SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Introducción al Análisis Forense en Servidores Web

CEILAC
Centro de Emprendimiento e Internet

ICANN

LACTLD
Latin American and Caribbean ccTLDs Organization

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

TETÃ REKUÁI
GOBIERNO NACIONAL
Jajapo ñande raperã ko'ãga guive
Construyendo el futuro hoy

Disclaimer

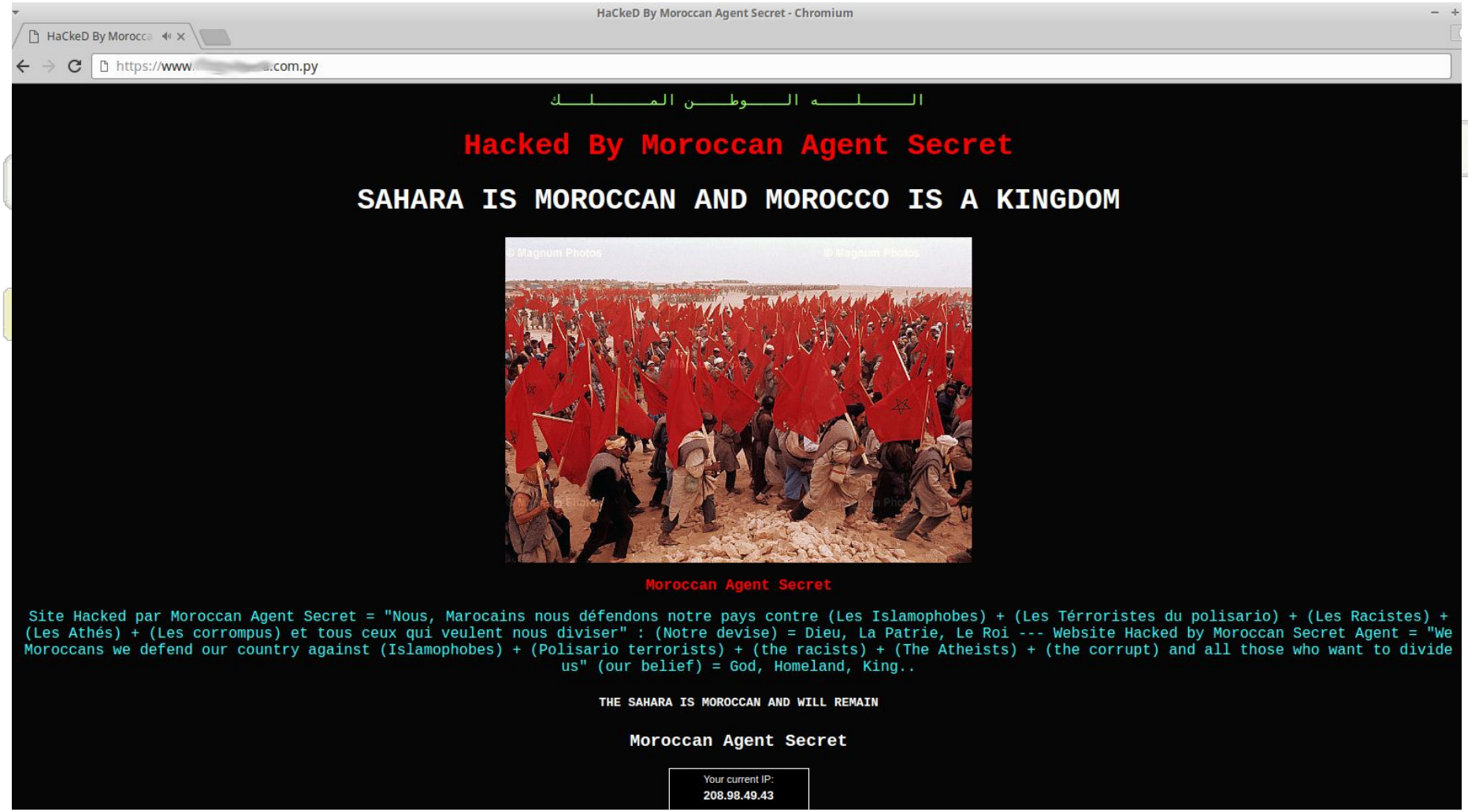
Todo el contenido de esta presentación es únicamente con fines didácticos y educativos. El uso indebido de las técnicas y/o conocimientos utilizadas en esta presentación puede ir en contra de las leyes nacionales e internacionales. El autor no se hace responsable por el uso del conocimiento contenido en la siguiente presentación. La información contenida debe ser utilizada únicamente para fines éticos y con la debida autorización.

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Mi sitio web fue hackeado!



Mi sitio web fue hackeado!

¿Para qué atacan mi servidor web?

- Hacktivismo/Defacement
- Distribución de malware
- Phishing
- Spam
- Proxies maliciosos
- DoS/DDoS
- Click Fraud

Errores comunes

- Eliminar el archivo visible
- Backup viejo sin verificar
- Solo actualizar CMS/plugin

Qué es lo correcto?

Auditoría!

