2016

HIGH LEVEL CONFERENCE ON ASSURANCE

8-9 de Junio, Madrid

AnÆlisis de las Tendencias de Ataques de Malware en Sistemas Seæuelo para InformÆtica Forense

Diego Jurado PallarØs y Juan Antonio Velasco G mez

*Ganadores del **#RetoISACA 2016***

ISACA®
Sistemas de información fiables y valiosos
Madrid Chapter

$whoarewe


MUNDO
HACKER
#mundohackerday
GANADOR
III CONCURSO JÓVENES PROFESIONALES
Análisis de las Tendencias de Ataques de Malware en
Sistemas Señuelo para Informática Forense
Páguese a: Juan Antonio Velasco Gómez y Diego Jurado Pallarés
La cantidad de: € 1.000,-
ISACA
Madrid Chapter

Esquema

- Introducción
- Definición de un Honeypot
  - Finalidad y Clasificación
- Diseño de la Red
  - Implementación, Mejoras y Ocultación.
- Resultados Obtenidos
- Análisis Forense
- Conclusiones y Trabajo Futuro

#RetoISACA 2016

Definici n

- Sistema muy flexible en la seguridad informática.
- Atrae y analiza el comportamiento de los atacantes en internet.
- Provee al informático forense de una información extremadamente valiosa.

Objetivo: Capturar todo el tráfico de red entrante y conocer los detalles acerca de las tendencias y metodologías de los atacantes así como los fallos de seguridad a los que se está expuesto.

Finalidad de un honeypot

- Expuesto deliberadamente para ser atacado.
- Desviar y distraer la atención del atacante.
- Detectar y aprender nuevas vulnerabilidades de los sistemas.
- Obtener información del atacante.
- Obtener tendencias de ataque y países más atacados.
- Detectar nuevas muestras de malware.
- Recopilar y estudiar tendencias de ataque.
- Aprendizaje en temas de malware.
- Uso como complemento a otras herramientas de seguridad.

Clasificaci n de honeypots

Uso

Producci n

- Prevenir, detectar y responder.
- Proteger organizaciones en ambientes reales
  de operación.
- Alertar a los administradores

Investigaci n

- Aprendizaje. Recursos educativos.
- Recuperar la mayor cantidad de información
  posible para detectar patrones o analizar
  nuevas tendencias.
- Retener al intruso el mayor tiempo posible
  dentro del honeypot.

Interacción

Baja

- Investigación de acciones fraudulentas en la red.
- Detectar nuevas amenazas.
- Fáciles de utilizar y de mantener, riesgo casi nulo.
- Instalación en herramientas de virtualización.

