



# Introducción al Análisis Forense en Servidores Web





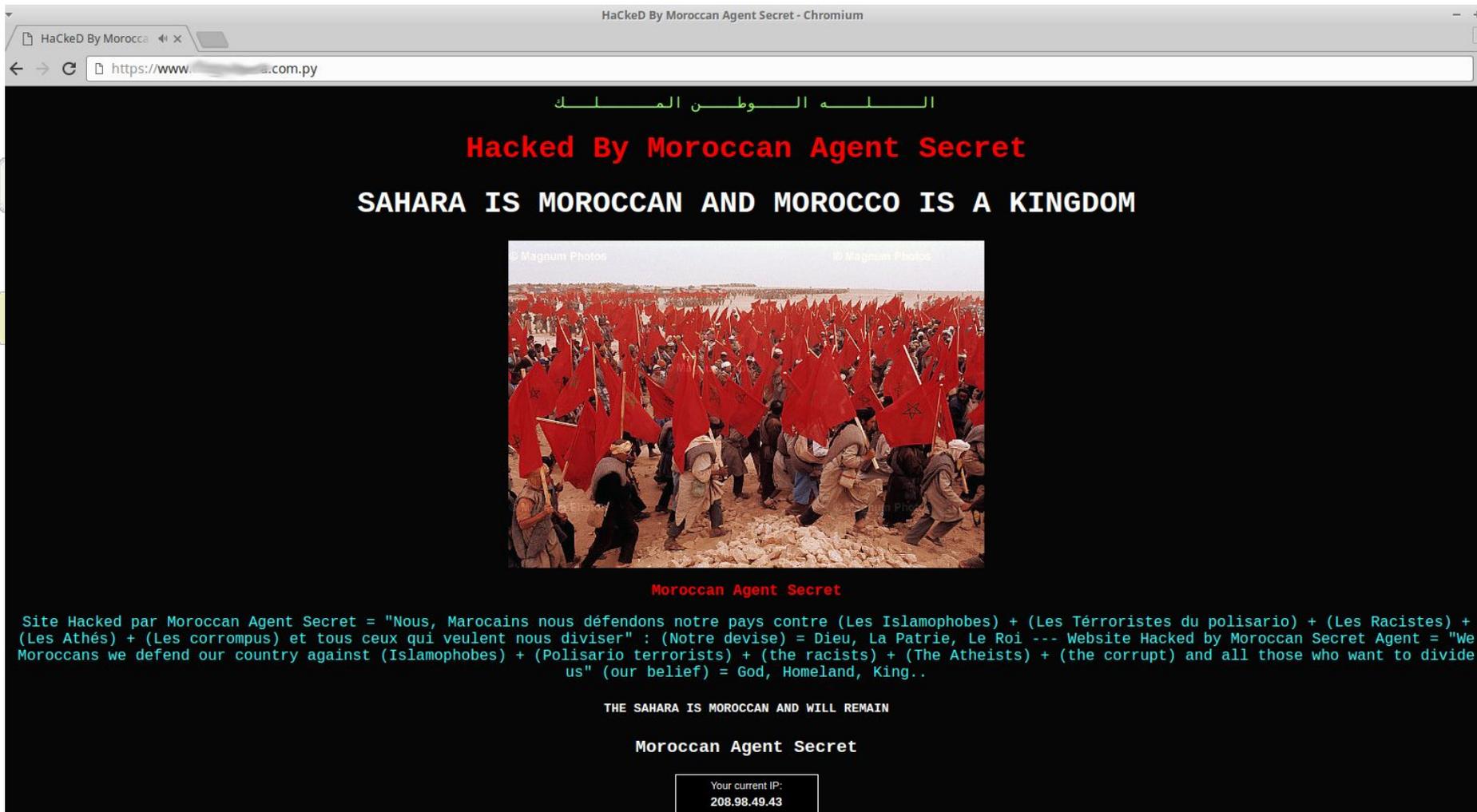
## Disclaimer

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.





# Mi sitio web fue hackeado!





# Mi sitio web fue hackeado!

Google ghana

Web Maps Images News Videos More Search tools

About 58,50,00,000 results (0.47 seconds)

**Ghana Homepage | Government of Ghana Official Portal**  
[www.ghana.gov.gh/](http://www.ghana.gov.gh/) ▼  
**This site may be hacked.**  
Official site of the government of Ghana provides news and information about the Parliament, ministries, constitution, districts, economy, education and tourism.