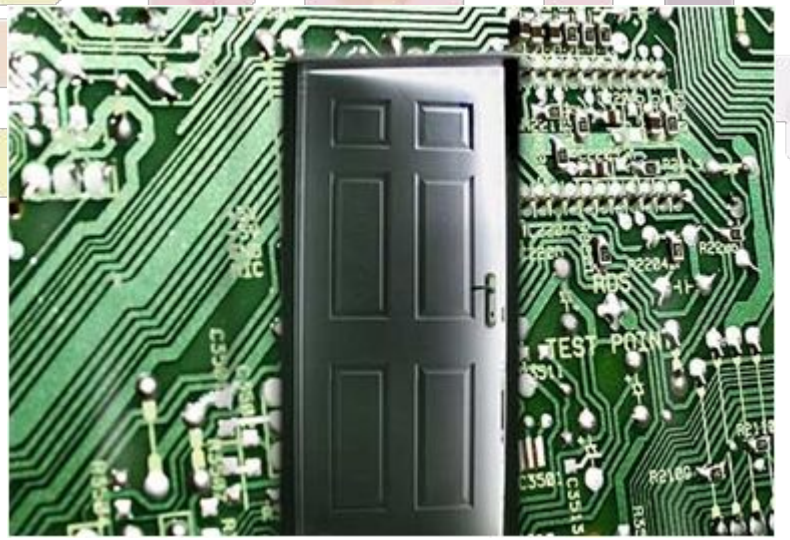
¿Cómo entraron? ...

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

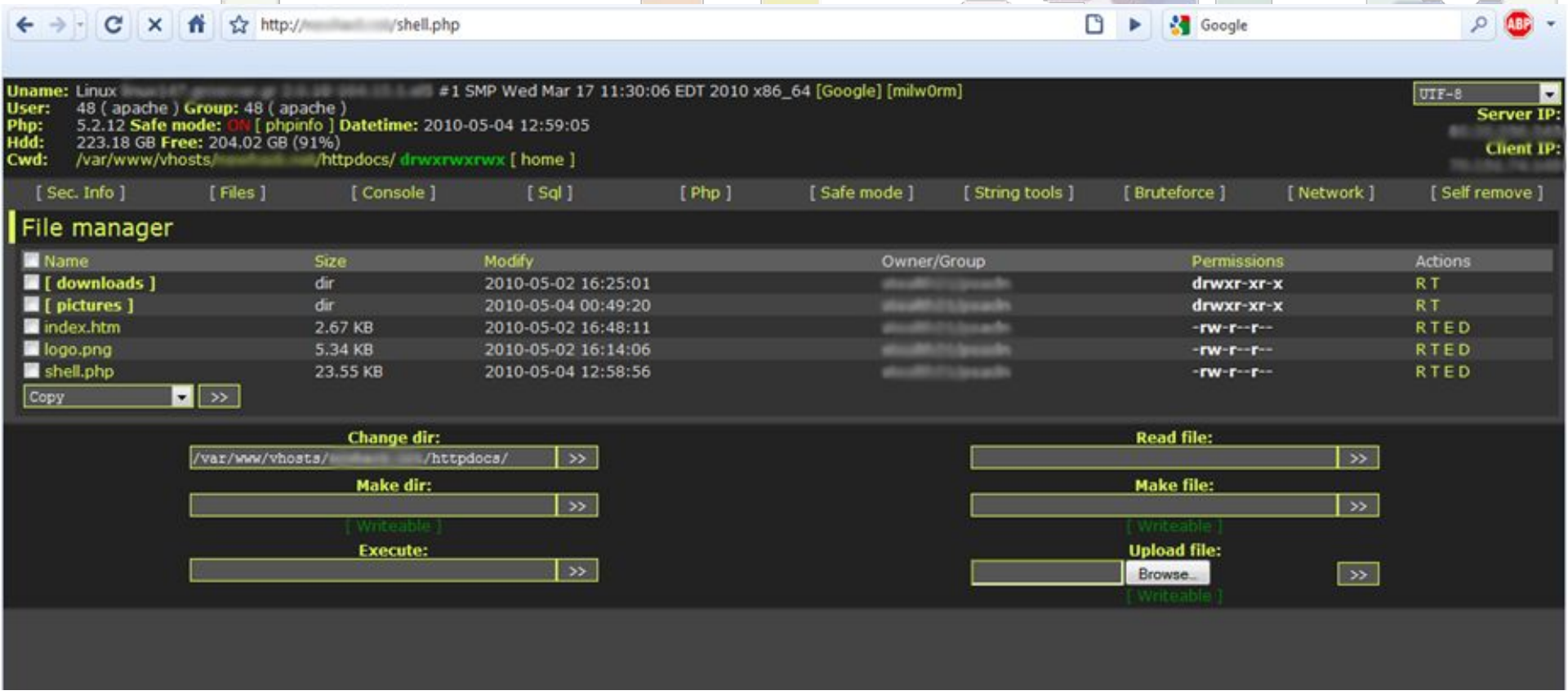
GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Webshell y Backdoors