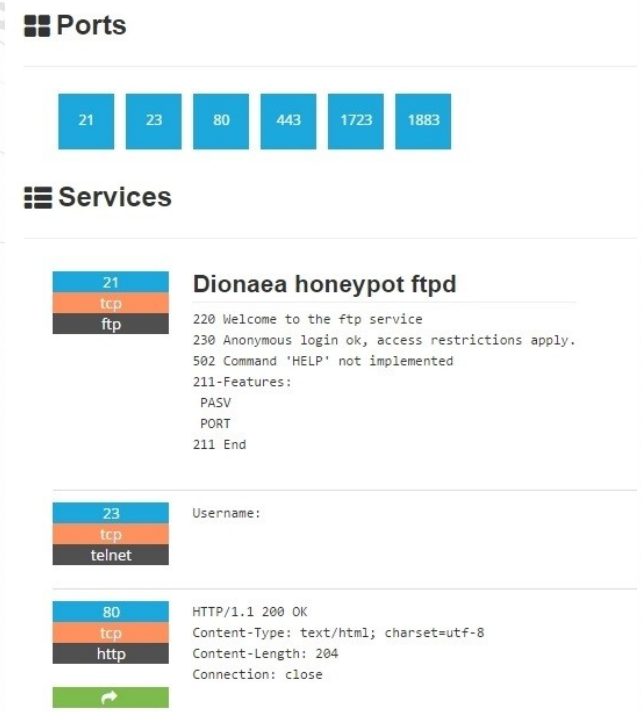
Media

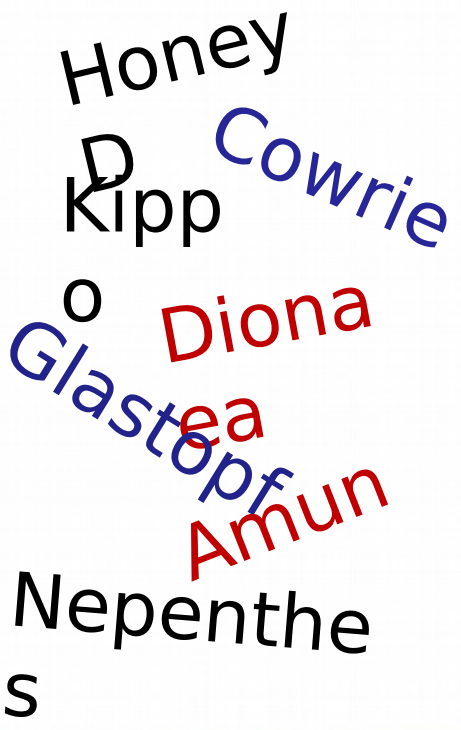
- Mayor nivel de interacción que los de bajo nivel.
- Recolectar información sobre actividades de atacantes.
- No emulan únicamente ciertos servicios, también software
  en particular. Mayor riesgo y más complejos.

Alta

- Construidos con máquinas reales, como un usuario normal.
- Usados en red interna y único objetivo: ser atacados.
- Cada interacción se considera sospechosa por definición.
- Tráfico monitorizado y almacenado en una zona segura.

¿Pero quØhoneypot usamos?