**Ghana - Wikipedia, the free encyclopedia**  
[en.wikipedia.org/wiki/Ghana](https://en.wikipedia.org/wiki/Ghana) ▼  
Ghana officially called the Republic of Ghana, is a sovereign multinational state and unitary presidential constitutional democracy, located along the Gulf of ...  
Accra - List of African countries by ... - John Dramani Mahama - Ghanaian people



## ¿Para qué atacan mi servidor web?

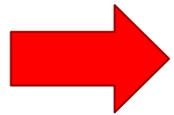
- Hacktivismo/Defacement
- Distribución de malware
- Phishing
- Spam
- Proxies maliciosos
- DoS/DDoS
- Click Fraud



## Errores comunes

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

Qué es lo correcto?



**Auditoría!**

*¿Cómo entraron? ...*







# Webshells

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

Uname: Linux #1 SMP Wed Mar 17 11:30:06 EDT 2010 x86\_64 [Google] [milw0rm]

User: 48 ( apache ) Group: 48 ( apache )

Php: 5.2.12 Safe mode: ON [ phpinfo ] Datetime: 2010-05-04 12:59:05

Hdd: 223.18 GB Free: 204.02 GB (91%)

Cwd: /var/www/vhosts/.../httpdocs/ drwxrwxrwx [ home ]

[ Sec. Info ] [ Files ] [ Console ] [ Sql ] [ Php ] [ Safe mode ] [ String tools ] [ Bruteforce ] [ Network ] [ Self remove ]

### File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[ downloads ]	dir	2010-05-02 16:25:01	www-data:www-data	drwxr-xr-x	RT
[ pictures ]	dir	2010-05-04 00:49:20	www-data:www-data	drwxr-xr-x	RT
index.htm	2.67 KB	2010-05-02 16:48:11	www-data:www-data	-rw-r--r--	RTED
logo.png	5.34 KB	2010-05-02 16:14:06	www-data:www-data	-rw-r--r--	RTED
shell.php	23.55 KB	2010-05-04 12:58:56	www-data:www-data	-rw-r--r--	RTED

Copy >>

Change dir: /var/www/vhosts/.../httpdocs/ >>

Make dir: >> [ Writeable ]

Execute: >>

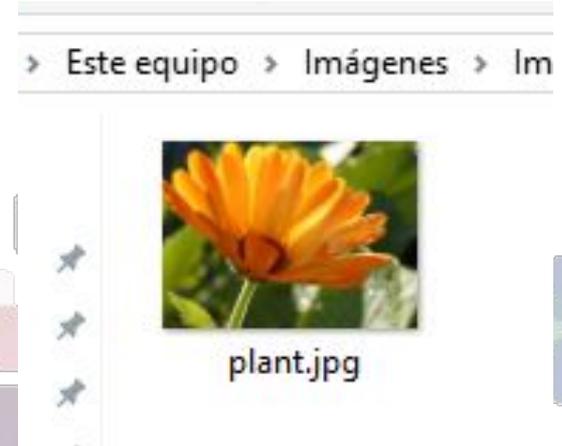
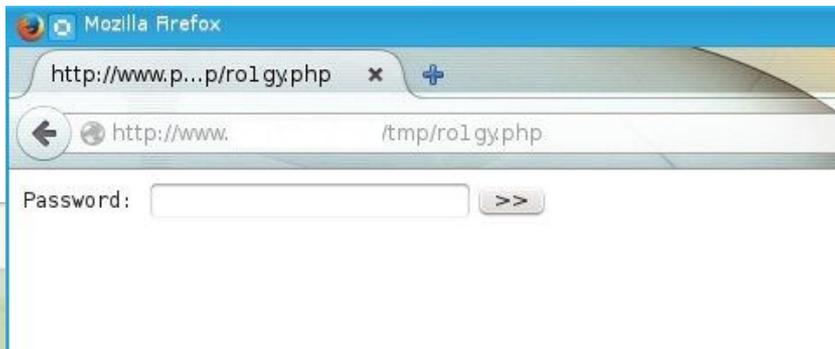
Read file: >>

Make file: >> [ Writeable ]

Upload file: >> [ Writeable ]