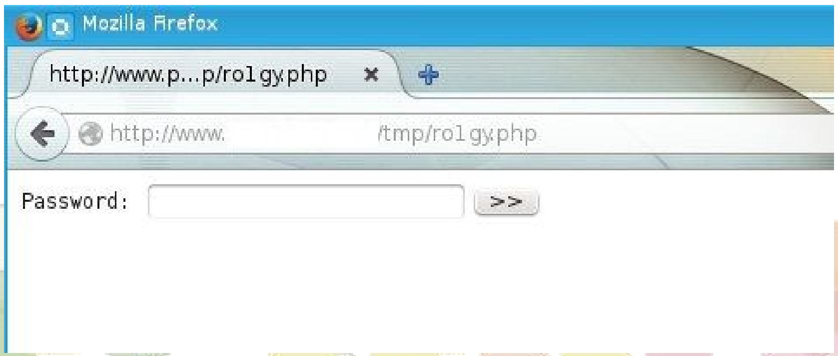


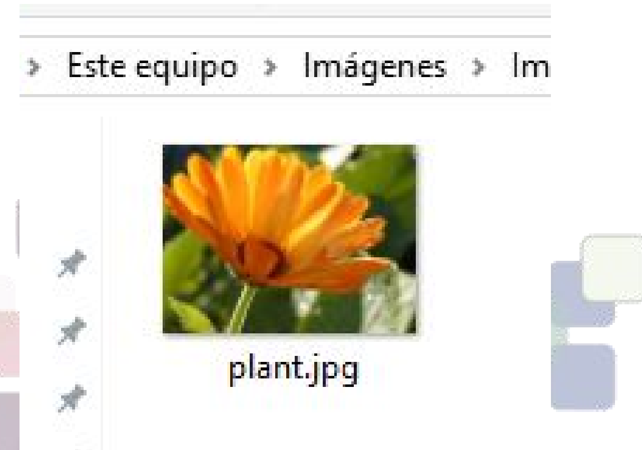
Webshells

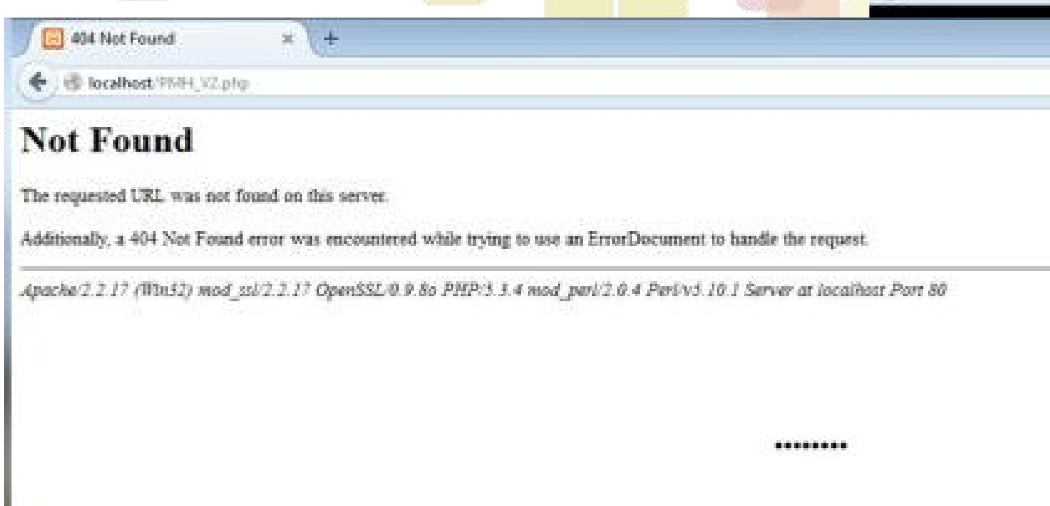
Script utilizado por un atacante como herramienta, cuya función es la de ejecutar comandos en el servidor donde se encuentra alojada.



Webshells (1)


Mozilla Firefox
http://www.p...p/ro1gy.php
http://www. /tmp/ro1gy.php
Password:
>>


Este equipo › Imágenes › Im
plant.jpg


404 Not Found
localhost/PMH_V2.php
Not Found
The requested URL was not found on this server.
Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.
Apache/2.2.17 (Win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1 Server at localhost Port 80


Team Pakistani Muslim Ha...

Backdoor

Un “hueco” por donde un atacante puede tomar control de un sistema sin necesidad de explotar vulnerabilidades, evitando las medidas de seguridad implementadas.

- Invisibles para el usuario
- Se ejecutan en modo silencioso al iniciar el sistema.
- Pueden tener acceso total a las funciones del host-víctima.
- Son difíciles de eliminar ya que se instalan en carpetas de sistema, registros o cualquier dirección.
- Usa un programa blinder para configurar y disfrazar al servidor

Backdoor (1)

```
root@encode:~# nc -l -v -p 4444
listening on [any] 4444 ...
172.16.212.133: inverse host lookup failed: Unknown server error : Connection timed out
connect to [172.16.212.1] from (UNKNOWN) [172.16.212.133] 34529
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
pwd
/
```

```
/ $ netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:5357            0.0.0.0:*
tcp        0      0 192.168.1.1:80          0.0.0.0:*
tcp        0      0 0.0.0.0:38777           0.0.0.0:*
udp        0      0 0.0.0.0:1025            0.0.0.0:*
udp        0      0 192.168.1.1:1027        0.0.0.0:*
udp        0      0 127.0.0.1:38032         0.0.0.0:*
udp        0      0 0.0.0.0:42000           0.0.0.0:*
udp        0      0 0.0.0.0:20000           0.0.0.0:*
udp        0      0 0.0.0.0:1701            0.0.0.0:*
udp        0      0 0.0.0.0:53413           0.0.0.0:*
udp        0      0 0.0.0.0:20010           0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:39000           0.0.0.0:*
udp        0      0 0.0.0.0:1900            0.0.0.0:*
udp        0      0 0.0.0.0:38000           0.0.0.0:*
```

SECRETARÍA
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

WELCOME TO HACKER-DEMO

Cuando la webshell no es suficiente..