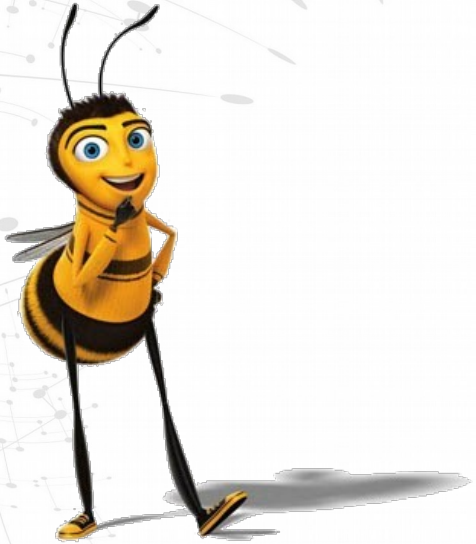


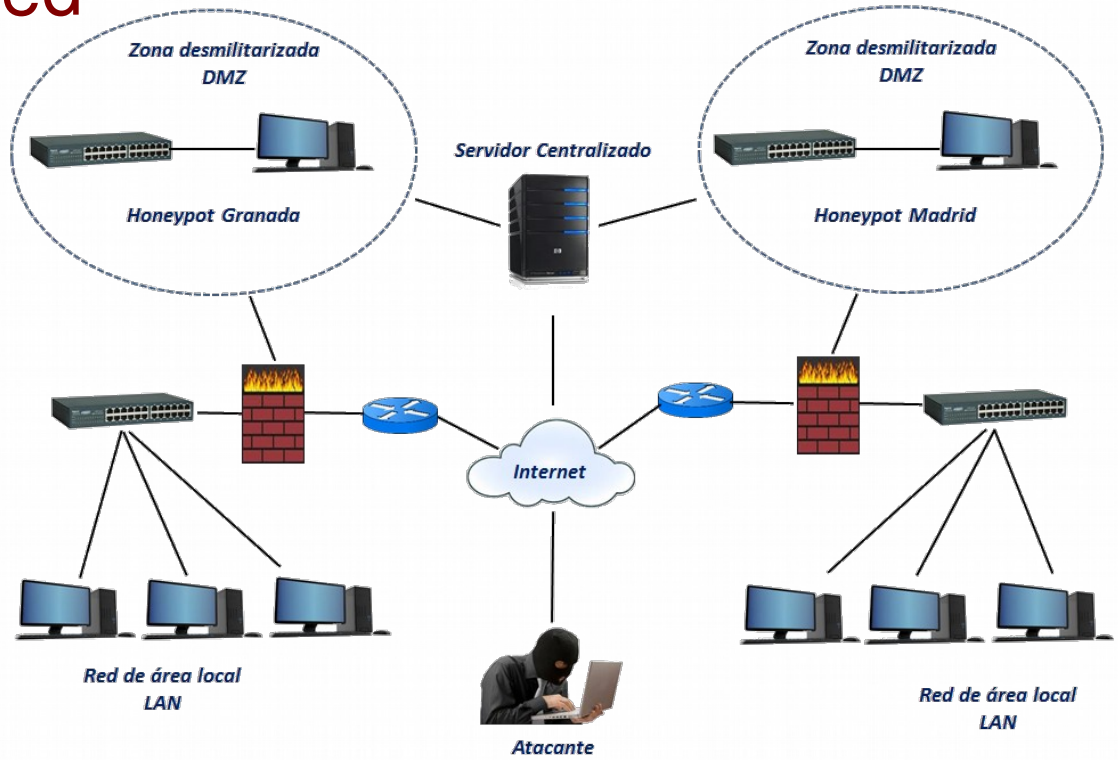


Caracter sticas Honeypot Cowrie

- Simula un sistema Debian real, con un sistema de archivos completamente personalizable.
- Recopila información sobre los intentos de sesión de los atacantes.
- Permite detectar ataques por fuerza bruta.
- Guarda las sesiones de los atacantes.
- Almacena los hashes de las muestras de Malware obtenidas.

Diseæo de la red





No es oro todo lo que reluce…

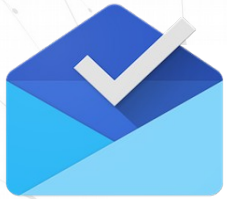
Mejora y ocultaci n honeypot

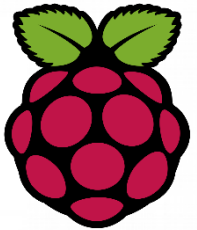
- Modificación y gestión de usuarios mediante sistemas de archivos.
  - Eliminando usuarios por defecto
  - Creación de usuarios reales
- Mejorando los directorios del sistema.
  - Sistema archivos básico
  - Editando directorios importantes (/etc, /tmp, /var, /opt)
  - Directorios para diferentes usuarios “trampa”

Mejora y ocultaci n honeypot

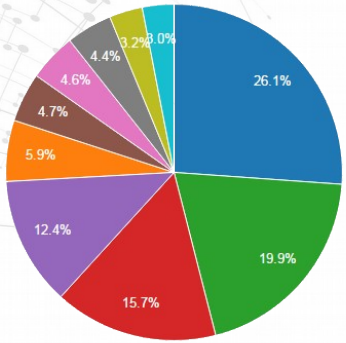
- Modificando archivos configuración del Honeypot Cowrie.
  - Hostname
  - Versiones del Cliente SSH

