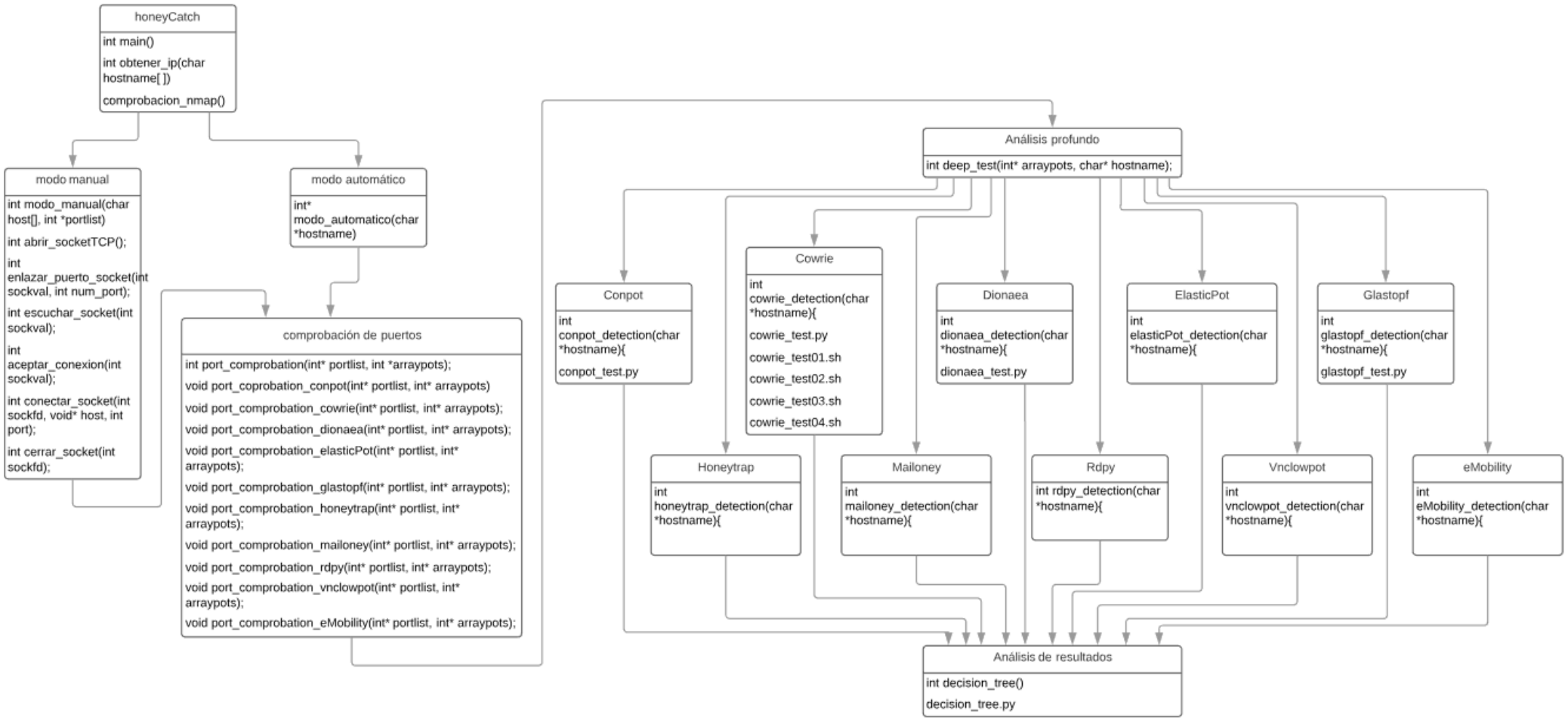
- Al finalizar la ejecución, se creará un documento en el que se indique la puntuación, así como información sobre las pruebas realizadas.

[R09] Sistema Operativo

- La herramienta soportará ser ejecutada en cualquier distribución Linux.

3.4 Diagrama completo de la herramienta de detección

A continuación se muestra el diagrama general de la herramienta implementada “honeyScore”.



3.5 *Etapas del proyecto*

Para la detección y ocultación de los honeypots se han realizado las siguientes etapas:

3.5.1 Estudio de los honeypots actuales para su detección:

Se ha realizado un análisis de los honeypots disponibles y sus características para comprobar cuáles eran más afines al estudio de las técnicas de ocultación y cuáles podrían instalarse en las máquinas virtuales para recibir ataques. Se analizó cada honeypot y se buscaron aquellos que pudieran ser compatibles entre sí.

Para la creación de las dos honeynets locales se usaron los siguientes recursos:

- Máquinas virtuales gestionadas por VirtualBox.
- Dos distribuciones Linux basadas en Debian.
- Dos direcciones IP estáticas cedidas por la Universidad Autónoma de Madrid, una bajo la protección del firewall y otra fuera de este.

3.5.2 Instalación de la infraestructura

Para comprobar más a fondo el funcionamiento de los honeypots y encontrar los rasgos que los caracterizaban como tales, se decidió instalar en la Universidad Autónoma de Madrid dos honeynets pertenecientes al proyecto T-Pot con un total de once honeypots cada una.

Así mismo se realizó un estudio de la infraestructura de la UAM, así como un análisis del firewall para poder obtener el máximo número de ataques posibles.
De ese modo, se decidió colocar una red de honeypots (honeynet) delante del firewall de la UAM y otra detrás, ambas configuradas para ser idénticas. Los detalles de configuración de estas se pueden consultar en el anexo A.

3.5.3 Recogida de datos:

Tras la instalación de las máquinas, se procedió a un periodo de recogida de datos en el que se dejó que las máquinas recibieran ataques constantemente. Se puede consultar el análisis de todos los datos recogidos por las dos honeynets antes y después de la ocultación de honeypots en el anexo E.

Además, al haber colocado una honeynet delante del firewall y otra detrás, se pudo analizar el firewall de la UAM poniendo los honeypots en espejo (las mismas honeynets con la misma configuración a ambos lados del firewall).
De esta forma se pudo comprobar la efectividad del firewall y la relación directa entre la ubicación y el tipo de ataques que recibe un honeypot. La comparación entre ambos se puede encontrar en la sección 5.3 “Recogida de datos” de este documento.

3.5.4 Desarrollo de herramienta de detección:

Tras analizar qué parámetros distinguen a un honeypot de una máquina real en cada tipo de honeypot, se pasó al desarrollo de una herramienta que permitiera detectar si una determinada dirección IP contenía o no un sistema trampa. Para ello se crearon varias métricas y se desarrolló un conjunto de software en el lenguaje de programación C y en Python para rastrear y analizar los puertos y servicios de una dirección IP.

Aunque una gran parte del desarrollo fue manual, se utilizaron potentes herramientas de pentesting para obtener aún más información de la dirección a auditar. La herramienta utiliza los programas Nmap y wdiff, y también necesita tener instalados algunos módulos de Python

como Mechanize o Urllib2. Se planteó utilizar la herramienta de Shodan (descrita en el Estado del Arte de este documento), pero se descartó la idea al comprobar que aún está en una fase inicial en la que tiene una baja tasa de éxito. No obstante, si en el futuro se actualizase y mejorase su funcionamiento, se podría incluir como módulo externo a la herramienta. En el anexo 0 se puede encontrar más información sobre cómo se ha implementado la herramienta.

La herramienta evalúa una dirección IP y realiza varios tests al objetivo. Según el resultado de esos múltiples tests ponderados, otorga una calificación al objetivo de 0 a 100 que se estima como el porcentaje de probabilidad de que cierta dirección IP aloje un honeypot, y de salir positivo informa del tipo de honeypot que tiene posibilidades de estar ejecutándose, para poder realizar posteriormente un análisis detallado del mismo y centrarse en sus características. La información sobre cómo la herramienta decide esta puntuación está disponible en el anexo 0. Una vez desarrollada, se probó en las honeynets de la Universidad Autónoma de Madrid.

3.5.5 Ocultación y aumento de la seguridad de las honeynets:

Tras finalizar el desarrollo de la herramienta, se cambiaron los parámetros de cada uno de los honeypots para ocultarlos y que pasasen por sistemas reales tanto para la herramienta desarrollada como para los verdaderos atacantes.
Algunas medidas que se tomaron fueron renombrar directorios, habilitar comandos específicos o desactivar puertos. En el anexo D se analizan todas las medidas de ocultación y detección de honeypots.
Una vez modificados, se volvió a probar la herramienta para verificar los resultados.

3.5.6 Recogida de datos después de la ocultación:

Para dar por finalizado el proyecto se volvió a realizar una segunda recogida de datos durante un intervalo de tiempo similar al primero para comprobar cómo había afectado la ocultación de los honeypots en la cantidad y el tipo de ataques recibidos.

4 Desarrollo e integración

4.1 Herramienta de detección de honeypots

A continuación, se describe el proceso que lleva a cabo mi herramienta "HoneyCatch" de detección de honeypots para tratar de discernir si una IP determinada hay ubicado un honeypot o no. HoneyCatch se ha programado en lenguaje de programación C, pero incluye módulos en Python (debido a la facilidad de programación para ciertas comprobaciones o a los scripts de detección que están escritos en este lenguaje) así como scripts en Bash.

4.1.1 Descripción General

En esta sección, una vez conocido el ámbito del sistema, se describen detalladamente las funcionalidades que incorpora la herramienta, así como los componentes que lo forman.
El pseudocódigo de la herramienta con muestras de las principales funciones de esta, así como el diagrama de clases y el análisis de flujo, puede encontrarse en el anexo 0.

Fase 0: Fijar objetivo
La primera acción de la herramienta es pedirle al usuario que introduzca una dirección IP sobre la que centrará todo el escaneo. Además, incluye una pequeña cabecera en ASCII con el nombre de la herramienta, como se puede ver en la Figura 2.1.

Figura 4.1 Inicio de HoneyCatch.

Fase 1: Escaneo de puertos
El primer paso para analizar una IP es comprobar qué puertos y servicios tiene abiertos.

- ***Comprobación de herramientas instaladas:***

La herramienta por excelencia para realizar esto es Nmap. Por este motivo, el programa comprueba en primer lugar si esta herramienta está instalada en el ordenador. Puede encontrarse más información sobre esta herramienta en el Estado del Arte de este documento. Además, se analizan otras herramientas que deben estar instaladas en el ordenador, como wdiff o algunos módulos de Python.

- ***Ejecución de escaneo de puertos:***

Si Nmap está instalado, se ejecuta sobre la IP introducida en la fase 0. La salida de esta herramienta se almacena en un fichero que posteriormente se lee y analiza para comprobar los distintos tipos de puertos que están abiertos. La Figura 4.2 muestra un ejemplo en el que nmap está instalado.

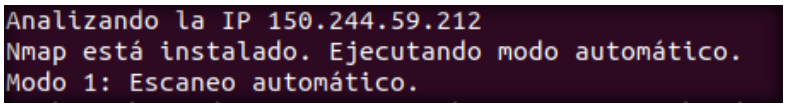


Figura 4.2 Comprobación de herramientas.

Si Nmap no está instalado, se ejecuta una función propia de escaneo de puertos que muestra los mismos resultados. Es recomendable tener Nmap instalado dado que esta obtención manual de los puertos es más lenta.

Fase 2: Análisis de puertos

A raíz de los resultados obtenidos, se analiza cada puerto y servicio abierto y se hace una comparación entre los puertos abiertos por la máquina objetivo y los puertos que los distintos honeypots tienen abiertos por defecto.

En la Figura 4.3 se muestra la ejecución de esta parte de la herramienta.

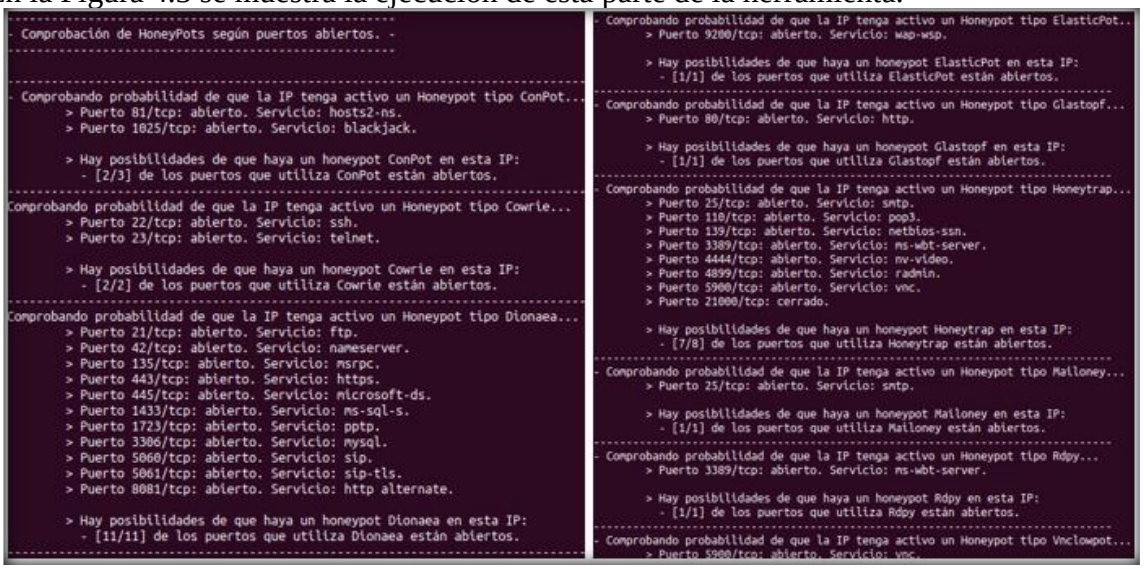


Figura 4.3 Comprobación de puertos abiertos.

De esta forma se descarta que exista un honeypot que simula un servicio http si el puerto 80 no está abierto, o uno que emule un servicio SSH si el puerto 22 está cerrado, por ejemplo.

Fase 3: Análisis profundo

Con los posibles honeypots detectados en la fase anterior, se hace un análisis profundo en cada uno de ellos, comprobando los distintos detalles que por culpa de una mala configuración pueden llevar a un atacante a averiguar que se encuentra bajo un honeypot.

- ***Introducción de credenciales:***

En primer lugar, la herramienta pide introducir un usuario y contraseña para poder realizar las comprobaciones que realizaría un atacante que ha vulnerado el sistema. En la Figura 4.4 se puede ver un ejemplo en el que el usuario es “root” y la contraseña “password”.

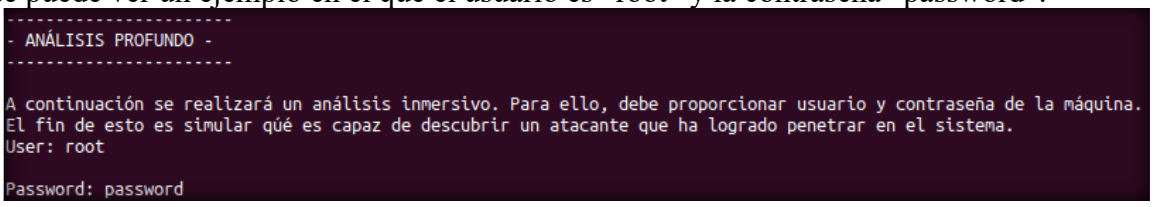


Figura 4.4 Introducción de credenciales.

- ***Comprobaciones ConPot:***

Este honeypot se caracteriza por el número de serie que posee el módulo, 88111222, y el tipo de módulo, IM151-8 PN/DP CPU. Si aparecen dichos valores, se trata de un honeypot ConPot. La Figura 4.5 muestra la comprobación contra una de las honeynets antes de ocultarla. Para comprobarlo se ha utilizado un script de Nmap que debe ser descargado para poder utilizarse (21) así como un script en Python que permite su detección (22).

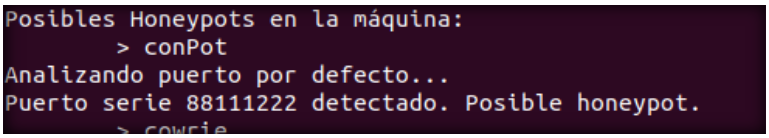


Figura 4.5 Comprobación ConPot positiva.

- ***Comprobaciones Cowrie:***

Cowrie simula el servicio SSH. Se han implementado cuatro métodos de detección, tal y como se puede ver en la Figura 4.6:

- **Comprobación de usuarios:** se consultan los usuarios del host. Cowrie está configurado por defecto con un usuario llamado "richard". Por tanto, si se encuentra el nombre de usuario "richard" se considera probable que pueda tratarse de un honeypot.
- **Comprobación de creación de directorios:** se comprueba si se puede crear un directorio. Para ello, introducimos el usuario y contraseña proporcionados por el administrador. Si creamos un directorio, nos desconectamos, nos volvemos a conectar y no aparece, entonces se trata de un honeypot.
- **Comprobación de comandos**: se prueban ciertos comandos que normalmente están instalados en entornos reales. Si estos comandos no se encuentran instalados, es probable que se trate de un honeypot.
- **Comprobación de directorios**: se comprueba que la estructura de los directorios sea la habitual de un sistema real. En caso de que haya diferencias grandes con un entorno real, así como en el caso de que directorios que normalmente contienen información se encuentran vacíos, puede tratarse de un honeypot.

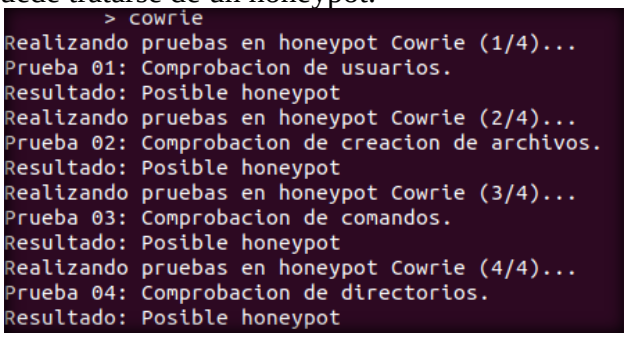


Figura 4.6 Comprobaciones Cowrie.

- ***Comprobaciones Dionaea:***

Este honeypot es fácilmente detectable utilizando Nmap si no se configura adecuadamente. En la herramienta se han utilizado tres scripts de Nmap (23), tal y como se muestra en la salida (Figura 4.7):

- **Dionaea-detect-mysql:** detecta si el servicio mysql está por defecto en dionaea.
- **Dionaea-detect-smb:** detecta si el servicio smb está por defecto en dionaea.
- **Dionaea-detect-ssl:** comprueba que la configuración SSL del servicio es la misma que la que tiene por defecto dionaea.

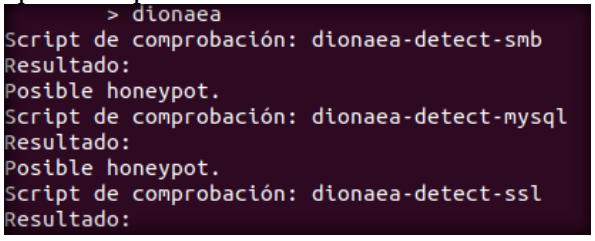


Figura 4.7 Comprobaciones de Dionaea.

- ***Comprobaciones ElasticPot:***

Este "honeypot" en realidad se emplea para almacenar toda la información del resto de honeypots, y manejarla cómodamente gracias a ElasticSearch. Es por eso por lo que la única forma de detectar su presencia, aparte de comprobar que el puerto 9200 está abierto, es consiguiendo acceso a la página de administración de honeypots.

- ***Comprobaciones Glastopf:***

Glastopf simula el servicio http. La peculiaridad de este honeypot es que cada vez que se reinicia la página aparece un HTML distinto, cogido al azar de una base de datos. Para ver si se trata de un honeypot se han hecho dos comprobaciones:

- Obtener el HTML de la página y comprobar que no se encuentre en la base de datos.
- Realizar varias peticiones del HTML de la página con pequeños intervalos de tiempo, y comprobar utilizando la herramienta wdiff las diferencias entre las mismas. Se ha puesto especial cuidado en que el algoritmo no considere como páginas distintas aquellas páginas dinámicas que al recargarlas muestran pequeñas variaciones en el código. Los porcentajes que salen en la salida (Figura 4.8) muestran el porcentaje de similitud en el html. De esta forma se estima que si la página cambia constantemente se trata de este honeypot.

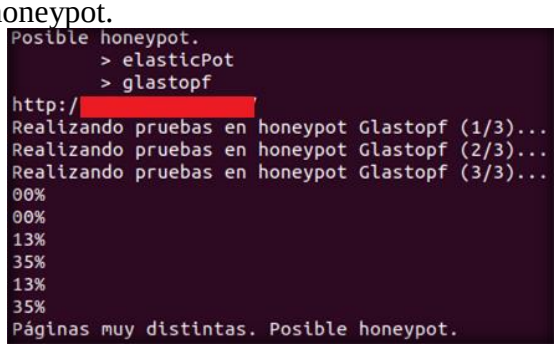


Figura 4.8 Comprobaciones Glastopf.

- ***Comprobaciones Honeytrap, Mailoney, Rdpy, Vnclowpot y eMobility:***

Dada la naturaleza maleable de estos honeypot, que no se basa en simular un solo servicio, sino que permite simular múltiples servicios distintos y ofrece respuestas distintas y personalizadas para cada uno de ellos, no ha sido posible encontrar una forma de detección a priori en estos honeypots. Sin embargo, dado que en la mayoría de las ocasiones estos honeypots de baja interacción no se colocan solos, sino que se colocan en honeynets como las creadas en la red de la Universidad Autónoma de Madrid, en caso de que haya puertos abiertos relacionados con estos honeypots hay que centralizar el esfuerzo en comprobar si existen otros honeypots en la IP introducida que puedan ser más fácilmente detectables.

Fase 4: Resultados

Por último, la herramienta analiza los resultados de cada una de las comprobaciones, cuyas salidas se han ido guardando en un fichero, y se asigna una nota del 0 al 100 de las posibilidades de que exista un honeypot en esa dirección IP (Figura 4.9). Se puede consultar más detalladamente el criterio con el que se han asignado estos porcentajes en el anexo 0. En la sección "Pruebas y resultados" de este documento se analizan los resultados obtenidos con esta herramienta.

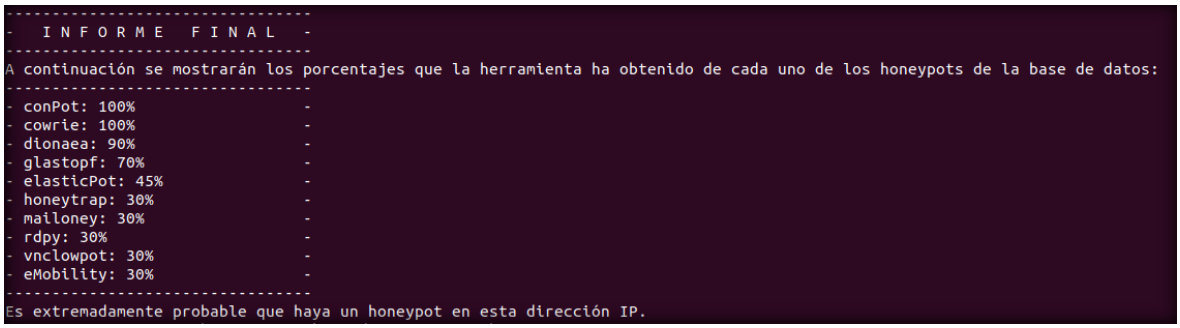


Figura 4.9 Resultado final de honeyCatch sobre la red honeynet A.

4.2 Ocultación de los honeypots

Los honeypots son un mecanismo de defensa "activo pasivo" por naturaleza, lo que es desfavorable para las confrontaciones de la red. Como resultado, cada día más y más atacantes utilizan tecnologías anti-honeypot para identificar, marcar, monitorizar y contra atacar honeypots.

Se ha realizado un análisis de las técnicas de ocultación de honeypots utilizadas hasta la fecha. A partir de los resultados obtenidos en dicho análisis, y con la experiencia obtenida al realizar la herramienta de detección, se describen a continuación las formas de ocultación de los honeypots. Se pueden consultar el análisis de las formas de detectar un honeypot en el anexo D.

Varias de las siguientes técnicas se han aplicado en las honeynets colocadas en la Universidad Autónoma de Madrid.

a) **Procesos ocultos**. Los procesos que corre el honeypot deben ser ocultos. Una forma de hacer esto es modificar el código de la lista de procesos para ignorarla explícitamente. (24)

b) **Registros ocultos.** Se deben ocultar los logs del honeypot para que el atacante no los borre. Esto puede hacerse modificando la lista de directorios y de archivos para que el sistema evite reportar esos en concreto (25).

c) **Información de registros oculta al atacante.** Se deben ocultar la salida de comandos que produce el tener registros más detallados en un honeypot. Se puede modificar el comando write del sistema para enviar los datos a otro lugar y se puede utilizar ofuscación de código para que el atacante no encuentre esto, o que el Sistema Operativo lo oculte si el usuario trata de listarlo (26). En t-Pot se guardan los datos en la máquina que hospeda la honeynet. En la Figura 4.10 se puede ver un volcado de los logs del honeypot Cowrie.

Figura 4.10 Volcado de logs de honeypot Cowrie.

d) **Información cifrada.** Los datos recogidos por el honeypot deben ser cifrados rápido. Los datos sin cifrar pueden alertar al hacker de que está siendo monitorizado. Aunque aun así, el atacante puede descubrir que los datos cifrados son su monitorización al ver que están constantemente aumentando de tamaño (27).
e) **Redes separadas.** En el caso de las honeynets, se deben poner los datos recopilados en una subred desconectada de la red principal. Esto requiere una segunda tarjeta de red para cada máquina que se conecte a la subred donde se están recopilando los datos. Es una gran inversión de hardware y tiempo, pero permite blindar el sistema y hacerlo aún más seguro.
f) **Honeywall y rastreo**. Se puede implementar una honeywall, esto es, un ordenador configurado para filtrar y observar el tráfico que generan uno o más honeypots, protegiendo al resto de la subred de los ataques de estos. Es una parte esencial de una honeynet y cuenta con varios mecanismos para controlar las acciones de los bots capturados. También se debe utilizar honeypots activos que rastreen de donde vienen los atacantes (28).
g) **Sistema operativo oculto**. Es posible encubrir la versión del sistema operativo que está ejecutando la máquina defensora. Se puede hacer que un Windows se haga pasar por un Linux manipulando los paquetes y las respuestas que da.
h) **IP dinámica.** También es una buena forma de ocultación cambiar de IP de forma asidua, así ataques diarios de footprinting fallarán. Y si alguien descubre que se encuentra ante un honeypot, no podrá alertar a otros atacantes poniendo la IP en una lista negra. Esto puede hacerse mediante hardware que mapee la IP que se usa en el momento para que las redes locales no se desconfiguren.
i) **Esteganografía.** Otra posible ocultación de logs consiste en aplicar esteganografía, de forma que se escriba el log de las acciones que realiza el atacante en los bits de los milisegundos de la marca de tiempo de un log normal, por ejemplo (26).

Además de estas medidas, es importante ocultar los honeypots modificando la información por defecto. Hoy en día hay un conjunto reducido de honeypots y si se colocan sin realizar ciertas modificaciones, serán fácilmente descubiertos. A continuación se describen los cambios realizados en la configuración de t-Pot.

a) Se han añadido nuevos usuarios. En la honeynet t-Pot hay un solo usuario llamado "richard". Para la ocultación, se añaden nuevos usuarios, y se elimina dicho usuario (Figura 4.11).

Figura 4.11 Eliminación de usuarios por defecto.

b) Se han añadido comandos comunes que faltaban como sudo o adduser (Figura 4.12).

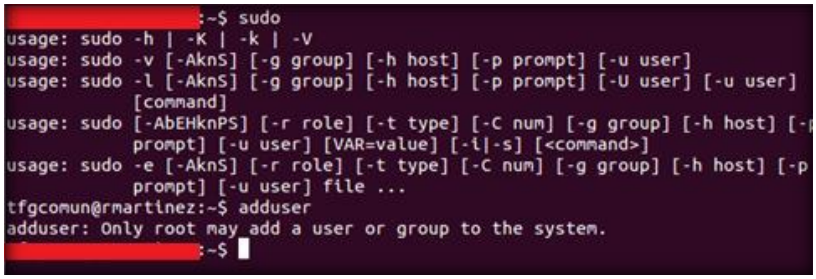


Figura 4.12 Comandos comunes instalados.

c) También se ha colocado un directorio www en var para que se asemeje a la estructura de un servidor web (Figura 4.13), así como directorios y archivos en la carpeta tmp que podría tener cualquier usuario, para que sea más creíble (Figura 4.14).

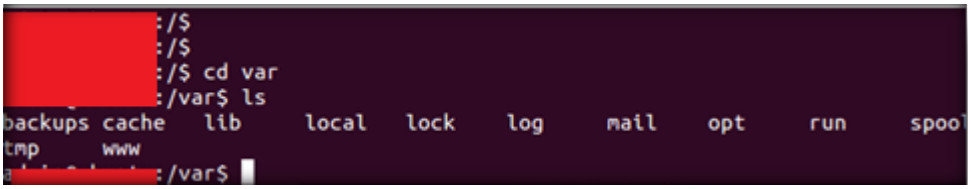


Figura 4.13 Directorio www añadido.

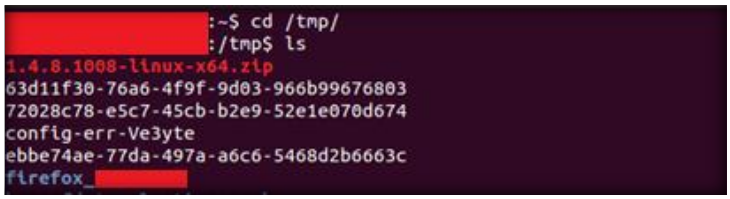


Figura 4.14 Archivos añadidos al directorio tmp.

d) Se ha modificado la página de administración de honeypots (Figura 4.15) para que los atacantes no puedan descubrirla. La página de administración de t-Pot ahora requiere una autenticación en la que la contraseña debe estar formada por mayúsculas, minúsculas y números, y debe tener una longitud mínima de 10 caracteres. De esa forma será muy difícil conseguir entrar en la página de administración y descubrir así ElasticPot.

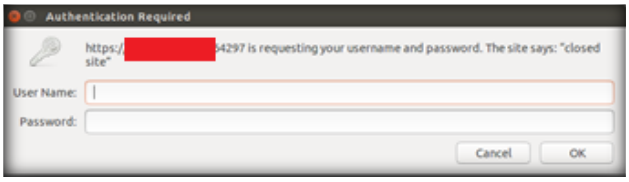


Figura 4.15 Acceso a página de administración de t-Pot.

e) Se ha cambiado el puerto serie 88111222 de Conpot alterando el archivo conpot/templates/default.xml, tal y como se puede observar en la Figura 4.16.

Figura 4.16 Izquierda: conpot/templates/default.xml original. Derecha: mismo archivo modificado.

f) Aunque enviar los logs a otro ordenador inaccesible para el atacante puede ser una buena idea, si abrimos un puerto inmediatamente después del primer acceso para enviar esta información, el atacante podría sospechar. Igualmente, si el comportamiento de los puertos del honeypot es distinto para cada paquete que le llegue (por ejemplo cerrado

para el primero, abierto para el segundo) entonces un atacante detectará enseguida que se trata de un honeypot. Por este motivo un método frecuente de los atacantes para detectar honeypots es realizar un gran número de peticiones de sincronización (29).

g) En t-Pot también se han cerrado varios puertos que no eran necesarios para la ejecución de los honeypots. De esta forma será más difícil identificar al honeypot por el puerto. Entre otros, se ha modificado el puerto 9200, que podía revelar la presencia de ElasticPot.

h) Se ha descubierto que la página web de Glastopf (Figura 4.17) cambiaba constantemente cuando se recargaba. Esto es útil para que no vaya el contenido de ese HTML a una lista negra, pero puede delatar el honeypot. Se ha modificado el intervalo de tiempo en el que se escoge un HTML aleatorio, adquiriendo un comportamiento más similar a la de las páginas webs habituales.

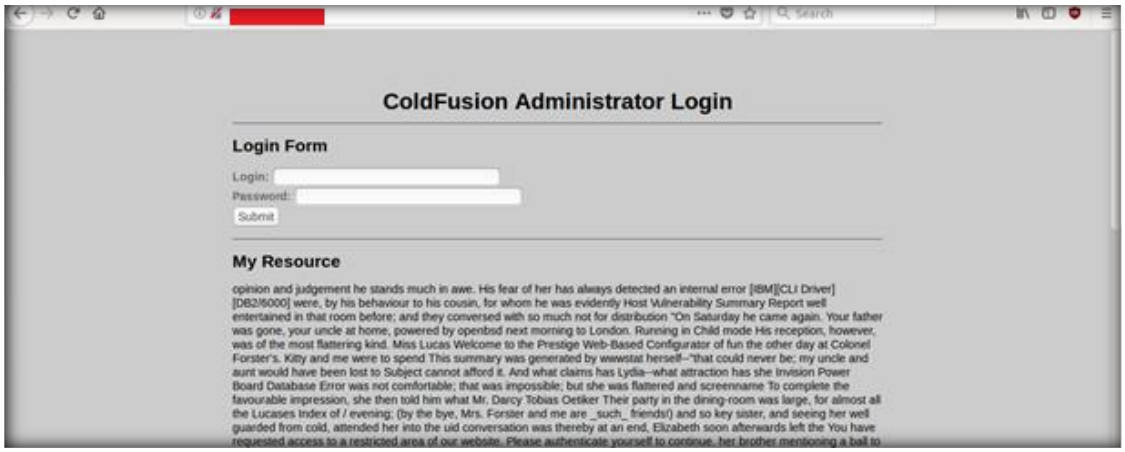


Figura 4.17 Página web Glastopf.

5 Pruebas y resultados

5.1 Herramienta de detección

Para realizar todas las funciones de manejo de errores y estructura de la herramienta, así como la entrada de parámetros, se emplea el lenguaje de programación C. Para realizar las funciones de detección de honeypots se utiliza Python. Ciertas funciones de contraste y manejo de archivos se llevan a cabo mediante scripts en Bash.
Todo está incorporado en el proyecto en C y tan solo hay que compilar y ejecutar el ejecutable de C para que la herramienta funcione. Se puede encontrar toda la información sobre la programación y arquitectura de la herramienta en el anexo 0.