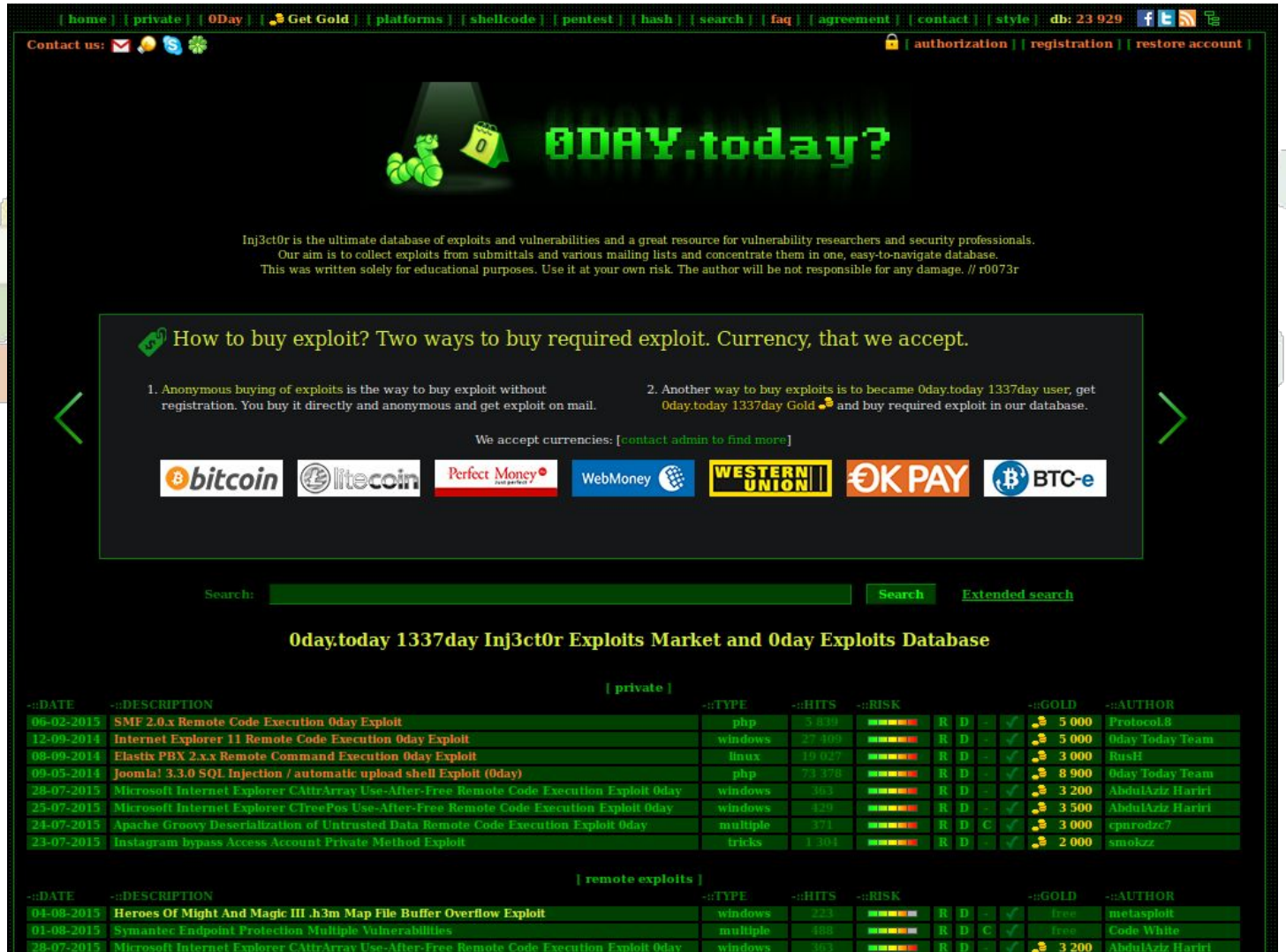
Escalación de privilegios

Para realizar un daño real y persistente en un sistema, se requiere privilegios de **root**

Explotación de vulnerabilidades → Escalación de privilegios

```
$gcc cve_2016_0728.c -o cve_2016_0728 -lkeyutils -Wall
$./cve_2016_0728 PP1
uid=1000, euid=1000
Increfing...
finished increfing
forking...
finished forking
caling revoke...
uid=0, euid=0
#
# whoami
root
#
```

Vulnerabilidades y exploits



Vulnerabilidades y exploits (1)

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security Exploit Database Archive

34045
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn **about the Exploit Database**.