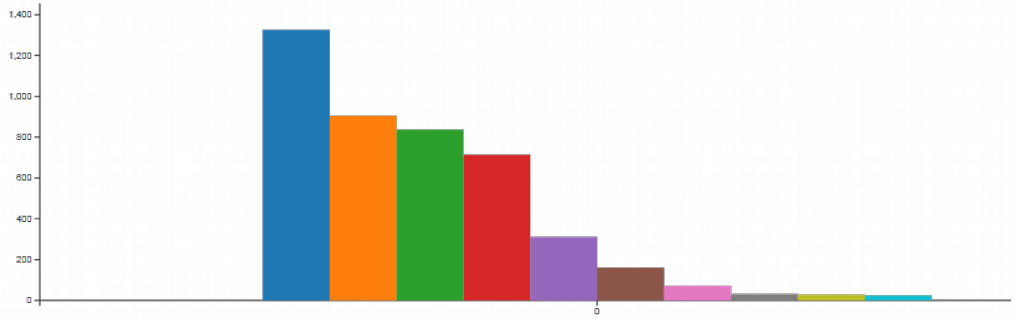
Implementaci n

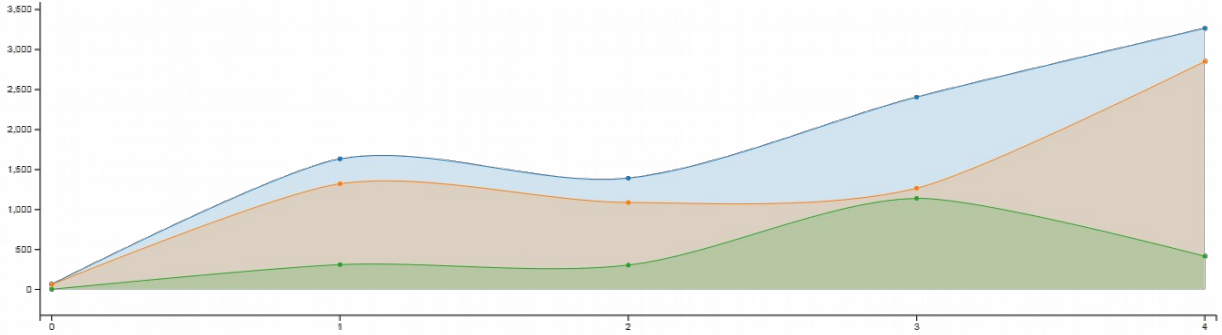




Herramienta de visualizaci n web







DECEPTIONPI

ISACA
Trust in, and value from, information systems

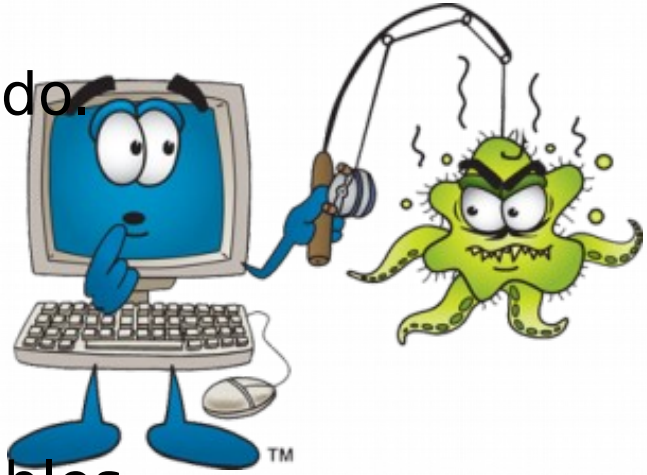
MUNDO HACKER 2016

A proyect build for

RetoISACA 2016

AnÆlisis Forense

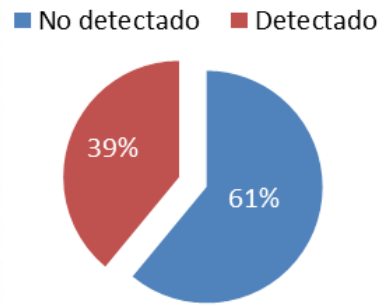
- Detección de Botnets.
- Análisis del Malware obtenido.
- Ataques de Fuerza Bruta.
- Securización mediante IPTables.



Detecci n de Botnets

- Identificación mediante comportamiento.
- Automatización mediante listas de reputación.

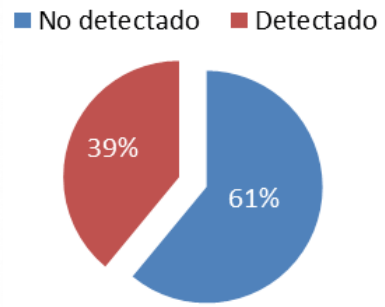
```
root@HoneyPi:/opt/PruebasIsaca# python3 IP-Repu.py suspicious_ips.txt
 [+] 58.218.199.166 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 27.72.64.222 Good IP Reputation
 [+] 74.208.127.6 Good IP Reputation
 [+] 95.128.43.164 Bad IP Reputation -> Unknown Spam Bot masking himself as a normal user on 15 July 2015
 [+] 178.151.69.1 Good IP Reputation
 [+] 58.218.204.248 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 139.162.4.25 Good IP Reputation
```



Detecci n de Botnets

- Identificación mediante comportamiento.
- Automatización mediante listas de reputación.