Una vez terminada la herramienta, se probó tanto en los honeypots de la UAM como en un equipo particular en el que levanté un servidor web pero no coloqué ningún honeypot, para comprobar la salida ante un equipo sin honeypots. A continuación, se muestra la salida de la herramienta tanto para una de las dos IPs de las honeynets como para la IP sin honeypots:

5.1.1 IP que alberga una honeynet t-Pot:

```
# ./honeyCatch
                                                  ___          _          _                \\//
      /\  /\___  _ __    ___ _   _  / __\__ _| |_ ___| |__       (°)))>-
     / /_/ / _ \| '_ \ / _ \ | | |/ /  / _` | __/ __| '_ \     __ ``` __
    / __  / (_) | | | |  __/ |_| / /__| (_| | || (__| | | |    /     \
    \/ /_/ \___/|_| |_|\___|\__, \____/\__,_|\__\___|_| |_|   (         )
                            |___/                             ¨¨¨¨¨¨¨¨¨
Introduce la IP del posible honeypot: XXX.XXX.XXX.XXX
Analizando la IP XXX.XXX.XXX.XXX
Nmap está instalado. Ejecutando modo automático.
Modo 1: Escaneo automático.
Se han obtenido los puertos abiertos. Comprobando coincidencias de puertos abiertos con la base de datos de honeypots...
------------------------------------------------------
- Comprobación de HoneyPots según puertos abiertos. -
------------------------------------------------------
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ConPot...
    > Puerto 81/tcp: abierto. Servicio: hosts2-ns.
    > Puerto 1025/tcp: abierto. Servicio: blackjack.
    > Hay posibilidades de que haya un honeypot ConPot en esta IP:
      - [2/3] de los puertos que utiliza ConPot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Cowrie...
    > Puerto 22/tcp: abierto. Servicio: ssh.
    > Puerto 23/tcp: abierto. Servicio: telnet.
    > Hay posibilidades de que haya un honeypot Cowrie en esta IP:
      - [2/2] de los puertos que utiliza Cowrie están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Dionaea...
    > Puerto 21/tcp: abierto. Servicio: ftp.
    > Puerto 42/tcp: abierto. Servicio: nameserver.
    > Puerto 135/tcp: abierto. Servicio: msrpc.
    > Puerto 443/tcp: abierto. Servicio: https.
    > Puerto 445/tcp: abierto. Servicio: microsoft-ds.
    > Puerto 1433/tcp: abierto. Servicio: ms-sql-s.
    > Puerto 1723/tcp: abierto. Servicio: pptp.
    > Puerto 3306/tcp: abierto. Servicio: mysql.
    > Puerto 5060/tcp: abierto. Servicio: sip.
    > Puerto 5061/tcp: abierto. Servicio: sip-tls.
    > Puerto 8081/tcp: abierto. Servicio: http alternate.
    > Hay posibilidades de que haya un honeypot Dionaea en esta IP:
      - [11/11] de los puertos que utiliza Dionaea están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ElasticPot...
    > Puerto 9200/tcp: abierto. Servicio: wap-wsp.
    > Hay posibilidades de que haya un honeypot ElasticPot en esta IP:
      - [1/1] de los puertos que utiliza ElasticPot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Glastopf...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Hay posibilidades de que haya un honeypot Glastopf en esta IP:
      - [1/1] de los puertos que utiliza Glastopf están abiertos.
------------------------------------------------------------------------
```

```
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Honeytrap...
    > Puerto 25/tcp: abierto. Servicio: smtp.
    > Puerto 110/tcp: abierto. Servicio: pop3.
    > Puerto 139/tcp: abierto. Servicio: netbios-ssn.
    > Puerto 3389/tcp: abierto. Servicio: ms-wbt-server.
    > Puerto 4444/tcp: abierto. Servicio: nv-video.
    > Puerto 4899/tcp: abierto. Servicio: radmin.
    > Puerto 5900/tcp: abierto. Servicio: vnc.
    > Puerto 21000/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot Honeytrap en esta IP:
      - [7/8] de los puertos que utiliza Honeytrap están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Mailoney...
    > Puerto 25/tcp: abierto. Servicio: smtp.
    > Hay posibilidades de que haya un honeypot Mailoney en esta IP:
      - [1/1] de los puertos que utiliza Mailoney están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Rdpy...
    > Puerto 3389/tcp: abierto. Servicio: ms-wbt-server.
    > Hay posibilidades de que haya un honeypot Rdpy en esta IP:
      - [1/1] de los puertos que utiliza Rdpy están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Vnclowpot...
    > Puerto 5900/tcp: abierto. Servicio: vnc.
    > Hay posibilidades de que haya un honeypot Vnclowpot en esta IP:
      - [1/1] de los puertos que utiliza Vnclowpot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo eMobility...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Puerto 8080/tcp: abierto. Servicio: http-proxy.
    > Hay posibilidades de que haya un honeypot eMobility en esta IP:
      - [2/2] de los puertos que utiliza eMobility están abiertos.
A continuación se analizarán posibles rasgos que indiquen que alguno de los honeypots de la lista
anterior se aloja en la IP auditada.
-----------------------
- ANÁLISIS PROFUNDO -
-----------------------
A continuación se realizará un análisis inmersivo. Para ello, debe proporcionar usuario y contraseña de
la máquina.
El fin de esto es simular qúé es capaz de descubrir un atacante que ha logrado penetrar en el sistema.
User: user
Password: password
Posibles Honeypots en la máquina:
    > conPot
Analizando puerto por defecto...
Puerto serie 88111222 detectado. Posible honeypot.
    > cowrie
Realizando pruebas en honeypot Cowrie (1/4)...
Prueba 01: Comprobacion de usuarios.
Resultado: Posible honeypot
Realizando pruebas en honeypot Cowrie (2/4)...
Prueba 02: Comprobacion de creacion de archivos.
Resultado: Posible honeypot
Realizando pruebas en honeypot Cowrie (3/4)...
Prueba 03: Comprobacion de comandos.
Resultado: Posible honeypot
Realizando pruebas en honeypot Cowrie (4/4)...
Prueba 04: Comprobacion de directorios.
Resultado: Posible honeypot
    > dionaea
Script de comprobación: dionaea-detect-smb
Resultado:
Posible honeypot.
Script de comprobación: dionaea-detect-mysql
Resultado:
Posible honeypot.
Script de comprobación: dionaea-detect-ssl
Resultado:
Posible honeypot.
    > elasticPot
    > glastopf
**************************************************************************
http://XXX.XXX.XXX.XXX/
Realizando pruebas en honeypot Glastopf (1/3)...
Realizando pruebas en honeypot Glastopf (2/3)...
Realizando pruebas en honeypot Glastopf (3/3)...
27%
11%
27%
11%
00%
00%
Páginas muy distintas. Posible honeypot.
    > honeytrap
    > mailoney
    > rdpy
    > vnclowpot
```

```
    > eMobility
---------------------------------
-   I N F O R M E   F I N A L   -
---------------------------------
A continuación se mostrarán los porcentajes que la herramienta ha obtenido de cada uno de los honeypots
de la base de datos:
--------------------------
- conPot: 100%           -
- cowrie: 100%           -
- dionaea: 90%           -
- glastopf: 70%          -
- elasticPot: 45%        -
- honeytrap: 30%         -
- mailoney: 30%          -
- rdpy: 30%              -
- vnclowpot: 30%         -
- eMobility: 30%         -
--------------------------
Es extremadamente probable que haya un honeypot en esta dirección IP.
```

5.1.2 IP que no alberga una honeynet t-Pot:

```
./honeyCatch
                                                  ___       _          _                \\//
      /\  /\___  _ __   ___ _   _   / __\__ _| |_ ___| |__       (°)))>-
     / /_/ / _ \| '_ \ / _ \ | | |/ /  / _` | __/ __| '_ \     __```__
    / __  / (_) | | | |  __/ |_| / /__| (_| | || (__| | | |    /      \
    \/ /_/ \___/|_| |_|\___|\__, \____/\__,_|\__\___|_| |_|   (        )
                               |___/                           ……….
Introduce la IP del posible honeypot: YYY.YYY.YYY.YYY
Analizando la IP YYY.YYY.YYY.YYY
Nmap está instalado. Ejecutando modo automático.
Modo 1: Escaneo automático.
Se han obtenido los puertos abiertos. Comprobando coincidencias de puertos abiertos con la base de datos
de honeypots...
------------------------------------------------------
- Comprobación de HoneyPots según puertos abiertos. -
------------------------------------------------------
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ConPot...
    > Puerto 81/tcp: cerrado.
    > No hay posibilidades de que haya un honeypot ConPot en esta IP.
--------------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Cowrie...
    > Puerto 22/tcp: cerrado.
    > Puerto 23/tcp: cerrado.
    > No hay posibilidades de que haya un honeypot Cowrie en esta IP.
--------------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Dionaea...
    > Puerto 21/tcp: abierto. Servicio: ftp.
    > Puerto 42/tcp: cerrado.
    > Puerto 135/tcp: cerrado.
    > Puerto 443/tcp: abierto. Servicio: https.
    > Puerto 445/tcp: cerrado.
    > Puerto 1433/tcp: cerrado.
    > Puerto 1723/tcp: cerrado.
    > Puerto 3306/tcp: cerrado.
    > Puerto 5060/tcp: cerrado.
    > Puerto 5061/tcp: cerrado.
    > Puerto 8081/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot Dionaea en esta IP:
      - [2/11] de los puertos que utiliza Dionaea están abiertos.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ElasticPot...
    > Puerto 9200/tcp: cerrado.
    > No hay posibilidades de que haya un honeypot ElasticPot en esta IP.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Glastopf...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Hay posibilidades de que haya un honeypot Glastopf en esta IP:
      - [1/1] de los puertos que utiliza Glastopf están abiertos.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Honeytrap...
    > Puerto 25/tcp: abierto. Servicio: smtp.
    > Puerto 110/tcp: cerrado.
    > Puerto 139/tcp: cerrado.
    > Puerto 3389/tcp: cerrado.
    > Puerto 4444/tcp: cerrado.
    > Puerto 4899/tcp: cerrado.
    > Puerto 5900/tcp: cerrado.
    > Puerto 21000/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot Honeytrap en esta IP:
      - [1/8] de los puertos que utiliza Honeytrap están abiertos.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Mailoney...
    > Puerto 25/tcp: abierto. Servicio: smtp.
```

```
    > Hay posibilidades de que haya un honeypot Mailoney en esta IP:
      - [1/1] de los puertos que utiliza Mailoney están abiertos.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Rdpy...
    > Puerto 3389/tcp: cerrado.
    > No hay posibilidades de que haya un honeypot Rdpy en esta IP.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Vnclowpot...
    > Puerto 5900/tcp: cerrado.
    > No hay posibilidades de que haya un honeypot Vnclowpot en esta IP.
--------------------------------------------------------------------------------
- Comprobando probabilidad de que la IP tenga activo un Honeypot tipo eMobility...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Puerto 8080/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot eMobility en esta IP:
      - [1/2] de los puertos que utiliza eMobility están abiertos.
A continuación se analizarán posibles rasgos que indiquen que alguno de los honeypots de la lista
anterior se aloja en la IP auditada.
-----------------------
- ANÁLISIS PROFUNDO -
-----------------------
A continuación se realizará un análisis inmersivo. Para ello, debe proporcionar usuario y contraseña de
la máquina.
El fin de esto es simular qué es capaz de descubrir un atacante que ha logrado penetrar en el sistema.
User: *****
Password: *******
Posibles Honeypots en la máquina:
    > dionaea
Script de comprobación: dionaea-detect-smb
Resultado:
No se ha encontrado configuración por defecto.
Script de comprobación: dionaea-detect-mysql
Resultado:
No se ha encontrado configuración por defecto.
Script de comprobación: dionaea-detect-ssl
Resultado:
No se ha encontrado configuración por defecto.
    > glastopf
**************************************************************************
http://YYY.YYY.YYY.YYY/
Realizando pruebas en honeypot Glastopf (1/3)...
Realizando pruebas en honeypot Glastopf (1/3)...
Realizando pruebas en honeypot Glastopf (2/3)...
Realizando pruebas en honeypot Glastopf (3/3)...
100%
100%
100%
100%
100%
100%
Páginas similares. Descartado posible honeypot.
    > honeytrap
    > mailoney
---------------------------------
-   I N F O R M E   F I N A L   -
---------------------------------
A continuación se mostrarán los porcentajes que la herramienta ha obtenido de cada uno de los honeypots
de la base de datos:
--------------------------
- conPot: 0%              -
- cowrie: 0%              -
- dionaea: 30%            -
- glastopf: 30%           -
- elasticPot: 0%          -
- honeytrap: 30%          -
- mailoney: 30%           -
- rdpy: 0%                -
- vnclowpot: 0%           -
- eMobility: 0%           -
--------------------------
Es improbable que haya un honeypot en esta dirección IP.
```

5.2 Comprobación de herramienta

Para comprobar que la ocultación de honeypots había sido correcta, se probó la herramienta creada antes y después de camuflarlos. Tras la ocultación, la herramienta no detectó ningún honeypot en la dirección IP:

```
# ./honeyCatch
                                        ___          _          _              \\//
      /\  /\___  _ __   ___ _   _     / __\__ _| |_ ___| |__      (°)))>-
     / /_/ / _ \| '_ \ / _ \ | | |/ /  / _` | __/ __| '_ \     __ ``` __
    / __  / (_) | | | |  __/ |_| / /__| (_| | || (__| | | |    /     \
    \/ /_/ \___/|_| |_|\___|\__, \____/\__,_|\__\___|_| |_|   (       )
                            |___/                             ‾‾‾‾‾‾‾‾‾
```

```
Introduce la IP del posible honeypot: XXX.XXX.XXX.XXX
Analizando la IP XXX.XXX.XXX.XXX
Nmap está instalado. Ejecutando modo automático.
Modo 1: Escaneo automático.
Se han obtenido los puertos abiertos. Comprobando coincidencias de puertos abiertos con la base de datos
de honeypots...
-----------------------------------------------------
- Comprobación de HoneyPots según puertos abiertos. -
-----------------------------------------------------
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ConPot...
    > Puerto 81/tcp: abierto. Servicio: hosts2-ns.
    > Puerto 1025/tcp: abierto. Servicio: blackjack.
    > Hay posibilidades de que haya un honeypot ConPot en esta IP:
      - [2/3] de los puertos que utiliza ConPot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Cowrie...
    > Puerto 22/tcp: abierto. Servicio: ssh.
    > Puerto 23/tcp: abierto. Servicio: telnet.
    > Hay posibilidades de que haya un honeypot Cowrie en esta IP:
      - [2/2] de los puertos que utiliza Cowrie están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Dionaea...
    > Puerto 21/tcp: abierto. Servicio: ftp.
    > Puerto 42/tcp: abierto. Servicio: nameserver.
    > Puerto 135/tcp: abierto. Servicio: msrpc.
    > Puerto 443/tcp: abierto. Servicio: https.
    > Puerto 445/tcp: abierto. Servicio: microsoft-ds.
    > Puerto 1433/tcp: abierto. Servicio: ms-sql-s.
    > Puerto 1723/tcp: abierto. Servicio: pptp.
    > Puerto 3306/tcp: abierto. Servicio: mysql.
    > Puerto 5060/tcp: abierto. Servicio: sip.
    > Puerto 5061/tcp: abierto. Servicio: sip-tls.
    > Puerto 8081/tcp: abierto. Servicio: http alternate.
    > Hay posibilidades de que haya un honeypot Dionaea en esta IP:
      - [11/11] de los puertos que utiliza Dionaea están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo ElasticPot...
    > Puerto 9200/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot ElasticPot en esta IP:
      - [0/1] de los puertos que utiliza ElasticPot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Glastopf...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Hay posibilidades de que haya un honeypot Glastopf en esta IP:
      - [1/1] de los puertos que utiliza Glastopf están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Honeytrap...
    > Puerto 25/tcp: abierto. Servicio: smtp.
    > Puerto 110/tcp: abierto. Servicio: pop3.
    > Puerto 139/tcp: abierto. Servicio: netbios-ssn.
    > Puerto 3389/tcp: abierto. Servicio: ms-wbt-server.
    > Puerto 4444/tcp: abierto. Servicio: nv-video.
    > Puerto 4899/tcp: abierto. Servicio: radmin.
    > Puerto 5900/tcp: abierto. Servicio: vnc.
    > Puerto 21000/tcp: cerrado.
    > Hay posibilidades de que haya un honeypot Honeytrap en esta IP:
      - [7/8] de los puertos que utiliza Honeytrap están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Mailoney...
    > Puerto 25/tcp: abierto. Servicio: smtp.
    > Hay posibilidades de que haya un honeypot Mailoney en esta IP:
      - [1/1] de los puertos que utiliza Mailoney están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Rdpy...
    > Puerto 3389/tcp: abierto. Servicio: ms-wbt-server.
    > Hay posibilidades de que haya un honeypot Rdpy en esta IP:
      - [1/1] de los puertos que utiliza Rdpy están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo Vnclowpot...
    > Puerto 5900/tcp: abierto. Servicio: vnc.
    > Hay posibilidades de que haya un honeypot Vnclowpot en esta IP:
      - [1/1] de los puertos que utiliza Vnclowpot están abiertos.
------------------------------------------------------------------------
Comprobando probabilidad de que la IP tenga activo un Honeypot tipo eMobility...
    > Puerto 80/tcp: abierto. Servicio: http.
    > Puerto 8080/tcp: abierto. Servicio: http-proxy.
    > Hay posibilidades de que haya un honeypot eMobility en esta IP:
      - [2/2] de los puertos que utiliza eMobility están abiertos.
A continuación se analizarán posibles rasgos que indiquen que alguno de los honeypots de la lista
anterior se aloja en la IP auditada.
-----------------------
- ANÁLISIS PROFUNDO -
-----------------------
A continuación se realizará un análisis inmersivo. Para ello, debe proporcionar usuario y contraseña de
la máquina.
El fin de esto es simular qué es capaz de descubrir un atacante que ha logrado penetrar en el sistema.
```

```
User: root
Password: password
Posibles Honeypots en la máquina:
    > conPot
Analizando puerto por defecto...
No se ha encontrado puerto por defecto.
    > cowrie
Realizando pruebas en honeypot Cowrie (1/4)...
Prueba 01: Comprobacion de usuarios.
Resultado: No parece haber honeypot
Realizando pruebas en honeypot Cowrie (2/4)...
Prueba 02: Comprobacion de creacion de archivos.
Resultado: No parece haber honeypot
Realizando pruebas en honeypot Cowrie (3/4)...
Prueba 03: Comprobacion de comandos.
Resultado: No parece haber honeypot
Realizando pruebas en honeypot Cowrie (4/4)...
Prueba 04: Comprobacion de directorios.
Resultado: No parece haber honeypot
    > dionaea
Script de comprobación: dionaea-detect-smb
Resultado:
No se ha encontrado configuración por defecto.
Script de comprobación: dionaea-detect-mysql
Resultado:
No se ha encontrado configuración por defecto.
Script de comprobación: dionaea-detect-ssl
Resultado:
No se ha encontrado configuración por defecto.
    > glastopf
**************************************************************************
http://XXX.XXX.XXX.XXX/
Realizando pruebas en honeypot Glastopf (1/3)...
Realizando pruebas en honeypot Glastopf (2/3)...
Realizando pruebas en honeypot Glastopf (3/3)...
100%
100%
100%
100%
100%
100%
Páginas similares. Descartado posible honeypot.
    > honeytrap
    > mailoney
    > rdpy
    > vnclowpot
    > eMobility
---------------------------------
-   I N F O R M E   F I N A L   -
---------------------------------
A continuación se mostrarán los porcentajes que la herramienta ha obtenido de cada uno de los honeypots
de la base de datos:
--------------------------
- conPot: 30%            -
- cowrie: 30%            -
- dionaea: 30%           -
- glastopf: 30%          -
- elasticPot: 0%         -
- honeytrap: 30%         -
- mailoney: 30%          -
- rdpy: 30%              -
- vnclowpot: 30%         -
- eMobility: 30%         -
--------------------------
Es improbable que haya un honeypot en esta dirección IP.
```

Además de pasar la prueba con la herramienta creada, también se han analizado las diferencias entre los ataques antes y después de la ocultación. Para ello se ha utilizado la herramienta Kibana, incorporada en la honeynet t-Pot. El algoritmo utilizado para calcular los porcentajes es completamente configurable y se puede consultar en el anexo 0.

5.3 Recogida de datos

Durante este proyecto se instauraron dos honeynets idénticas en la red de la Universidad Autónoma de Madrid. Una de las honeynets se colocó antes del firewall de la UAM y la otra detrás. Se han denominado a dichas honeynets “honeynet A” y “honeynet B” respectivamente, para proteger la seguridad y privacidad de la Universidad Autónoma de Madrid.

Los honeypots han estado varios meses recogiendo datos, y en total se recogieron varias decenas de millones de ataques de todo el mundo. Se han escogido intervalos de tiempo iguales en fechas cercanas para poder hacer un análisis que sea lo más fiel posible, y tratar de que el factor temporal afecte mínimamente al estudio.

A continuación se muestra un análisis global de los honeypots de los datos obtenidos durante 15 días antes de ocultar los honeypots y los obtenidos en el mismo intervalo de tiempo después de camuflarlos como se ha visto en la sección 4.2 “Ocultación de los honeypots”. Se incluye un análisis más detallado de cada honeypot en el anexo E, así como dos gráficas comparativas que muestran el número de ataques antes y después de la ocultación.

5.3.1 Honeynet A (Fuera del firewall de la UAM)

Antes de la ocultación

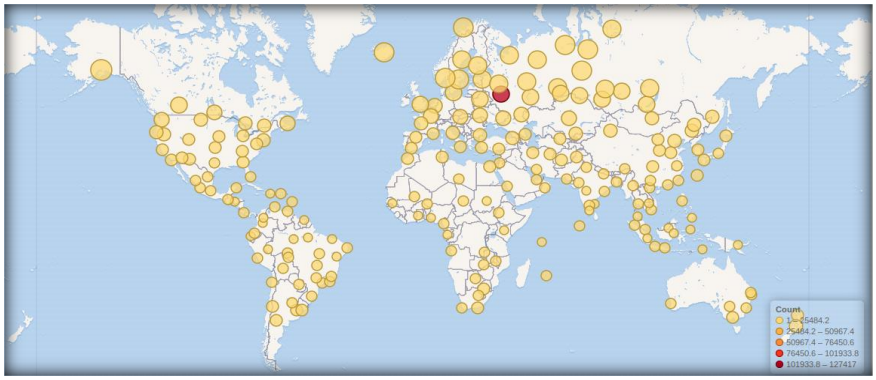


Figura 5.1 Mapa de ataques honeynet A (15/4 – 30/4).

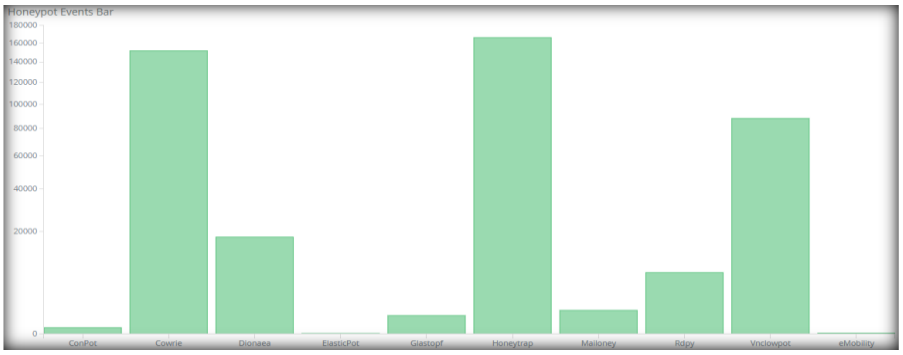


Figura 5.2 Honeypots más atacados de la honeynet A (15/4 – 30/4).

Entre los ataques que se han recogido en este intervalo destacan notablemente los dirigidos a Cowrie, Dionaea, Honeytrap y Vnclowpot (Figura 5.2). Como se aprecia en la Figura 5.1, se han recogido ataques provenientes de todo el mundo.

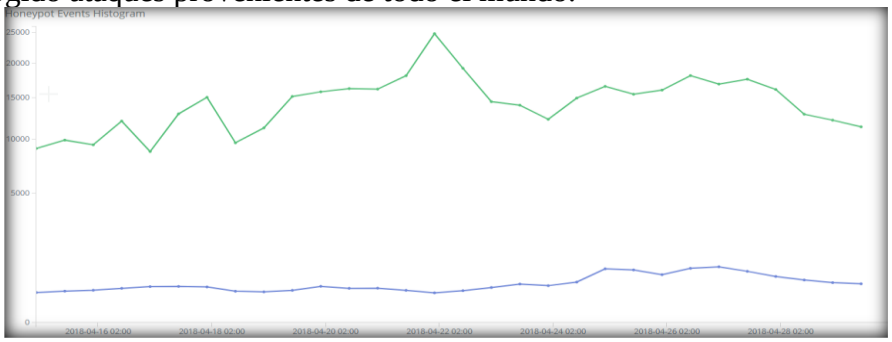


Figura 5.3 Histograma de ataques en la honeynet A (15/4 – 30/4).

El número de ataques diario fluctuó entre los 10000 y 25000 ataques diarios (línea verde de la Figura 5.3), frente al número de IPs distintas por día que atacaban, que varió entre 300 y 900 IPs (línea azul de la Figura 5.3).

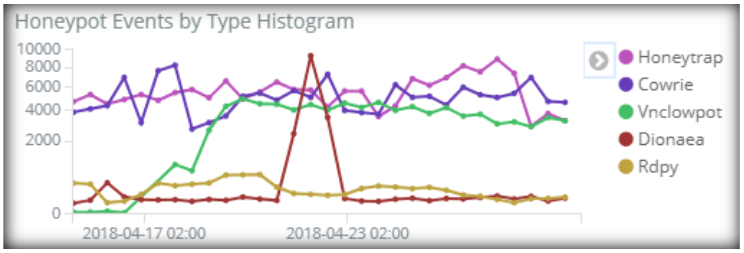


Figura 5.4 Ataques de la honeynet A según el tipo de honeypot. (15/4 – 30/4).

En la Figura 5.4 vemos que la variación más alta fue con el honeypot Dionaea, que pasó de mantenerse en los 100 ataques diarios a los 10000 ataques en un solo día.
También se incrementaron notablemente los ataques de Vnclowpot, que pasaron de ser 0 durante 2 días a rondar los 4000 ataques diarios.

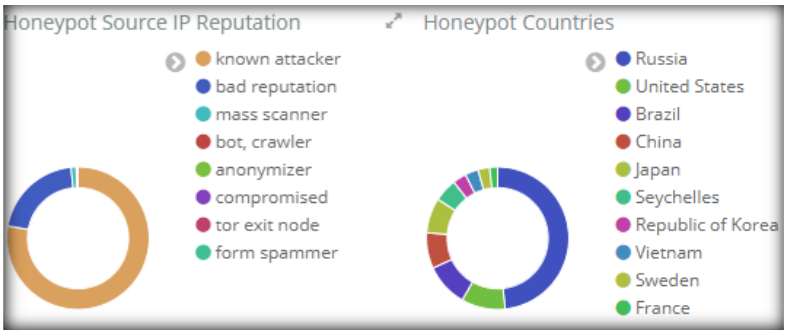


Figura 5.5 Izquierda: Reputación de las IP atacantes. Derecha: Top 10 países atacantes. (15/4 – 30/4).

Por otro lado, tal y como muestra la Figura 5.5, los ataques vinieron en un 77.76% de atacantes conocidos y registrados en la base de datos de t-Pot, y un 20.67% provenían de IPs con mala reputación en la red, esto es, que estaban en listas negras de atacantes comunes.

El país que más ataques realizó con diferencia fue Rusia, realizando el 48% de los ataques, seguido de Estados Unidos, Brasil, China y Japón con entorno a un 8% de ataques cada uno.
Los nombres de usuario más utilizados para acceder por ssh fueron “root”, “admin”, “shell”, “enable”, “support”, “guest”, “default”, “supervisor”, “ubnt” y “user”.
Las contraseñas más utilizadas para acceder por ssh fueron “system”, “sh”, “SH”, “1234”, “12345”, “admin”, “password”, “123456”.

Después de la ocultación

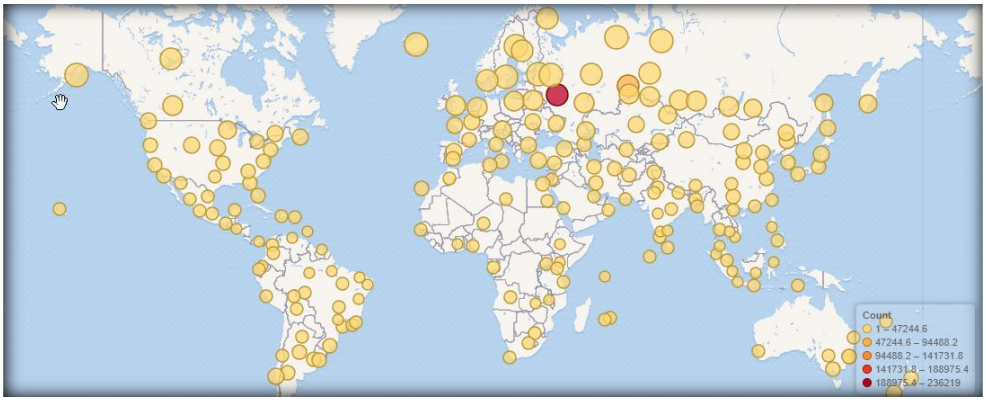


Figura 5.6 Mapa de ataques honeynet A (1/6 – 15/6).

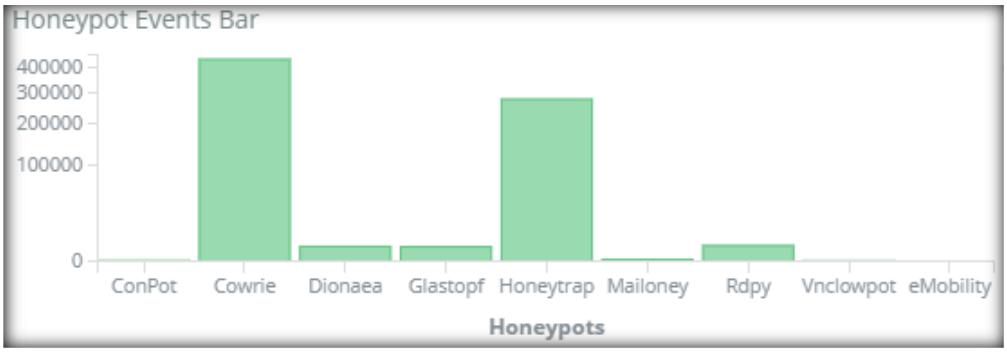


Figura 5.7 Honeypots más atacados de la honeynet A (1/6 – 15/6).

Tras la ocultación, los ataques por todo el planeta (Figura 5.6) a los honeypots Cowrie, Glastopf y Honeytrap se han multiplicado a más del doble con respecto a antes de la ocultación (Figura 5.2 y Figura 5.7). Este es un primer indicio de que la ocultación ha funcionado. Sin embargo, los ataques a Vnclowpot se han reducido drásticamente. Dado que Honeytrap en concreto no se ocultó, la conclusión a la que se ha llegado es que los atacantes no solo han atacado un único servicio, y la ocultación de unos honeypots ha afectado a los ataques del resto, aumentándolos también.

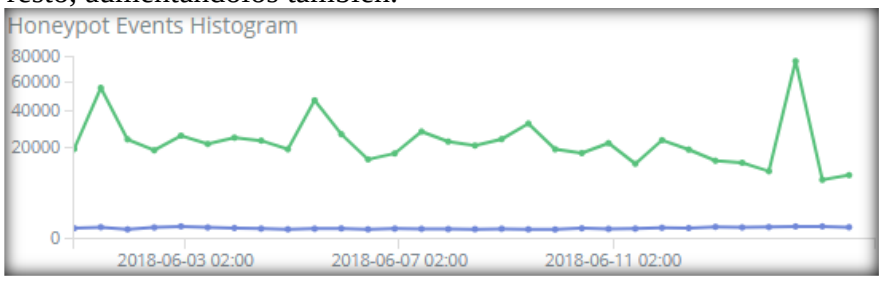


Figura 5.8 Histograma de ataques en la honeynet A (1/6 – 15/6).

El número de ataques diario fluctuó entre los 20000 y 80000 ataques diarios (línea verde de la Figura 5.8), frente al número de IPs distintas que atacaban, que varió en las 300 IPs (línea azul de la Figura 5.8). Este es un indicio aún más claro, puesto que el número de IPs diarias no ha aumentado (de hecho, ha disminuido) pero los ataques se han multiplicado. Esto implica que cada atacante ha realizado un mayor número de ataques, por lo que ha permanecido más tiempo en la honeynet creyendo que se trataba de un sistema real.

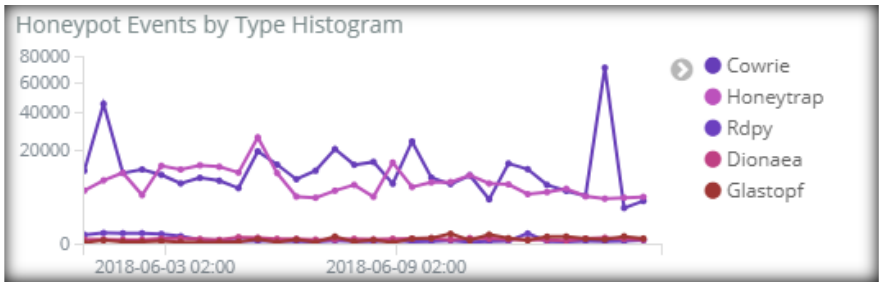


Figura 5.9 Ataques de la honeynet A según el tipo de honeypot. (1/6 – 15/6)

En la Figura 5.9 vemos que la variación más alta fue con el honeypot Cowrie, que pasó de mantenerse en los 20000 ataques diarios a los 80000 ataques en un solo día. En comparación con la Figura 5.4, destaca la ausencia de ataques del honeypot Vnclowpot, que antes de la ocultación tuvo momentos de recibir 4000 ataques diarios.

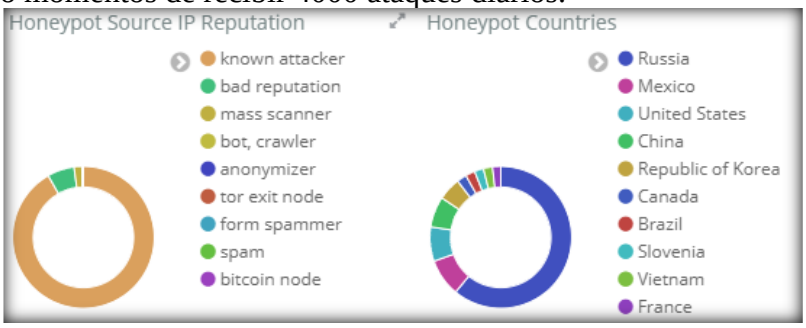


Figura 5.10 Izquierda: Reputación de las IP atacantes. Derecha: Top 10 países atacantes. (1/6 – 15/6).

Al igual que antes de la ocultación, en la Figura 5.10 observamos que la mayoría de los ataques proviene de atacantes conocidos, y el resto de los atacantes con mala reputación.

El país que más ataques realizó nuevamente fue Rusia, realizando el 61% de los ataques, seguido de México, Estados Unidos, China y Corea con entorno a un 7% de ataques cada uno.
Los nombres de usuario más utilizados para acceder por ssh fueron “root”, “admin”, “shell”, “enable”, “default”, “tech”, “user”, “guest” y “Administrator”.
Las contraseñas más utilizadas para acceder por ssh fueron “system”, “sh”, “user”, “admin”, “password”, “1234”, “12345”, “123456” y “7ujMko0admin”.

5.3.2 Honeynet B (Dentro de UAM)

Antes de la ocultación

Figura 5.11 Mapa de ataques honeynet B (15/4 – 30/4).

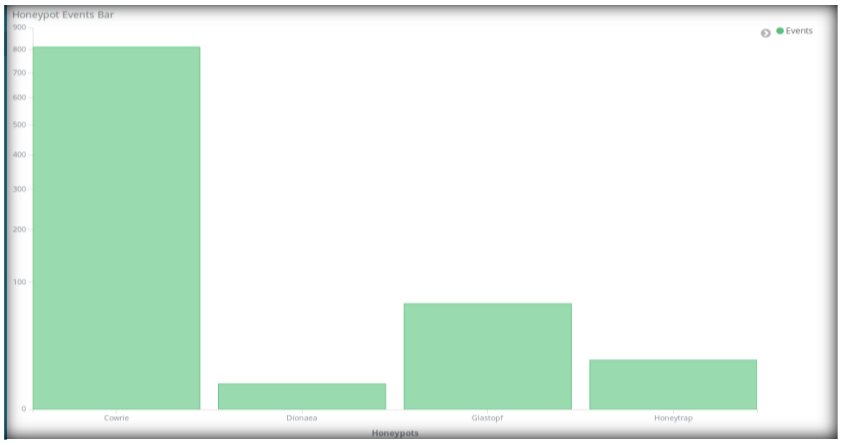


Figura 5.12 Histograma de Eventos en la honeynet B (15/4 – 30/4).

En la honeynet B la mayoría de los ataques se han producido en el honeypot Cowrie, seguido de Glastopf, Honeytrap y Dionaea (Figura 5.12).
Podemos observar que en este caso el firewall de la Universidad Autónoma de Madrid ha bloqueado cualquier tipo de ataque al resto de honeypots (Figura 5.13Figura 5.13).

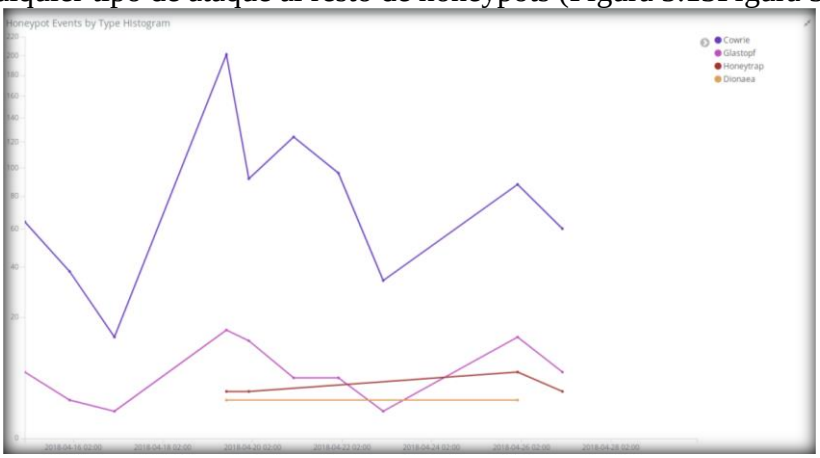


Figura 5.13 Histograma de eventos en la honeynet B (15/4 – 30/4).

Como muestra la Figura 5.13, el número de ataques es muy inferior a la honeynet que se ha colocado en el exterior del firewall, rondando los cien ataques diarios, desde unas 20 IPs distintas por día.

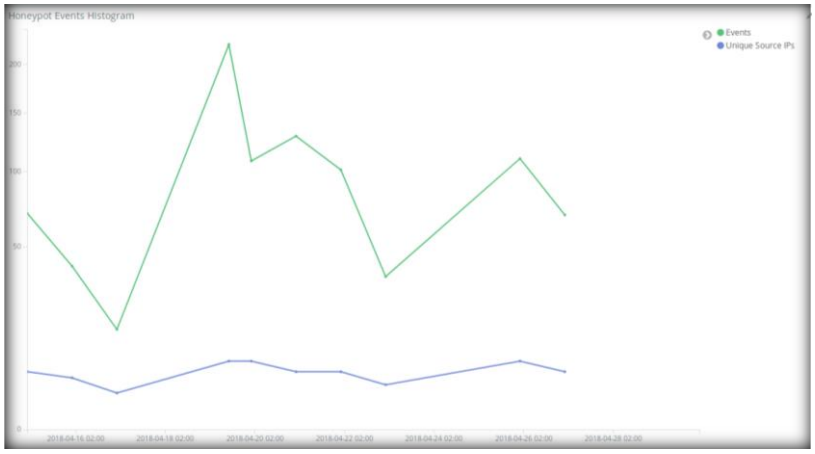


Figura 5.14 Eventos de la honeynet B según el tipo de honeypot (15/4 – 30/4).

Podemos observar que los ataques realizados a Cowrie y Glastopf han sido diarios, mientras que los ataques recibidos en Honeytrap y Dionaea fueron puntuales (Figura 5.14).

La variación más alta fue con el honeypot Cowrie, que cuadruplicó el número de ataques pasando de una media de 50 ataques diarios hasta los 200 ataques diarios. Sin embargo, tras analizar los ataques, se descubrió que una buena parte de ellos fueron causados debido a las pruebas que realicé con mi propio equipo, con lo que estos ataques no son reales.
Encontramos que se da una cierta relación entre los ataques de Cowrie y Glastopf, lo que podría indicar que varios atacantes han tratado de vulnerar ambos honeypots.

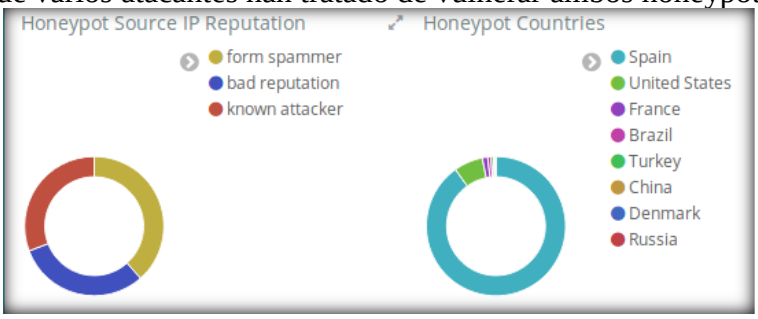


Figura 5.15 Izquierda: Reputación de las IP atacantes. Derecha: Top 10 países atacantes (15/4 – 30/4).

También se ha observado que los ataques provenían, de forma igualitaria, tanto de "form spammers" (bots cuya función es realizar formularios introduciendo valores aleatorios), como de direcciones IP que tienen mala reputación en la red o de direcciones que la base de datos tiene registrada como atacantes (Figura 5.15).

El 90% de los ataques recibidos provienen de España, y el resto vienen mayoritariamente de Estados Unidos. Esto se puede observar en la Figura 5.11. Los usuarios más comunes que ha recogido Cowrie son "root", "pedro", "OPTIONS / RTSP/1.0", "OPTIONS / HTTP/1.0", "GET / HTTP /1.0" y "GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0". Las contraseñas que los atacantes han dejado en Cowrie son "default", "123456", "Zte521" , "12345" y "12345[A"

Después de la ocultación

Figura 5.16 Mapa de ataques honeynet B (1/6 – 15/6).

Figura 5.17 Histograma de Eventos en la honeynet B (1/6 – 15/6).

Tras la ocultación, ha habido un descenso del número de ataques en la honeypot de dentro del firewall. Mientras que en antes de la ocultación los honeypots Cowrie, Glastopf, Honeytrap y Dionaea recogieron una gran cantidad de ataques, llegando a los 800 en el caso de Cowrie (Figura 5.12), esta vez tan solo se han registrado 24 ataques de Cowrie y 26 de Glastopf (Figura 5.17). Se ha realizado un análisis profundo a las IPs que causaron estos ataques, y se ha descubierto que la IP que realizó los ataques a Glastopf era un crawler de Google, que indexó la página antes de la ocultación, y las dos IPs que atacaron Cowrie tanto antes como después de la ocultación pertenecen a dos ordenadores de la UAM que pueden estar comprometidos. Nos hemos puesto en contacto con el departamento de Tecnologías de la Información y les hemos transmitido esta información para que el problema pueda ser solventado rápidamente.

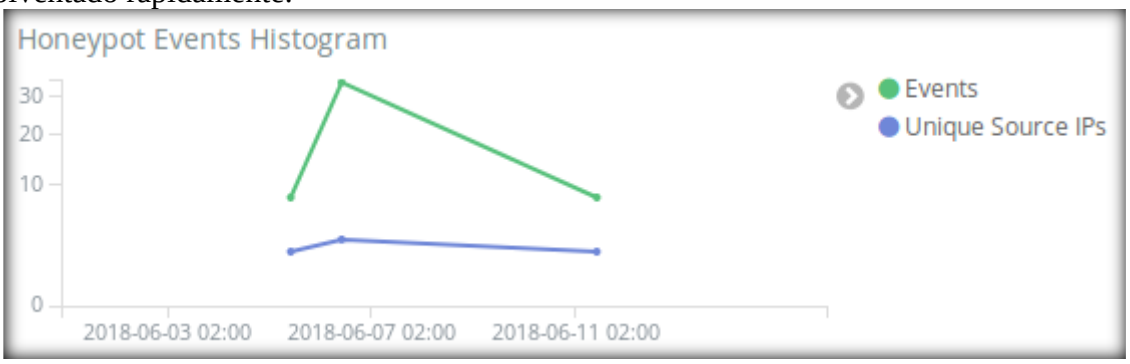


Figura 5.18 Histograma de eventos en la honeynet B (1/6 – 15/6).

Como muestra la Figura 5.18, el número de ataques es extremadamente reducido, tan solo hubo 3 días en los que se recibió ataques, no llegando en ninguna ocasión a los 40 ataques. Además, solo fueron entre 3 y 4 IPs distintas por día, mientras que antes de la ocultación había unas 20 IPs distintas por día, como se puede ver en la Figura 5.13. Al tratarse de un número de ataques tan reducido, proveniente en su mayoría de dos ordenadores de la universidad, no consideramos que exista una relación clara entre este decremento de ataques y la ocultación de los honeypots. Además se analizaron estos ataques y se descubrió que tan solo trataban de explorar distintos puertos a través de peticiones ping y ssh, sin llegar a realizar ningún intento de inicio de sesión.