# Webshells (1)





## 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         State
tcp        0      0 0.0.0.0:5357             0.0.0.0:*                LISTENING
tcp        0      0 192.168.1.1:80          0.0.0.0:*                LISTENING
tcp        0      0 0.0.0.0:36777           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:1025            0.0.0.0:*                LISTENING
udp        0      0 192.168.1.1:1027       0.0.0.0:*                LISTENING
udp        0      0 127.0.0.1:38032         0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:42000           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:20000           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:1701            0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:53413           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:20010           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:67              0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:39000           0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:1900            0.0.0.0:*                LISTENING
udp        0      0 0.0.0.0:38000           0.0.0.0:*                LISTENING
```



SECRETARÍA  
**NACIONAL DE TECNOLOGÍAS  
DE LA INFORMACIÓN  
Y COMUNICACIÓN**



**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
calling revoke...
uid=0, euid=0
#
# whoami
root
# █
```



# Vulnerabilidades y exploits

[ home ] | [ private ] | [ 0Day ] | [ Get Gold ] | [ platforms ] | [ shellcode ] | [ pentest ] | [ hash ] | [ search ] | [ faq ] | [ agreement ] | [ contact ] | [ style ] | db: 23 929

Contact us: [ icons ]
[ authorization ] | [ registration ] | [ restore account ]



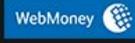
Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.  
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.  
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

**How to buy exploit? Two ways to buy required exploit. Currency, that we accept.**

- Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
- Another way to buy exploits is to became 0day.today 1337day user, get 0day.today 1337day Gold and buy required exploit in our database.

We accept currencies: [contact admin to find more]






Search:  [ Search ] [ Extended search ]

### 0day.today 1337day Inj3ct0r Exploits Market and 0day Exploits Database

[ private ]

DATE	DESCRIPTION	TYPE	HITS	RISK	GOLD	AUTHOR
06-02-2015	SMF 2.0.x Remote Code Execution 0day Exploit	php	5 849	R D	5 000	Protocol8
12-09-2014	Internet Explorer 11 Remote Code Execution 0day Exploit	windows	27 409	R D	5 000	0day Today Team
08-09-2014	Elastix PBX 2.x.x Remote Command Execution 0day Exploit	linux	19 027	R D	3 000	RusH
09-05-2014	Joomla! 3.3.0 SQL Injection / automatic upload shell Exploit (0day)	php	73 376	R D	8 900	0day Today Team
28-07-2015	Microsoft Internet Explorer CAttrArray Use-After-Free Remote Code Execution Exploit 0day	windows	363	R D	3 200	AbdulAziz Hariri
25-07-2015	Microsoft Internet Explorer CFreePos Use-After-Free Remote Code Execution Exploit 0day	windows	429	R D	3 500	AbdulAziz Hariri
24-07-2015	Apache Groovy Deserialization of Untrusted Data Remote Code Execution Exploit 0day	multiple	373	R D C	3 000	rpnrodzc7
23-07-2015	Instagram bypass Access Account Private Method Exploit	tricks	1 394	R D	2 000	smokzz

[ remote exploits ]

DATE	DESCRIPTION	TYPE	HITS	RISK	GOLD	AUTHOR
04-08-2015	Heroes Of Might And Magic III .h3m Map File Buffer Overflow Exploit	windows	223	R D	free	metasploit
01-08-2015	Symantec Endpoint Protection Multiple Vulnerabilities	multiple	488	R D C	free	Code White
28-07-2015	Microsoft Internet Explorer CAttrArray Use-After-Free Remote Code Execution Exploit 0day	windows	363	R D	3 200	AbdulAziz Hariri



# Vulnerabilidades y exploits (1)



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](#)



## 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.







## 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

```
return $lang;  
}  
/* If the client's language is not supported, we try to detect the language by  
* see if it is a known language.  
*/  
if ($HTTP_ACCEPT_LANGUAGE) {  
    $accepted_languages = explode(',', $HTTP_ACCEPT_LANGUAGE);  
    for ($i = 0; $i < count($accepted_languages); $i++) {  
        if ($supported_languages[$accepted_languages[$i]]) {  
            return $accepted_languages[$i];  
        }  
    }  
}  
/* One last desperate try: check for a valid language by checking the  
* top-level domain of the client's IP address.  
*/  
if (ereg( "\\.[^\\.]+$", $REMOTE_HOST)) {  
    $lang = strtolower($arr[1]);  
    if ($supported_languages[$lang]) {  
        return $lang;  
    }  
}
```



# Detectando webshell y artefactos maliciosos

## Herramientas y técnicas:

- Findbot: <http://168.90.179.118/ceilac/forense/findbot.pl>
- Shelldetect: <http://shelldetector.com/>
- img-analyze.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





A person's hands are shown typing on a laptop keyboard. The scene is illuminated with a green glow, and the background is a digital rain effect of binary code (0s and 1s) falling from the top. The text "Hands-On!" is prominently displayed in the center of the image.