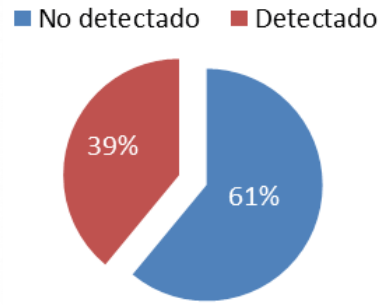
```
root@HoneyPi:/opt/PruebasIsaca# python3 IP-Repu.py suspicious_ips.txt
 [+] 58.218.199.166 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 27.72.64.222 Good IP Reputation
 [+] 74.208.127.6 Good IP Reputation
 [+] 95.128.43.164 Bad IP Reputation -> Unknown Spam Bot masking himself as a normal user on 15 July 2015
 [+] 178.151.69.1 Good IP Reputation
 [+] 58.218.204.248 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 139.162.4.25 Good IP Reputation
```



Detecci n de Botnets

- Identificación mediante comportamiento.
- Automatización mediante listas de reputación.

```
root@HoneyPi:/opt/PruebasIsaca# python3 IP-Repu.py suspicious_ips.txt
 [+] 58.218.199.166 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 27.72.64.222 Good IP Reputation
 [+] 74.208.127.6 Good IP Reputation
 [+] 95.128.43.164 Bad IP Reputation -> Unknown Spam Bot masking himself as a normal user on 15 July 2015
 [+] 178.151.69.1 Good IP Reputation
 [+] 58.218.204.248 Bad IP Reputation -> User Submission - Hacker from this IP on 16 April 2016
 [+] 139.162.4.25 Good IP Reputation
```



AnÆlisis de Malware

- Parada de Cortafuegos.
- Comprobación del sistema en que se encuentra
  - Ejecución de Comandos.
- Inclusión del sistema en una Bot
- Borrado de huellas.
  - Historial y logs.
- Descargas de Malware con WGE
  - Independientes de la arquit

AnÆÈsis de Malware

Número de muestras registradas : 830

```
Results for MD5:  320adee47e53823a1be8a335e4beb246

Detected by:  33 / 57

Sophos Detection: Mal/Generic-S

Kaspersky Detection: Trojan.Linux.Agent.f

ESET Detection: Linux/PNScan.A

Scanned on: 2016-06-06 20:13:04

Results for MD5:  5afdcceb2fc5fc1c15d7fdbef674c6a5

Detected by:  27 / 57

Sophos Detection: Mal/Generic-S

Kaspersky Detection: Backdoor.Linux.Agent.ac

ESET Detection: a variant of Linux/PNScan.A

Scanned on: 2016-06-06 20:05:54

Results for MD5:  856f14251f643bac62b9193c54449472

Detected by:  31 / 57

Sophos Detection: Mal/Generic-S

Kaspersky Detection: Backdoor.Linux.Agent.ae

ESET Detection: Linux/PNScan.A

Scanned on: 2016-06-06 20:06:13
root@HoneyPi:/opt/PruebasIsaca#
```

Ataques de Fuerza Bruta y Securizaci n

- Detección de ataques de fuerza bruta por diccionario
- Registradas 8700 combinaciones usuario/contraseña
  - 33% son únicas
  - 11% consigue su objetivo -> comprometer
- Solución!! ... configuración de reglas con IPTables
  - Ignorar tráfico que proviene de IPs sospechosas (Blacklist)
  - Mejor aún : bloquear todo el tráfico & permitir conexiones fiables (Whitelist)


```
iptables -A INPUT -s 155.67.33.49 -j DROP
```

Conclusiones

- Cambiar el puerto SSH por defecto.
- No permitir la autentificación como usuario root.
- Implementar medidas contra ataques por fuerza bruta.
- Uso de contraseñas más fuertes.
- Hacer uso de las opciones host.allow y host.deny para especificar que IP’s se van permitir y cúales no.

Trabajo futuro

- Implementar otras honeypots en nuestra red.
- Mejorar la automatización de extración de datos.
- Fortificar nuestros servicios.
- Emular otros servicios como Telnet.
- Reconfigurar reglas de firewalls e iptables.
- Mejorar la visualización de datos.
- Machine learning y obtener inteligencia.

¿Preguntas?