Sin embargo, los resultados recogidos en la honeypot A, en la que se han recogido millones de ataques y estos se han visto incrementados tras la ocultación en varios ordenes de magnitud, sí que conforman una evidencia de que los honeypots se han ocultado con éxito.

6 Conclusiones y trabajo futuro

6.1 Conclusiones

A lo largo de este proyecto se ha estudiado el comportamiento de los honeypots con el objetivo de la ocultación y mejora de los mismos frente a atacantes cada vez más cualificados. Para ello se fijaron una serie de objetivos que a continuación se evalúan:

- ***Objetivo 0: Implantación de un sistema de honeypots en la Universidad Autónoma de Madrid***.

La implantación de este sistema se ha realizado correctamente (como podemos ver en el punto 3.5.2 "Instalación de la infraestructura"), y ahora la Universidad Autónoma de Madrid dispone de dos redes honeynet de once honeypots cada una. Este proyecto ha ofrecido a la universidad una gran herramienta de investigación que permitirá incrementar su seguridad.

- ***Objetivo 1: Creación de herramienta que evalúe la posibilidad de que un determinado sistema sea un señuelo***.

Se ha creado una herramienta en la que se realizan un conjunto de tests y comprobaciones para determinar si una dirección IP es realmente una máquina trampa. Para ello se han realizado auditorías sobre las honeynets lanzadas en la UAM, adquiriendo el rol de atacante.

- ***Objetivo 2: Mejora y ofuscación de sistemas señuelo con los datos obtenidos.***

Con la información recopilada para crear la herramienta de detección se han aplicado diversos cambios para camuflar mejor a los honeypots y que aparenten ser sistemas reales. Esto se ha conseguido modificando muchas configuraciones por defecto que tenían ambas honeynets. De esa forma ahora a los atacantes les costará más reconocer que se encuentran en un sistema trampa y se podrán registrar más ataques (como se ha visto en la sección 5.3 "Recogida de datos") y descubrir técnicas nuevas que empleen los atacantes.

- ***Objetivo 3: Estudio y Análisis de los Ataques en una red de honeypots (Honeynet).***

Se han analizado los ataques realizados a los honeypots de la Universidad Autónoma de Madrid antes y después de mejorar su ocultación con los datos recogidos tras probar la herramienta, para realizar un estudio sobre cómo mejorar el nivel de detección.

Los cuatro objetivos marcados han sido cumplidos, se ha probado que la herramienta creada funciona correctamente y cumple el propósito con el que se creó, la detección de honeypots, y en las secciones 5.2 "Comprobación de herramienta" y 5.3 "Recogida de datos" se ha recogido información suficiente para demostrar que, tras las implementaciones llevadas a cabo en este proyecto, la ocultación de los honeypots ha sido satisfactoria y se han recogido muchos más ataques. Además, se ha recogido una gran cantidad de información en los meses en los que los honeypots han estado levantados en la Universidad Autónoma de Madrid, y se ha comprobado que la universidad tiene un potente firewall que bloquea la mayoría de los ataques.

En conclusión, este Trabajo de Fin de Grado ha abierto las puertas a una profunda rama de investigación en la que se podrá aprender mucho y seguir mejorando las dos honeynets que se han colocado en la universidad y que continuarán recibiendo ataques en el futuro. Se ha confirmado que el nivel de ocultación de los honeypots influye en el número de ataques recibidos y que tras la ocultación la duración de los ataques aumentó, y se ha proporcionado una herramienta capaz de detectar sistemas que albergan honeypots.

6.2 Trabajo futuro

Este proyecto ofrece una primera versión de una herramienta de detección de honeypots. Como tal, sienta las bases de la detección de máquinas trampa. Tras estos meses de trabajo, considero que es importante continuar la línea investigatoria en este campo, no solo para reforzar los usos ya conocidos de los honeypots, sino porque estos son una herramienta en potencia que podría revolucionar el mundo de la ciberseguridad tal y como conocemos hoy en día. Existen una gran variedad de campos a mejorar en dicha herramienta a disposición de futuros investigadores, entre ellos:

- ***Aumento del número de pruebas de detección que realiza la herramienta***: ya sea implementando los tests que se han descartado para la primera versión, o descubriendo otras nuevas formas de detección.
- ***Mejora de rendimiento***: debido a la gran cantidad de puertos que debe escanear, así como las pruebas que realiza en cada honeypot, la herramienta es lenta. Una posible mejora sería la implementación de hilos y la optimización de las funciones para aumentar su rendimiento.
- ***Detección de nuevos tipos de honeypots:*** la herramienta está basada en los once honeypots que conforman la honeynet de la Universidad Autónoma de Madrid. Una vía de investigación podría consistir en añadir a la honeynet otros tipos de honeypots que simulen servicios distintos, y buscar sus puntos débiles para reforzarlos y añadirlos a la herramienta.

Además, durante el desarrollo de este proyecto se ha creado una base de datos de gran tamaño que ha registrado durante meses millones de ataques en los distintos honeypots.
Estos datos solo se han analizado superficialmente para comprobar las diferencias antes y después de la ocultación de honeypots. Un posible trabajo futuro sería el estudio exhaustivo de todos estos datos para entender y clasificar los ataques recibidos, y poder establecer distintos patrones de ataque.

Referencias

1. *RSA Report: 71 percent of IT pros believe they can hack any organization.* Outpost24. Abril 2018.
2. https://www.honeynet.org/node/158. [Online]
3. Spitzner, Lance. Honeytokens: The Other Honeypot. *SecurityFocus.* 2003.
4. Yizhi Ren, Yang Xiang, Ming Xu, Jingyu Hua. Google hacking defence based on honey pages. *International Journal of Applied Mathematics and Statistics.* 51(22):284-292, Enero 2013.
5. https://www.honeynet.org/. [Online]
6. Hunt, David. One HoneyPot Farm's Quest to Protect the Net. *Catching Bees with Honey.* Junio 2015.
7. http://dtag-dev-sec.github.io. [Online]
8. http://conpot.org/. [Online]
9. http://www.micheloosterhof.com/cowrie/. [Online]
10. https://dionaea.readthedocs.io/en/latest/. [Online]
11. https://hub.docker.com/r/honeynet/elasticpot/. [Online]
12. http://mushmush.org/. [Online]
13. https://pentestlab.blog/2012/02/24/credential-harvester-attack-method/]. [Online]
14. https://github.com/citronneur/rdpy. [Online]
15. https://suricata-ids.org/. [Online]
16. https://github.com/magisterquis/vnclowpot. [Online]
17. https://github.com/msbeiti/eMobility-honeypot. [Online]
18. https://honeyscore.shodan.io. [Online]
19. https://nmap.org. [Online]
20. https://www.elevenpaths.com/es/labstools/foca-2/index.html. [Online]
21. https://github.com/digitalbond/Redpoint). [Online]
22. https://github.com/meeas/plcscan. [Online]
23. (http://blog.prowling.nu/2012/04/detecting-dionaea-honeypot-using-nmap.html). [Online]
24. Wouters, Niels. Uncovering the Honeypot Effect: How Audiences Engage with Public Interactive Systems. *Proceedings of the 2016 ACM Conference on Designing Interactive Systems.* Pages 5-16 , 2016.
25. Spitzner, Lance. Sebek tool. *honeynet Project.* 2004.
26. Heiderich. Defensive Camouflage. *Introduction to Cyberdeception.* s.l. : Springer, Cham, 2010.
27. Jeremy Briffaut, Christian Toinard, Jean-Franc Lalande. A proposal for securing a large-scale high-interaction honeypot. *Workshop on Security and High Performance Computing Systems.* IEEE Computer Society, pp.206-212, 2008.
28. Li, Tian. Design and Implementation of a Distributed Intelligent Network Intrusion Detection System. *Department of Computer Science, New Mexico Tech, USA.* pp. 683-686, 2010.
29. Song, Takakura and Okabe. Cooperation of Intelligent Honeypots to Detect Unknown Malicious Codes. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing.* pp. 31-39., 2008.
30. http://k-oox.blogspot.com.es/2016/03/ids-sistemas-de-deteccion-de-intrusos.html. [Online]
31. http://www.adminso.es/index.php/IDS-Tipos_de_IDS. [Online]

32. Xin Yue, Wei Chen, Yantao Wang. The research of firewall technology in computer network security. *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA).* pp. 421-424., 2009.
33. Schaefer, Guenter. A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks. [book auth.] W. A. Halang. *Informatik aktuell.* 2005.
34. Kondra, J.R. Honeypot-Based Intrusion Detection System: A Performance Analysis. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).* pp. 1-8., 2016.
35. Leyi Shi, Lanlan Jiang, Deli Liu, and Xu Han. Mimicry Honeypot: A Brief Introduction. *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing.* pp. 1-4., 2012.
36. Yizhi Ren, Yang Xiang, Jingyu Hua, Ming Xu. Google hacking defence based on honey pages. *International Journal of Applied Mathematics and Statistics.* 51(22):284-292, 2013.
37. Simon Innes, Craig Valli. Honeypots: How do you know when you are inside one. *Edith Cowan University.* 2006.

Glosario

Honeypot	Herramienta dispuesta en una red o sistema con el fin de actuar de cebo ante un posible ataque informático.
Dirección IP	Número que identifica una interfaz de red de un dispositivo que utilice el Internet Protocol.
Pentesting	Práctica de atacar diversos entornos informáticos con la intención de descubrir vulnerabilidades para así prevenir posibles ataques externos.
SCADA	Supervisory Control And Data Acquisition.
Firewall	Elemento de una red diseñado para bloquear el acceso no autorizado.
Exploit	Secuencia de acciones o de datos que permiten explotar una vulnerabilidad.
Malware	Software malicioso.
Honeytoken	Técnica de marcado de documentos para que cualquier acceso a estos se considere un ataque.
Honeypage	Página web inaccesible por medios legítimos. Advierte al administrador en caso de que alguien llegue hasta ella.
Crawler	Software que recorre los enlaces de las páginas webs de forma automática para recopilar información.
Honeynet	Red de honeypots.
Honeyfarm	Sistema de redirección en una red hacia un honeypot.
SSH	Secure Shell Protocol.
SMTP	Simple Mail Transfer Protocol.
JSON	JavaScript Object Notation.
Query	Consulta a base de datos.
SQL Injection	Técnica por la cual se consigue información sobre una base de datos introduciendo queries en los formularios.
Footprinting	Técnica de recopilación de información pública sin vulnerar el sistema objetivo.
Nmap	Herramienta de escaneo de puertos.

SNMP	Protocolo simple de administración de red.
Zero-day	Ataque informático a un sistema con el objetivo de ejecutar código malicioso gracias al conocimiento de vulnerabilidades desconocidas por el fabricante del producto.

Anexos

A Manuales de la honeynet T-Pot

En este anexo se detallan las instrucciones para instalar, configurar, manejar y actualizar t-Pot en una máquina virtual. en el ordenador proporcionado por la UAM para realizar este proyecto.

A.1 Manual de instalación

Para instalar la honeynet t-Pot, el primer paso es descargar del repositorio https://github.com/dtag-dev-sec/t-Potce la imagen t-Pot.iso.

A continuación debemos crear una nueva máquina virtual en VirtualBox, configurándola de forma que tenga 4096 MB de RAM, y adjuntando un disco dvi de 64GB. Además, se debe cambiar el modo de red "NAT" a "Bridge". Después tan solo es necesario adjuntar la imagen descargada y añadírsela al controlador IDE.

Arrancar la máquina virtual, y seguir las instrucciones del instalador hasta que aparezca el mensaje "No se ha podido configurar el DHCP". Debemos configurar la red manualmente, dado que en el ordenador proporcionado para realizar este proyecto TFG no hay DHCP.

Cuando nos lo pida, introducimos la IP en la que deseamos que se aloje el honeypot reciba ataques, la máscara subred, el Gateway y el DNS.

En caso de que se instale en un ordenador que esté en una red con DHCP, tan solo hay que seguir los pasos del instalador en modo automático.

Tras finalizar la instalación, volverá a aparecer el menú de instalación. Se debe apagar la máquina, entrar en la configuración de VirtualBox y eliminar el archivo t-Pot.iso que añadimos anteriormente.

A.2 Manual de configuración

Una vez realizada la instalación base, se debe arrancar de nuevo la máquina. Para una configuración completa del honeypot, hay que elegir la opción "everything". Nos pedirá que introduzcamos la contraseña y el usuario con el que acceder en el panel de administración a los datos de los ataques realizados al honeypot.

El usuario para entrar en nuestro honeypot es "tsec". La contraseña, la primera que hayamos puesto en el paso anterior.
Para ser root se debe escribir 'sudo su –' e introducir la contraseña que se eligió previamente.

Para comprobar el estado de los honeypots levantados en la honeynet, se debe escribir el comando 'dps.sh'

A.3 Manual de utilización

A continuación podremos acceder a la información sobre los ataques recibidos con Kibanna introduciendo en el navegador la dirección IP del honeypot desde el puerto 64297:

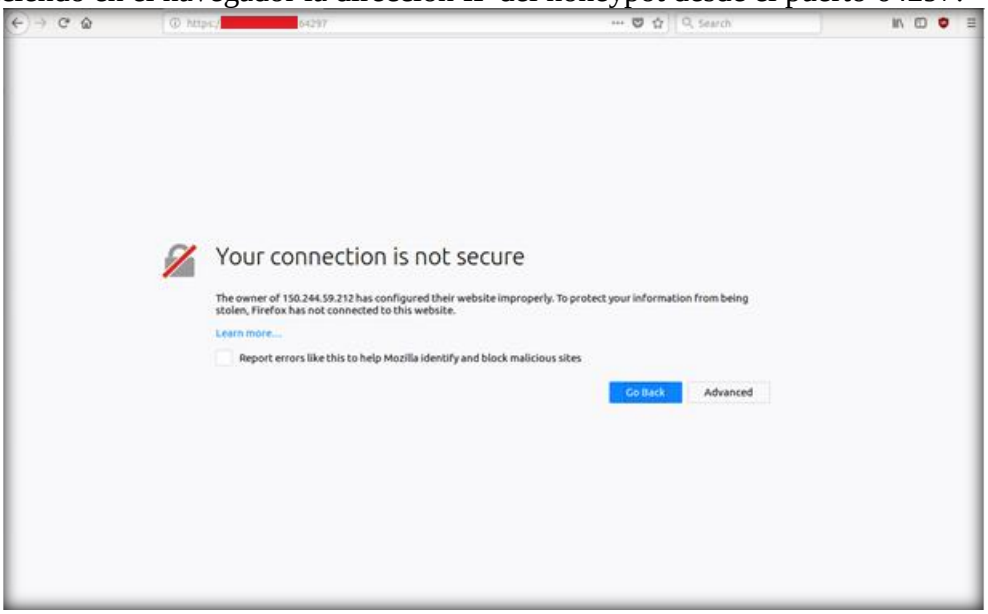


Figura A.0.1 Conexion insegura a la página de administración t-Pot

Debemos entrar en “Advanced” (Figura A.0.1) y seleccionar la opción de añadir excepción (Figura A.0.2), ya que el navegador lo detectará como un sitio no seguro.

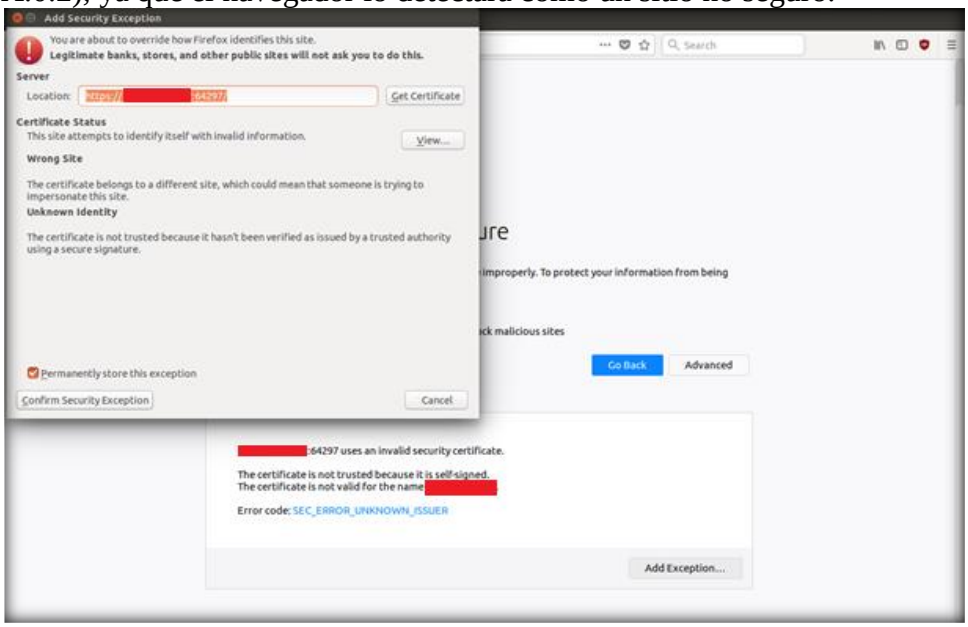


Figura A.0.2 Habilitar conexión insegura.

Tras esto nos pedirá un usuario y contraseña (Figura A.0.3). Deberá ser el que configuramos previamente.

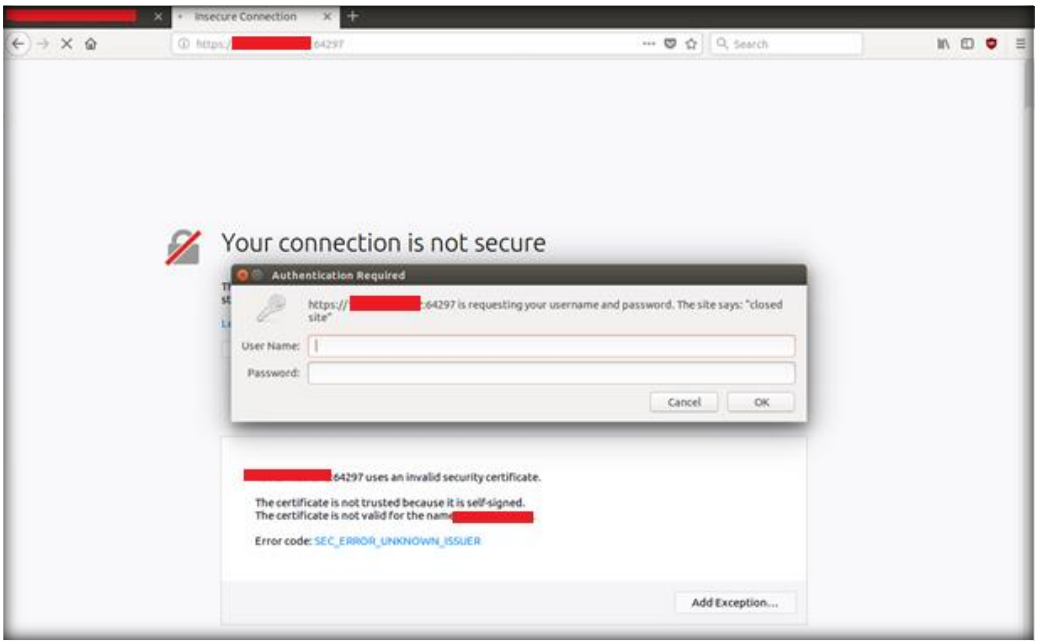


Figura A.0.3 Introducción de credenciales

Ya en Kibanna (Figura A.0.4), escogemos T-Pot, y tendremos gráficos de todos los ataques realizados.

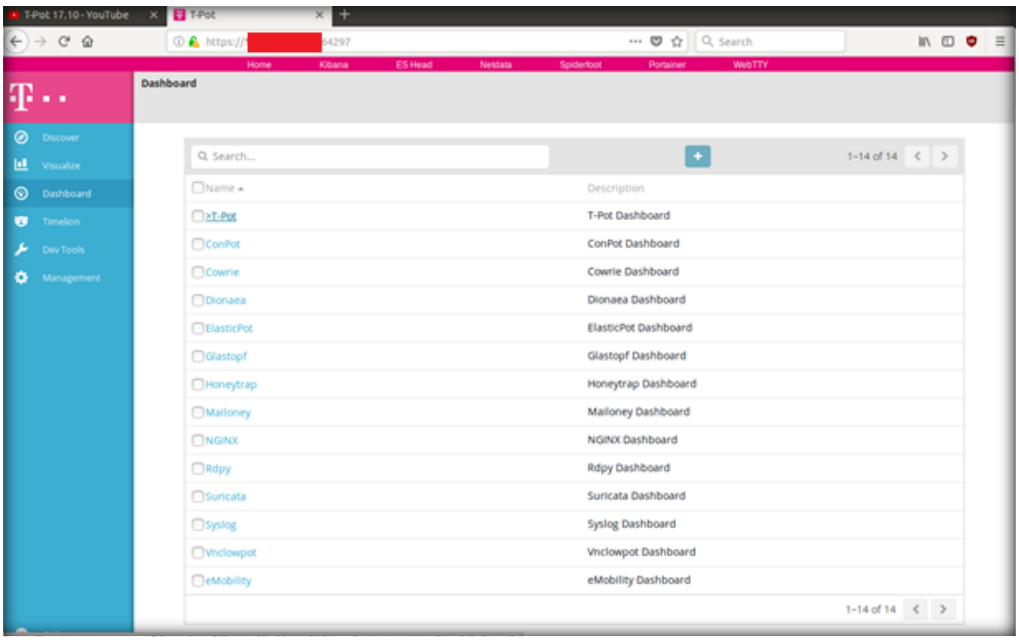


Figura A.0.40.4 Gestor de honeypots Kibanna

En la pestaña de la barra de opciones, a la derecha, podemos configurar el rango de tiempo en el que se muestran los ataques recibidos (Figura A.0.5).

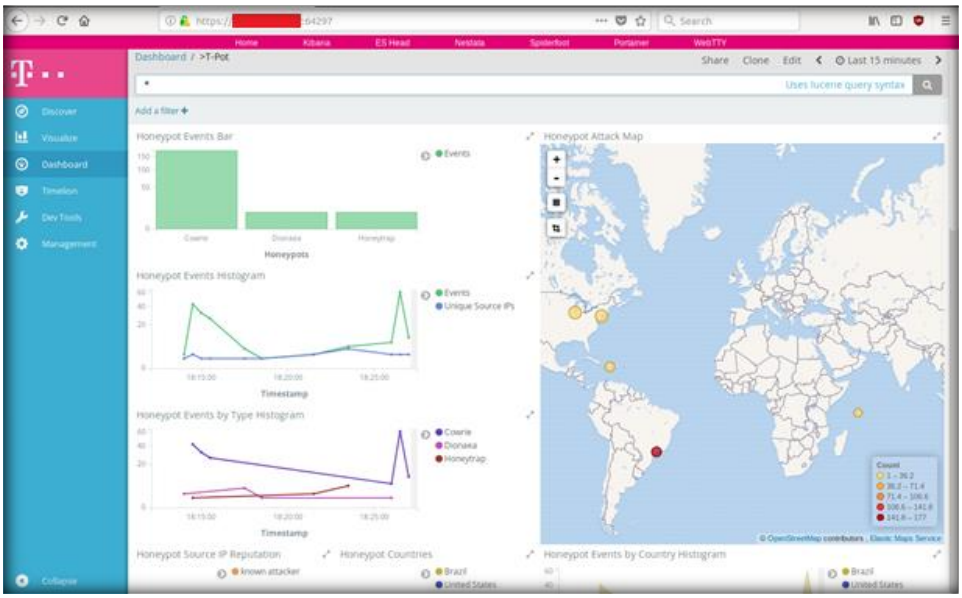


Figura A.0.5 Página web de administración de la honeynet

Si en vez de escoger T-Pot escogemos uno de los honeypots instalados, podremos ver los ataques específicos a ese honeypot (Figura A.0.6).

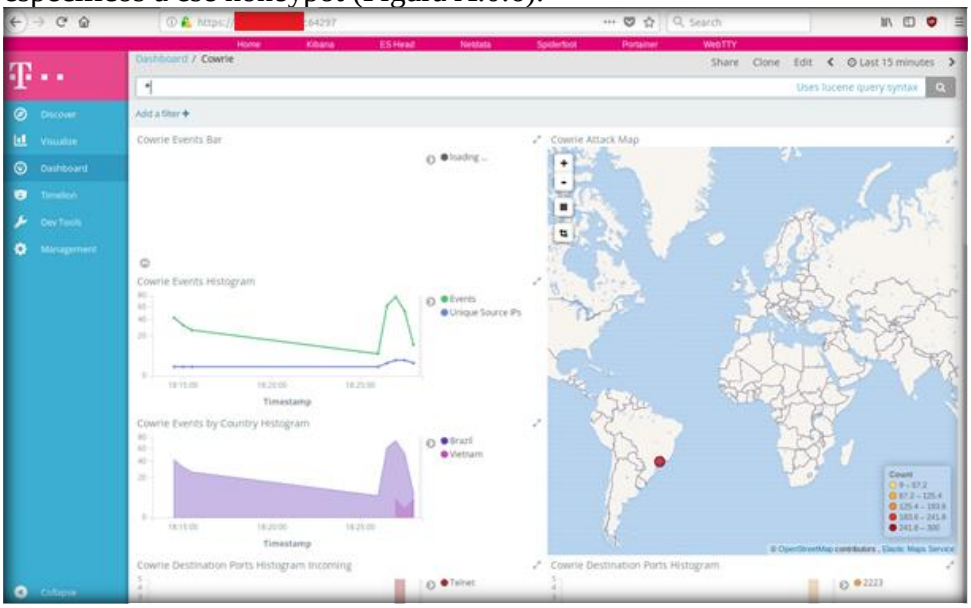


Figura A.0.6 Información del honeypot Cowrie

Si en la cabecera elegimos ES Head, entraremos en el buscador ElasticSearch, podremos comprobar todos los logs (Figura A.0.7).

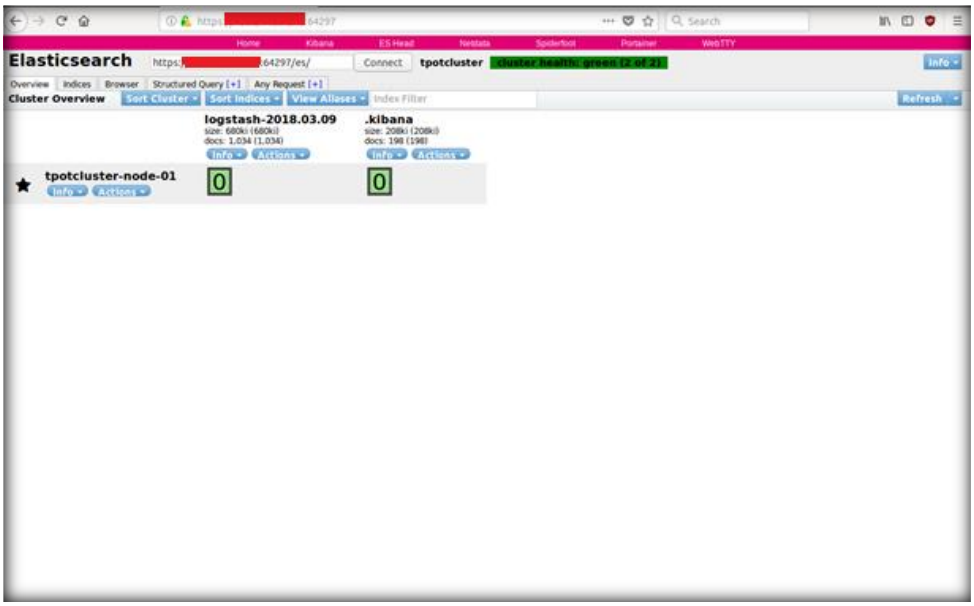


Figura A.0.7 Panel de control de ElasticSearch

Si elegimos Netdata, estaremos viendo la monitorización del honeypot, con información sobre la CPU, lectura y escritura, consumo de RAM, etc (Figura A.0.8).

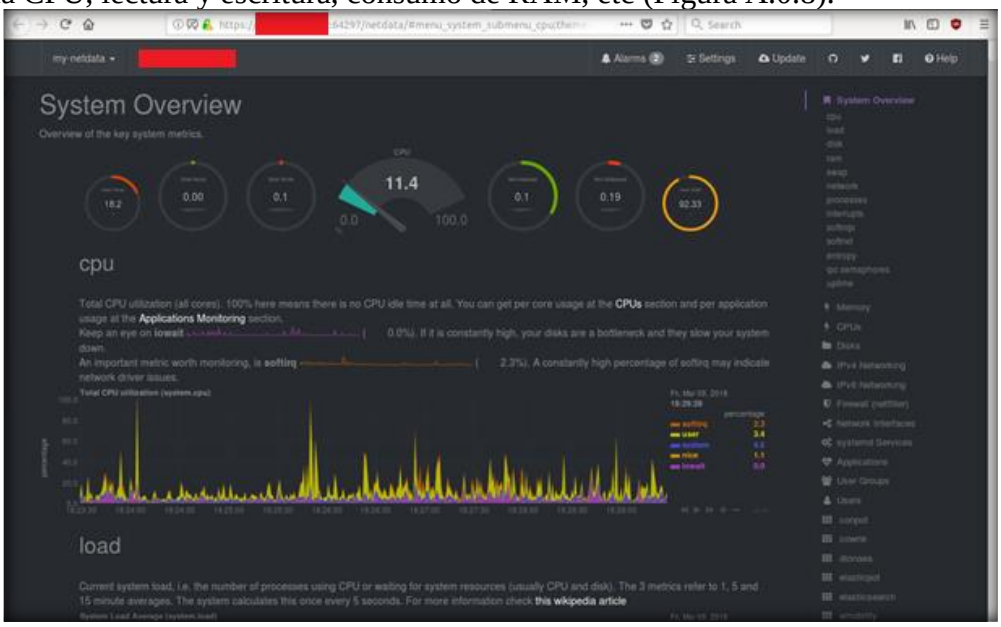


Figura A.0.8 Panel de control de Netdata

Si escogemos SpiderFoot, podremos realizar escaneos web (Figura A.0.9).

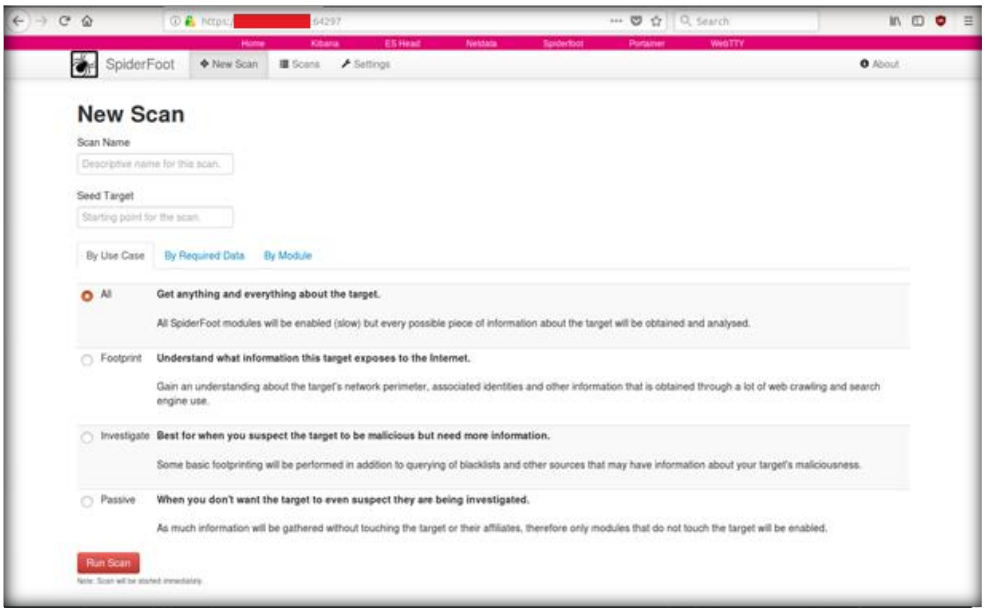


Figura A.0.9 Panel de control de SpiderFoot

En portainer podemos ver cada "contenedor" (cada honeypot) y la información relacionada con el mismo (si está activo, su IP, puertos abiertos...). Además podemos administrarlos, pararlos, apagarlos, etc (Figura A.0.10).

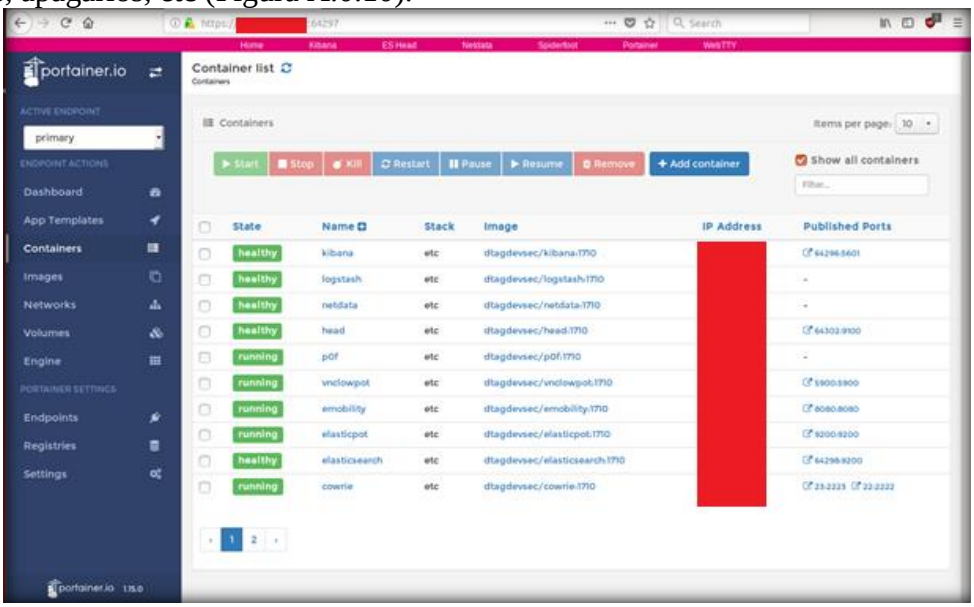


Figura A.0.10 Panel de control de Portainer

En WebTTY tenemos una consola de acceso al honeypot (Figura A.0.11).

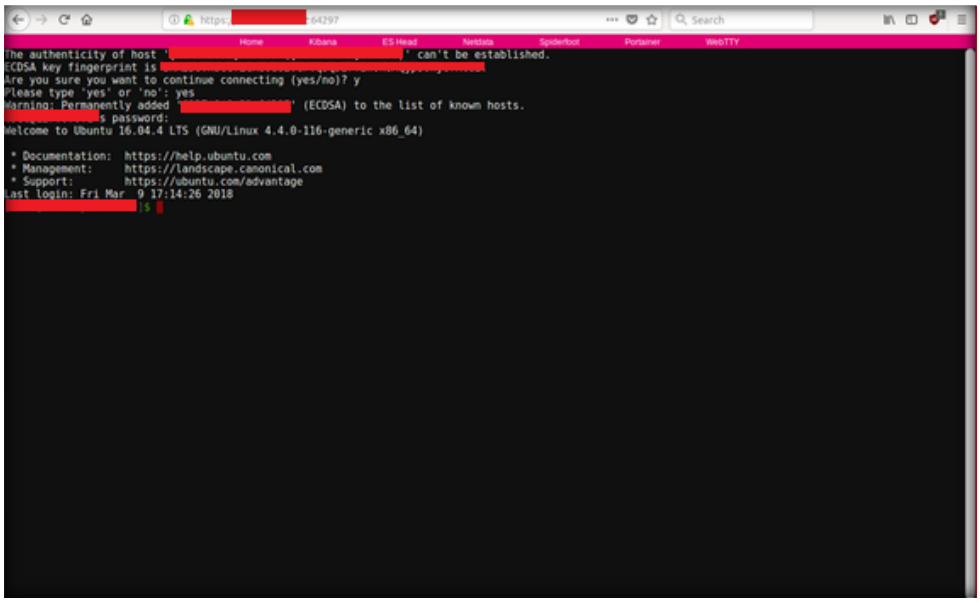


Figura A.0.11 Panel de control de WebTTY

A.4 Actualizaciones

Para actualizar cada honeypot tan solo hay que ejecutar los comandos:

```
$ cd /opt/t-Pot
$ ./update.sh -y
```

B Información relacionada sobre honeypots y Sistemas de Seguridad

En el anexo B se ofrece más información sobre los honeypots. En primer lugar se hace una comparación entre los honeypots y otros sistemas de seguridad como los firewalls o los IDS. Además, se analiza la estructura de los honeypots, su funcionalidad, los distintos sitios donde se pueden ubicar y la clasificación de estos por nivel de interacción, por medio y por propósito.

B.1 Sistemas de seguridad

En este apartado se describen con más detalle los tres sistemas de seguridad que han sido mencionados anteriormente y que más relación tienen con este Trabajo de Fin de Grado, para poder tener una comparativa clara del rol que adquieren los honeypots en el mundo de la seguridad.

(1) Intrusion Detection Systems (IDS)

Los IDS son sistemas de detección de intrusos cuya funcionalidad es observar y detectar cualquier comportamiento sospechoso de la red en la que se encuentra, para poder alertar del mismo. Al igual que un antivirus, se ocupa de detectar patrones que coincidan con su base de datos y hayan sido clasificados como maliciosos (30).

Hay tres tipos según el lugar donde se instalen:

- HIDS (Sistema de Detección de Intrusos de Host). Este IDS comprueba la información de la red de un solo host. Debe haber, por tanto, uno por cada host a monitorizar.
- NIDS (Sistema de Detección de Intrusos de Red). Se coloca en segmentos de red, de forma que con un único IDS se detecten los comportamientos anómalos de todos los equipos conectados a la red. Su comportamiento es el de un sniffer, pues leen todo el tráfico que pasa por la red, y lo clasifican según ciertas reglas.
- DIDS (Sistema de Detección de Intrusos Distribuido). Se trata de un IDS con sensores en distintos puntos de la red que recogen información y envían alertas a un sistema descentralizado (31).

Los principales problemas de los IDS son los siguientes:

- Generan un gran porcentaje de falsos positivos.
- Al leer todo el tráfico de la red reduce considerablemente la velocidad de esta.
- Si se utiliza un switch, el IDS no podrá obtener todo el tráfico de la red. Si se sitúa en el Gateway, el IDS no podrá rastrear y evitar ataques internos.
- Son inútiles ante el tráfico cifrado.
- No pueden detectar nuevos tipos de ataque, pues se basan en patrones ya almacenados previamente en su base de datos.
- No son escalables.

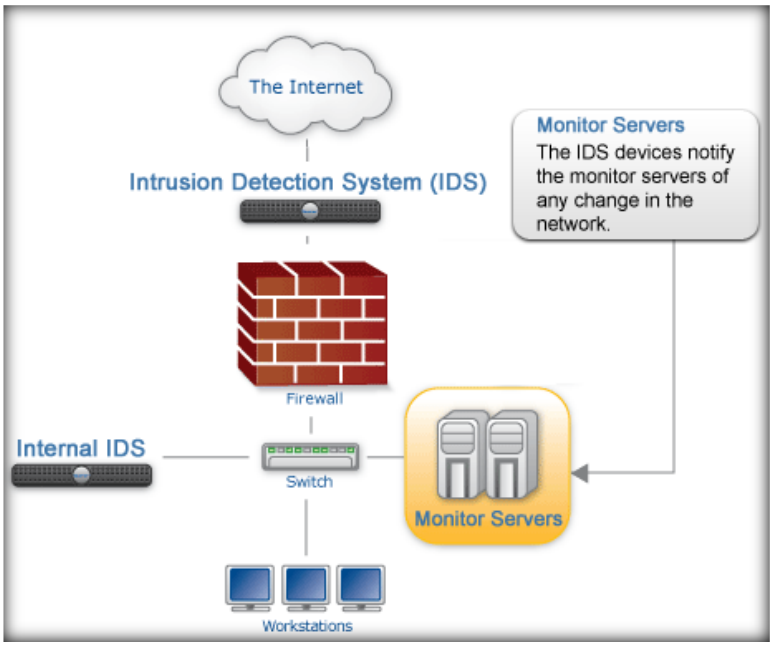


Figura B.0.12 Esquema de la arquitectura de un IDS. – Fuente: https://www.fwhibbit.es

(2) Firewalls

Los firewalls son dispositivos que bloquean o permiten el paso del tráfico según una serie de reglas definidas. Estas reglas pueden venir dadas por el tipo de servicio que se solicita, la dirección IP desde donde se envía, etc.
Los firewalls conforman una barrera entre una red interna segura e Internet (32). Este modo de encapsulación se ha utilizado en las redes de todo el mundo durante décadas, sin embargo tiene graves problemas que se listan a continuación:

- Un firewall no puede proteger de ataques generados en la red interna del sistema.
- No detecta programas maliciosos.
- Puede ser sobrepasado por un exceso de carga en el sistema, en cuyo caso se satura y deja pasar libremente todo el tráfico que no pueda manejar.