Google Hacking Database

The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more.

Visit the Google Hacking Database

GOOGLE HACKING DATABASE
BY OFFENSIVE SECURITY

Remote Exploits

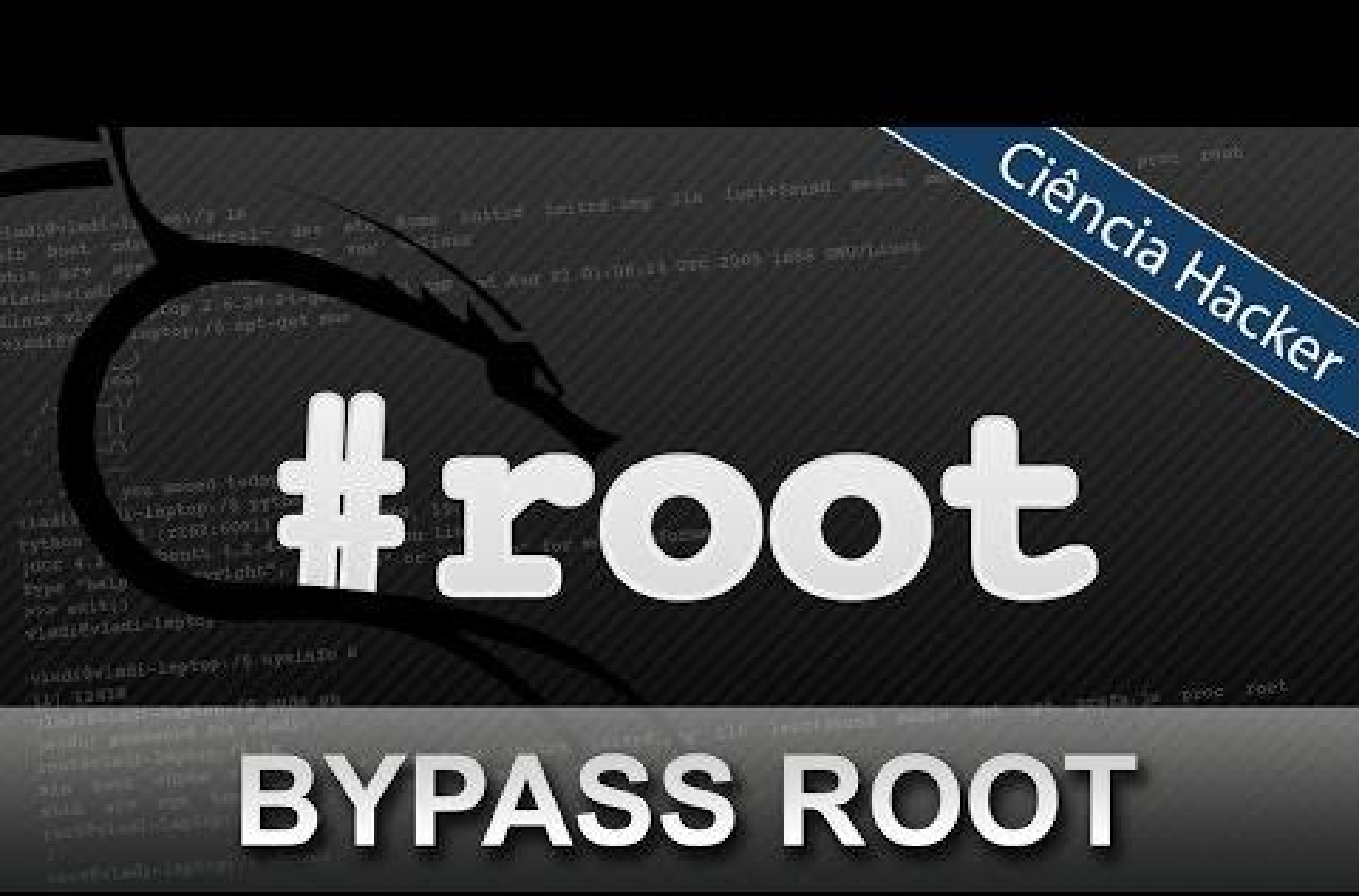
This exploit category includes exploits for remote services or applications, including client side exploits.

Date	D	A	V	Title	Platform	Author
2015-07-21		-		SysAid Help Desk 'rdslogs' Arbitrary File Upload	java	metasploit
2015-07-21		-		Internet Download Manager - OLE Automation Array Remote Code Execution	windows	Mohammad Reza .
2015-07-17		-		D-Link Cookie Command Execution	hardware	metasploit
2015-07-14		-		Impero Education Pro - SYSTEM Remote Command Execution	windows	slipstream
2015-07-13		-		Accellion FTA getStatus verify_oauth_token Command Execution	hardware	metasploit
2015-07-13		-		VNC Keyboard Remote Code Execution	multiple	metasploit
2015-07-13		-		Adobe Flash opaqueBackground Use After Free	windows	metasploit

Web Application Exploits

This exploit category includes exploits for web applications.