# 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-analyze.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>







# Actualización

- **Sistema Operativo:**

- Linux, Windows Server

- **Software:**

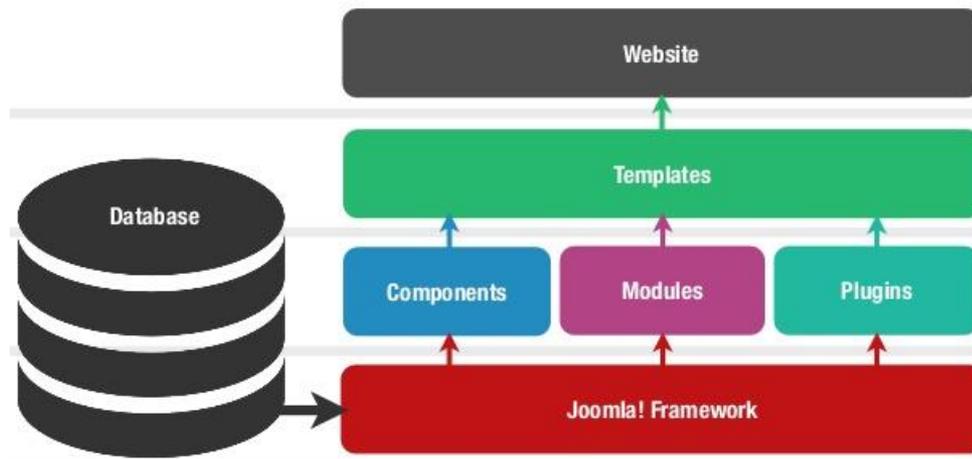
- MySQL
- PHP
- Apache
- Zimbra
- Librerías: OpenSSL, glibC, etc.
- BIND
- Paquetes adicionales



# Actualización (1)

## Aplicaciones Web:

- CMS: Wordpress, Joomla, Concrete5, Alfresco, Liferay
- Plugins y componentes
- Temas y plantillas
- Librerías: 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

```
-- Table structure for table `users`
--
DROP TABLE IF EXISTS `users`;
CREATE TABLE `users` (
  `username` varchar(32) NOT NULL default '',
  `pwhash` char(40) default NULL,
  `sessionid` char(32) default NULL,
  `exptime` datetime default NULL,
  PRIMARY KEY (`username`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table `users`
--

/*!40000 ALTER TABLE `users` DISABLE KEYS */;
LOCK TABLES `users` WRITE;
INSERT INTO `users` VALUES ('admin','cbcb57332ea0290af7ca6b61df97e644','b7f3597d98f4782b3beee88a228b91f3','0000-00-00
00:00:00'),('demo','fe01ce2a7fbac8faaed7c982a04e229','bcdc7030ed10d4e46f91f11fc921b31','2007-09-14 11:56:12');
UNLOCK TABLES;
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
```



# Hardening de SO y aplicaciones

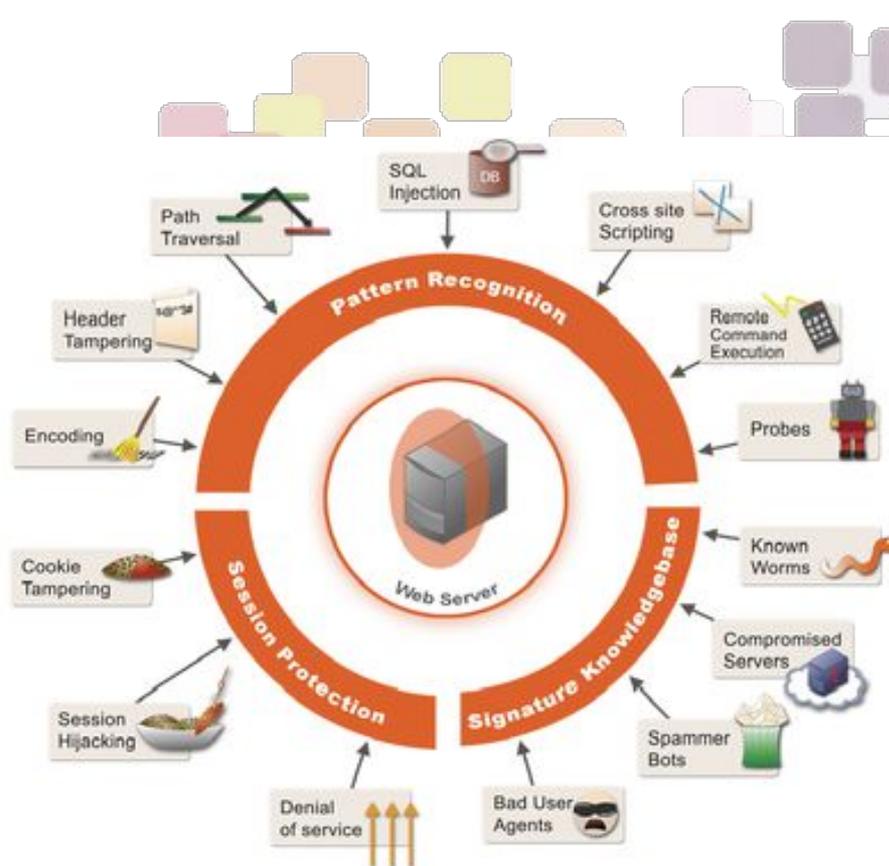
## *Haciéndole la vida difícil al atacante*