Se puede observar una arquitectura con firewall e IDS en la Figura B.0.12

(3) Honeypots

La gran ventaja de los honeypots es que cubren las debilidades de los IDS y los Firewall.
Dado que todo movimiento que ocurra en un honeypot es considerado un ataque, no genera falsos positivos, como ocurre con los IDS.
Además, cada ataque realizado es capturado, por lo que se pueden investigar y detectar nuevos ataques nunca vistos hasta ahora, incluso aunque estén cifrados.
Y por último, son fácilmente escalables y de muy bajo coste.

B.2 Estructura de los honeypots

A continuación se muestran los distintos elementos que conforman un honeypot (33).

- **Honeypot Production System:** es el sistema falso que los atacantes van a tratar de manipular. Debe aparentar ser un sistema real, y contener datos que interesen al atacante.
- **Firewall**: genera los logs de cada movimiento que realice el atacante para tratar de acceder al honeypot.
- **Monitoring Unit:** realiza el seguimiento de cada atacante, capturando toda secuencia de comandos, ficheros modificados, etc. Esto puede ser un IDS, por ejemplo.
- **Logging Unit:** almacena los logs generados por el Firewall y el Monitoring Unit.
- **Alert Unit:** crea alertas que advierten al administrador de que un atacante está intentando explotar alguna supuesta vulnerabilidad del honeypot en ese momento.

B.3 Funcionalidad de los honeypots

Las principales funciones de un sistema señuelo o honeypot son:

- Obtener información sobre métodos de ataque novedosos, tipos de malware desconocidos, información sobre los atacantes...
- Detectar ataque zero-day, esto es, ataques en los que se aprovecha una vulnerabilidad que es desconocida para el fabricante y para el público en general.
- Entretener al atacante, haciéndole perder el tiempo y distrayendo su atención, para evitar que ataque el sistema principal. De esta forma se consigue que el atacante cese en su empeño de vulnerar la máquina, al descubrir que es un honeypot, o el tiempo suficiente para reaccionar contra el mismo y desplegar las medidas necesarias para defender el sistema.

B.4 Ubicación de los honeypots

Como los honeypots pueden recibir tanto ataques externos como internos, la ubicación es uno de los puntos clave de las características del honeypot. Hay varias zonas posibles donde colocar el honeypot dentro de una red. Dependiendo del uso que se le quiera dar y el fin de este, deberemos estudiar cada lugar para colocarlo en el entorno que maximice su efectividad y beneficie las estadísticas que deseemos potenciar, como el número de ataques o los tipos. A continuación se describen detalladamente las posibles opciones.

(1) Antes del Firewall

El honeypot está completamente expuesto a Internet, lo que permite que efectúe el máximo número de ataques sin ningún tipo de filtro (Figura B.0.13).
De esta forma se pueden realizar mediciones sobre el número de ataques que llegan a la red donde se aloja el honeypot desde otra red externa.

Sin embargo, el inconveniente de colocar un honeypot antes del firewall es que no se reciben los posibles ataques internos de la red. Por ello hemos estimado que la medición de los mismos es un factor importante en nuestra investigación. Para llevarlo a cabo se colocará una honeynet antes del firewall y otra después.

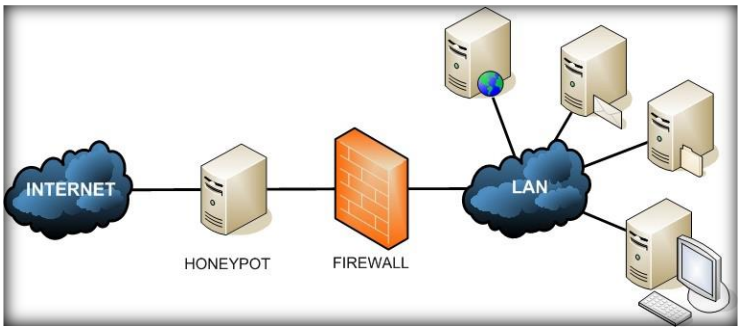


Figura B.0.13 Honeypot ubicado antes del firewall – Fuente: https://www.fwhibbit.es

https://www.fwhibbit.es/deceptionpi-estudiando-a-los-atacantes-mediante-sistemas-señuelo

Una de las honeynets de este proyecto se colocará antes del firewall.

(2) Después del Firewall

El honeypot está detrás de un firewall, dentro de nuestra red (Figura B.0.14). De esta forma, el honeypot es capaz de analizar y recibir ataques internos. Dado que el firewall filtra la mayoría de las amenazas conocidas, el honeypot no recopila tanta información del exterior como en el caso anterior.

Estos honeypots no son recomendables para investigación si se quiere analizar cualquier ataque externo, sin embargo son muy útiles en caso de una investigación interna o para detectar configuraciones inadecuadas del firewall.

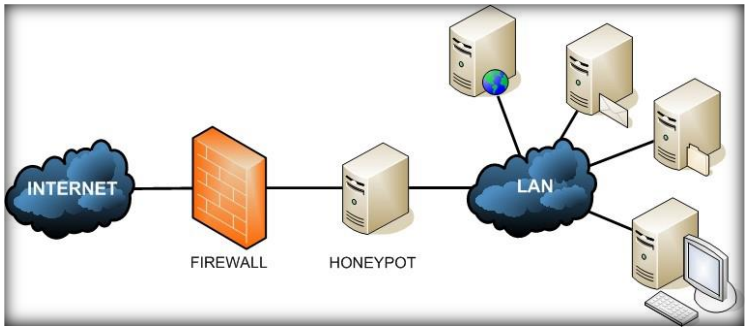


Figura B.0.14 Honeypot ubicado dentro del firewall - Fuente: https://www.fwhibbit.es

Una de las honeynets del proyecto se desplegará después del firewall.

(3) En una zona desmilitarizada

Una zona desmilitarizada (DMZ) o red perimetral es una zona que se encuentra entre la red interna y la externa (Internet). Su función es permitir las conexiones desde la red interna y la externa a la DMZ, pero que las conexiones desde la DMZ solo se producen hacia la red externa, evitando que una máquina situada en esta zona pueda comunicarse con la red interna (Figura B.0.15).

Situar un honeypot en una DMZ es una idea interesante si nuestra red cuenta con un IDS, ya que de esta forma evitamos que las alertas que se generan en el IDS no se vean intensificadas por el tráfico en el honeypot, al estar fuera de su alcance.

Sin embargo, el inconveniente de colocar un honeypot en esta zona es que se pierde la ventaja de los honeypots de poder recibir ataques internos.

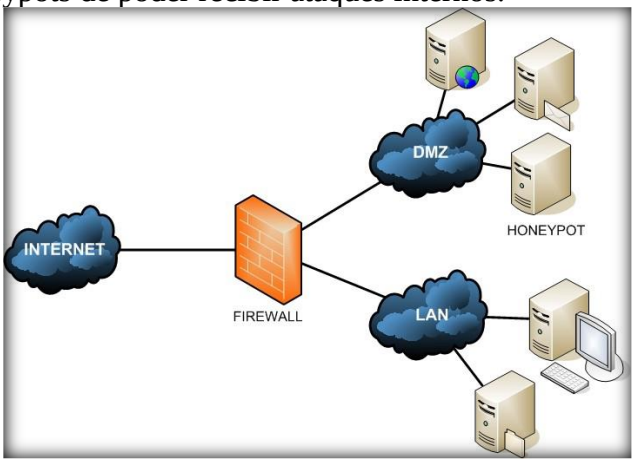


Figura B.0.15 Honeypot en DMZ - Fuente: https://www.fwhibbit.es

B.5 Clasificación de los honeypots

Existen diversas formas de clasificar los honeypots: según el nivel de interacción con el atacante, según su propósito, según el hardware o software en el que se desplieguen, según el papel que asumen… A continuación se muestra una explicación detallada de las distintas clasificaciones.

(1) Clasificación por nivel de interacción

(a) Honeypots de baja interacción

Apenas hay interacción con el atacante. Simulan servicios y protocolos frecuentes que tienen vulnerabilidades comunes. Tienen una estructura sencilla y son fáciles de mantener. Están por encima del sistema operativo, por lo que un atacante no podría en ningún caso llegar a la máquina real (34).

Su ventaja es la sencillez de uso e instalación, pero tienen grandes limitaciones, puesto que en general no posee todas las herramientas y comandos del sistema operativo que simula, con lo que un atacante podría descubrir fácilmente que se trata de un sistema trampa. Su uso más frecuente es para detectar las direcciones IPs de donde vienen los ataques que reciben.

Se deben utilizar cuando no tengamos muchos recursos y no queramos arriesgarnos a utilizar otro tipo de honeypot. Lo usaremos con el objetivo de identificar escaneos y ataques automatizados, así como para entretener a los atacantes, puesto que mientras estén ocupados con este tipo de honeypots, no atacarán el sistema real.

(b) Honeypots de media interacción

Son honeypots híbridos, una mezcla entre los honeypots de baja interacción y los honeypots de alta interacción. Están por encima del sistema operativo al igual que los honeypots de baja interacción, y no implementan todos los entresijos de los protocolos que simulan.

Sin embargo permiten opciones de configuración muy avanzadas, aunque son más complicadas de instalar. Son capaces de dar respuestas específicas según lo que el atacante pida para tratar de mantenerle el máximo tiempo posible dentro del sistema trampa.
Cabe destacar que es complicado discernir la diferencia entre esta clase de honeypots y los de baja interacción. Durante la investigación de este trabajo se han encontrado referencias distintas al mismo honeypot describiéndolo en unos casos como baja interacción y en otros como media.

Se utilizan cuando el riesgo de tener un honeypot de este tipo en la red es asumible. Su objetivo principal es atrapar a aquellos atacantes que utilizan herramientas complejas de ataque, distrayéndolos de atacar a los documentos que son realmente importantes.

(c) Honeypots de alta interacción

Son máquinas reales que se han instalado con el único propósito de ser atacadas. Al ser sistemas reales, son realmente complicados de detectar, dado que la única trampa visible es que todos los datos que contienen son falsos. Permiten obtener absolutamente toda la información sobre cada paso que da el atacante.

Son los más útiles dado que pueden detectar ataques de zero-day, pero a la vez los más peligrosos, ya que cabe la posibilidad de que el atacante obtenga información sobre el resto del sistema e incluso realice pivoting a otra máquina real y acabe finalmente haciéndose con el sistema.

Para evitar esto se debe colocar el honeypot en una zona desmilitarizada, con un Firewall entre las maquinas reales y el honeypot que impida cualquier fuga de información.

Al tener un alto coste de mantenimiento y ser altamente inseguros, no se utilizarán en este proyecto honeypots de alta interacción.

Se deben utilizar cuando necesitemos observar y monitorizar el comportamiento en tiempo real de cada atacante dentro del sistema, como ayuda al análisis forense.

(2) Clasificación por medio

(a) Honeypots software

Son honeypots que se encuentran dentro de una sola máquina física, mediante algún tipo de servicio de virtualización que emula un sistema real. De esa forma se pueden desplegar varios honeypots con distintas IP desde una sola máquina.

(b) Honeypots hardware

Son máquinas físicas reales que están destinadas a servir como sistemas trampa. Están limitados a una sola dirección IP y requieren de un gasto mayor. Normalmente son sistemas dedicados únicamente a honeypots de alta interacción.

(3) Clasificación por propósito

(a) Honeypots de investigación

Han sido creados para recopilar todas las técnicas de ataque. Por ello tratan de ser interesantes para los atacantes, puesto que de esa forma se recibe el máximo número de ataques posible, y hay más posibilidades de descubrir ataques nuevos nunca vistos hasta ahora. Es una herramienta muy útil para la informática forense, aunque su uso no está muy extendido en el campo de la investigación al considerarse en muchos casos muy arriesgado y costoso.

Así mismo, son los honeypots que más necesitan la ocultación, ya que en cualquier otro caso un atacante experto detectará fácilmente que se encuentra ante una máquina trampa y la razón de ser del honeypot se verá comprometida.
Todos los honeypots de este proyecto pertenecen a esta clase de honeypots.

(b) Honeypots de producción

Su principal función es la distracción. Se colocan en entornos de producción reales, para que si un atacante consigue entrar en ellos, se entretenga con el sistema trampa mientras se avisa al administrador y éste toma las medidas adecuadas para frenar el ataque al sistema real antes de que se produzca.
Aunque no es tan importante como en los de investigación, la correcta ocultación de estos honeypots también es muy importante ya que se necesita que el cebo tenga mucha información que aparentemente sea atractiva para el atacante, y de esa forma aguante el máximo tiempo posible dentro del sistema trampa.

(4) Clasificación por tipo de ocultación.

En cuanto a ocultación, podemos encontrar dos tipos de mimetización en una red honeypot (35):

(a) Protective coloration

Los honeypots se asemejan al hardware, software, datos e información de servicio de los servidores de su entorno. De esa forma son difíciles de detectar por los atacantes, y pueden registrar y estudiar la información de los intrusos.

(b) Warning coloration

Los servidores se asemejan al hardware, software y datos de los honeypots de su red. De esta forma un intruso los tomará por honeypots y pasará de largo sin atacarlos.
El problema principal de esto es que son fácilmente detectables, ya que es muy complicado realizar esta mimetización y reaccionan de forma distinta a un sistema real (29).

C Programación de la herramienta

En este anexo se describe la arquitectura de la herramienta, el pseudocódigo de las funciones principales y los diagramas de flujo de estas.

C.1 Estructura del proyecto

El proyecto se ha dividido en diferentes subcarpetas para permitir gran modularización, de forma que sea muy sencillo añadir nuevos tests que permitan detectar más tipos de honeypots.

A continuación se muestra un esquema de la estructura del proyecto.

HoneyCatch: directorio raíz del proyecto.

- **bash:** directorio que contiene los scripts de test en bash.
  - **cowrie_test01.sh**: test de comprobación de usuarios
  - **cowrie_test02.sh**: test de comprobación de creación de ficheros.
  - **cowrie_test03.sh**: test de comprobación de comandos.
  - **cowrie_test04.sh:** test de comprobación de directorios.
- **files**: directorio con archivos externos
  - **scripts-nmap**: scripts externos de Nmap para comprobaciones de Dionaea.
  - **bash_output:** ficheros de salida de los scripts en bash.
  - **html_pages**: páginas html descargadas de Glastopf.
  - **results**: ficheros de salida de los scripts en Python.
- **includes**: archivos de cabecera en C.
  - **deep_detection.h:** archivo con las cabeceras de las funciones de deep_detection.c
  - **modos.h:** archivo con las cabeceras de las funciones de modos.c
  - **port_comprobation.h:** archivo con las cabeceras de las funciones de port_comprobation.c
  - **sockets.h:** archivo con las cabeceras de las funciones de sockets.c
  - **types.h:** archivo con las cabeceras de las funciones de types.c
- **obj:** directorio con los archivos .o creados durante la compilación del programa.
- **python**: directorio que contiene los scripts de test en Python.
  - **conpot_test.py**: script en Python con los test de ConPot.
  - **cowrie_test.py:** script en Python con los test de
  - **decision_tree.py**: script en Python con la lógica del árbol de decisión necesario para el cálculo de la probabilidad de que exista un honeypot en base a los resultados de los tests.
  - **dionaea_test.py**: script en Python con los test de Dionaea.
  - **glastopf_test.py:** script en Python con los test de Glastopf.
- **src:** directorio con los archivos de código fuente.
  - **deep_detection.c:** fichero que contiene las llamadas a funciones que comprueban la detección individual de cada honeypot.
  - **main.c**: fichero principal, desde él se llama al resto de funciones. Hace las comprobaciones de los programas instalados.
  - **modos.c:** fichero que contiene las funciones necesarias para ejecutar el programa en distintos modos, según los programas instalados en el ordenador.
  - **port_comprobation.c:** realiza la primera fase del análisis, detectando posibles honeypots en función de los puertos abiertos escaneados.

- **sockets.c:** contiene las funciones necesarias para comunicarse con la dirección IP, y de esa forma averiguar qué puertos tiene abiertos, en caso de que no esté instalado Nmap.
- **types.c:** contiene las definiciones y utilidades necesarias para el correcto funcionamiento del resto de la aplicación.

C.2 Pseudocódigo y diagramas de flujo

A continuación, se describe brevemente las funciones principales de la herramienta, acompañado del diagrama de flujo correspondiente. Esta arquitectura se ha diseñado especialmente para ser modular y poder incorporar muy fácilmente nuevos tipos de scripts de detección en cualquier lenguaje de programación.

(1) Main

Función principal del programa, se encarga de ejecutar el resto de funciones. Podemos ver el pseudocódigo de esta función en la Figura C.0.16 y el diagrama de flujo de la misma en la Figura C.0.17.

```
1  ----------
2  - main() -
3  ----------
4
5  crearCabecera()
6  obtenerIP (IP)
7
8  si nmap instalado:
9      modoAutomático(IP)
10 en otro caso:
11     modoManual(IP)
12
13 comprobarPuertos(lista de puertos, lista de honeypots)
14 comprobaciónProfunda(lista de honeypots, IP)
15
16 mostrar resultados
```

Figura C.0.16 Pseudocódigo función main.

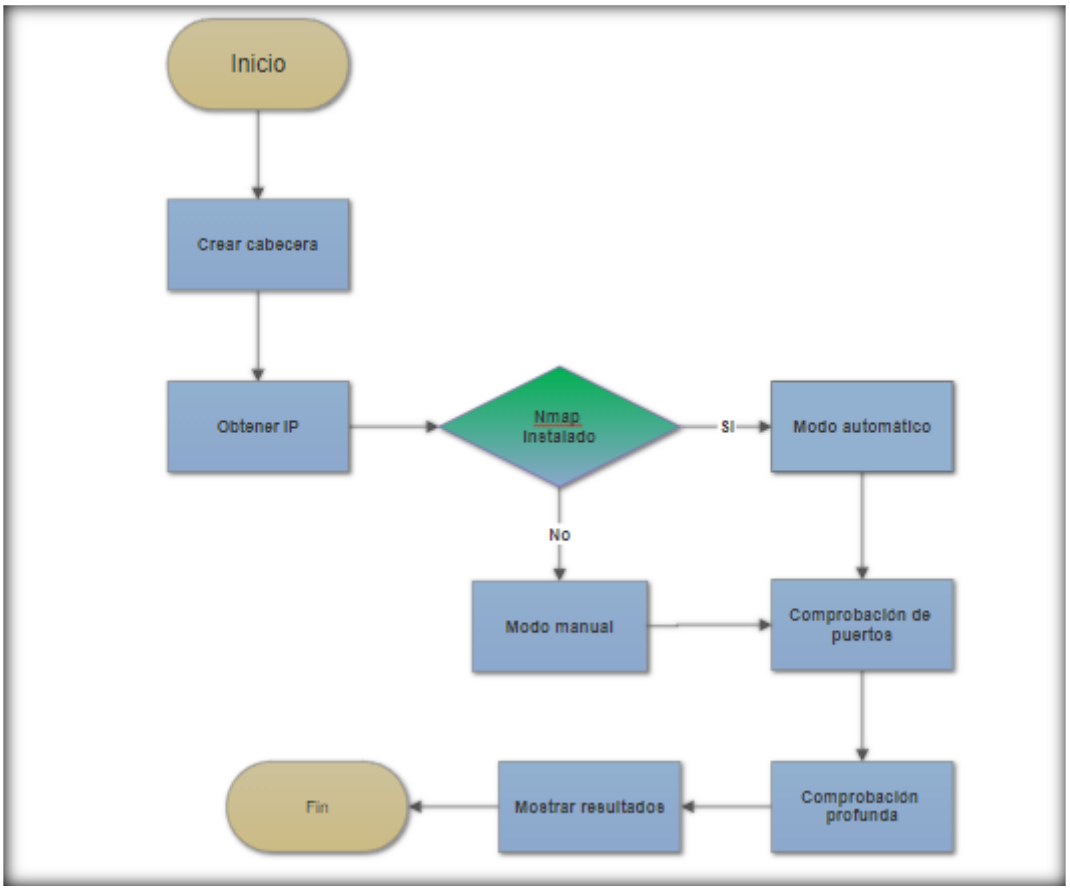


Figura C.0.17 Diagrama de flujo de función main

(2) Modo manual

Función del programa encargada de realizar la comprobación de puertos en caso de que Nmap no esté instalado. Podemos ver el pseudocódigo de esta función en la Figura C.0.18 y el diagrama de flujo de la misma en la Figura C.0.19

```
1  ------------------------------------
2  - modo_manual(IP, lista de puertos) -
3  ------------------------------------
4
5  abrirSocketsTCP()
6  server = obtenerHost(IP)
7
8  si server no existe:
9      Mensaje de error
10
11 para cada puerto de la lista:
12     conectarSocket(socket, server, puerto)
13
14     si conexion con exito:
15         puerto abierto
16     en otro caso:
17         puerto cerrado
18
19 cerrarSocket(socket)
```

Figura C.0.18 Pseudocódigo función modo_manual

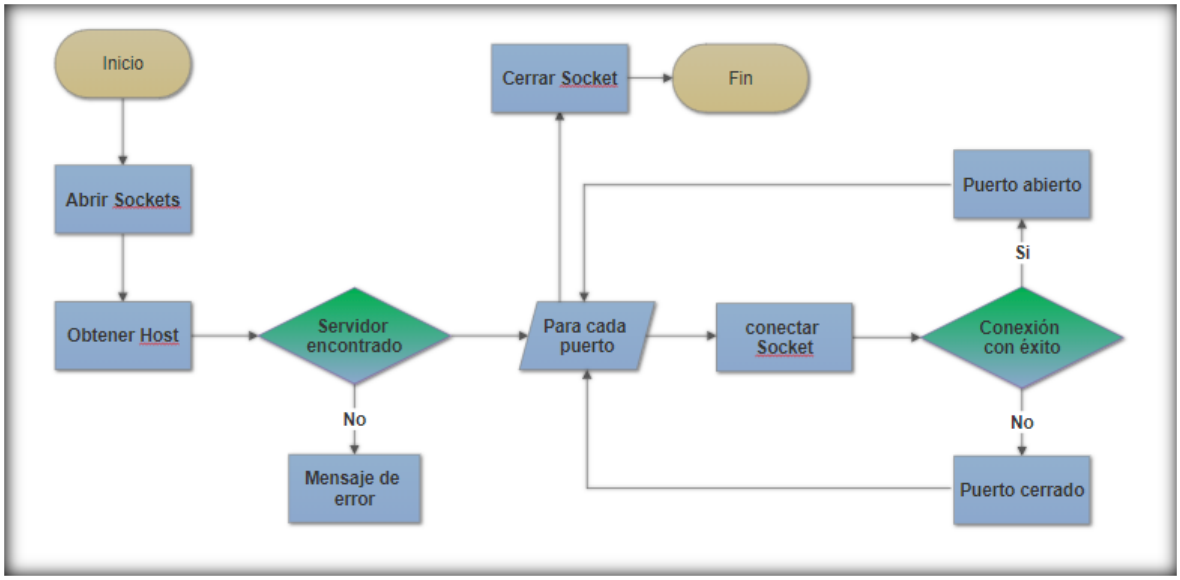


Figura C.0.19 Diagrama de flujo de función modo_manual

(3) Modo automático

Esta función es similar a la función anterior, pero utiliza nmap para el escaneo de puertos. Podemos ver el pseudocódigo de esta función en la Figura C.0.20 y el diagrama de flujo de la misma en la Figura C.0.21.

```
1   ------------------------------------
2   - modo_automatico(IP) -
3   ------------------------------------
4
5   nmap(IP) -> nmap.out
6
7   abrir nmap.out
8
9   por cada puerto encontrado:
10      añadir a lista de puertos abiertos (puerto)
11
12  cerrar nmap.out
```

Figura C.0.20 Pseudocódigo de función modo_automático

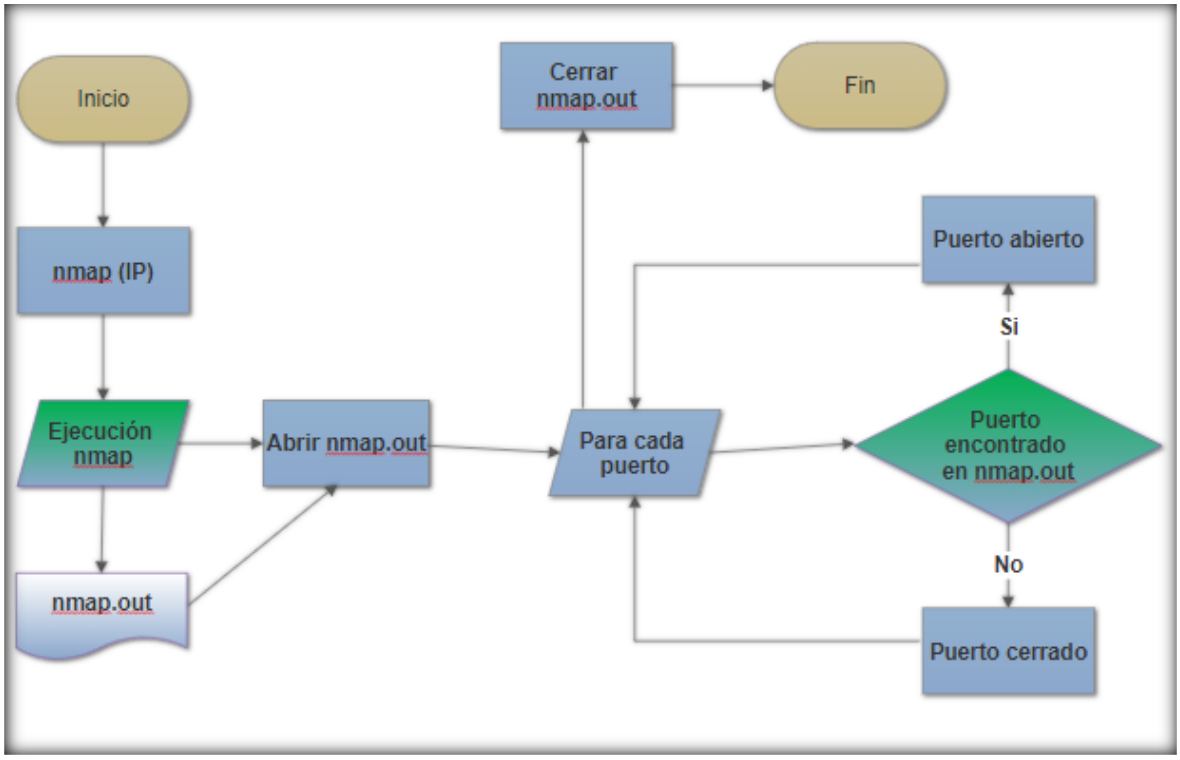


Figura C.0.21 Diagrama de flujo de función modo_automatico

(4) Comprobación de puertos

Tras realizar el escaneo de puertos, esta función se encarga de determinar qué honeypots puede haber en función de los puertos abiertos. Podemos ver el pseudocódigo de esta función en la Figura C.0.22 y el diagrama de flujo de la misma en la Figura C.0.23

```
1   ------------------------------------------------------------
2   - port_comprobation(lista de puertos, lista de honeypots) -
3   ------------------------------------------------------------
4
5   lista_pa = lista de puertos abiertos en la IP
6
7
8   por cada honeypot:
9       puertos_comunes = 0
10      lista_hp = puertos abiertos por defecto del honeypot
11
12      por cada puerto de lista_hp:
13          si puerto está en lista_pa:
14              puertos_comunes++
15          en otro caso:
16              continuar
17      si puertos_comunes != 0:
18          posible honeypot
19      en otro caso:
20          honeypot descartado
21
```

Figura C.0.22 Pseudocódigo de la función port_comprobation

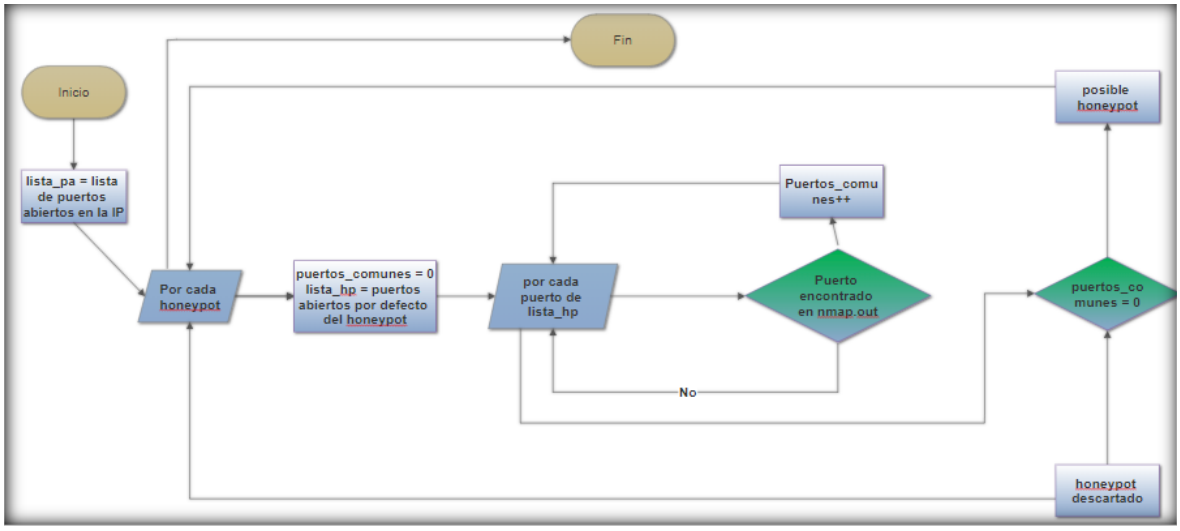


Figura C.0.23 Diagrama de flujo de función port_comprobation

(5) Comprobación profunda

Por último, esta función analiza cada honeypot que haya devuelto la función anterior individualmente, aplicando tests específicos para averiguar si la IP introducida aloja un honeypot de ese tipo. Podemos ver el pseudocódigo de esta función en la Figura C.0.24 y el diagrama de flujo de la misma en la Figura C.0.25.

```
1   ------------------------------------------------------------
2   - deep_test(lista de honeypots no descartados, IP) -
3   ------------------------------------------------------------
4
5   por cada honeypot no descartado:
6       por cada función de detección de ese honeypot:
7           detectar_honeypot()
8
9           si honeypot detectado:
10              escribir éxito en resultados.out
11          en otro caso:
12              escribir fracaso en resultados.out
```

Figura C.0.24 Pseudocódigo de función deep_test

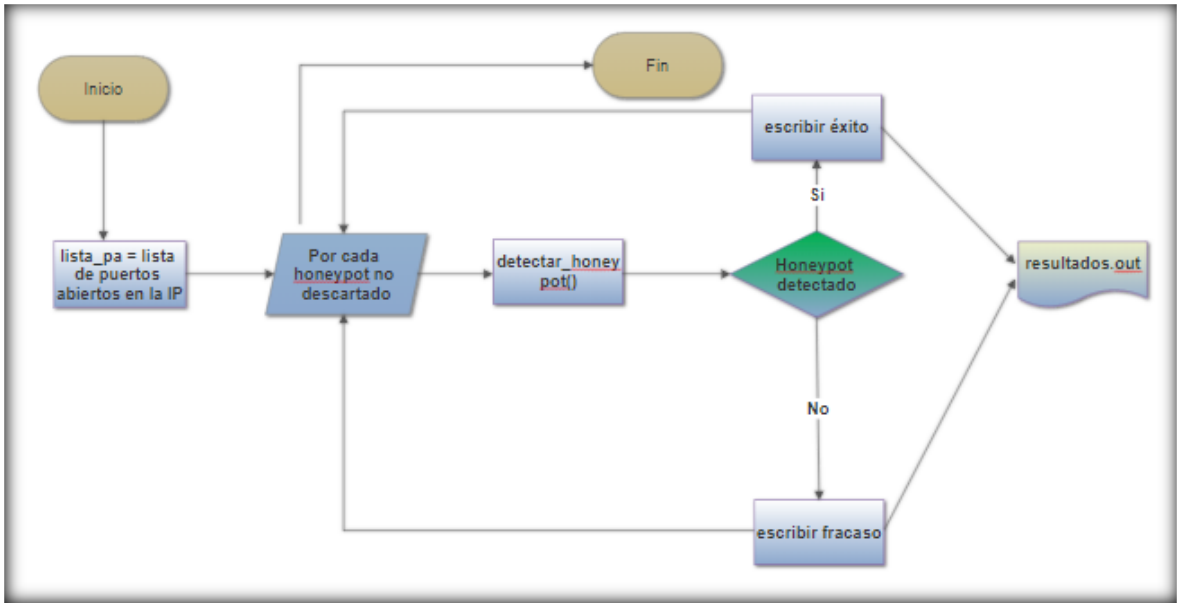


Figura C.0.25 Diagrama de flujo de función deep_test

D Formas de detectar un honeypot

La cantidad de información que podemos obtener de los atacantes depende de cómo son de realistas los honeypots.
Para realizar un estudio profundo de los distintos métodos de ocultación de honeypots, se realizan pruebas utilizadas en el pentesting de sistemas reales. Con estas pruebas, se puede crear un conjunto de pautas para determinar la existencia de un honeypot.

A continuación se listan algunas de las herramientas que se emplean comúnmente para la detección de honeypots:

- **Shodan**: Es un motor de búsqueda que permite encontrar routers, servidores, etc. conectados a Internet, ofreciendo varios tipos de filtros distintos, así como otorgar información que proviene de los metadatos que el servidor envía cuando un cliente hace una petición. Se puede obtener una explicación más detallada del mismo en el Estado del Arte de este documento.
- **Nmap**: Esta potente herramienta permite realizar escaneos de puertos para averiguar qué servicios o servidores tiene abiertos una red informática.
- **FOCA**: Es una herramienta para encontrar metadatos y otra información no visible a primera vista de un conjunto de documentos.

Seguidamente se describen una serie de técnicas que pueden utilizar los atacantes para detectar diferentes tipos de honeypots. Muchas de estas comprobaciones se han añadido a la herramienta de detección de honeypots desarrollada en este proyecto.

- **Averiguar la página de administración para ver los resultados de los ataques registrados:** Los honeypots poseen una página de administración que permite ver los registros de cada ataque realizado hasta el momento de una forma gráfica. Las páginas de administración de honeypots suelen contener métodos para comprobar los ataques realizados, modificar la configuración del honeypot y analizar toda la información obtenida (Figura D.0.26 y Figura D.0.27). Esto es muy útil para los administradores, pero todo atacante que conozca este sistema de administración puede dirigirse a esa página y comprobar que efectivamente se trata de un honeypot. Además, podría obtener información sensible e incluso llegar a averiguar cómo penetrar en el sistema real que hay detrás del honeypot.

Figura D.0.26 Ejemplo: página de administración del honeypot Kippo – Fuente: https://bruteforcelab.com

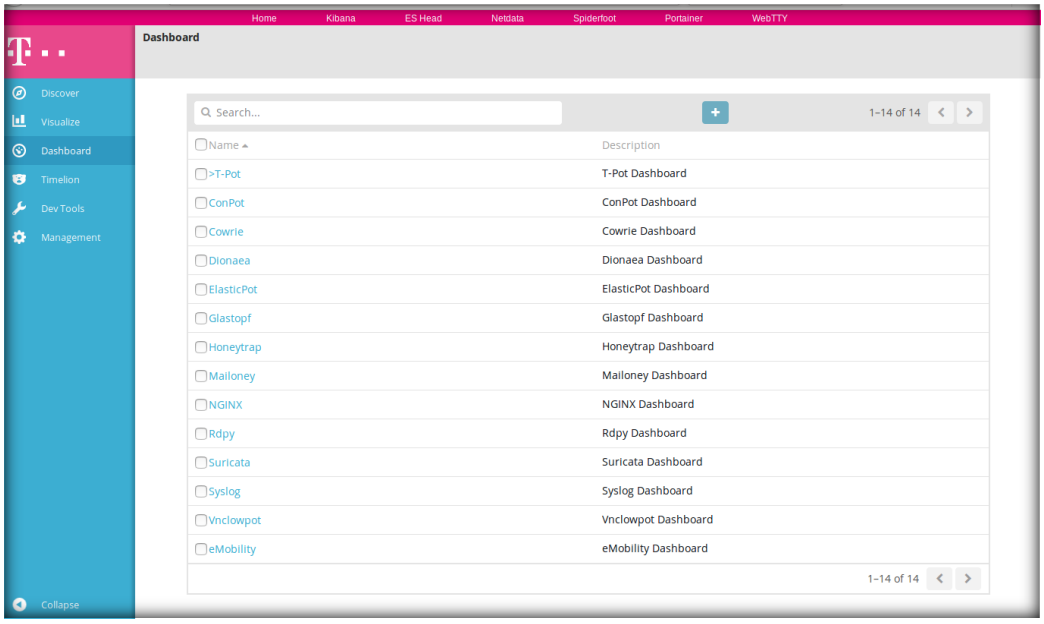


Figura D.0.27 Ejemplo: página de administración de la honeynet T-Pot

Otra manera de averiguar información sobre el honeypot es **el ataque "inside".** Si un atacante logra penetrar en la máquina trampa, averiguando la contraseña mediante un ataque de fuerza bruta, tras conseguir tener acceso a la máquina el atacante comprobará si la misma es real o es un señuelo. La forma que tiene de hacer esto un atacante es examinar a fondo todo el sistema, con distintas técnicas explicadas a continuación.

Comprobación de usuario: lo que ocurre normalmente en algunos honeypots es que si el atacante consigue conectarse mediante ssh con, por ejemplo, usuario "root", el honeypot

muestra el usuario “webserver”, con la idea de engañar al atacante haciéndole creer que está en un servidor web. O “ubuntu” para que parezca que está en una distribución de Linux.

Lo que ocurre en el t-Pot es que tras conectarnos por ssh vemos que en home hay un solo directorio con un usuario llamado “richard” (Figura D.0.28). Este es un usuario por defecto con un nombre común en los honeypots, por tanto se modificó este directorio y se añadieron nuevos usuarios para que pareciera un sistema real:

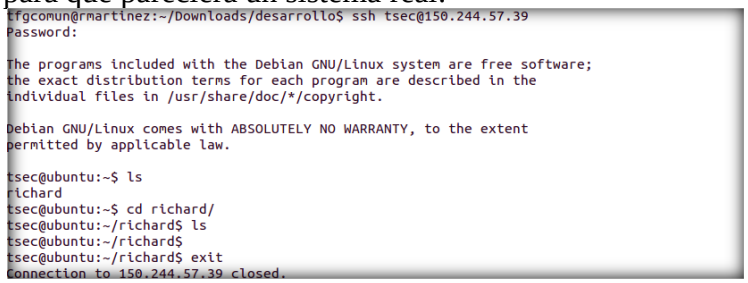


Figura D.0.28 Comprobación de usuarios en t-Pot

Comprobación de comandos: hay ciertos comandos implementados en todas las distribuciones Linux que los honeypots no tienen instalados. Una de las técnicas más utilizadas es realizar una batería de comandos básicos (sudo, reset, ln, grep, apt-get remove/update/upgrade, chown) para comprobar si están todos instalados.
Por ejemplo, podemos observar que en t-Pot no está instalado el comando man, o el comando useradd (Figura D.0.30 y Figura D.0.31).
En t-Pot lo que ocurre es que si tratas de hacer un ‘sudo’, se escribe dos veces el usuario en la terminal (Figura D.0.29).