Date	D	A	V	Title	Platform	Author
2015-07-29				phpFileManager 0.9.8 - CSRF Vulnerability	php	John Page
2015-07-29				Tendoo CMS 1.3 - XSS Vulnerabilities	php	Arash Khazaei


Ciência Hacker
#root
BYPASS ROOT

Rootkit

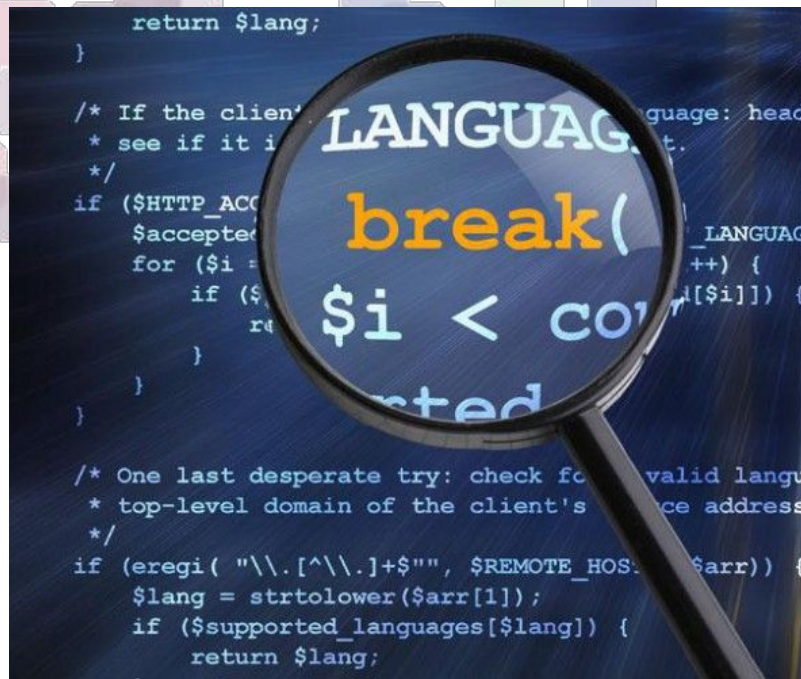
Herramienta cuya finalidad es esconderse a sí misma, esconder otros programas, procesos, directorios, archivos y conexiones, que permite a usuarios no autorizados mantener el acceso y comandar remotamente nuestro equipo.


ROOTKIT
ROOTKIT.BOOT.CIDOX.B
DEMO

Cómo detectarlos?

Posibles indicadores de artefactos maliciosos:

- Nombres de archivos extraños o desconocidos
- Funciones sospechosas
- Patrones atípicos
- Permisos, dueños y grupos
- Fechas de creación y modificación
- Procesos extraños o desconocidos
- Usuarios desconocidos
- Conexiones y puertos extraños o desconocidos



Detectando webshell y artefactos maliciosos

Herramientas y técnicas:

- Findbot: http://168.90.179.118/ceilac/forense/findbot.pl
- Shelldetect: http://shelldetector.com/
- img-analize.sh: script desarrollado por el CERT-PY
- Comandos útiles: grep, find, locate, ps, netstat, lsmod
  - Expresiones regulares
- Plugins y herramientas específicas según el CMS:
  - Wordpress: Sucuri scanner, CWIS
  - Joomla: Akeeba Admin Tools, SecurityChek Pro, Antivirus Website Protection
- Análisis de Logs

Análisis de Logs

Dónde buscar?

- **Logs de Apache:** /var/log/httpd o /var/log/apache2
  - access.log - peticiones HTTP
  - error.log - errores
- **Logs de SO:** /var/log/
  - /var/log/auth.log: log de autenticación.
  - /var/log/kern.log: registro del kernel
  - /var/log/cron.log: registro de la herramienta de crond
  - /var/log/maillog: registro del servidor de emails.
  - /var/log/boot.log: registro de inicio del sistema
  - /var/log/secure: log de autenticación, incluye SSH
  - /var/log/utmp o /var/log/wtmp: registro de logins. Ver con *last*
- **Logs de Base de Datos**: /var/log/mysqld.log o /var/log/mysql/

Análisis de Logs (1)

Qué buscar?

- Peticiones POST
- UA extraños
- Exclusión de patrones de peticiones comunes
- Exclusión de IPs confiables

Detectando Rootkits

En servidores Linux:

- ClamAV
- unhide.rb / unhide
- Rkhunter
- Chkrootkit
- Volatility (técnicas avanzadas)

REINSTALACIÓN DE S.O.

Hands-On!

Instrucciones

Repositorio: http://168.90.179.118/ceilac/forense/

1. Descargar servidor_webshell.ova
2. Importar en Virtualbox e iniciar la VM
3. Credenciales de acceso:
   - S.O.:
     - Usuario: admin (sudo su para escalar de privilegios a root)
     - Contraseña: password
   - Base de datos: MySQL
     - Usuario: root
     - Contraseña: password
4. Herramientas disponibles en /home/admin/tools
5. Analizar con findbot.pl, shelldetect y/o img-analize.sh
6. Buscar artefactos con grep, find, etc..
7. Analizar logs para encontrar artefactos y punto de entrada