- 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

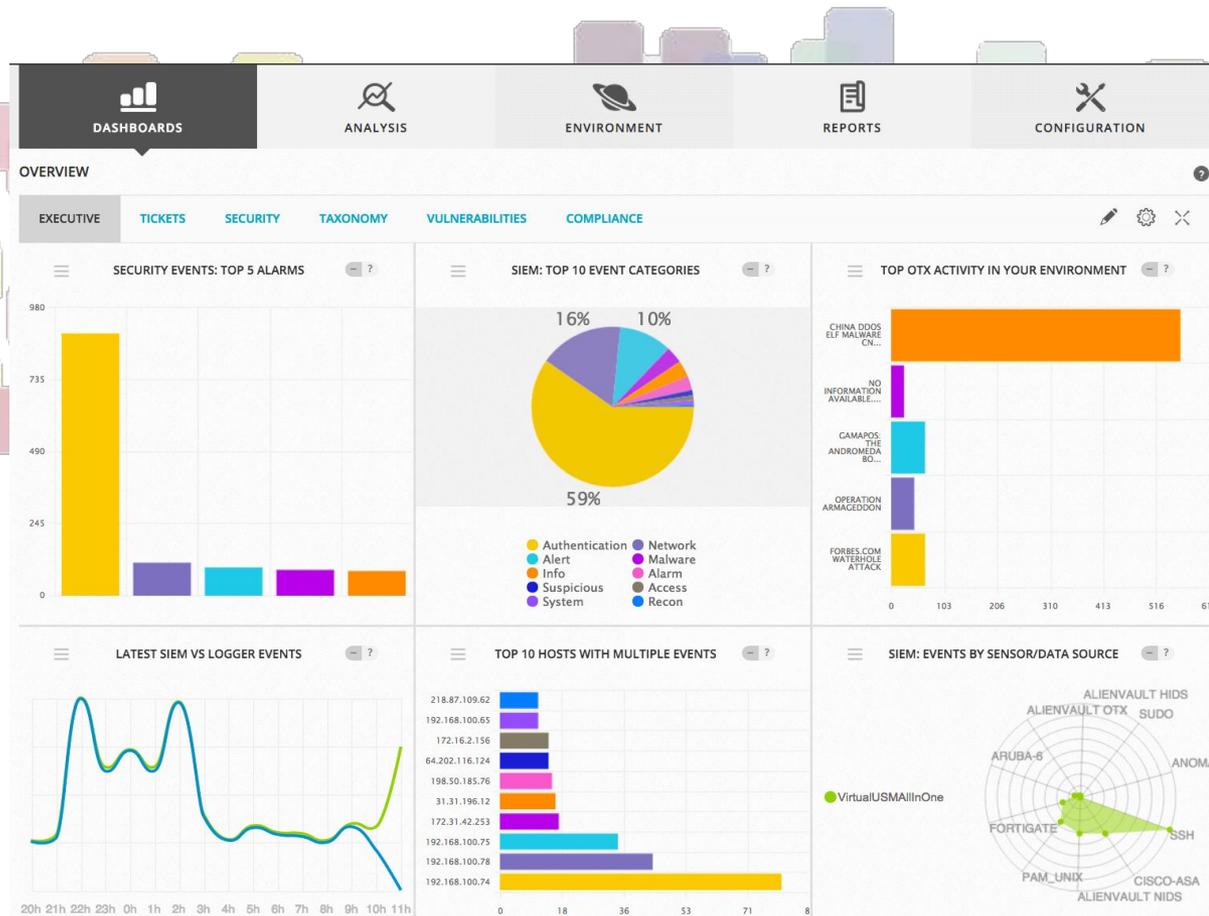




# Seguridad Perimetral

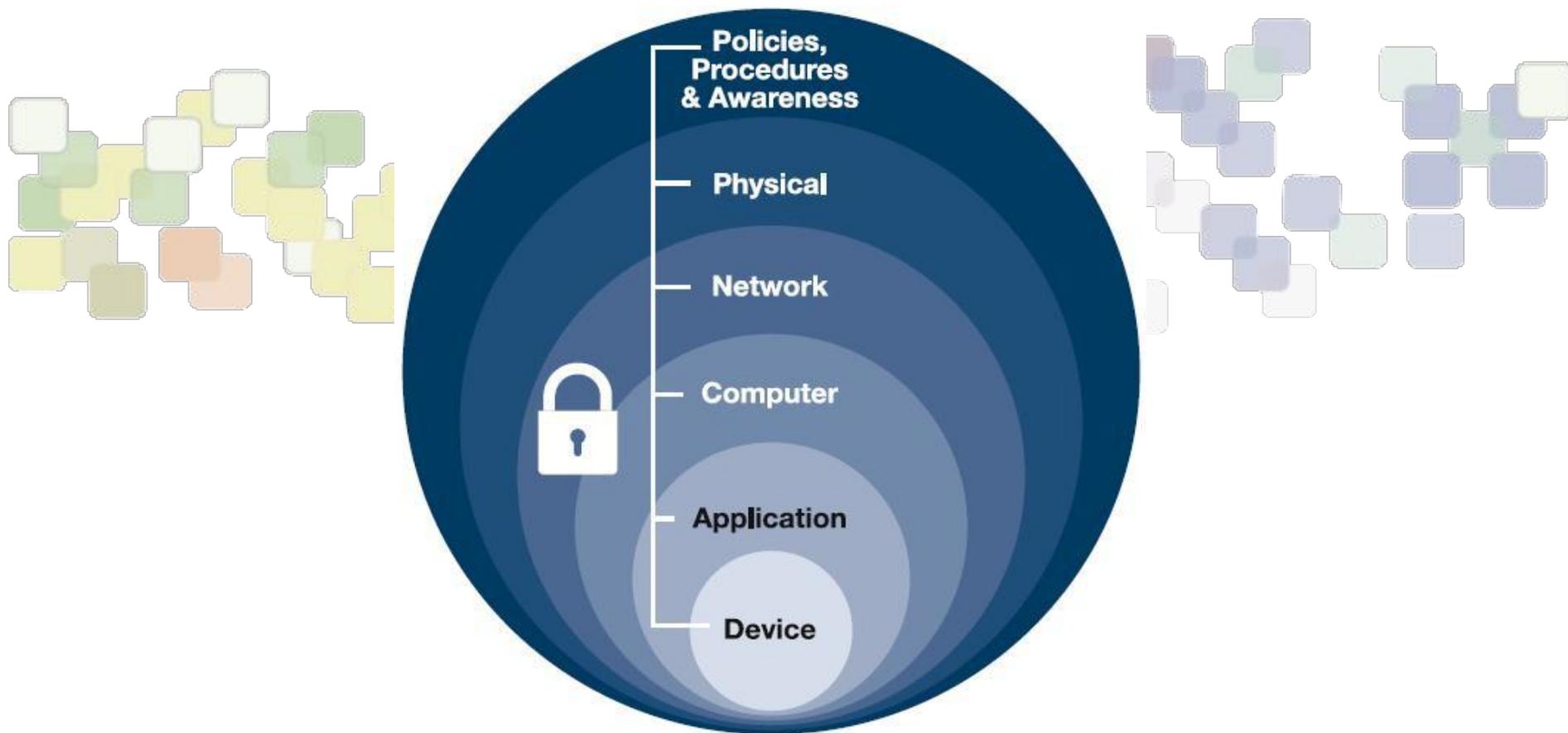
## Firewall + IDS/IPS + SIEM

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





# Defensa en Profundidad





# Muchas gracias!



**CERT-PY**



**@CERTpy**



**/CERT-Py**

**[www.cert.gov.py](http://www.cert.gov.py)**

**denuncias:** [abuse@cert.gov.py](mailto:abuse@cert.gov.py)

**contactos:** [cert@cert.gov.py](mailto:cert@cert.gov.py)