Figura D.0.29 Izquierda, salida al ejecutar instrucción sudo en sistema ubuntu real. Derecha, salida al ejecutar instrucción sudo en honeypot.

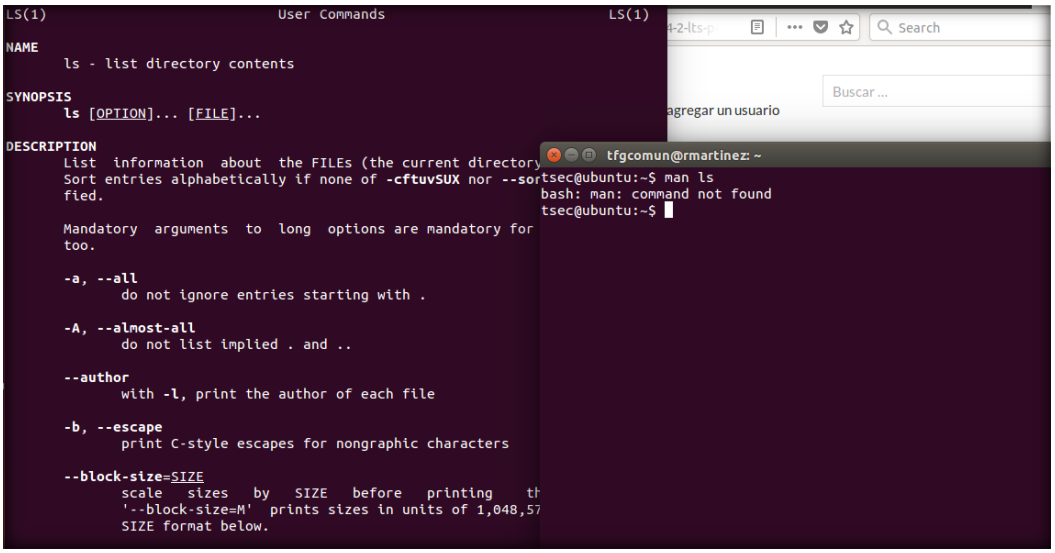


Figura D.0.30 Izquierda: comando "man ls" en un sistema real. Derecha: comando "man ls" en un honeypot.

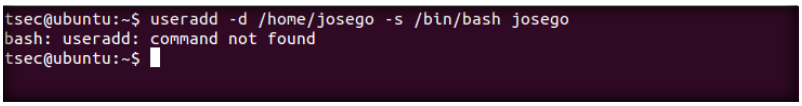


Figura D.0.31 Comprobación de comando "useradd" en honeypot.

Estos son comportamientos extraños que deben alertarnos.

Comprobación de directorios: otra técnica usual en los atacantes es comprobar los directorios que hay en el sistema que ha vulnerado, y los archivos que contienen los mismos. Si hay muchas carpetas y las mismas están distribuidas tal y como lo está un sistema real, entonces el atacante no sospechará.

- El directorio home debe contener a varios usuarios del sistema. Es común que en los honeypots haya un solo directorio con un usuario por defecto llamado "richard" vacío. Encontrar esto para un atacante es una gran señal de alerta.
- En el directorio usr están las utilidades y aplicaciones de usuario. En algunos honeypots se ha detectado que la estructura en que están dispuestas las subcarpetas es diferente a la de un sistema real.
- En el directorio var se guardan los comandos y archivos temporales ejecutados.

Detección por chroot: en algunos honeypots se puede detectar que los números de inodo no son los esperados en un directorio raíz real. (ls -ialgG) .

Otra forma de detectar que nos encontramos en un honeypot es analizando el tráfico de la red. En la mayoría de las organizaciones en las que se coloca un honeypot como defensa ante ataques, este se coloca de forma que ante la sospecha de cualquier anomalía, todo el tráfico se redirija al honeypot.

Por ello, si al atacar una determinada IP se analiza el tráfico con WireShark (Figura D.0.32) o cualquier otro sniffer de red (incluso el comando 'traceroute' puede darnos información) y se descubre que está dirigiendo el tráfico de red a otro sitio sin haberlo solicitado el usuario, es muy probable que estemos ante un caso de honeyfarm (descrito en el Estado del Arte de este documento).
Para este caso es muy interesante analizar las políticas del gateway para descubrir en el SNMP posibles redirecciones.

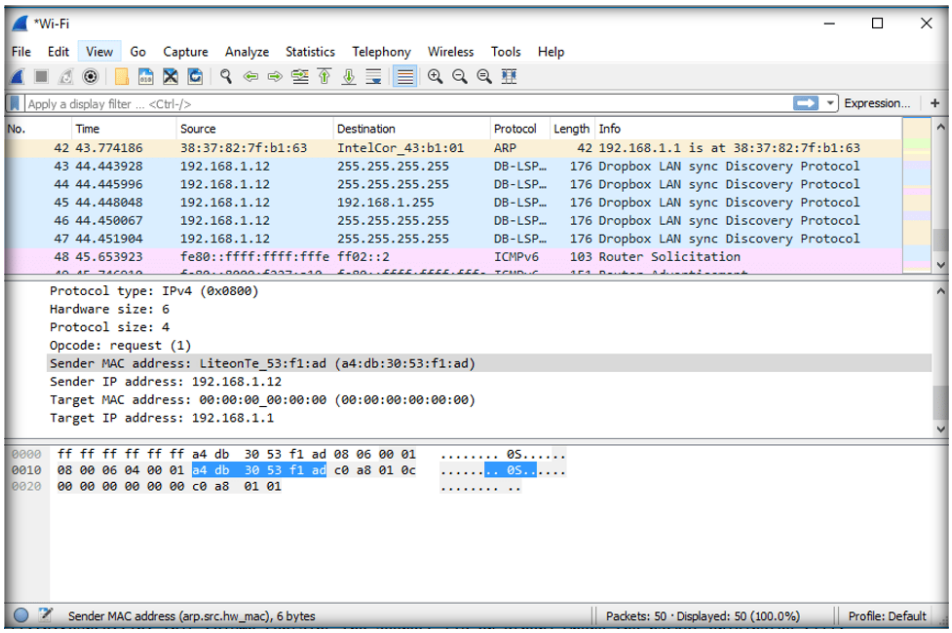


Figura D.0.32 Ejemplo de uso herramienta Wireshark – Fuente: www.lifewire.com

En la herramienta creada no se ha implementado esta comprobación, ya que las honeynets que se han instalado en la Universidad Autónoma de Madrid no se colocaron como honeyfarms, con lo que no fue posible realizar las pruebas necesarias para añadir este test a la herramienta.

Para la detección de honeytokens y honeypages se puede utilizar la herramienta FOCA. Estos elementos se han incorporado en los últimos años en muchos servidores web, como defensa ante gusanos cuyo objetivo son las páginas que pueden contener vulnerabilidades de aplicaciones web.
(36)
Estos marcadores son indetectables a simple vista, pero en los metadatos de los archivos o en el código fuente se pueden encontrar mediante el uso de FOCA (Figura D.0.33).

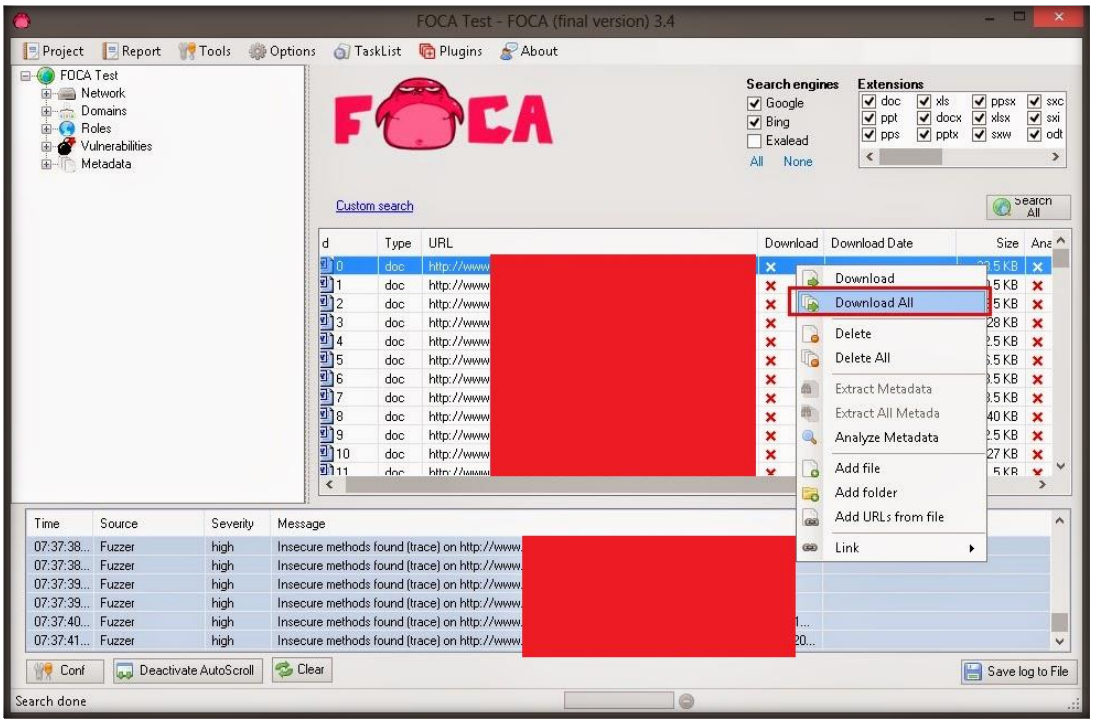


Figura D.0.33 Ejemplo de ejecución FOCA – Fuente: http://p01n7l355.blogspot.com

No se ha implementado el uso de FOCA en la herramienta debido a que requiere de numerosas acciones manuales difíciles de ejecutar en un programa automático. Además, es más complicado ver patrones claros en estos tipos de marcadores.

La última forma que se expone en este documento de comprobar si estamos ante un honeypot es realizar un gran conjunto de peticiones y medir los tiempos de respuesta. A continuación, se compara con el tiempo de respuesta de algún sistema de características parecidas al que sospechamos que tiene un honeypot. Si hay una gran diferencia de latencia, es posible que se deba a que no es lo mismo la latencia de un servidor web donde se ejecuta un sistema real a la de un honeypot de baja interacción que tan solo ejecuta un sistema virtualizado.
Este método no serviría para los honeypot hardware. Sin embargo, la mayoría de honeypots de la red son software, dado el caro mantenimiento y el riesgo que suponen los honeypots hardware (37).

E Análisis detallado de cada honeypot

En el anexo E se realiza un análisis detallado de toda la información recogida por los distintos honeypots, en la honeynet colocada delante del firewall y en la colocada después. Además, en cada caso se analizan las diferencias (en caso de que existan) de los ataques recibidos antes y después de la ocultación.

E.1 Honeynet A

En este apartado se muestran los resultados obtenidos tras la recogida de datos en la honeynet A, que se encuentra fuera del firewall de la Universidad Autónoma de Madrid.

(1) ConPot

A continuación se analizan los resultados del honeypot ConPot, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.34 Mapa de ataque de honeypot ConPot.

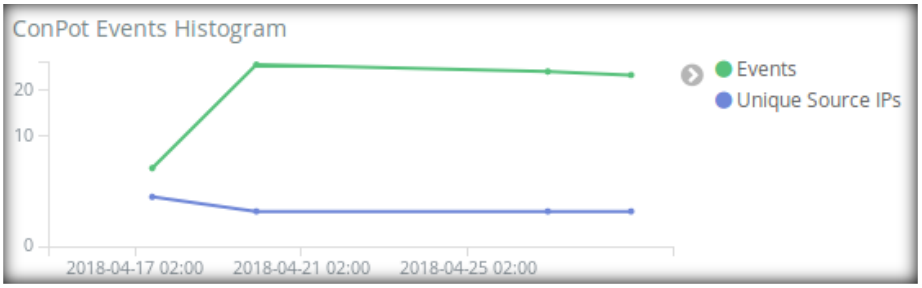


Figura E.0.35 Histograma de ataques de honeypot ConPot.

En este intervalo de tiempo solo hubo 4 ataques procedentes de distintas IPs, haciendo en torno a 25 ataques por IP (Figura E.0.35).

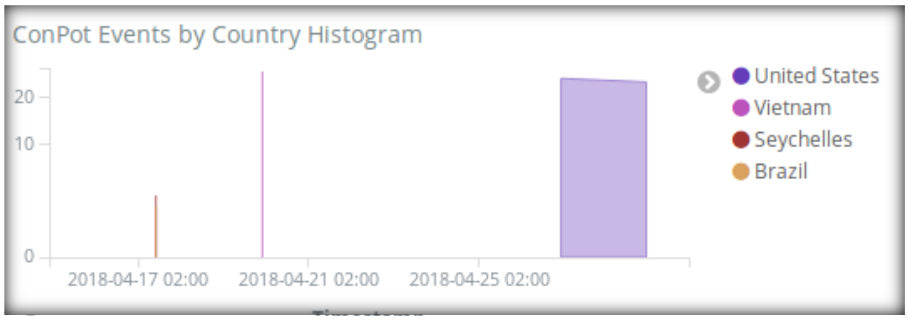


Figura E.0.36 Histograma de ataques por país de honeypot ConPot.

La duración de los ataques fue mucho mayor en Estados Unidos que en el resto de los países (Figura E.0.36).

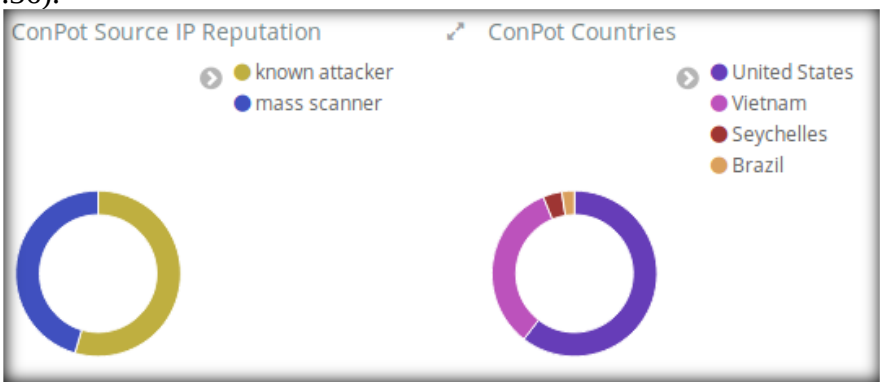


Figura E.0.37 Reputación de las IPs atacantes de honeypot ConPot.

La mitad de los ataques vinieron de IPs de atacantes conocidos, la otra mitad de bots de escaneo masivo. Los países que más atacaron fueron Estados Unidos y Vietnam (Figura E.0.34 y Figura E.0.37).

En la Tabla E.0.1 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
CHT Company Ltd	27
SingleHop, Inc.	25
Linode, LLC	24
Flokinet Ltd	3
CLARO S.A.	2

Tabla E.0.1 Proveedores de las IPs atacantes en ConPot.

Tras analizar los logs, se ha realizado una lista de los inputs más introducidos y las respuestas más frecuentes. Puede consultarse en la Tabla E.0.2 y en la Tabla E.0.3.

Input	Nº veces encontrado
010001	2
010002	2
01000d	2
01000e	2
01041e	2
01041f	2
010420	2
010434	2
010435	2
010436	2

Tabla E.0.2 Inputs introducidos por atacantes de honeypot ConPot.

Respuesta	Nº veces encontrado
? Command not found. Send 'H' for help.	6
403f10000202044100000000b23f	2
403f10000e020444000000001b7fdf0d	2
403f10041e21020000e4f8240d	2
403f10041f21020000e5ada50d	2
403f10042021020000e0178f0d	2
403f100434220442000001ff45220d	2
403f10043522044200001a6c92d0d	2
403f100436220442000009064fc0d	2
403f10043816024303e8fbd50d	2

Tabla E.0.3 Respuestas a comandos introducidos en el honeypot ConPot.

(b) Después de la ocultación

Figura E.0.38 Mapa de ataque de honeypot ConPot.

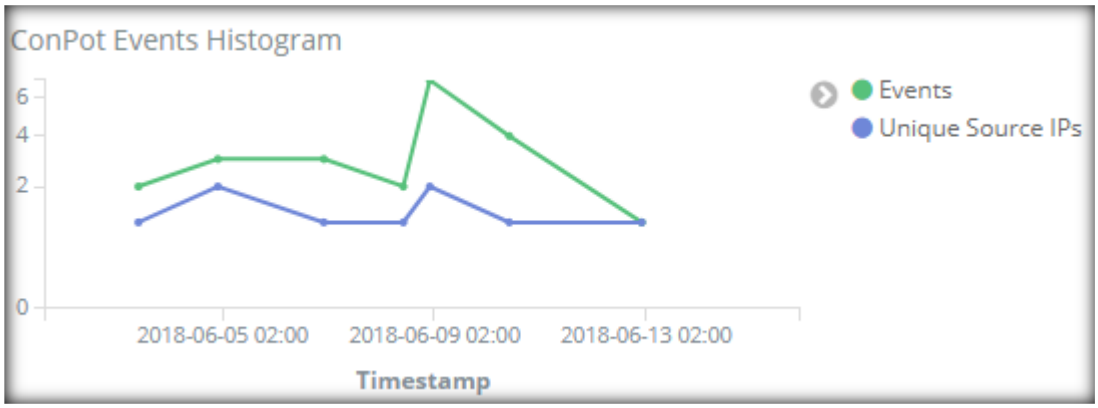


Figura 0.39 Histograma de ataques de honeypot ConPot.

Tras la ocultación el número de ataques de este honeypot se mantuvo prácticamente imperturbable (Figura E.0.38).

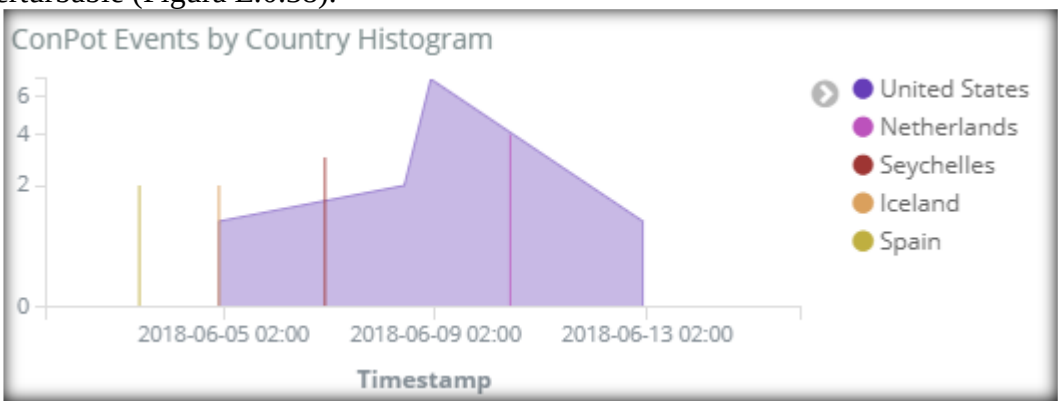


Figura 0.40 Histograma de ataques por país de honeypot ConPot.

Igualmente, la duración de los ataques fue mucho mayor en Estados Unidos que en el resto de los países (Figura 0.40).

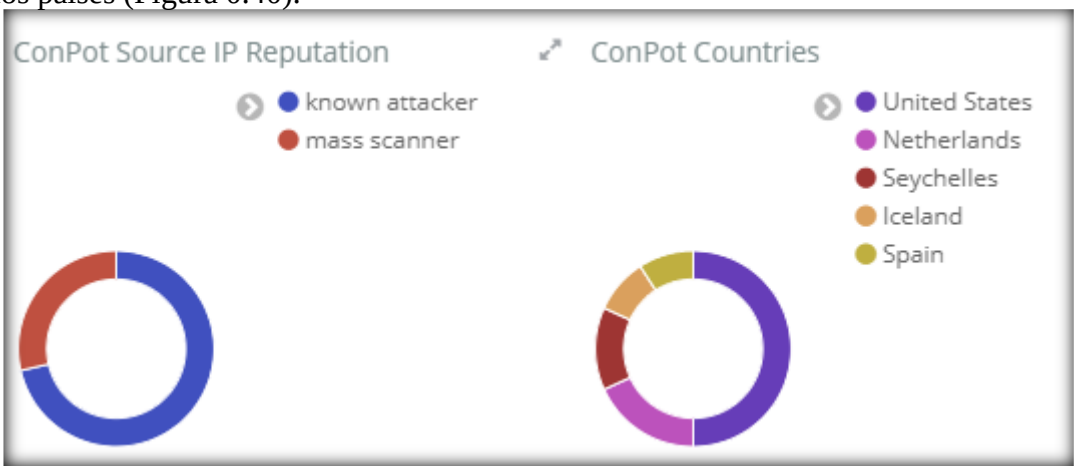


Figura E.0.41 Reputación de las IPs atacantes de honeypot ConPot.

La mayoría de los ataques vinieron de IPs de atacantes conocidos y el resto de bots de escaneo masivo. Los países que más atacaron fueron Estados Unidos y Países Bajos (Figura E.0.38 y Figura E.0.41).

En la Tabla E.0.4 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
VolumeDrive	6
Hostmaster, Ltd.	4
Quasi Networks LTD.	3
LeaseWeb Netherlands B.V.	3
Telefonica De Espana	2

Tabla E.0.4 Proveedores de las IPs atacantes en ConPot.

Tras analizar los logs, se ha obtenido un único input con código "010001" y la respuesta "403f10000102044100011adbdbd40d".

(2) Cowrie

Resultados del honeypot Cowrie, antes y después de la ocultación.

(a) Antes de la ocultación

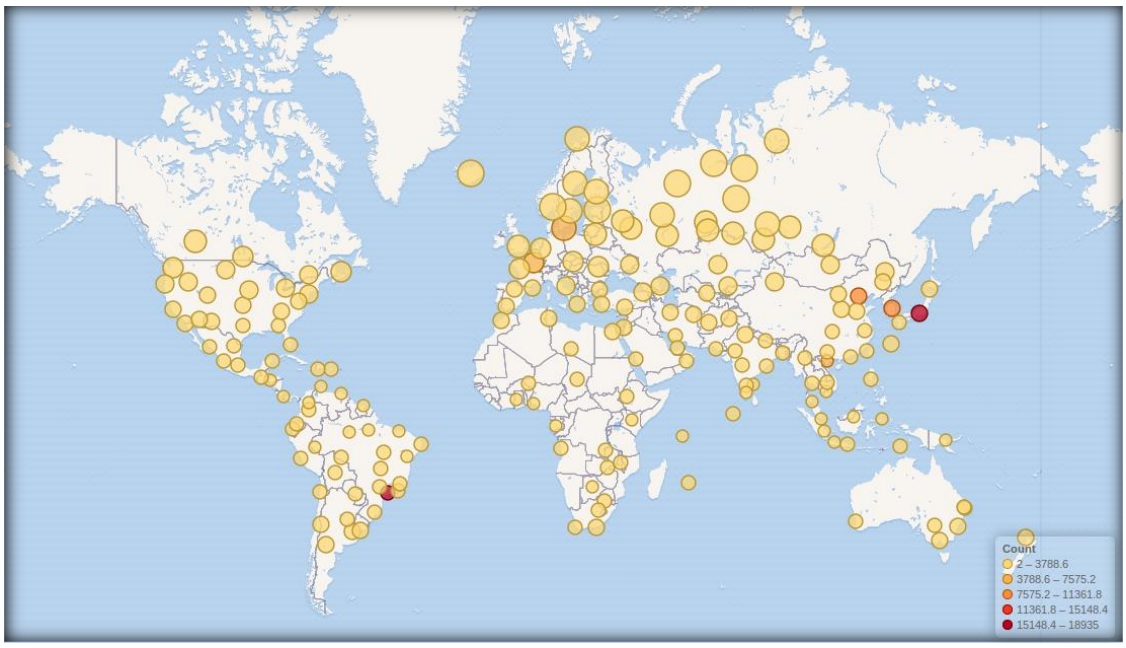


Figura E.0.42 Mapa de ataque de honeypot Cowrie

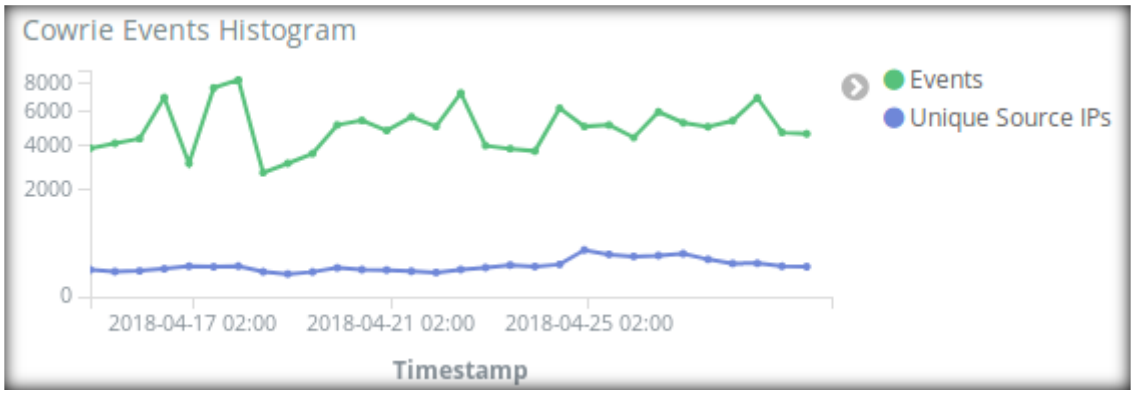


Figura E.0.43 Histograma de ataques de honeypot Cowrie.

En el honeypot Cowrie encontramos en torno a 7000 ataques diarios de 300 IPs distintas (Figura E.0.43).

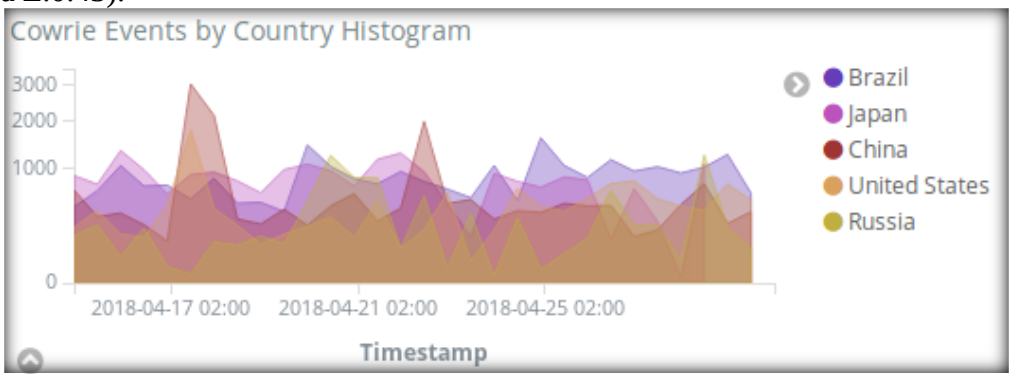


Figura E.0.44 Histograma de ataques por país de honeypot Cowrie.

En esta gráfica podemos observar la cantidad de ataques de los países a lo largo del tiempo. Se ha observado que en países como China o Estados Unidos hay una bajada en el número de ataques en fin de semana, mientras que en países como Brasil o Japón el número de ataques ha sido bastante constante (Figura E.0.44).

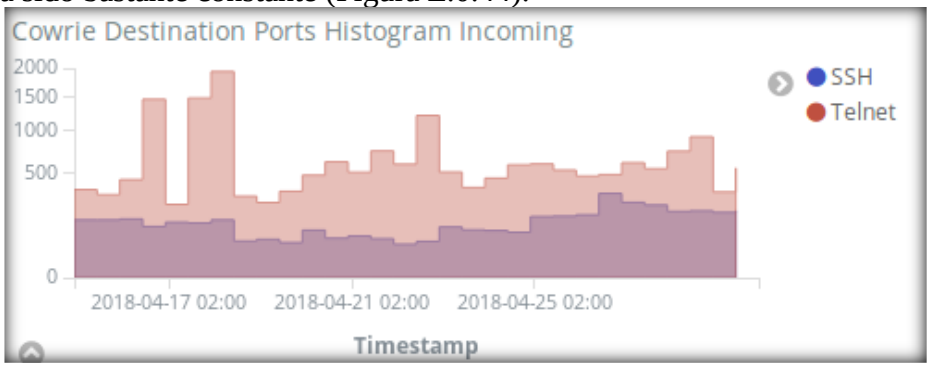


Figura E.0.45 Histograma de puertos atacados de honeypot Cowrie.

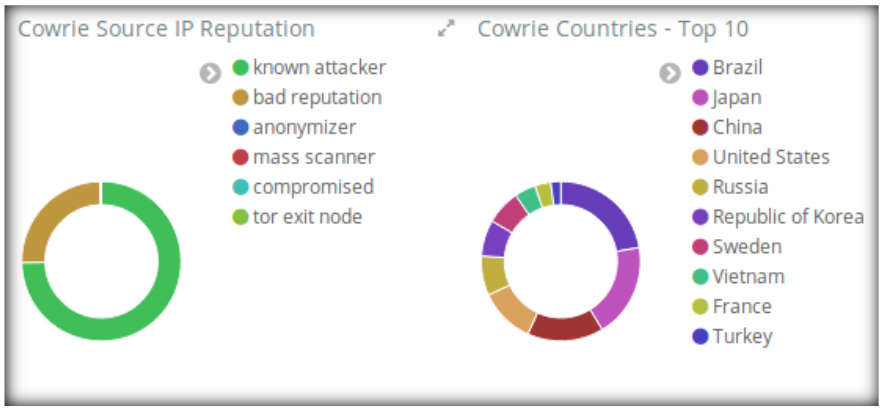


Figura E.0.46 Izquierda: Reputación de IPs atacantes de Cowrie. Derecha: Top 10 países atacantes honeypot Cowrie.

En cuanto al servicio atacado, se detecta que hay bastantes más ataques por SSH que por Telnet (Figura E.0.45).
El 75% de los ataques provinieron de atacantes conocidos, y prácticamente el 15% restante de IPs con mala reputación en la red (Figura E.0.46).

Los países que más atacaron fueron Brasil, Japón, China y Estados Unidos (Figura E.0.42).

En la Figura E.0.47 se muestra una "nube de tags" con los usuarios y contraseñas más probados para tratar de entrar en Cowrie.

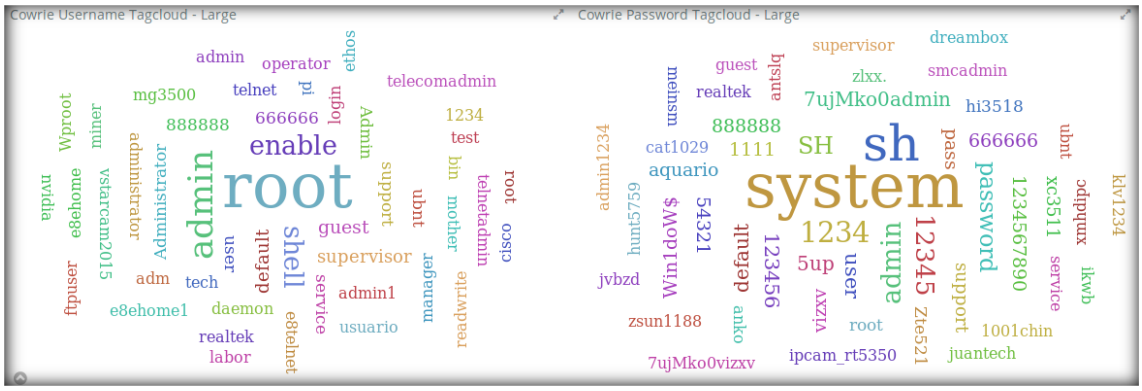


Figura E.0.47 Tagcloud de usuarios y contraseñas más probados por los atacantes de Cowrie.

En la Tabla E.0.5 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
TELEFÔNICA BRASIL S.A	19438
Bredband2 AB	6534
PJSC Rostelecom	5705
No.31,Jin-rong Street	4491
China Networks Inter-Exchange	4355
NTT Communications Corporation	4205
CHINA UNICOM China169 Backbone	3814
Korea Telecom	3687
Viettel Group	2500
OVH SAS	2216

Tabla E.0.5 Proveedores de las IPs atacantes en Cowrie.

Además, analizando los logs se ha obtenido una lista de los comandos más ejecutados tras obtener acceso al honeypot (Tabla E.0.6).

Comando	Número de veces ejecutado
cat /proc/cpuinfo	338
free -m	338
ps -x	338
Uname168	168
uname	168
export HISTFILE=/dev/null	167
export HISTFILESIZE=0	167
export HISTSIZE=0	167
history -n	167
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH	167

Tabla E.0.6 Comandos introducidos en honeypot Cowrie.

(b) Después de la ocultación

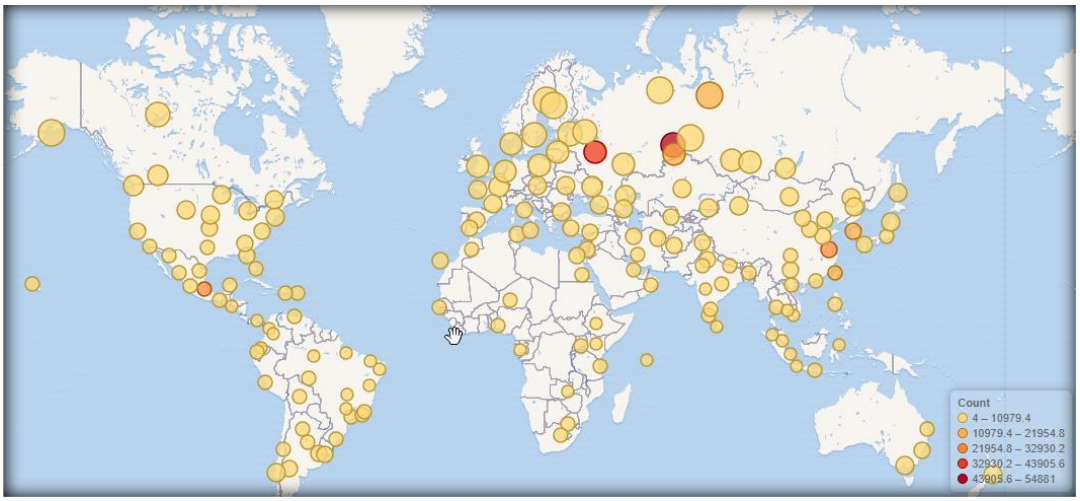


Figura E.0.48 Mapa de ataque de honeypot Cowrie

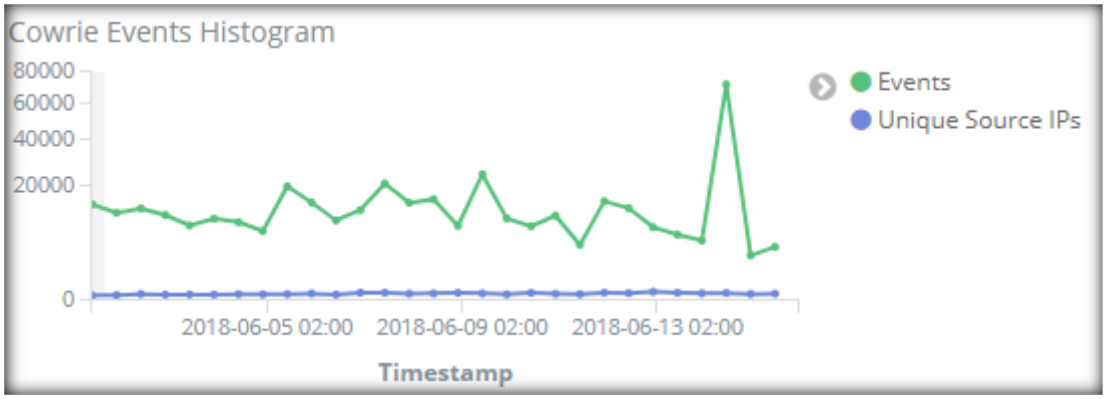


Figura E.0.49 Histograma de ataques de honeypot Cowrie.

En el honeypot Cowrie encontramos en torno a 20000 ataques diarios de 300 IPs distintas, con un pico de 80000 ataques (Figura E.0.49). Esto supone el triple de ataques que antes de la ocultación.

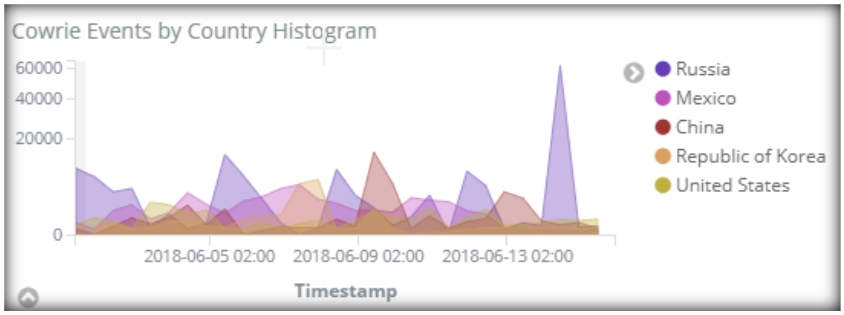


Figura E.0.50 Histograma de ataques por país de honeypot Cowrie.

En esta gráfica podemos observar que este pico de ataques es debido a los atacantes rusos (Figura E.0.50). China y México han realizado bastantes ataques a lo largo de los 15 días.

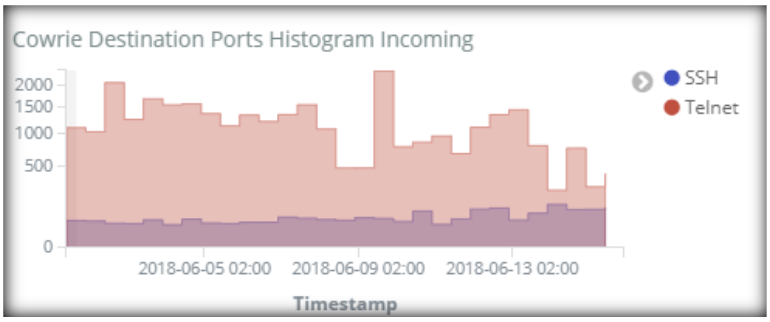


Figura E.0.51 Histograma de puertos atacados de honeypot Cowrie.

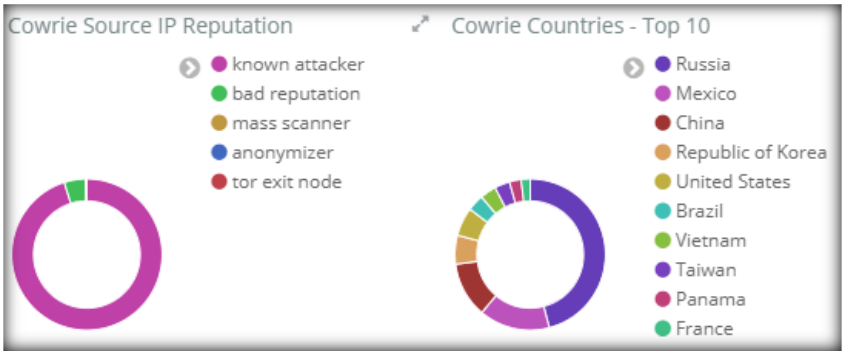


Figura E.0.52 Izquierda: Reputación de IPs atacantes de Cowrie. Derecha: Top 10 países atacantes honeypot Cowrie.

En cuanto al servicio atacado, se detecta que hay bastantes más ataques por SSH que por Telnet (Figura E.0.51), igual que ocurrió antes de la ocultación.
Prácticamente el 100% de los ataques proviene de atacantes conocidos (Figura E.0.52).