Instrucciones

Repositorio: http://168.90.179.118/ceilac/forense/

1. Descargar servidor_rootkit.ova
2. Importar en Virtualbox e iniciar la VM
3. Credenciales de acceso:
   - S.O.:
     - Usuario: admin (sudo su para escalar de privilegios a root)
     - Contraseña: password
4. Verificar procesos, conexiones, módulos, etc.
5. Analizar con chkrootkit, rkhunter y/o unhide
6. Buscar otros posibles indicadores de compromiso

⇨ *Se pudo encontrar todos los rootkits?*

Resultado de ejercicios: http://168.90.179.118/ceilac/forense/resultado.txt

Servidor Web comprometido: acciones a seguir

1. Aislar el servidor de Internet
2. Verificar procesos y conexiones activas
3. Buscar webshells, backdoor y código malicioso y remover
4. Verificar y reparar integridad de archivos de aplicación web
   - ➢ *En caso de CMS, resguardar/exportar contenido, reinstalar core e importar contenido limpio.*
5. Buscar y eliminar usuarios no autorizados
6. Buscar rootkits, malware y/o otra modificación al SO
7. Buscar indicadores de escalación de privilegios
   - ➢ *En caso de que el paso 8 y/o 9 son afirmativos, considerar reinstalación de SO*
8. Revisar logs - identificación de punto de entrada y acciones
9. Corregir vulnerabilidades, actualizar y securización adicional

Ejemplo de recuperación - Wordpress

1. Análisis forense del servidor
2. Si encontramos que está comprometido el core, exportar el contenido:
   Panel de admin > Herramientas > Exportar > Todo el contenido
3. Copiar el contenido de /wp-content/uploads (asegurar que esté limpio!)
4. Eliminar todo el sitio
5. Reinstalar Wordpress
6. Importar el contenido: Panel de admin > Importar
7. Reinstalar plugins y plantillas

Otra guía:

https://sucuri.net/guides/how-to-clean-hacked-wordpress

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Cómo protegernos?

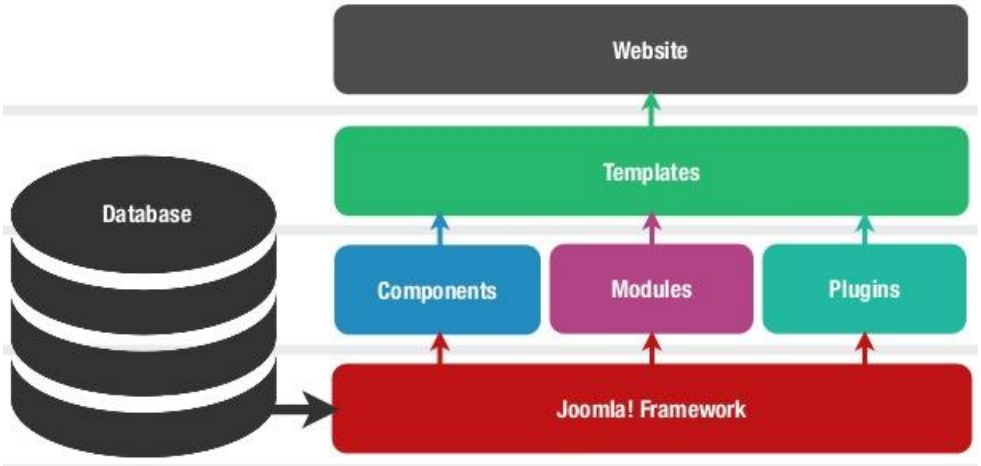
Actualización

- **Sistema Operativo:**
  - Linux, Windows Server
- **Software:**
  - MySQL
  - PHP
  - Apache
  - Zimbra
  - Librerias: OpenSSL, glibC, etc.
  - BIND
  - Paquetes adicionales

Actualización (1)

Aplicaciones Web:

- CMS: Wordpress, Joomla, Concrete5, Alfresco, Liferay
- Plugins y componentes
- Temas y plantillas
- Librerias: PHP, Java, ASP.NET, Ruby On Rails, Python, PERL
- Servidor: Apache, IIS, nginx
- Base de datos: MySQL, Oracle, MSSQL



Contraseña robustas

- Longitud: mínimo 12 caracteres – no hay máximo
- Combinación de caracteres
- Usar frases en vez de palabras
- No usar palabras comunes o de “diccionario”

DATO:
Contraseñas más comunes:

1) **123456**
2) **password**
3) **12345678**
4) **qwerty**
5) **abc123**
6) **111111**

Buenas prácticas de contraseñas

- No usar la misma contraseña para todo
- Cambiar contraseñas regularmente
- Cambiar las contraseñas por defecto
- No escribirlas en papeles o documentos accesibles