Los países que más atacaron fueron Rusia, México, China y Corea (Figura E.0.48 y Figura E.0.52), mientras que antes de la ocultación fueron Brasil, Japón, China y Estados Unidos.

En la Figura E.0.53 se muestra una "nube de tags" con los usuarios y contraseñas más probados para tratar de entrar en Cowrie.

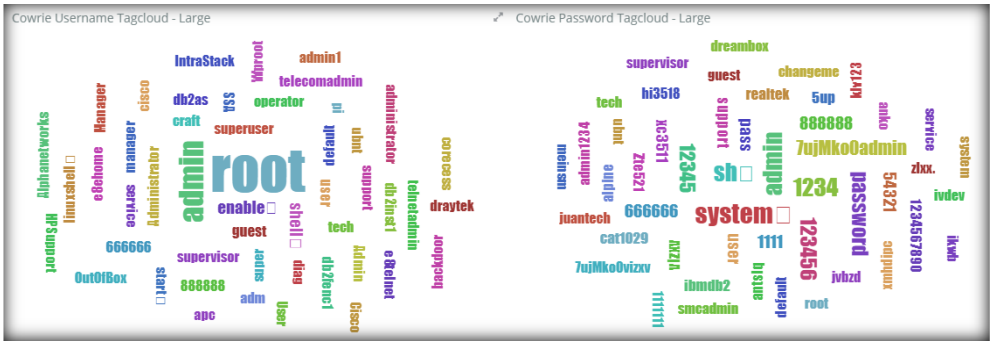


Figura E.0.53 Tagcloud de usuarios y contraseñas más probados por los atacantes de Cowrie.

En la Tabla E.0.7 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
Rostelecom	125617
Uninet S.A. de C.V.	46193
No.31,Jin-rong Street	26156
CJ Hello Co., Ltd.	11671
DigitalOcean, LLC	10666
Asia Pacific On-line Service Inc.	8629
Cable Onda	8221
Korea Telecom	7514
The Corporation for Financing & Promoting Technology	7057
CHINA UNICOM China169 Backbone	6557

Tabla E.0.7 Proveedores de las IPs atacantes en Cowrie.

Además, analizando los logs se ha obtenido una lista de los comandos más ejecutados tras obtener acceso al honeypot (Tabla E.0.8). La mayoría coinciden con la etapa anterior.

Comando	Número de veces ejecutado
cat /proc/cpuinfo	208
free -m	202
ps -x	202
Uname168	101
export HISTFILE=/dev/null	101
export HISTFILESIZE=0	101
export HISTSIZE=0	101
history -n	101
uname	101
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG WATCH	101

Tabla E.0.8 Comandos introducidos en honeypot Cowrie.

(3) Dionaea

Resultados del honeypot Dionaea, antes y después de la ocultación.

(a) Antes de la ocultación

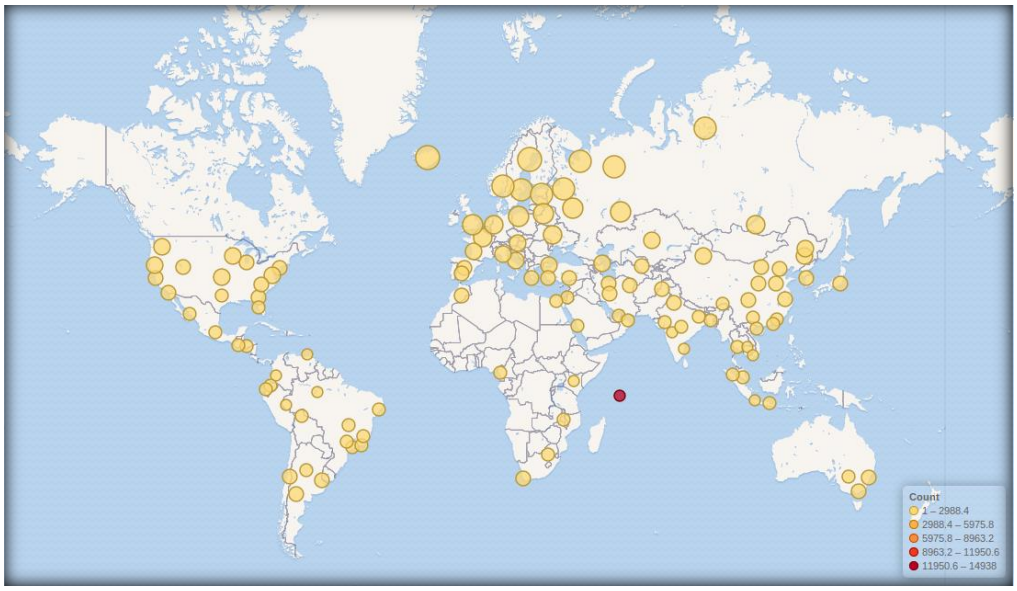


Figura E.0.54 Mapa de ataque de honeypot Dionaea.

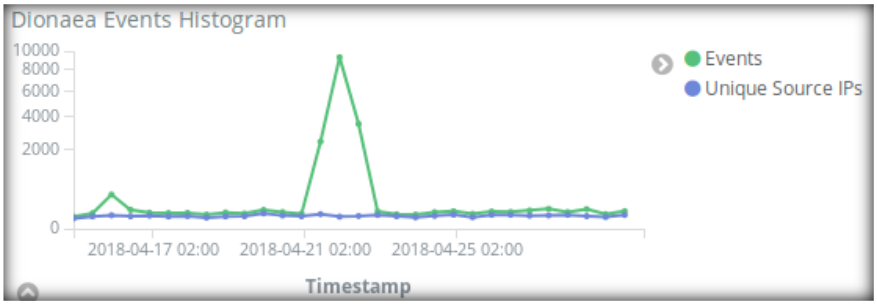


Figura E.0.55 Histograma de ataques de honeypot Dionaea.

En el honeypot Dionaea se ha detectado que hay un gran pico de ataques el fin de semana, en el que se han detectado más de diez mil ataques, frente a los 50 de media que se produjeron el resto de los días (Figura E.0.55).

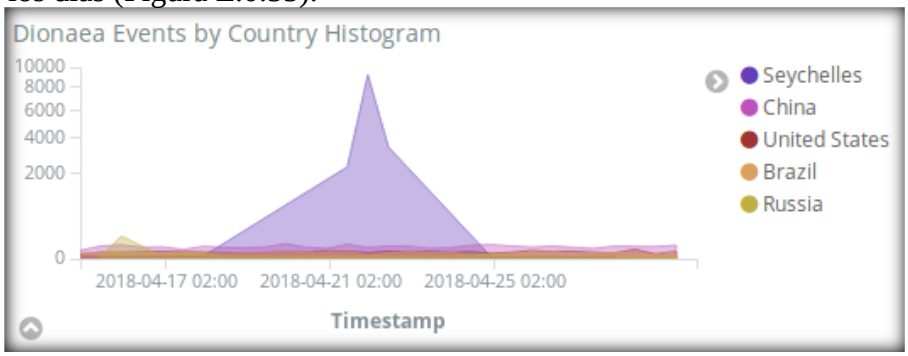


Figura E.0.56 Histograma de ataques por país de honeypot Dionaea.

Este pico se debe sin duda a los ataques realizados por la República de las Seychelles, al norte de Madagascar (Figura E.0.56).

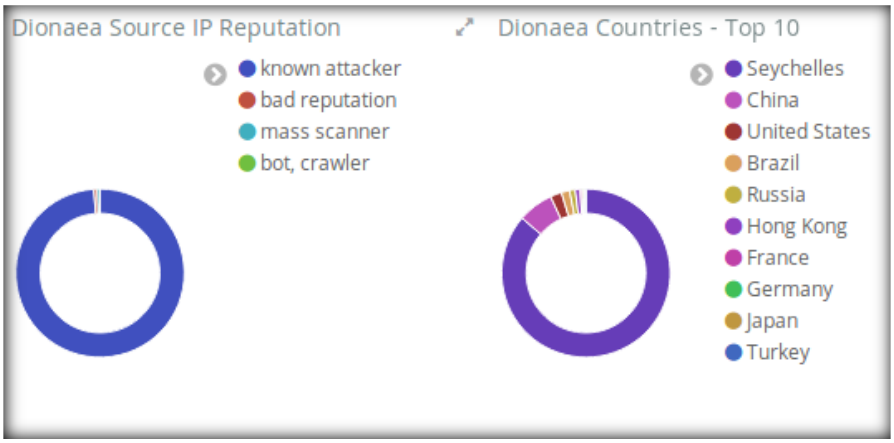


Figura E.0.57 Izquierda: reputación de las IPs atacantes de Dionaea. Derecha: Top 10 países atacantes de Dionaea.

Este país realizo una cantidad enorme de ataques en un corto periodo de tiempo, mientras que países como China, Estados Unidos, Brasil o Rusia se mantuvieron en 2 o 3 ataques por día (Figura E.0.54).

Los ataques provenían casi en su totalidad de IPs de atacantes conocidos (Figura E.0.57).

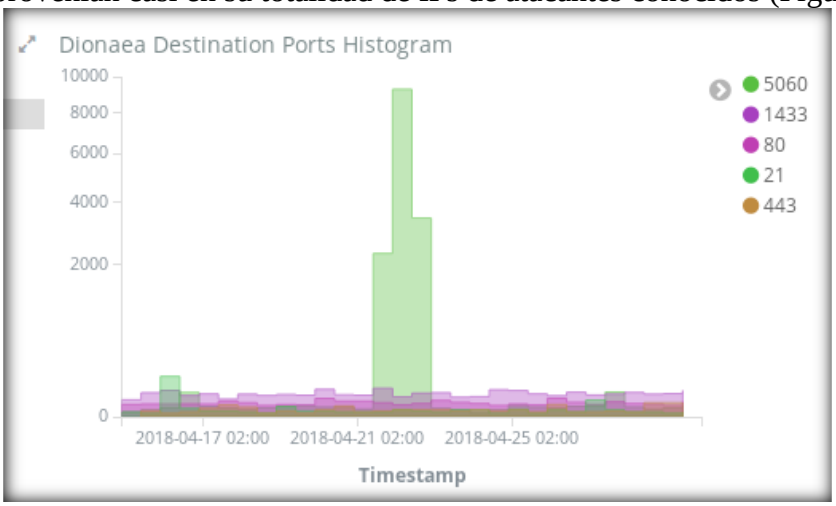


Figura E.0.58 Histograma de puertos atacados en honeypot Dionaea.

Los puertos más atacados fueron el 80 y el 1433, hasta que Seychelles realizó el ataque contra el puerto 5060 (Figura E.0.58).

En la Figura E.0.59 podemos observar la “Nube de tags” de usuarios y contraseñas más empleados tras vulnerar el sistema.

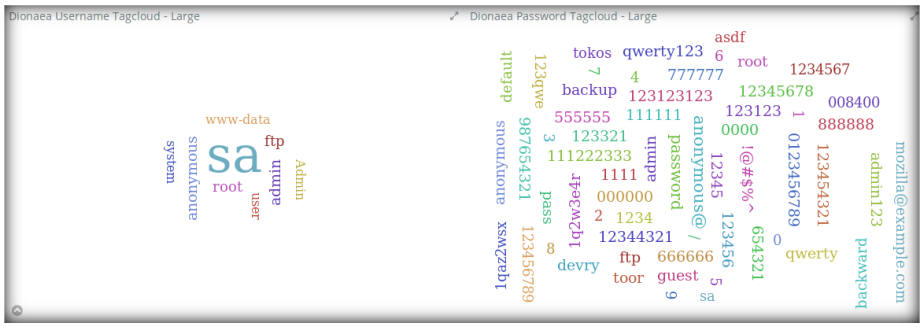


Figura E.0.59 Tagcloud de usuarios y contraseñas más utilizados al atacar el honeypot Dionaea.

En la Tabla E.0.9 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
Quasi Networks LTD.	14936
No.31,Jin-rong Street	545
CHINA UNICOM China169 Backbone	228
TELEFÔNICA BRASIL S.A	228
Capitalonline Data Service Co.,LTD	147
PJSC Rostelecom	139
velia.net Internetdienste GmbH	83
Linode, LLC	81
LeaseWeb Netherlands B.V.	79
China Unicom Beijing Province Network	74

Tabla E.0.9 Proveedores de las IPs atacantes en Dionaea.

(b) Después de la ocultación

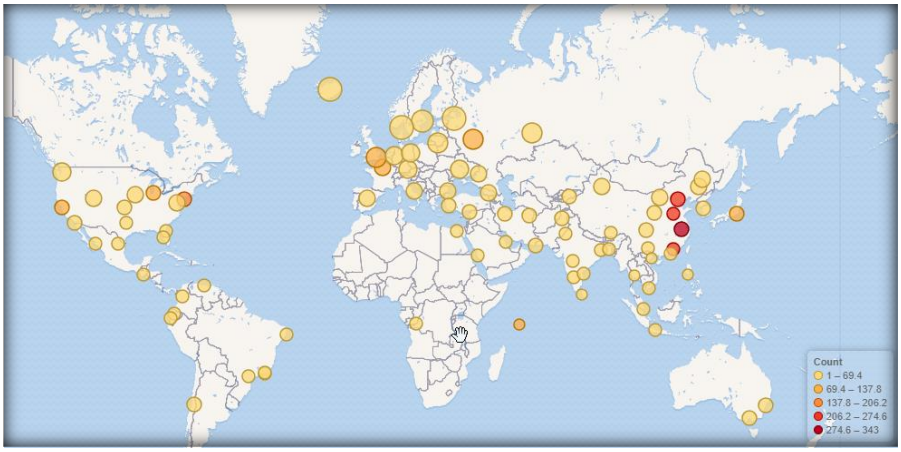


Figura E.0.60 Mapa de ataque de honeypot Dionaea.

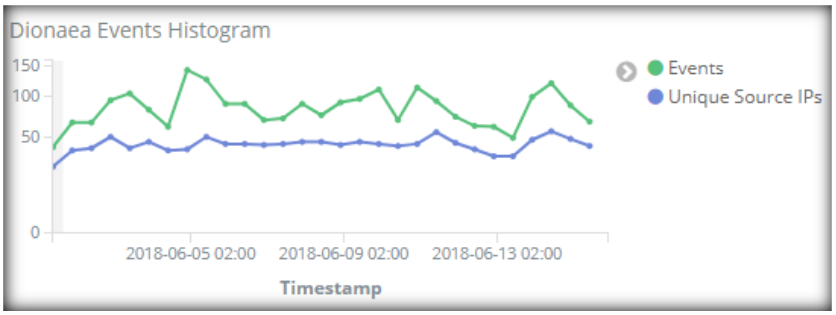


Figura E.0.61 Histograma de ataques de honeypot Dionaea.

En el honeypot Dionaea se han producido entre 50 y 100 ataques al día, unos pocos más que la vez anterior (Figura E.0.61). Sin embargo, antes de la ocultación se produjo un pico en fin de semana que esta vez no se ha dado.

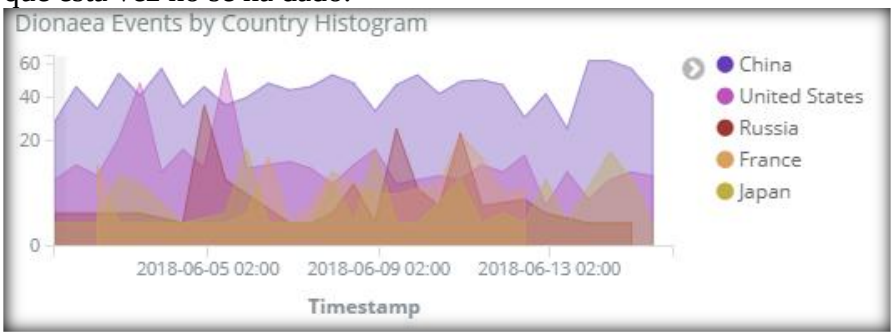


Figura E.0.62 Histograma de ataques por país de honeypot Dionaea.

Los países que más han atacado han sido China, Estados Unidos, Rusia, Francia y Japón (Figura E.0.62). Esta vez no se han dado los ataques realizados por la República de las Seychelles, al norte de Madagascar, que produjeron ese pico de ataques antes de la ocultación (Figura E.0.60).

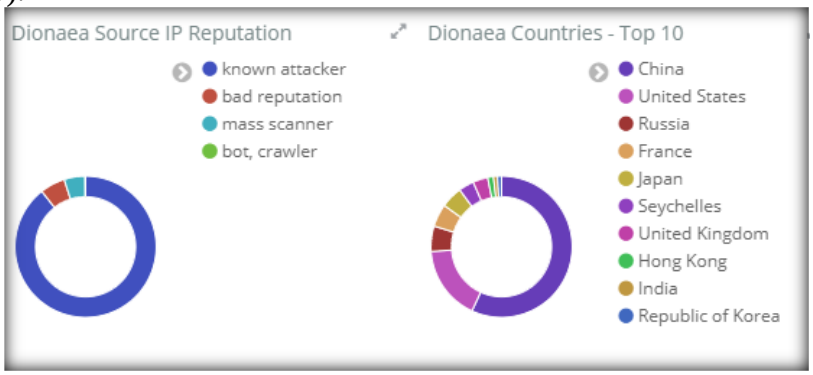


Figura E.0.63 Izquierda: reputación de las IPs atacantes de Dionaea. Derecha: Top 10 países atacantes de Dionaea.

Los ataques provenían casi en su totalidad de IPs de atacantes conocidos (Figura E.0.63).

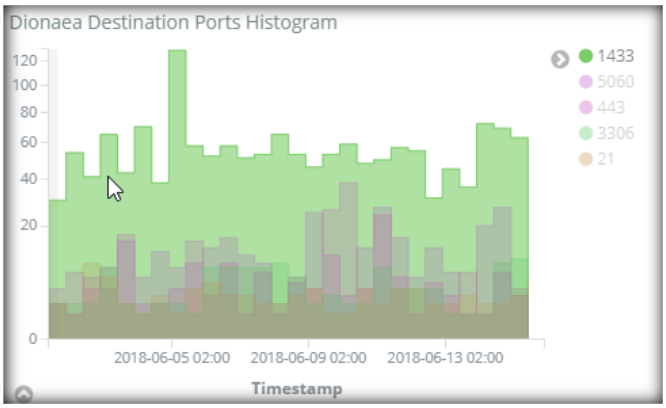


Figura E.0.64 Histograma de puertos atacados en honeypot Dionaea.

Los puertos más atacados fueron el 1433, el 5060 y el 443. A diferencia de la vez anterior, no se ha atacado al puerto 80 (Figura E.0.64).

En la Figura E.0.65 podemos observar la "Nube de tags" de usuarios y contraseñas más empleados tras vulnerar el sistema.

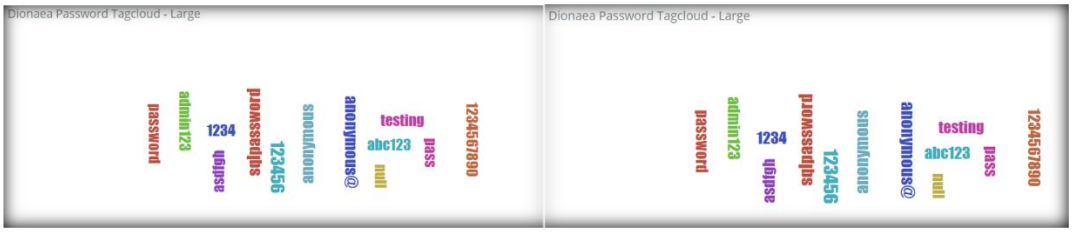


Figura E.0.65 Tagcloud de usuarios y contraseñas más utilizados al atacar el honeypot Dionaea.

En la Tabla E.0.10 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
No.31,Jin-rong Street	562
CHINA UNICOM China169 Backbone	296
Linode, LLC	209
China Unicom Beijing Province Network	98
LeaseWeb Netherlands B.V.	79
Quasi Networks LTD.	74
velia.net Internetdienste GmbH	68
OVH SAS	63
Petersburg Internet Network ltd.	52
Hurricane Electric LLC	51

Tabla E.0.10 Proveedores de las IPs atacantes en Dionaea.

(4) ElasticPot

Resultados del honeypot ElasticPot, antes y después de la ocultación.

(a) Antes de la ocultación

Tan solo se ha registrado un ataque en este honeypot, proveniente de China.
La empresa tras la IP que atacó es Guangdong Mobile Communication Co.Ltd. y realizó una sola Query:

POST /_search?pretty

(b) Después de la ocultación

No se han registrado ataques.

(5) Glastopf

Resultados del honeypot Glastopf, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.66 Mapa de ataques de honeypot Glastopf.

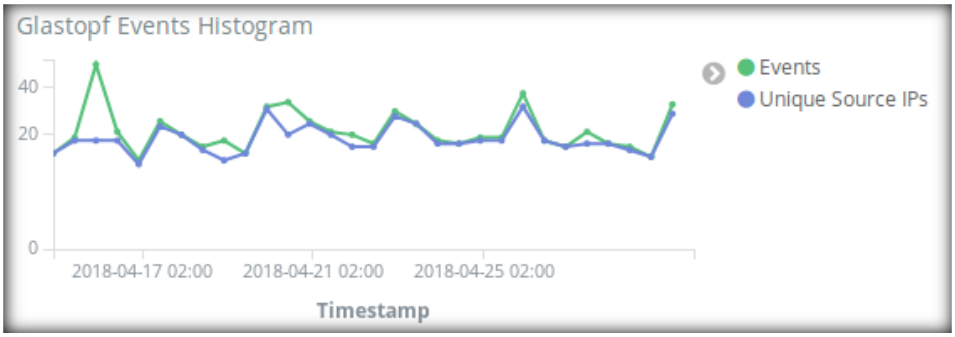


Figura E.0.67 Histograma de ataques de honeypot Glastopf.

En los resultados obtenidos por el honeypot Glastopf podemos comprobar que el número de ataques realizado se corresponde en casi todos los casos con el número de IPs que atacaron, de lo que se deduce que cada IP realizó un solo ataque. Se han registrado entre 20 y 50 ataques al día (Figura E.0.67).

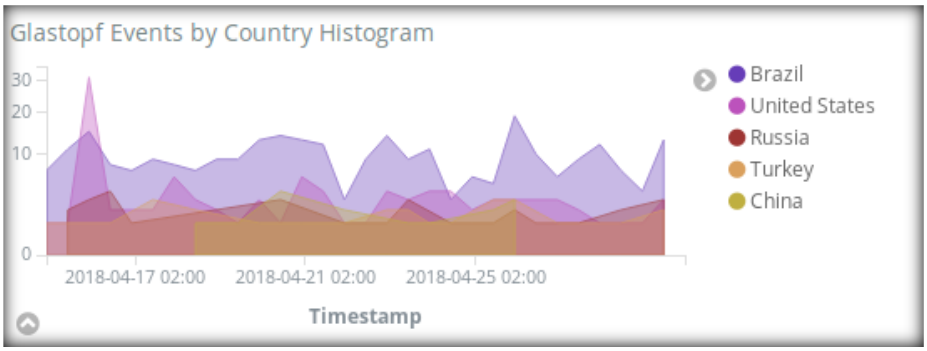


Figura E.0.68Histograma de ataques por país de honeypot Glastopf.

Los países que más atacaron fueron Brasil, Estados Unidos, Rusia, Turquía y China. En Estados Unidos y en Rusia se observa un descenso moderado de ataques el fin de semana, mientras que en el resto de los países la cantidad de ataques es constante (Figura E.0.68).

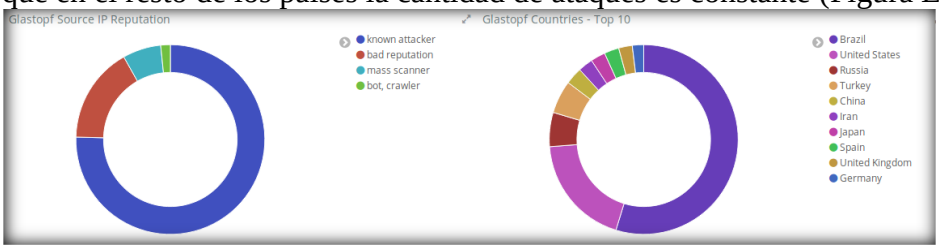


Figura E.0.69 Izquierda: Reputación de IPs atacantes de Glastopf. Derecha: Top 10 países atacantes de Glastopf.

Tres cuartos de los ataques se hicieron desde IPs de atacantes conocidos, y el resto fueron producidos por IPs con mala reputación en la red y por escáneres masivos (Figura E.0.69).

El país que más atacó con diferencia fue Brasil, que realizó la mitad de los ataques, seguido de Estados Unidos, que efectuó en torno al 20% de estos (Figura E.0.66).

En la Tabla E.0.11 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
TELEFÔNICA BRASIL S.A	227
Cogeco Peer 1	28
TELEFÔNICA BRASIL S.A	25
CLARO S.A.	14
Turk Telekom	13
Linode, LLC	12
Amazon.com, Inc.	11
Charter Communications	10
Telefonica De Espana	8
No.31,Jin-rong Street	7

Tabla E.0.11 Proveedores de las IPs atacantes en Glastopf.

(b) Después de la ocultación

Figura E.0.70 Mapa de ataques de honeypot Glastopf.

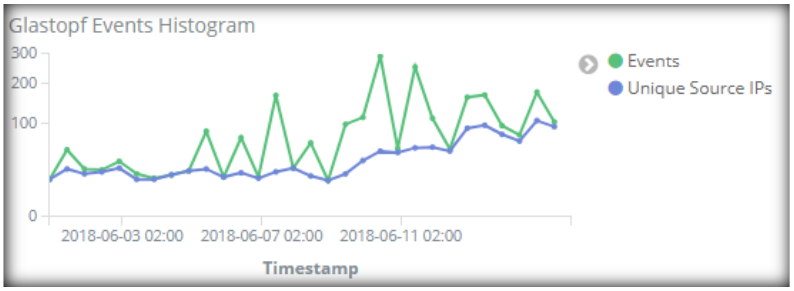


Figura E.0.71 Histograma de ataques de honeypot Glastopf.

En los resultados obtenidos por el honeypot Glastopf podemos apreciar los efectos de la ocultación. Mientras que antes de ocultarlo el número de ataques realizado se correspondía en casi todos los casos con el número de IPs que atacaron, en este caso son muchas las IPs que han realizado varios ataques. Además, el número de ataques llega hasta 300 en varias ocasiones, duplicando la cifra anterior. (Figura E.0.71).

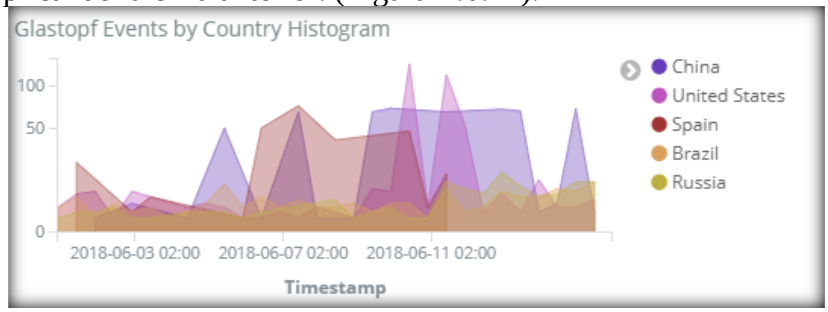


Figura E.0.72Histograma de ataques por país de honeypot Glastopf.

Los países que más atacaron fueron China, Estados Unidos, España, Brasil y Rusia (Figura E.0.72).

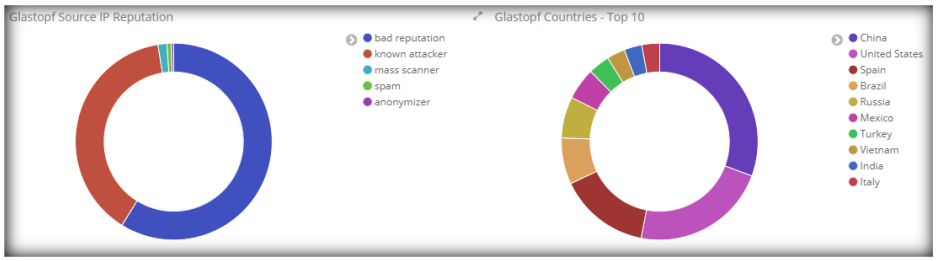


Figura E.0.73 Izquierda: Reputación de IPs atacantes de Glastopf. Derecha: Top 10 países atacantes de Glastopf.

Más de la mitad de los ataques se hicieron desde IPs con mala reputación en la red, y el resto fueron producidos por IPs de atacantes conocidos (Figura E.0.73).

El país que más atacó con diferencia fue China, seguido de Estados Unidos (Figura E.0.70). Apenas hubo ataques de Brasil, que la vez anterior realizó la mitad de los ataques.

En la Tabla E.0.12 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
Shenzhen Tencent Computer Systems Company Limited	340
AT&T Services, Inc.	183
Telefonica De Espana	156
Uninet S.A. de C.V.	90
China Telecom (Group)	69
Beijing Baidu Netcom Science and Technology Co., Ltd.	68
Alibaba (China) Technology Co., Ltd.	66
Entidad Publica Empresarial Red.es	65
No.31,Jin-rong Street	61
Windstream Communications LLC	60

Tabla E.0.12 Proveedores de las IPs atacantes en Glastopf.

(6) Honeytrap

Resultados del honeypot Honeytrap, antes y después de la ocultación.

(a) Antes de la ocultación

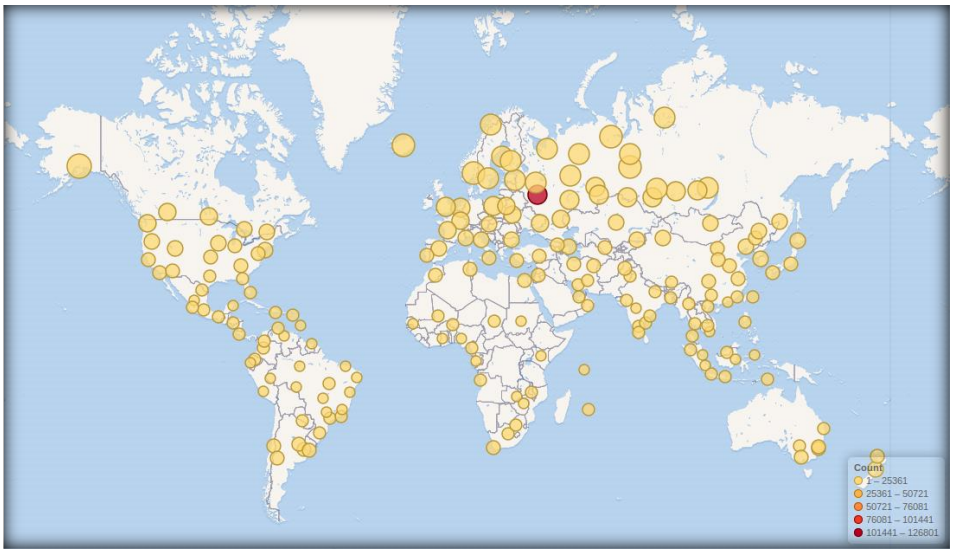


Figura E.0.74 Mapa de ataque de honeypot Honeytrap.

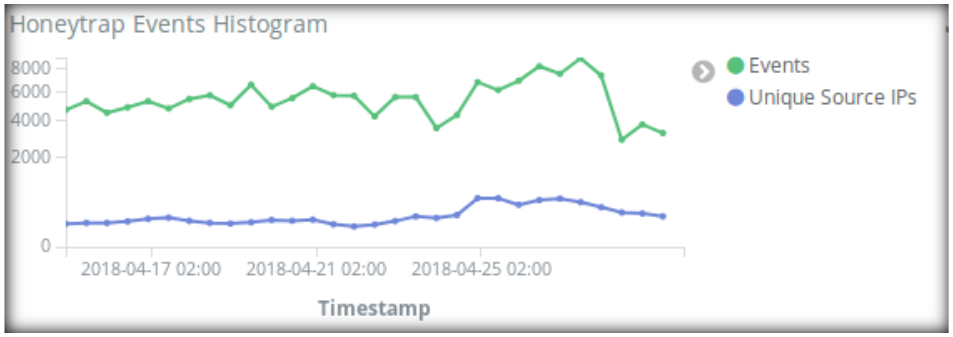


Figura E.0.75 Histograma de ataques de honeypot Honeytrap.

El número de ataques que ha captado Honeytrap ronda los seis mil ataques diarios, proveniente de unas 300 IPs distintas cada día. De esto se deduce que cada IP ha realizado varios cientos de ataques al día (Figura E.0.75)

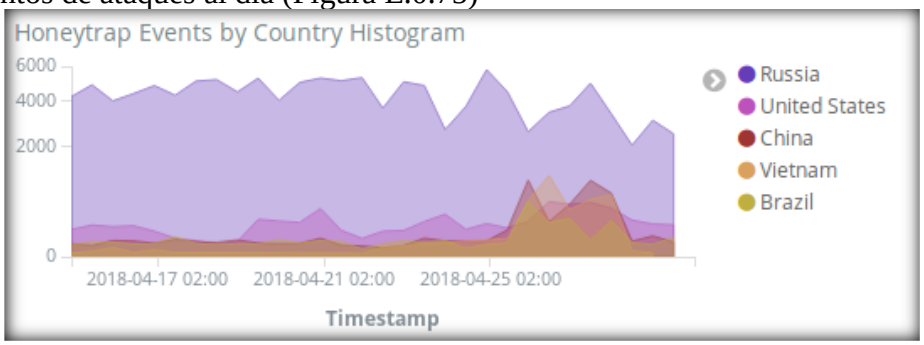


Figura E.0.76 Histograma de ataques por país de honeypot Honeytrap.

El país que más ha atacado con diferencia ha sido Rusia, seguida de Estados Unidos, China, Vietnam y Brasil, países donde se ha detectado un aumento de actividad a mediados de la segunda semana (Figura E.0.74 y Figura E.0.76).

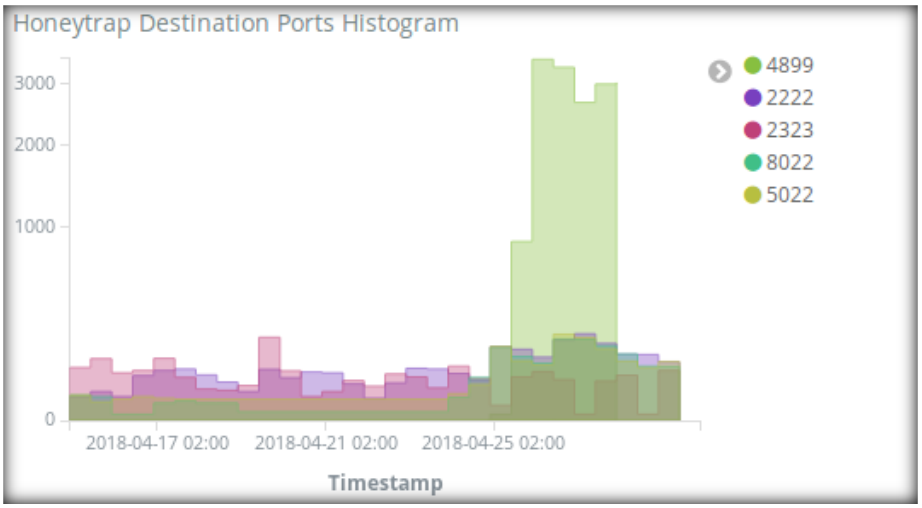


Figura E.0.77 Histograma de puertos atacados de honeypot Honeytrap.

El puerto más atacado con diferencia ha sido el 4899. Sufrió un pico de ataques muy alto a mediados de la segunda semana (Figura E.0.77).
En la Figura E.0.78 podemos ver un mapa de calor de los ataques en función de los puertos a los que fueron destinados.

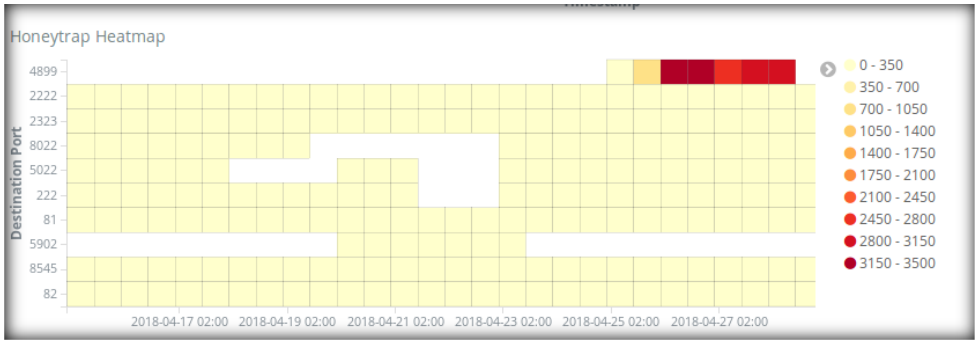


Figura E.0.78 Mapa de calor de puertos de honeypot Honeytrap.

Dado que este puerto ha sufrido bastantes más ataques que el resto, se ha realizado el mapa de calor excluyendo el puerto para comprobar la actividad del resto (Figura E.0.79).

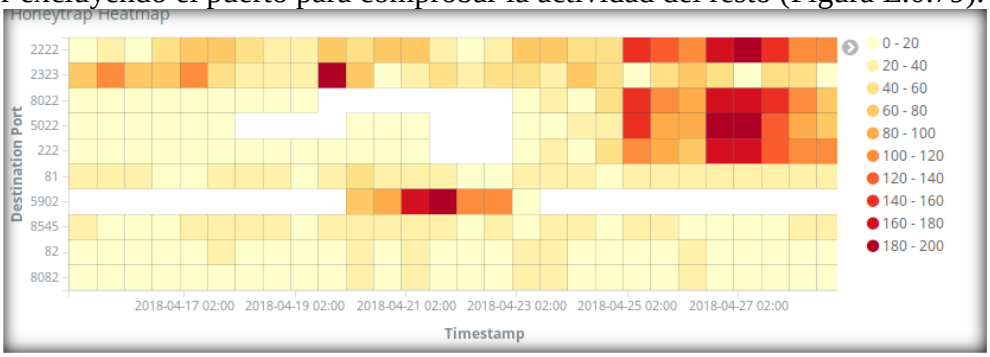


Figura E.0.79 Mapa de calor de puertos (excluyendo el puerto 4899) de honeypot Honeytrap.

Así, observamos que varios otros puertos como el 2222, el 8022, el 5022 o el 222 sufrieron un aumento de ataques a sus puertos a mediados de la segunda semana. También cabe destacar los ataques sufridos al puerto 5902, que fueron muy concentrados en un corto intervalo de tiempo.

En la Tabla E.0.13 podemos ver los proveedores de las IPs que más atacaron.

Proveedor de servicios	Número de ataques
LLC CloudSol	122882
Linode, LLC	3244
Quasi Networks LTD.	1320
Solar Invest UK LTD.	1041
Content Delivery Network Ltd	912
NForce Entertainment B.V.	874
Hostkey B.v.	761
TELEFÔNICA BRASIL S.A	693
OOO Sirius-Project	692
CariNet, Inc.	634

Tabla E.0.13 Proveedores de las IPs atacantes en Honeytrap.

(b) Después de la ocultación

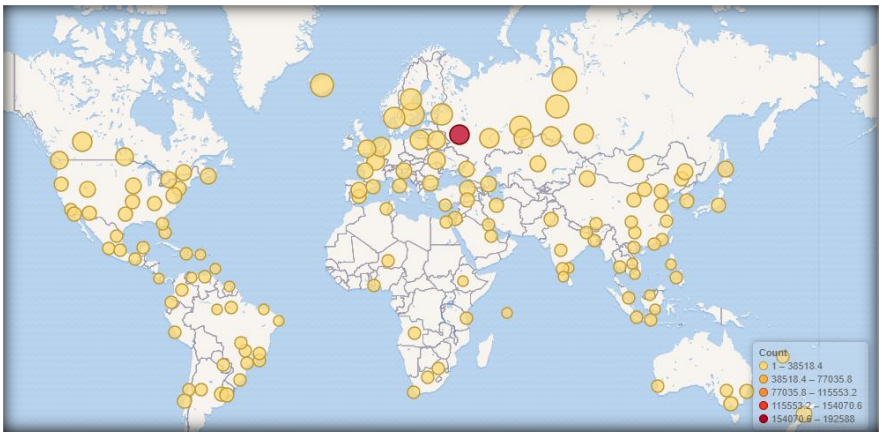


Figura E.0.80 Mapa de ataque de honeypot Honeytrap.

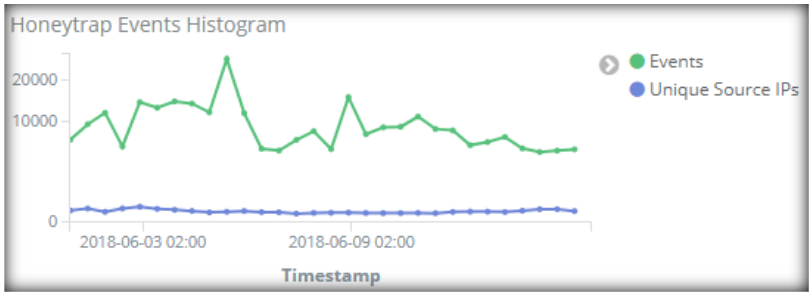


Figura E.0.81 Histograma de ataques de honeypot Honeytrap.

El número de ataques que ha captado Honeytrap ronda los diez mil ataques diarios, proveniente de unas 300 IPs distintas cada día, frente a los seis mil de antes de la ocultación,

casi duplica los ataques diarios. Sin embargo el número de IPs se ha mantenido (Figura E.0.81)

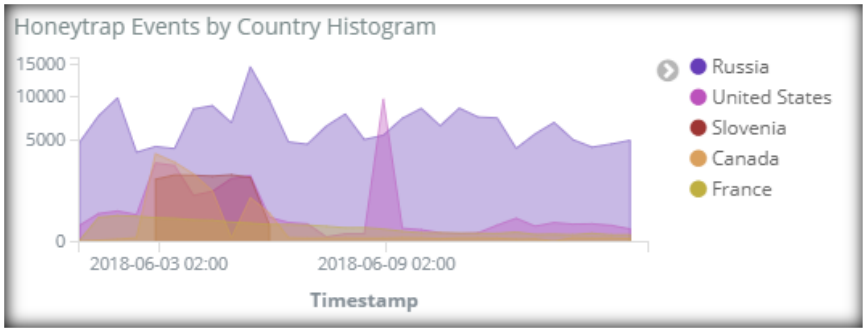


Figura E.0.82 Histograma de ataques por país de honeypot Honeytrap.

El país que más ha atacado con diferencia ha sido Rusia (al igual que la vez anterior), seguida de Estados Unidos, Eslovenia, Canadá y Francia, países donde se ha detectado un aumento de actividad durante la primera semana mientras que en la segunda apenas ha habido ataques de otros países que no fueran Rusia (Figura E.0.80 y Figura E.0.82).

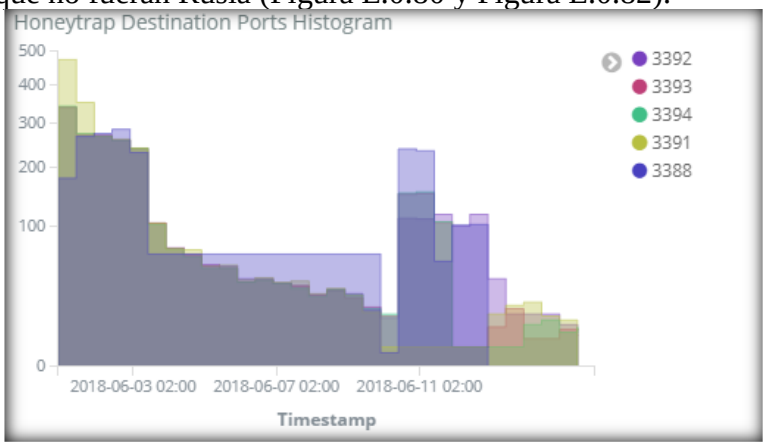


Figura E.0.83 Histograma de puertos atacados de honeypot Honeytrap.

Los ataques han ido dirigidos bastante uniformemente a los puertos 3392, 3393, 3394, 3391 y 3388 (Figura E.0.83).

En la Figura E.0.84 podemos ver un mapa de calor de los ataques en función de los puertos a los que fueron destinados.

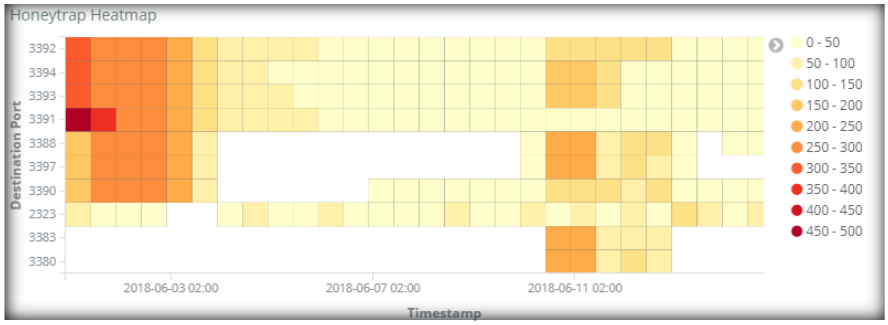


Figura E.0.84 Mapa de calor de puertos de honeypot Honeytrap.

En la Tabla E.0.14 podemos ver los proveedores de las IPs que más atacaron.

Proveedor de servicios	Número de ataques
Hostkey B.v.	191604
ARNES	12615
ADVANCED KNOWLEDGE NETWORKS	10228
VolumeDrive	9626
OVH SAS	5012
Cox Communications Inc.	4836
TIS Dialog LLC	4550
Linode, LLC	3700
Time Warner Cable Internet LLC	3279
MCI Communications Services, Inc. d/b/a Verizon Business	2930

Tabla E.0.14 Proveedores de las IPs atacantes en Honeytrap.

(7) Mailoney

Resultados del honeypot Mailoney, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.85 Mapa de ataques de honeypot Mailoney.

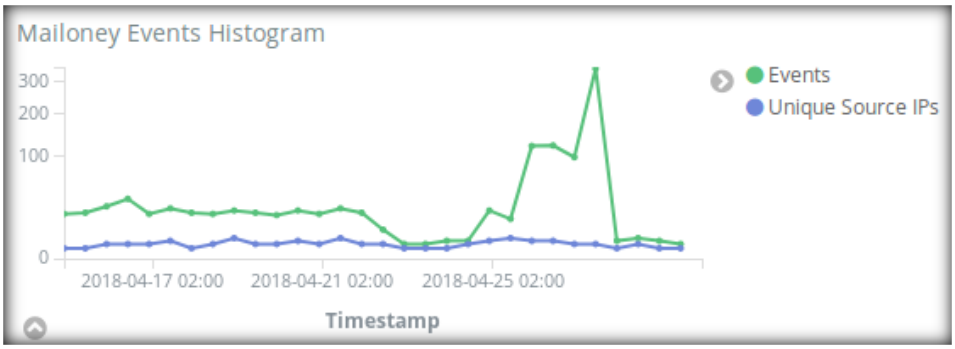


Figura E.0.86 Histograma de ataques de honeypot Mailoney.

En el honeypot Mailoney se ha observado un aumento de los ataques en la mitad de la segunda semana (Figura E.0.86).

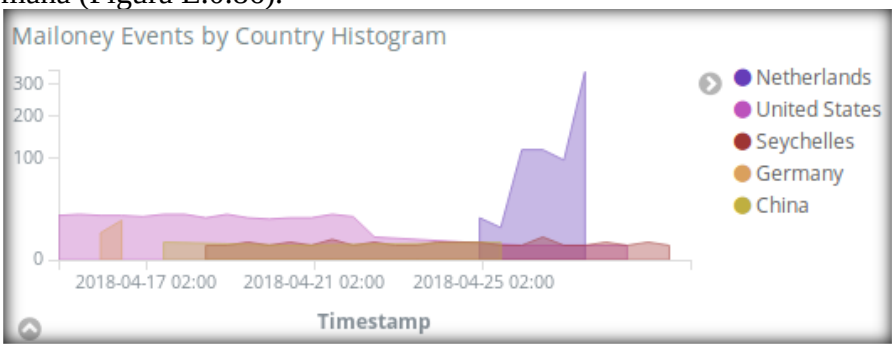


Figura E.0.87 Histograma de ataques por país de honeypot Mailoney.

Dado que en otros honeypots también se ha observado esta subida, podríamos deducir que los atacantes no solo se han centrado en un único honeypot (Figura E.0.87). Sin embargo, al observar la procedencia de los ataques se descubrió que este pico se debió a ataques realizados en Países Bajos, mientras que los demás fueron causados por Rusia. Por tanto, se descarta esta hipótesis (Figura E.0.85 y Figura E.0.88).

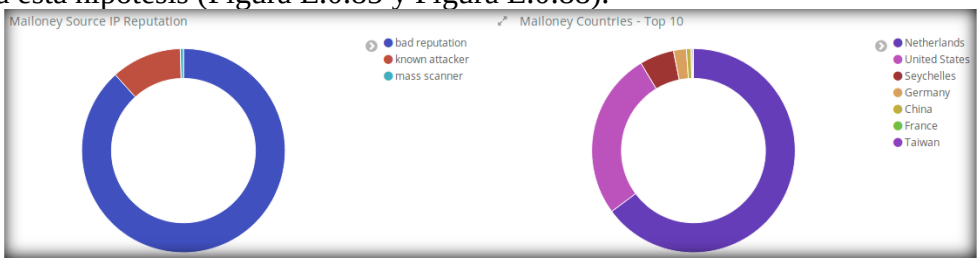


Figura E.0.88 Izquierda: Reputación de IPs atacantes de Mailoney. Derecha: top 10 países atacantes de Mailoney.

En la Tabla E.0.15 podemos ver los proveedores de las IPs que más atacaron.

Proveedor de servicios	Número de ataques
NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	277
Quasi Networks LTD.	59
CHINA TELECOM (AMERICAS) CORPORATION	22
CHINANET Sichuan province Chengdu MAN network	6
CariNet, Inc.	4
University of Michigan	4
Data Communication Business Group	2
No.31,Jin-rong Street	2
Online S.a.s.	2
Amazon.com, Inc.	1

Tabla E.0.15 Proveedores de las IPs atacantes en Mailoney.

En la Tabla E.0.16 aparecen los comandos introducidos por SMTP que más se repitieron.

SMTP Input	Veces introducido
EHLO User	444
QUIT	117
AUTH LOGIN	111
data	17
mail FROM:<un.compi@trio-cloud.com> size=3626	15
quit	6
Data	3
HELP	3
Mail from:<spameri@tiscali.it>	3
Quit	3

Tabla E.0.16 Comandos introducidos por SMTP en honeypot Mailoney.

(b) Después de la ocultación

Figura E.0.89 Mapa de ataques de honeypot Mailoney.

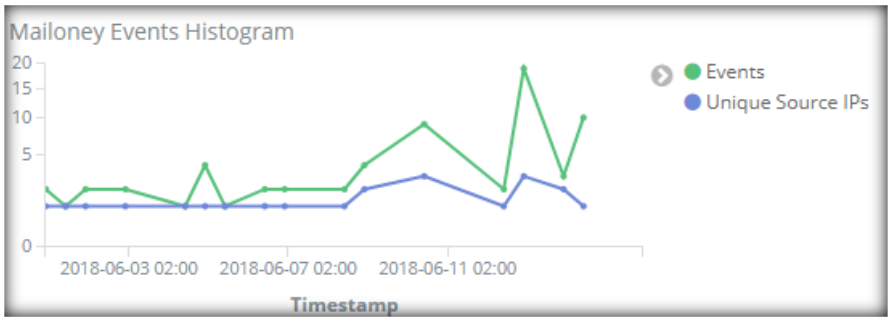


Figura E.0.90 Histograma de ataques de honeypot Mailoney.

En el honeypot Mailoney se ha observado un aumento de los ataques en la mitad de la segunda semana, tal y como pasó la vez anterior (Figura E.0.90).

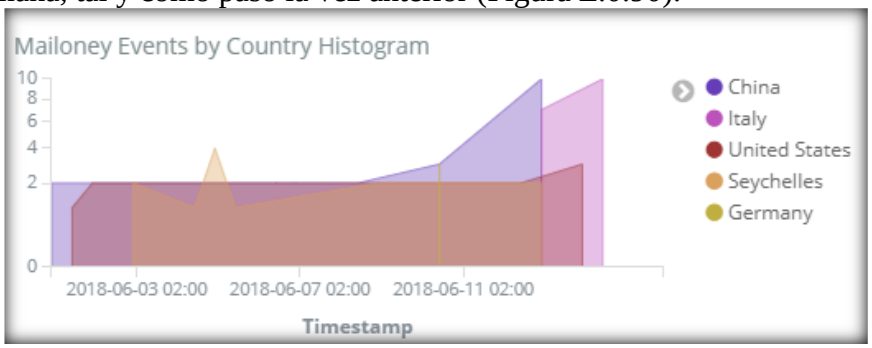


Figura E.0.91 Histograma de ataques por país de honeypot Mailoney.

China, Italia, Estados Unidos y la República de Seychelles han sido los mayores atacantes (Figura E.0.91). Cada uno ha realizado prácticamente el mismo número de ataques (Figura E.0.89 y Figura E.0.92). El 75% de los ataques provenían de atacantes conocidos y el 25% restante de escaneadores masivos.

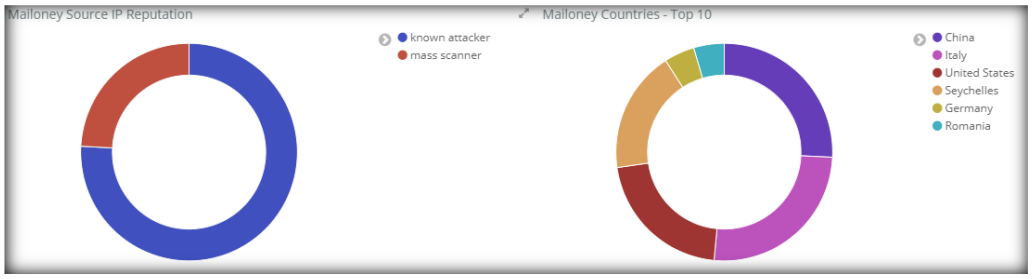


Figura E.0.92 Izquierda: Reputación de IPs atacantes de Mailoney. Derecha: top 10 países atacantes de Mailoney.

En la Tabla E.0.17 podemos ver los proveedores de las IPs que más atacaron.

Proveedor de servicios	Número de ataques
Vodafone Italia S.p.A.	17
No.31,Jin-rong Street	15
Quasi Networks LTD.	12
University of Michigan	6
CariNet, Inc.	5
Vodafone GmbH	3
Flokinet Ltd	3
China Unicom Beijing Province Network	2
DigitalOcean, LLC	2
Amazon.com, Inc.	1

Tabla E.0.17 Proveedores de las IPs atacantes en Mailoney.

En la Tabla E.0.18 aparecen los comandos introducidos por SMTP que más se repitieron.

SMTP Input	Veces introducido
STARTTLS	444
QUIT	117
EHLO User	111
EHLO masscan	17
HELP	15
EHLO eecs.umich.edu	6
DATA	3
EHLO zx1.quadmetrics.com	3
HELO User	3
MAIL FROM:<info@mobigen.com>	3

Tabla E.0.18 Comandos introducidos por SMTP en honeypot Mailoney.

(8) Rdpy

Resultados del honeypot Rdpy, antes y después de la ocultación.

(a) Antes de la ocultación

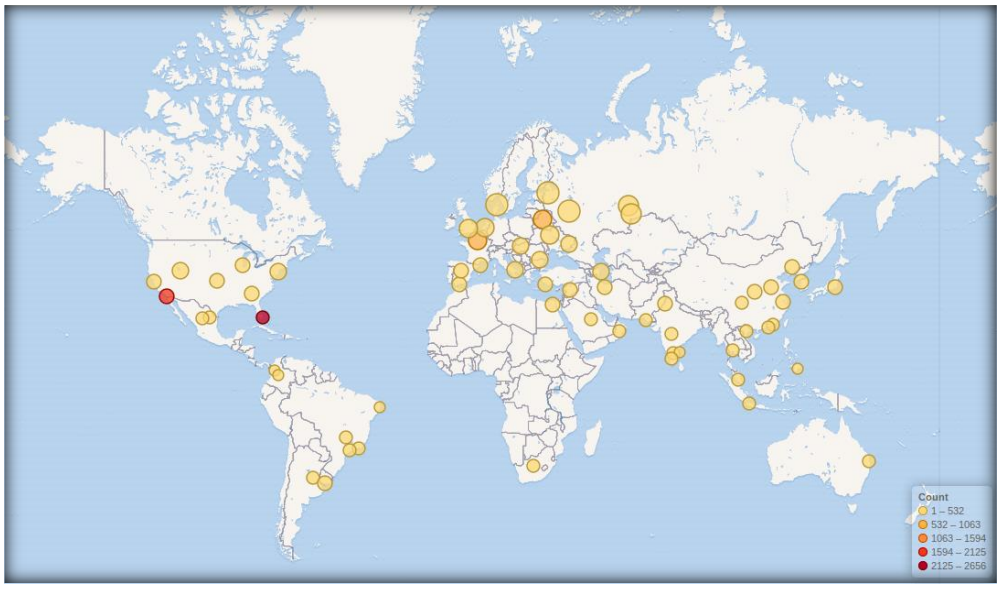


Figura E.0.93 Mapa de ataques de honeypot Rdpy.

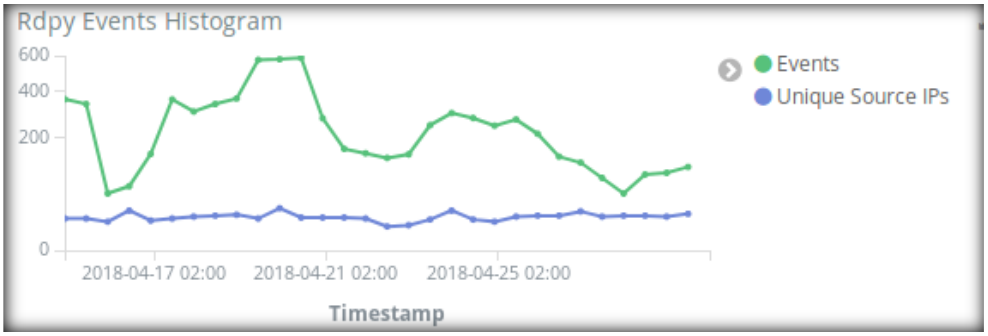


Figura E.0.94 Histograma de ataques de honeypot Rdpy.

El honeypot Rdpy ha recogido una media de 400 ataques al día (Figura E.0.94). Se puede observar en la Figura E.0.95 que el número de ataques decae mucho en fin de semana, sobre todo en los producidos por Estados Unidos.

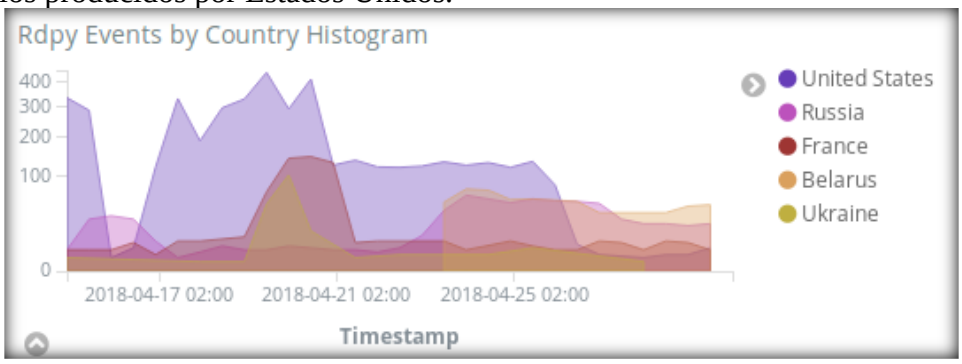


Figura E.0.95 Histograma de ataques por país de honeypot Rdpy.

Estados Unidos fue el país que más atacó con diferencia, y la mayoría de las IPs provenían de atacantes conocidos (Figura E.0.93 y Figura E.0.96).

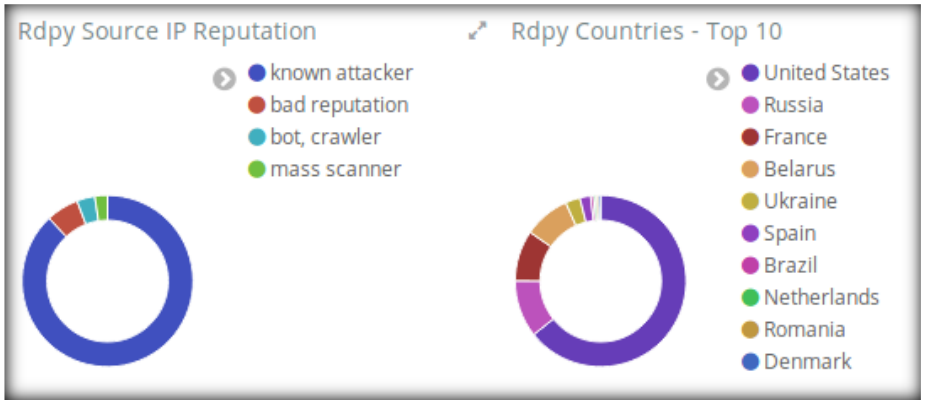


Figura E.0.96 Izquierda: Reputación de las IPs atacantes de Rdpy. Derecha: Top 10 países atacantes de Rdpy.

En la Tabla E.0.19 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
CariNet, Inc.	1662
Velcom AZS LLC	598
OVH SAS	466
PJSC Rostelecom	328
Online S.a.s.	192
MT-Telecom LLC	190
Elenkom LLC	168
Cogent Communications	107
Limited liability company Mail.Ru	83
LeaseWeb Netherlands B.V.	57

Tabla E.0.19 Proveedores de las IPs atacantes en Rdpy.

(b) Después de la ocultación

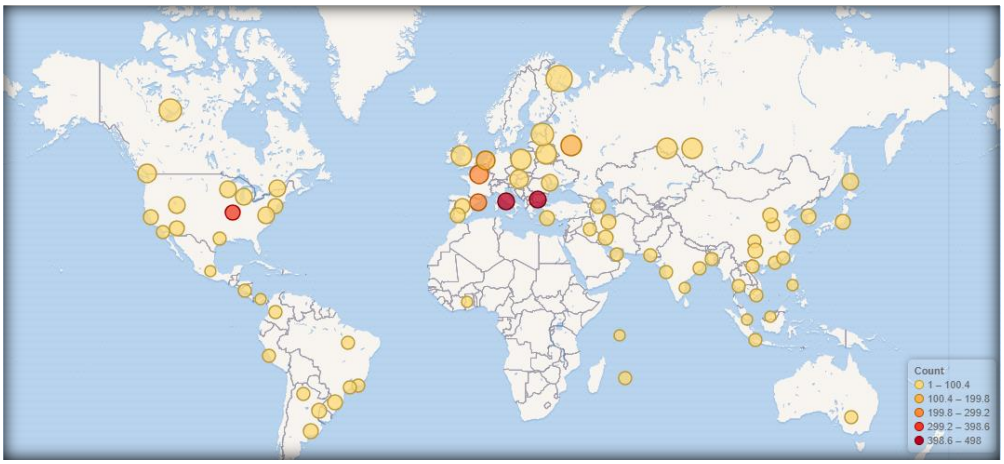


Figura E.0.97 Mapa de ataques de honeypot Rdpy.

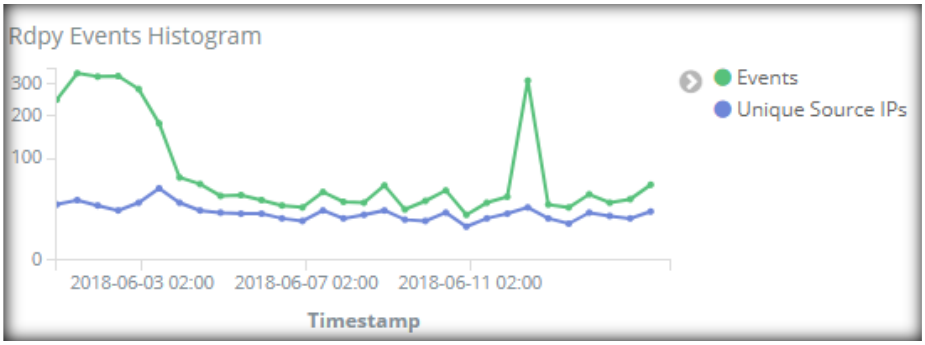


Figura E.0.98 Histograma de ataques de honeypot Rdpy.

El honeypot Rdpy ha recogido una media de 100 ataques al día (Figura E.0.98), frente a los 400 de antes de la ocultación. Este ha sido uno de los únicos honeypots que ha recibido menos ataques tras la ocultación. Se puede observar en la Figura E.0.99 que el número de ataques se centra básicamente en el fin de semana.

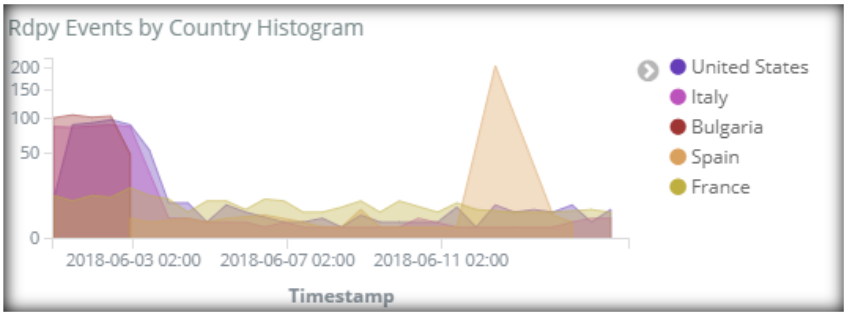


Figura E.0.99 Histograma de ataques por país de honeypot Rdpy.

Estados Unidos, Italia y Bulgaria fueron los países que más atacaron, y la mayoría de las IPs provenían de atacantes conocidos (Figura E.0.97 y Figura E.0.100).

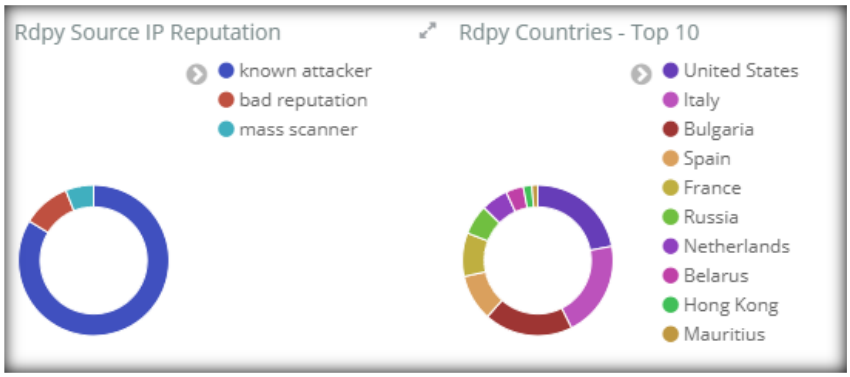


Figura E.0.100 Izquierda: Reputación de las IPs atacantes de Rdpy. Derecha: Top 10 países atacantes de Rdpy.

En la Tabla E.0.20 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
Mobiltel Ead	458
Vodafone Italia S.p.A.	445
AT&T Services, Inc.	355
Telefonica De Espana	229
Online S.a.s.	184
NForce Entertainment B.V.	114
Velcom AZS LLC	63
LeaseWeb Netherlands B.V.	63
Hostkey B.v.	53
Aruba S.p.A.	52

Tabla E.0.20 Proveedores de las IPs atacantes en Rdpy.

(9) Suricata

Resultados del honeypot Suricata, antes y después de la ocultación.

(a) Antes de la ocultación

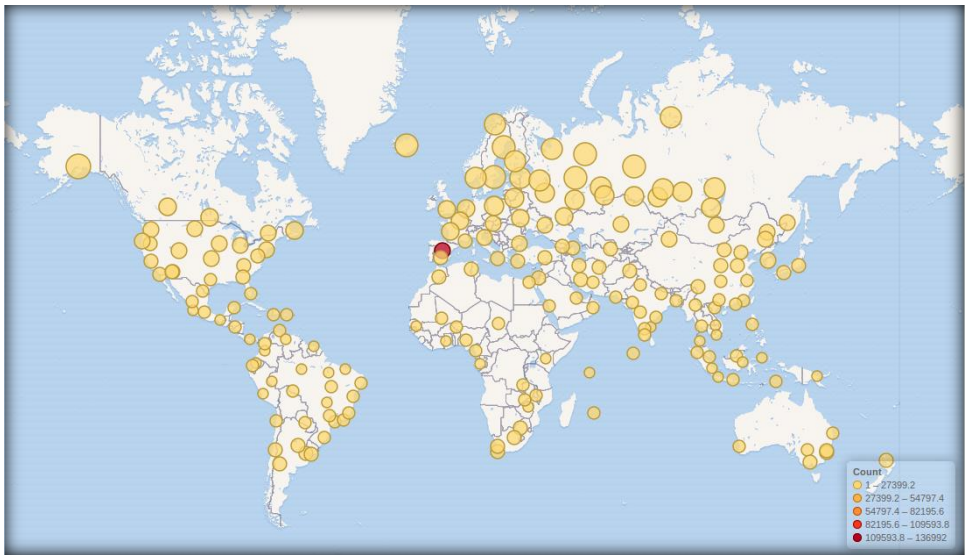


Figura E.0.101 Mapa de ataques de honeypot Suricata.

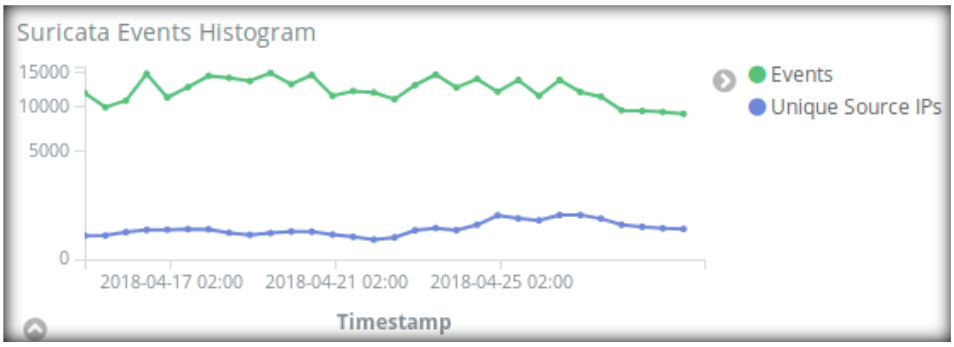


Figura E.0.102 Histograma de ataques de honeypot Suricata.

Podemos observar que se han realizado miles de ataques contra este honeypot, en torno a doce mil por día, desde una media de 400 IPs (Figura E.0.102).

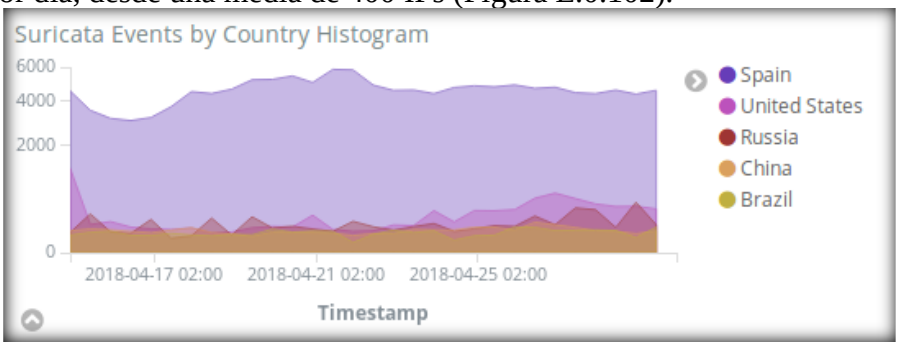


Figura E.0.103 Histograma de ataques por país de honeypot Suricata.

Aunque ha recibido ataques desde todas partes del mundo, destacan notablemente los ataques realizados en España (Figura E.0.101 y Figura E.0.103), y mayoritariamente sobre el puerto 53 (Figura E.0.104).

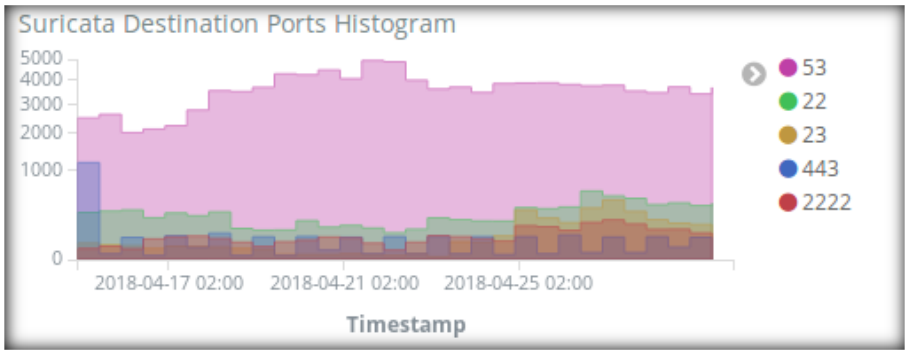


Figura E.0.104 Histograma de puertos atacados de honeypot Suricata.

A continuación podemos ver los rankings de los datos que ha recogido el honeypot Suricata, como los métodos http más utilizados, los tipos de archivo más enviados o los clientes SSH que se han utilizado (Figura E.0.105).

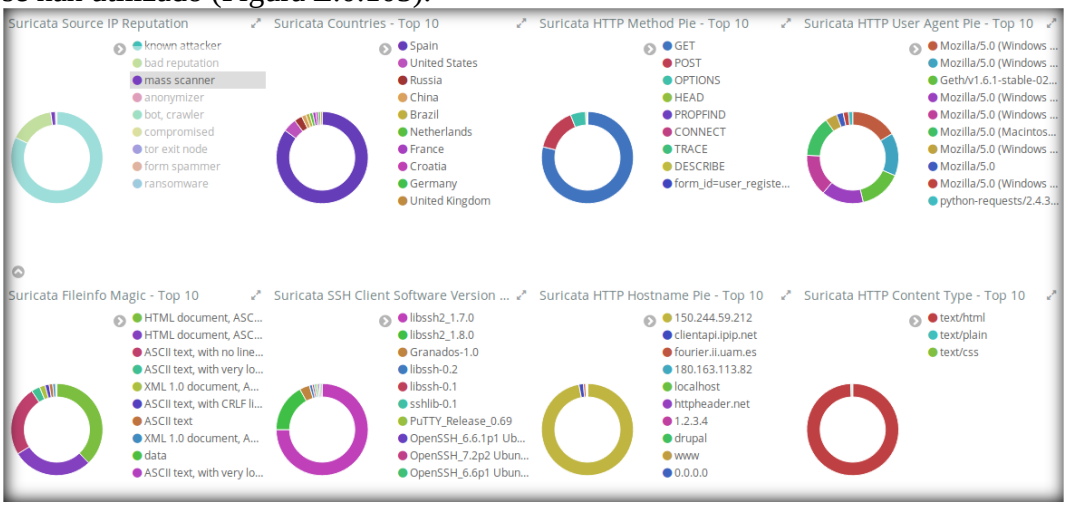


Figura E.0.105 Top 10 de datos de atacantes recogidos por honeypot Suricata.

Por último se muestra una lista de los mensajes más frecuentes de este honeypot en la *Tabla E.0.21*.

Descripción	Número de veces
SURICATA zero length padN option	187913
SURICATA IPv4 padding required	35563
ET POLICY SSH session in progress on Unusual Port	7398
SURICATA STREAM Packet with broken ack	5590
GPL ICMP_INFO Destination Unreachable Communication with Destination Host is Administratively Prohibited	3926
ET POLICY SSH session in progress on Expected Port	3721
SURICATA Applayer Detect protocol only one direction	2036
SURICATA STREAM FIN recv but no session	1327
SURICATA STREAM ESTABLISHED packet out of window	1119
SURICATA STREAM ESTABLISHED invalid ack	555

Tabla E.0.21 Descripción de los mensajes intercambiados de honeypot Suricata.

(b) Después de la ocultación

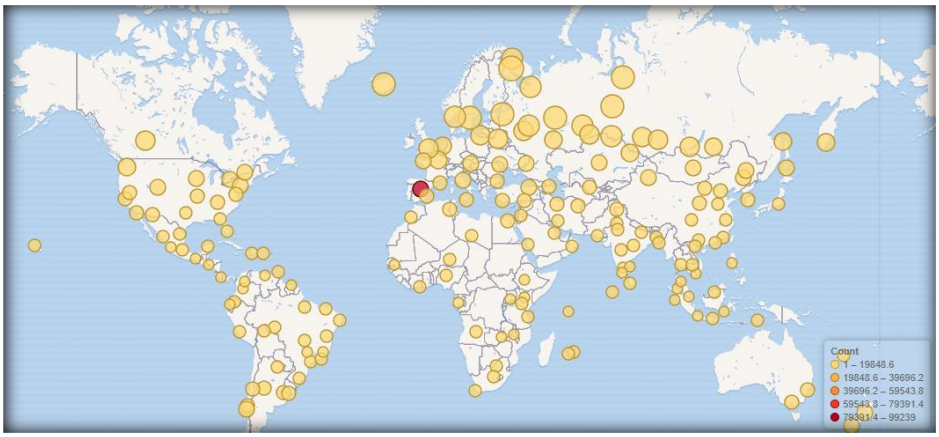


Figura E.0.106 Mapa de ataques de honeypot Suricata.

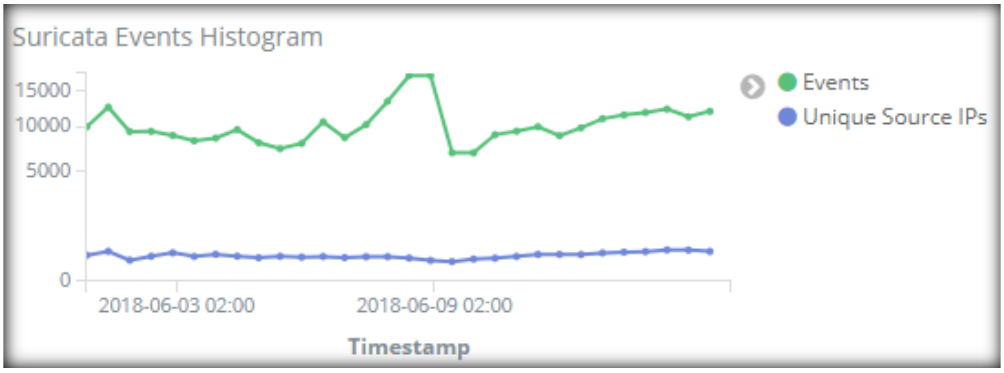


Figura E.0.107 Histograma de ataques de honeypot Suricata.

Podemos observar que los ataques realizados a este honeypot no han variado con respecto a antes de la ocultación, pues se han realizado miles de ataques contra este honeypot, en torno a doce mil por día, desde una media de 400 IPs (Figura E.0.107).

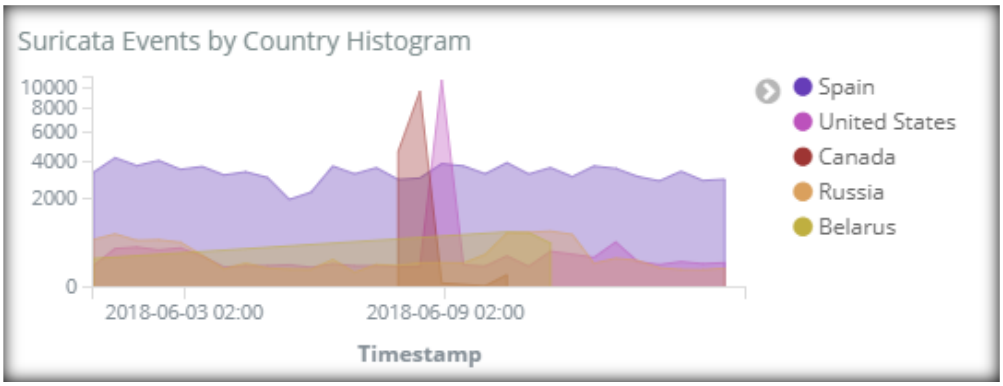


Figura E.0.108 Histograma de ataques por país de honeypot Suricata.