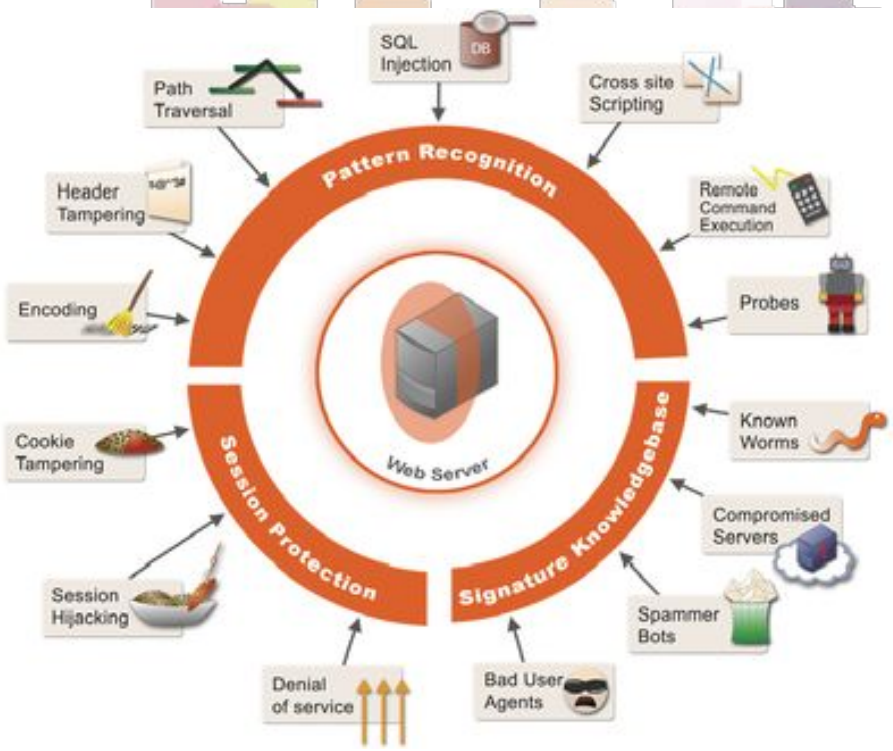
Hardening de SO y aplicaciones

Haciéndole la vida difícil al atacante

- Desactivar y/o desinstalar servicios y software innecesarios
- Evitar usar usuario root – Usar sudo
- Implementar políticas de administración de usuarios y contraseñas
- Otorgar los mínimos privilegios necesarios
- Implementar límites de intentos fallidos de autenticación
- Desactivar SUID no deseado y SGID Binarios
- Activar y configurar logs de auditoría
- Utilizar SELinux
- Implementar mecanismos de backup
- ...

Firewall de Aplicación Web (WAF)

- ModSecurity
- OpenWAF
- Ironbee
- ESAPI WAF

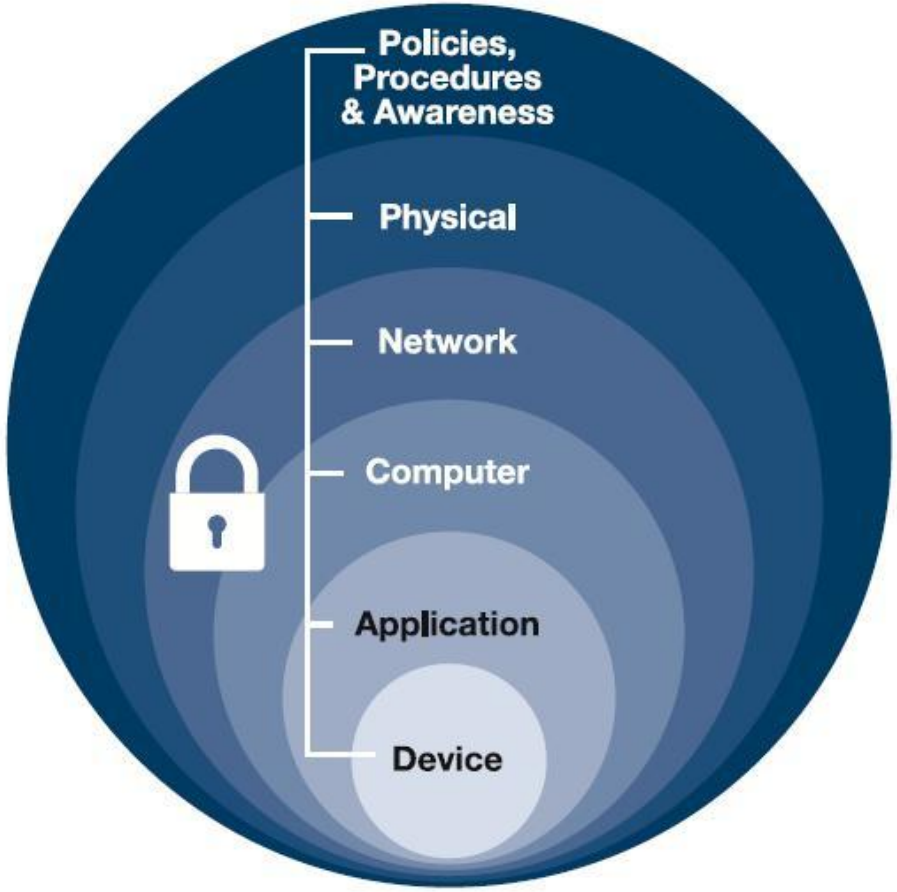


Seguridad Perimetral

Firewall + IDS/IPS + SIEM

- Iptables
- CSF
- Snort
- Suricata
- Pfsense
- OSSIM

Defensa en Profundidad



SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

@CERTpy

/CERT-Py

www.cert.gov.py

denuncias: abuse@cert.gov.py
contactos: cert@cert.gov.py