Aunque ha recibido ataques desde todas partes del mundo, destacan notablemente los ataques realizados en España (Figura E.0.106 y Figura E.0.108), y mayoritariamente sobre el puerto 53 (Figura E.0.109). Esto no ha variado con respecto a las medidas tomadas antes de la ocultación. También cabe destacar los dos picos de ataques que se produjeron el fin de semana por parte de Estados Unidos y Canadá.

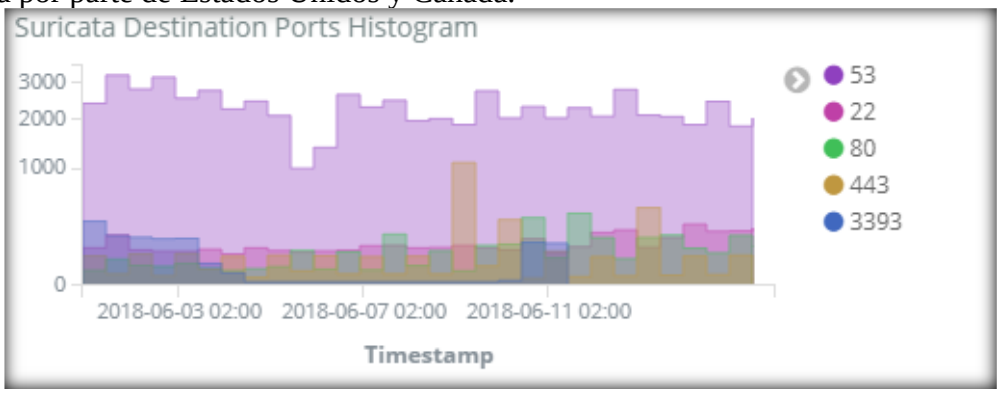


Figura E.0.109 Histograma de puertos atacados de honeypot Suricata.

A continuación podemos ver los rankings de los datos que ha recogido el honeypot Suricata, como los métodos http más utilizados, los tipos de archivo más enviados o los clientes SSH que se han utilizado (Figura E.0.110).

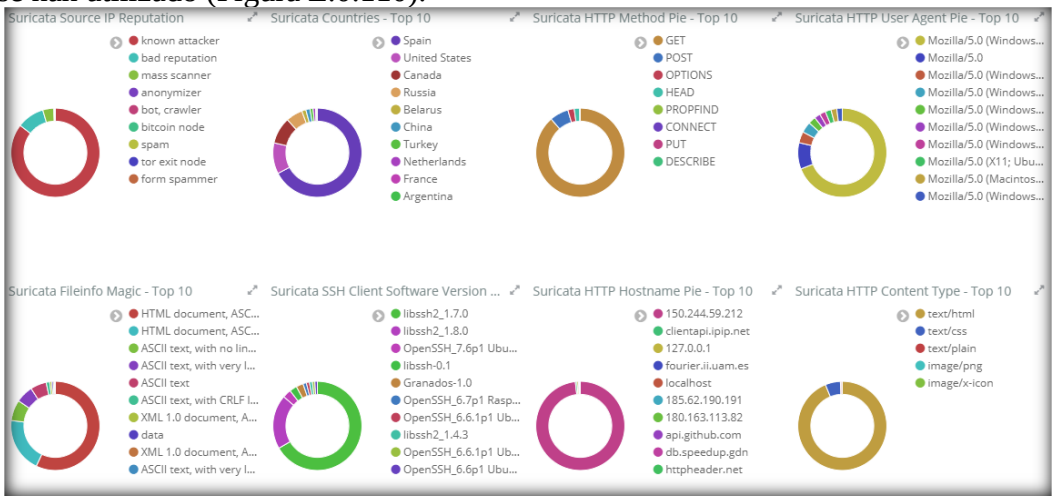


Figura E.0.110 Top 10 de datos de atacantes recogidos por honeypot Suricata.

Por último se muestra una lista de los mensajes más frecuentes de este honeypot en la *Tabla E.0.22*.

Descripción	Número de veces
Entidad Publica Empresarial Red.es	98801
B2 Net Solutions Inc.	14236
VolumeDrive	9599
TIS Dialog LLC	4019
Velcom AZS LLC	2255
DigitalOcean, LLC	2092
Quasi Networks LTD.	1932
Turk Telekom	1597
GitHub, Inc.	1425
AT&T Services, Inc.	1348

Tabla E.0.22 Descripción de los mensajes intercambiados de honeypot Suricata.

(10) Vnclowpot

Resultados del honeypot Vnclowpot, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.111 Mapa de ataques de honeypot Vnclowpot.

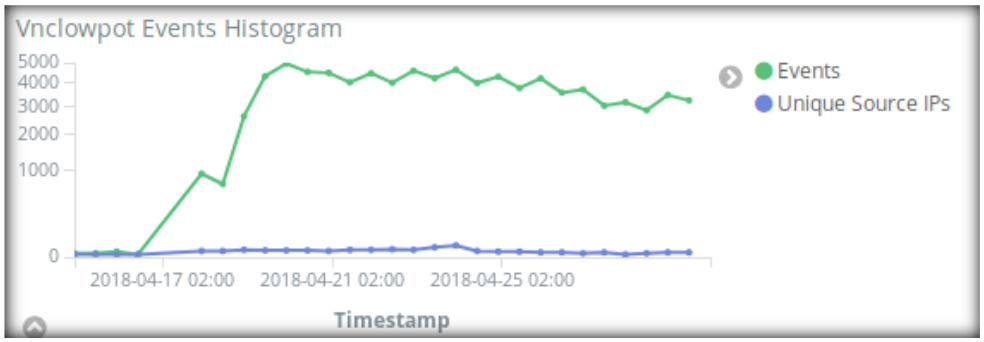


Figura E.0.112 Histograma de honeypot Vnclowpot.

El honeypot Vnclowpot empezó recibiendo prácticamente cero ataques en la primera semana. Sin embargo, a mediados de esa primera semana el número de ataques se incrementó masivamente, y después se mantuvo constante entre los cinco mil y los tres mil ataques por día (*Figura E.0.112*).

Dado que el número de direcciones IP no aumentó, se deduce que fueron esos mismos atacantes los que aumentaron el número de ataques que realizaban muy significativamente.

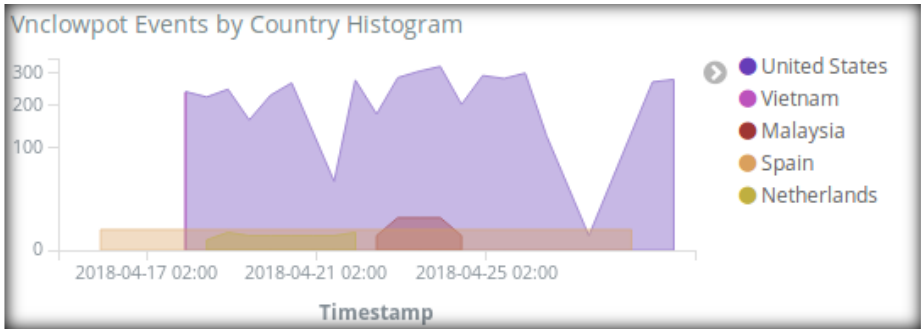


Figura E.0.113 Histograma de ataques por país de honeypot Vnclowpot.

El mayor atacante fue sin lugar a dudas Estados Unidos, aunque tuvo picos altos y bajos constantemente, sobre todo entre semana (*Figura E.0.111* y *Figura E.0.113*). Casi el 100% los ataques provenían de atacantes conocidos (*Figura E.0.113*).

Figura E.0.114 Izquierda: Reputación de IPs atacantes de honeypot Vnclowpot. Derecha: Top 10 países atacantes de Vnclowpot.

En la Tabla E.0.23 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
Hydra Communications Ltd	73609
sprint S.A.	9584
QuadraNet, Inc	4417
Viettel Group	237
Comcast Cable Communications, LLC	44
FranTech Solutions	43
MyKRIS Asia Sdn Bhd	34
Telefonica De Espana	20
RouteLabel V.O.F.	17
PCCW Limited	11

Tabla E.0.23 Proveedores de las IPs atacantes en Vnclowpot.

Además, analizando los logs se han obtenido los handshakes que más veces se realizaron en este honeypot (*Tabla E.0.24*).

VNC Handshake	Número de veces
vnc*00000000000000000000000000000000*00000000000000000000000000000000	143
vnc*00000000000000000000000000000000*D29F6E7F0456F8DED29F6E7F0456F8DE	142
vnc*00000000000000000000000000000000*00000002000000000000000000000000	36
vnc*00000000000000000000000000000000*B2730E28F81F8EB6B2730E28F81F8EB6	23
vnc*00000000000000000000000000000000*CD3CF4715B60D59CCD3CF4715B60D59C	23
vnc*00000000000000000000000000000000*91481F4EACBD55D291481F4EACBD55D2	14
vnc*00000000000000000000000000000000*A8A6A1DCA07614BEA8A6A1DCA07614BE	14
vnc*00000000000000000000000000000000*37D5DA0FD47CDC4937D5DA0FD47CDC49	13
vnc*00000000000000000000000000000000*5C7E94F0C6DAA3F25C7E94F0C6DAA3F2	13
vnc*00000000000000000000000000000000*FB9FD7D82DFAC165FB9FD7D82DFAC165	12

Tabla E.0.24 Intercambio VNC de honeypot Vnclowpot.

(b) Después de la ocultación

Figura E.0.115 Mapa de ataques de honeypot Vnclowpot.

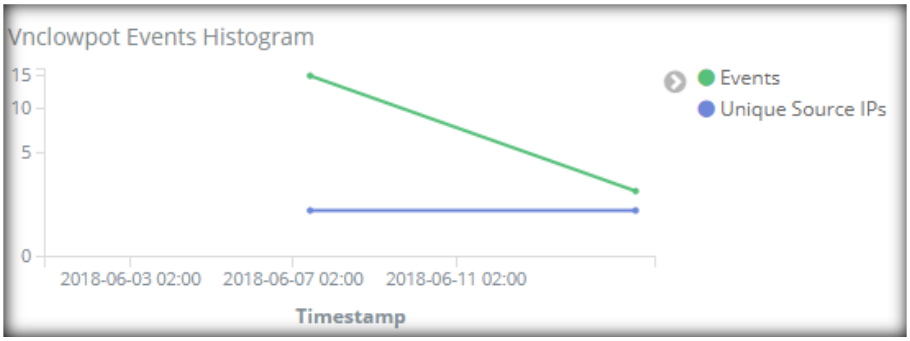


Figura E.0.116 Histograma de honeypot Vnclowpot.

En este honeypot se recogieron muchos menos ataques que antes de la ocultación. Apenas se recibieron ataques provenientes de muy pocas IPs (*Figura E.0.116*).

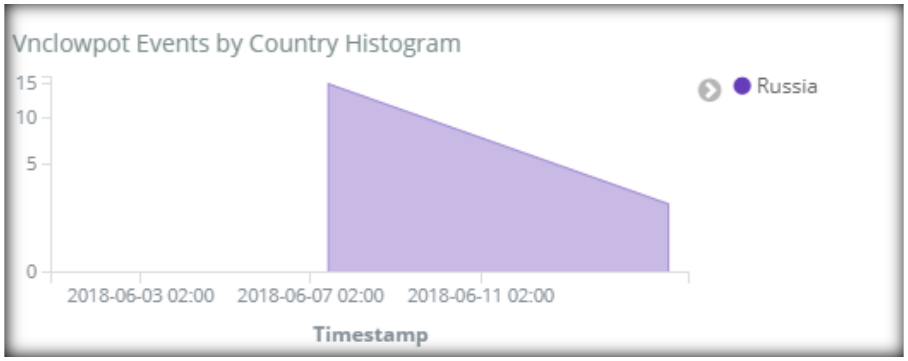


Figura E.0.117 Histograma de ataques por país de honeypot Vnclowpot.

El único país atacante fue Rusia, y no realizó ataques hasta la segunda semana (*Figura E.0.115* y *Figura E.0.117*).

En la Tabla E.0.25 podemos ver los proveedores de las IPs que más atacaron.

Compañía	Número de ataques
Rostelecom	15
Host Sailor Ltd.	2

Tabla E.0.25 Proveedores de las IPs atacantes en Vnclowpot.

Además, analizando los logs se han obtenido los handshakes que más veces se realizaron en este honeypot (*Tabla E.0.26*).

VNC Handshake	Número de veces
vnc*00000000000000000000000000000000*D29F6E7F0456F8DED29F6E7F0456F8DE	3
vnc*00000000000000000000000000000000*31FC1A8360CAFE2231FC1A8360CAFE22	1
vnc*00000000000000000000000000000000*37EDF607EF000000426430070058233	1
vnc*00000000000000000000000000000000*3BE9606AA472220F3BE9606AA472220F	1
vnc*00000000000000000000000000000000*3D237A19965ABE973D237A19965ABE97	1
vnc*00000000000000000000000000000000*6770889C612E9F276770889C612E9F27	1
vnc*00000000000000000000000000000000*77DFA81C9FD7B40777DFA81C9FD7B407	1
vnc*00000000000000000000000000000000*7B9511ECB4102AF77B9511ECB4102AF7	1
vnc*00000000000000000000000000000000*7EA5F49369FEA97B7EA5F49369FEA97B	1
vnc*00000000000000000000000000000000*BFF48BBEC9D1F29CBFF48BBEC9D1F29C	1

Tabla E.0.26 Intercambio VNC de honeypot Vnclowpot.

(11) eMobility

Resultados del honeypot eMobility, antes y después de la ocultación.

(a) Antes de la ocultación

Tan solo se registró un único ataque desde Brasil.

(b) Después de la ocultación

Nuevamente, solo se registraron dos ataques de Brasil, uno de España y uno de Estados Unidos. Este es con diferencia el honeypot que menos ataques ha recibido de toda la honeynet.

E.2 Honeynet B

En este apartado se muestran los resultados obtenidos tras la recogida de datos en la honeynet B, que se encuentra dentro del firewall de la Universidad Autónoma de Madrid.

(1) ConPot

Resultados del honeypot ConPot, antes y después de la ocultación.

(a) Antes de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(2) Cowrie

Resultados del honeypot Cowrie, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.118 Mapa de ataques de Cowrie.

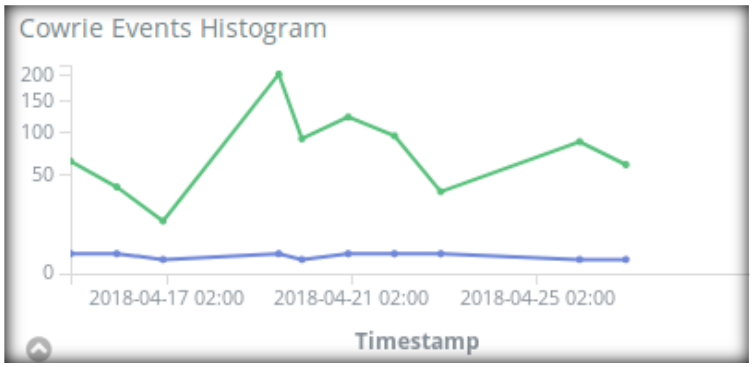


Figura E.0.119 Histograma de ataques de honeypot Cowrie.

En el honeypot Cowrie encontramos en torno a 100 ataques diarios de 10 IPs distintas (Figura E.0.119). Esto es cien veces menos que en el mismo Cowrie que recogió datos delante del firewall.

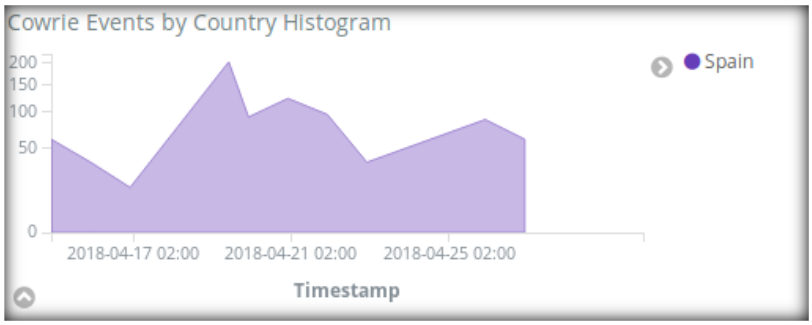


Figura E.0.120 Histograma de ataques por país de honeypot Cowrie.

En la gráfica de la Figura E.0.120 podemos observar que los ataques provenían únicamente de España (como también muestra el mapa de la Figura E.0.118), frente al Cowrie de la honeynet A que era atacada a nivel mundial.

Se ha descubierto que la gran mayoría de los ataques realizados en este honeypot han sido del CSIC de la UAM.
Todos los ataques se han producido mediante SSH, al puerto 2222 (Figura E.0.121).

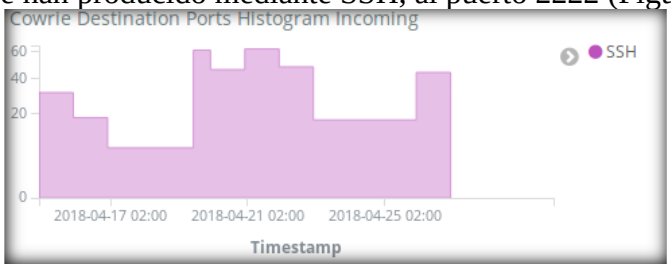


Figura E.0.121 Histograma de puertos atacados de honeypot Cowrie.

Por último se muestran en la Tabla E.0.27 los comandos más utilizados.

Command Line Input	CNT
ls	6
exit	3
cd /home/richard	2
cd richard/	2
	1
cd , ,	1
cd ,,	1
cd ..	1

Tabla E.0.27 Comandos más introducidos por los atacantes de honeypot Cowrie.

(b) Después de la ocultación

Se han registrado ocho ataques durante tres días, provenientes de tres direcciones IP distintas, todas ellas con geolocalización en España. No se ha podido obtener más información al respecto.

(3) Dionaea

Resultados del honeypot Dionaea, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.122 Mapa de ataques de honeypot Dionaea.

Solo hubo 4 ataques a Dionaea, como se puede ver en la Figura E.0.122.
Los nombres de usuarios utilizados para intentar este ataque fueron “user” y “null”, y las contraseñas “iloveyou” y “null”.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(4) ElasticPot

Resultados del honeypot ElasticPot, antes y después de la ocultación.

(a) Antes de la ocultación

No se ha realizado ningún ataque al honeypot ElasticPot de la honeynet que se encuentra dentro del firewall de la Universidad Autónoma de Madrid mientras ha durado este experimento.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(5) Glastopf

Resultados del honeypot Glastopf, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.123 Mapa de ataque de honeypot Glastopf.

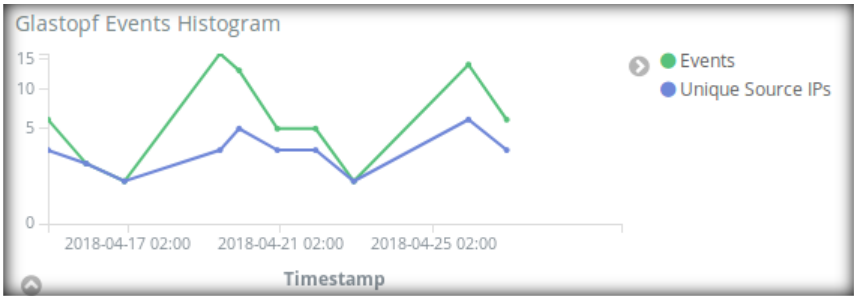


Figura E.0.124 Histograma de ataques de honeypot Glastopf.

En los resultados obtenidos por el honeypot Glastopf podemos comprobar que el número de ataques realizado tiene una estrecha relación en casi todos los casos con el número de IPs que atacaron (Figura E.0.124), de lo que se deduce que cada IP realizó solo uno o dos ataques. Este fenómeno también se dio en la honeynet A. Se han registrado entre 2 y 15 ataques al día.

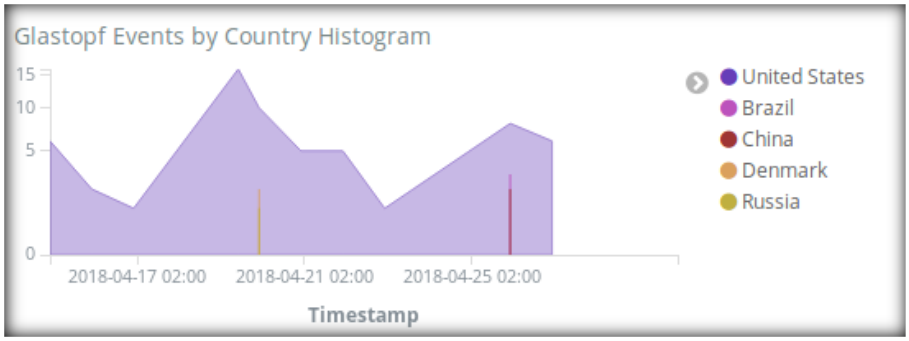


Figura E.0.125 Histograma de ataques de honeypot Glastopf.

Los países que más atacaron fueron Estados Unidos, Brasil, China y Rusia (Figura E.0.123). En este honeypot también coinciden los países atacantes con respecto a la honeynet A. Y de igual modo, en Estados Unidos y en Rusia se observa un descenso moderado de ataques el fin de semana (Figura E.0.125).

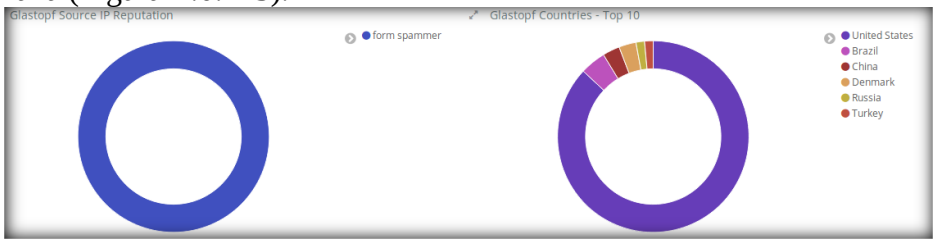


Figura E.0.126 Izquierda: Reputación de IPs atacantes de honeypot Glastopf. Derecha: Top 10 países de honeypot Glastopf.

Todos los ataques venían de bots especializados en rellenar formularios con spam, y casi el 90% de los ataques se produjo desde Estados Unidos (Figura E.0.126).
En la Tabla E.0.28 podemos ver los proveedores de las IPs que más atacaron.

Compañía	**Número de ataques**
Google LLC	60
China Unicom Beijing Province Network	2
Aruba S.p.A.	2
GIGANET SERVICOS DE INTERNET LTDA ME	2
TurkNet Iletisim Hizmetleri A.S	1
TELEFÔNICA BRASIL S.A	1
ABN LTD	1

Tabla E.0.28 Proveedores de las IPs atacantes en Glastopf.

(b) Después de la ocultación

Se han registrado 25 ataques provenientes de una sola dirección IP con geolocalización en España. No se han podido capturar más datos al respecto.

(6) Honeytrap

Resultados del honeypot Honeytrap, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.127 Mapa de ataques de honeypot Honeytrap.

El honeypot Honeytrap apenas ha tenido ataques, y menos aún en comparación con los seis mil ataques por día que recibía en la honeynet A.

Aunque los países que han atacado se asemejan bastante a los que atacaron la honeynet A (Figura E.0.127 y Figura E.0.74), es interesante puntuar que el puerto más atacado ha sido el 79 (Figura E.0.128), mientras que en la otra honeynet recibió la mayor cantidad de ataques en el puerto 4899 (Figura E.0.77).

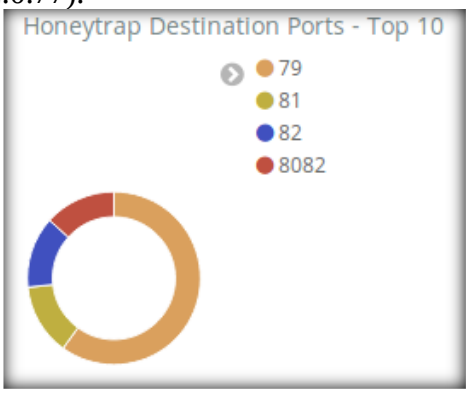


Figura E.0.128 Puertos atados de honeypot Honeytrap.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(7) Mailoney

Resultados del honeypot Mailoney, antes y después de la ocultación.

(a) Antes de la ocultación

No se han recogido ataques al honeypot Mailoney durante la fase de experimentación de este proyecto.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(8) Rdpy

Resultados del honeypot Rdpy, antes y después de la ocultación.

(a) Antes de la ocultación

No se han recogido ataques al honeypot Rdpy durante la fase de experimentación de este proyecto.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(9) Suricata

Resultados del honeypot Suricata, antes y después de la ocultación.

(a) Antes de la ocultación

Figura E.0.129 Mapa de ataques de honeypot Suricata.

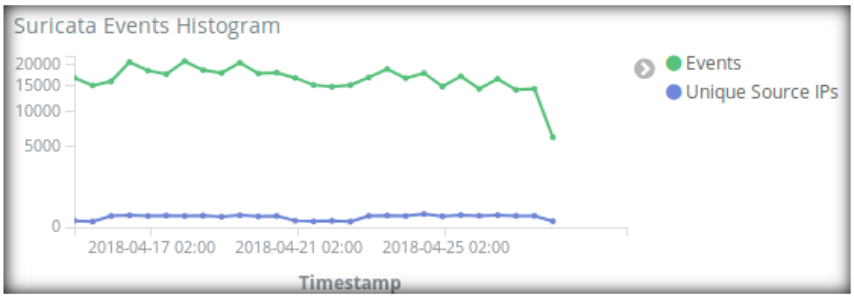


Figura E.0.130 Histograma de ataques de honeypot Suricata.

El honeypot Suricata ha sido el único que ha recibido más ataques que su correspondiente de la honeynet A. Ha recibido entre quince y veinte mil ataques al día (Figura E.0.130), frente a los doce mil que recibió el honeypot situado delante del firewall (Figura E.0.102). El número de IPs que han realizado estos ataques se mantiene constante en cifras pequeñas, tal y como ocurre en su siamesa de la honeypot A.

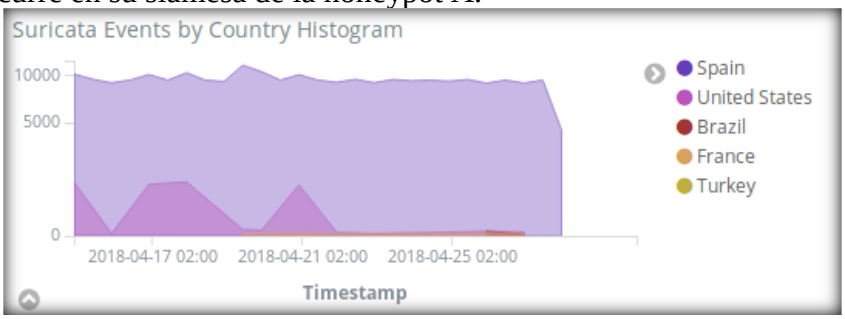


Figura E.0.131 Histograma de ataques de honeypot Suricata.

Podemos observar que la mayoría de los ataques provienen de España (Figura E.0.101 y Figura E.0.103), tal y como ocurrió en la honeynet A. Esto puede explicar por qué hay más ataques en este honeypot: el firewall de la universidad impide el paso a IPs que provengan de fuera del país, eliminando la mayoría de los ataques al resto de honeypots.

A continuación se muestran los rankings de los datos que ha recogido el honeypot Suricata, tales como los métodos http más utilizados, los tipos de archivo más enviados o los clientes SSH que se han utilizado (Figura E.0.132).

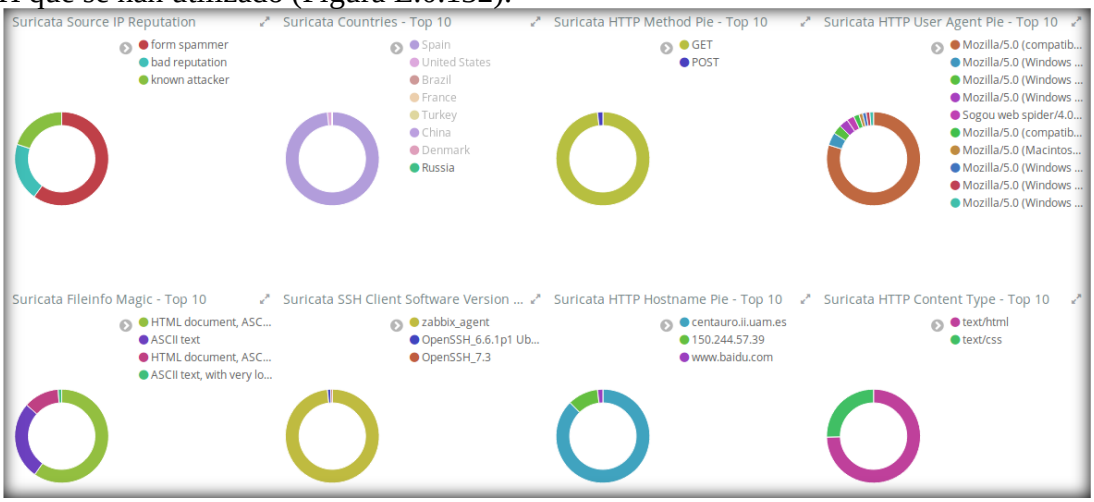


Figura E.0.132 Top 10 de datos de atacantes recogidos por honeypot Suricata.

Los dos puertos más atacados fueron el puerto 53 y el puerto 443 (Figura E.0.133).

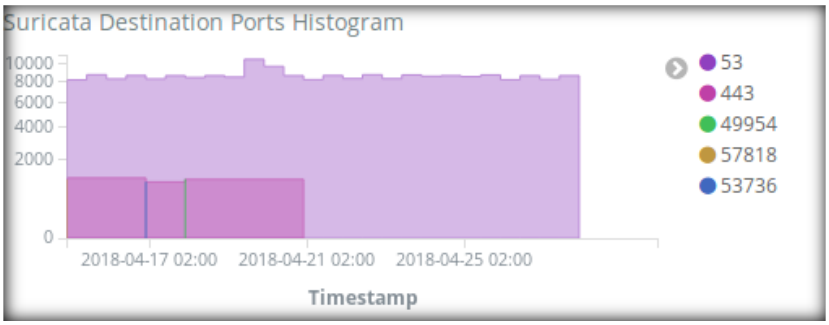


Figura E.0.133 Histograma de puertos atacados de honeypot Suricata.

Por último se muestra una lista de los mensajes más frecuentes de este honeypot en la *Tabla E.0.29*.

CNT	
SURICATA zero length padN option	177887
SURICATA IPv4 padding required	31453
SURICATA STREAM ESTABLISHED packet out of window	4296
SURICATA STREAM ESTABLISHED invalid ack	2185
SURICATA STREAM Packet with invalid ack	2185
ET POLICY SSH session in progress on Expected Port	43
SURICATA STREAM FIN recv but no session	15
SURICATA UDPv4 invalid checksum	13
ET POLICY Reserved Internal IP Traffic	6
SURICATA STREAM Packet with broken ack	4

Tabla E.0.29 Descripción de los mensajes intercambiados de honeypot Suricata

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(10) Vnclowpot

Resultados del honeypot Vnclowpot, antes y después de la ocultación.

(a) Antes de la ocultación

No se han capturado ataques contra el honeypot Vnclowpot durante la fase de experimentación de este proyecto.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

(11) eMobility

Resultados del honeypot eMobility, antes y después de la ocultación.

(a) Antes de la ocultación

No se han capturado ataques contra el honeypot eMobility durante la fase de experimentación de este proyecto.

(b) Después de la ocultación

No se han capturado ataques contra este honeypot durante la fase de experimentación de este proyecto.

E.3 Conclusiones del análisis

A partir de todos los datos recogidos, se han llegado a las siguientes conclusiones:

Los ataques recogidos en la honeynet B son escasos y proceden de un grupo tan reducido de IPs que no pueden ser considerados como válidos para esclarecer la eficacia de la ocultación de los honeypots. No obstante, se puede observar una comparativa de los ataques realizados a esta honeynet antes y después de la ocultación en la Figura E.0.135.

Los ataques de la honeynet A, sin embargo, han superado el millón, y provienen de cientos de IPs distintas, por lo que conforman una base de datos lo suficientemente grande como para sacar conclusiones.

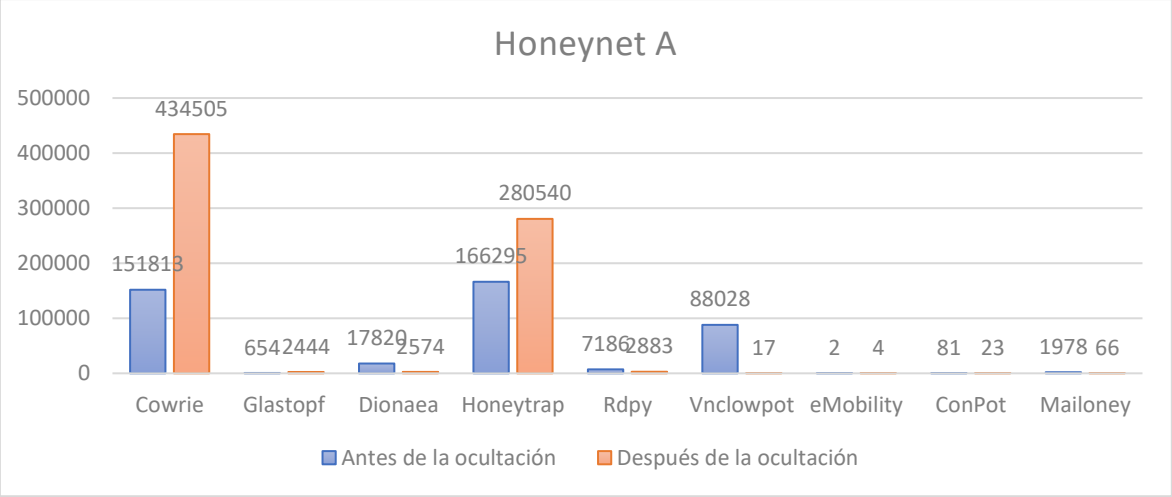


Figura E.0.134 Comparativa de ataques en la honeynet A antes y después de la ocultación.

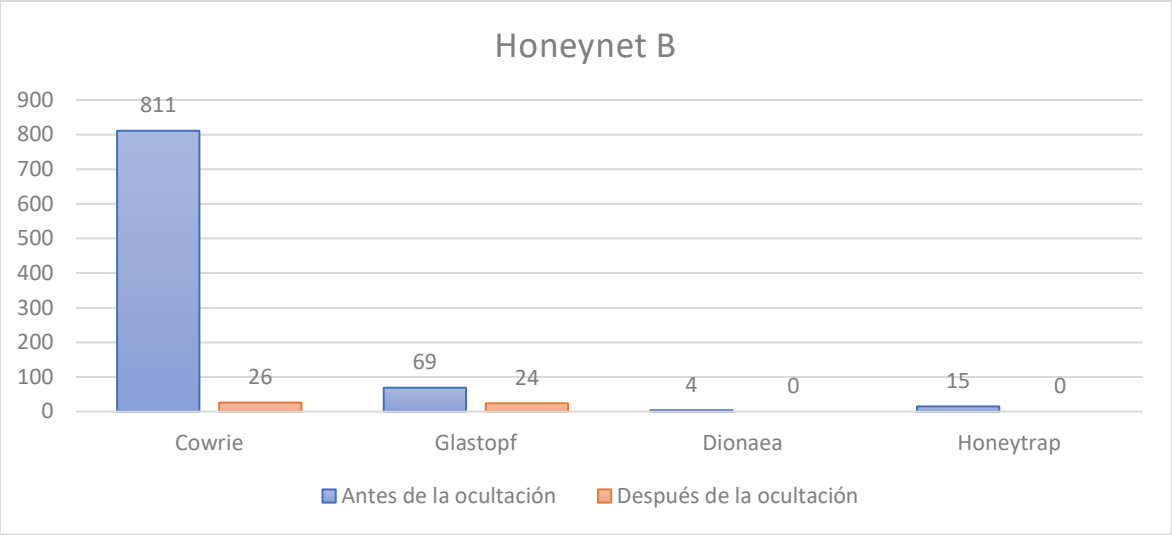


Figura E.0.135 Comparativa de ataques en la honeynet B antes y después de la ocultación.

Como podemos apreciar en la Figura E.0.134, el número de ataques recibidos tras la ocultación en la mayoría de los honeypots es mayor. En dicha figura podemos apreciar como Cowrie y Glastopf, que fueron fuertemente ocultados, triplicaron el número de ataques.

Sin embargo, también se descubrió que la cantidad de ataques al honeypot Honeytrap aumentó sustancialmente, a pesar de que este honeypot no se ocultó. La conclusión que se puede sacar de este dato es que los atacantes en la mayoría de las ocasiones no se limitan a atacar a un solo puerto y servicio, sino que al descubrir una IP tratan de vulnerarla de distintas formas. Por ello, la ocultación de cuatro honeypots ha supuesto también un aumento en el número de ataques del resto de honeypots de la honeynet.

F Grados de confianza que asigna la herramienta de detección

El algoritmo que he empleado para dar una probabilidad de que una dirección IP contenga un honeypot se basa en dar un grado de confianza según el número de tests que haya pasado y los puertos abiertos que tenga.

De esa forma, en el caso de que tras realizar un escaneo de puertos a una IP se detecte que tiene abiertos los mismos puertos que utiliza un determinado honeypot, se le da a ese honeypot un +30% de posibilidades de base.

Además, por cada test de ese honeypot que de positivo, se incrementará esa posibilidad un tanto por ciento que dependerá del tipo de test. De esa forma, un solo test decisivo podría sumar un +70% (que unido al 30% inicial haría el 100% de probabilidades de que ese honeypot resida en esa IP), mientras que test que simplemente indican indicios de posibles honeypots pueden sumar solo un 10%. Cada test puede ser suficiente, pero no necesario.

El motivo por el que se ha decidido que esta medición sea aditiva en vez de dotar de un tanto por ciento determinado a cada test y después normalizarlo con el número de tests es que pueden darse ocasiones en el que una IP con honeypot de negativo en un test decisivo, pero positivo en todos los tests secundarios, confirmando de igual manera que se trata de un honeypot que quizá se ha tratado de ocultar contra ese determinado test.

Además, al implementar el algoritmo de esta forma aditiva, será más sencillo realizar el cálculo al añadir nuevos tests a la herramienta.
En la Tabla F.0.30 se pueden ver los valores que se ha dado para este proyecto a los distintos tests implementados. No obstante, cabe destacar que estos parámetros son configurables, y en el futuro se podrían modificar.

Test	Adición	Combinación 2 o más
mismos puertos	30%	
conpot01	70%	
cowrie01	70%	
cowrie02	70%	
cowrie03	20%	40%
cowrie04	30%	
dionaea01	30%	
dionaea02	30%	60%
dionaea03	30%	
glastopf01	40%	

Tabla F.0.30 Porcentajes del grado de confianza que aporta cada test.

De esta forma, una IP que tenga los mismos puertos que Cowrie será puntuada con un 30% de probabilidad, pero si además da positivo el test cowrie03 será puntuada con un 30+20=50%, y si da positivo tanto en el test cowrie03 como en el test cowrie04 será puntuada con 30+40=70% de probabilidad.

En caso de que la dirección IP de positivo en varios tests y la suma sea superior a 100, se normaliza mostrando un 100% de probabilidades de que exista un honeypot alojado en esa dirección.