



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



**GOBIERNO NACIONAL**  
Construyendo Juntos Un Nuevo Rumbo  
agendaDigital

# **BOTNETS, ROOTKITS Y BACKDOORS**

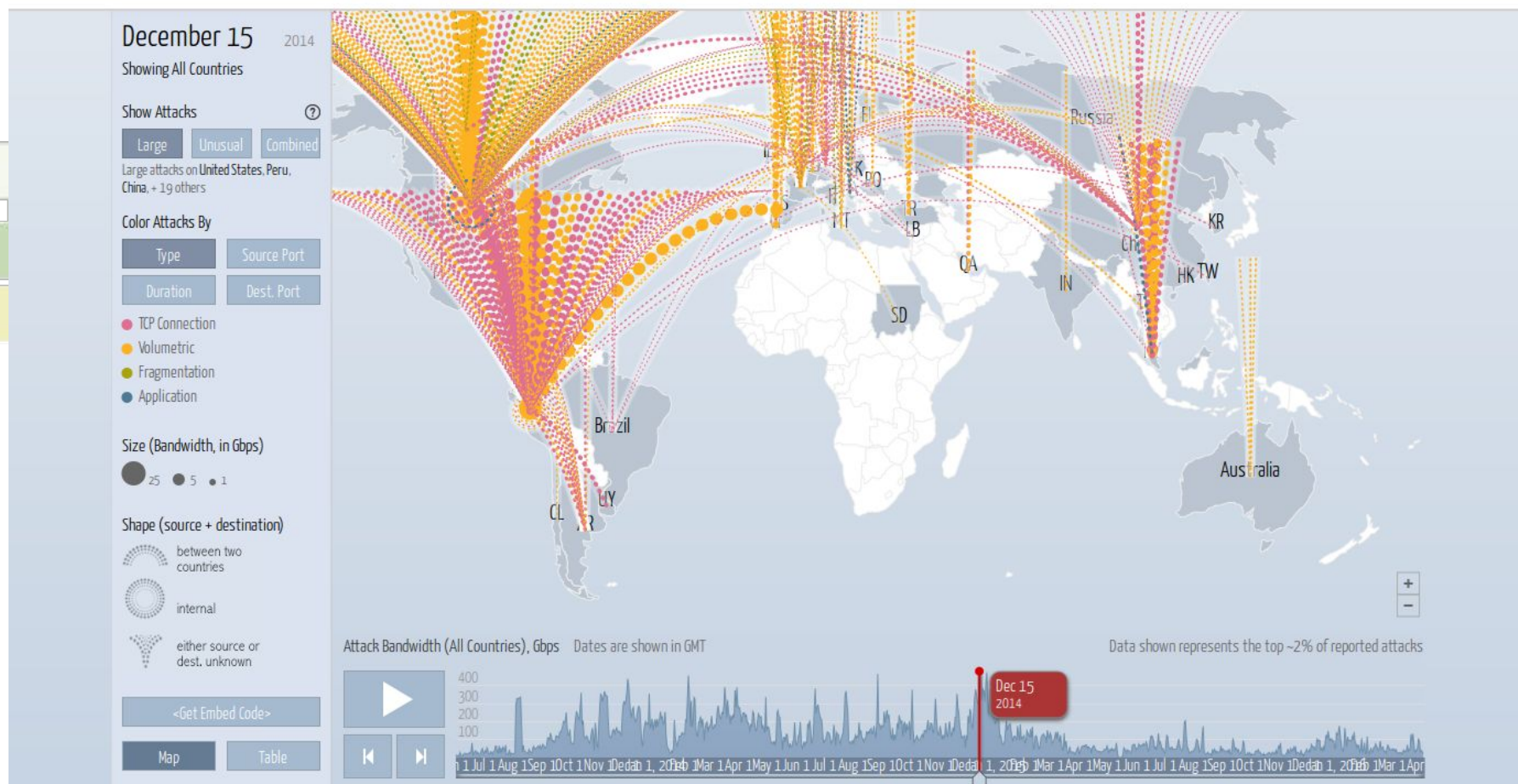
## **SERVIDORES EN LA MIRA DEL CIBERCRIIMEN**



# Ataques DDoS en el mundo

Digital Attack Map Top daily DDoS attacks worldwide

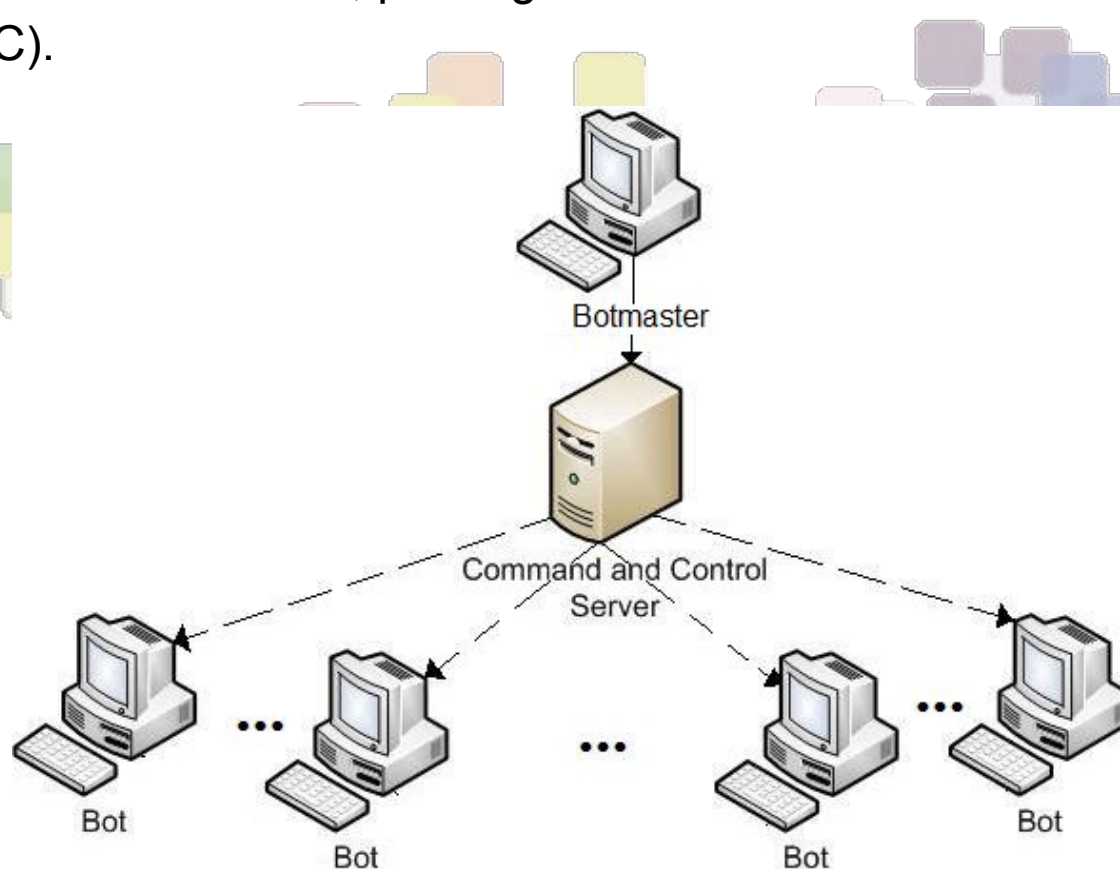
[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#) · [g+](#) [t](#) [f](#)





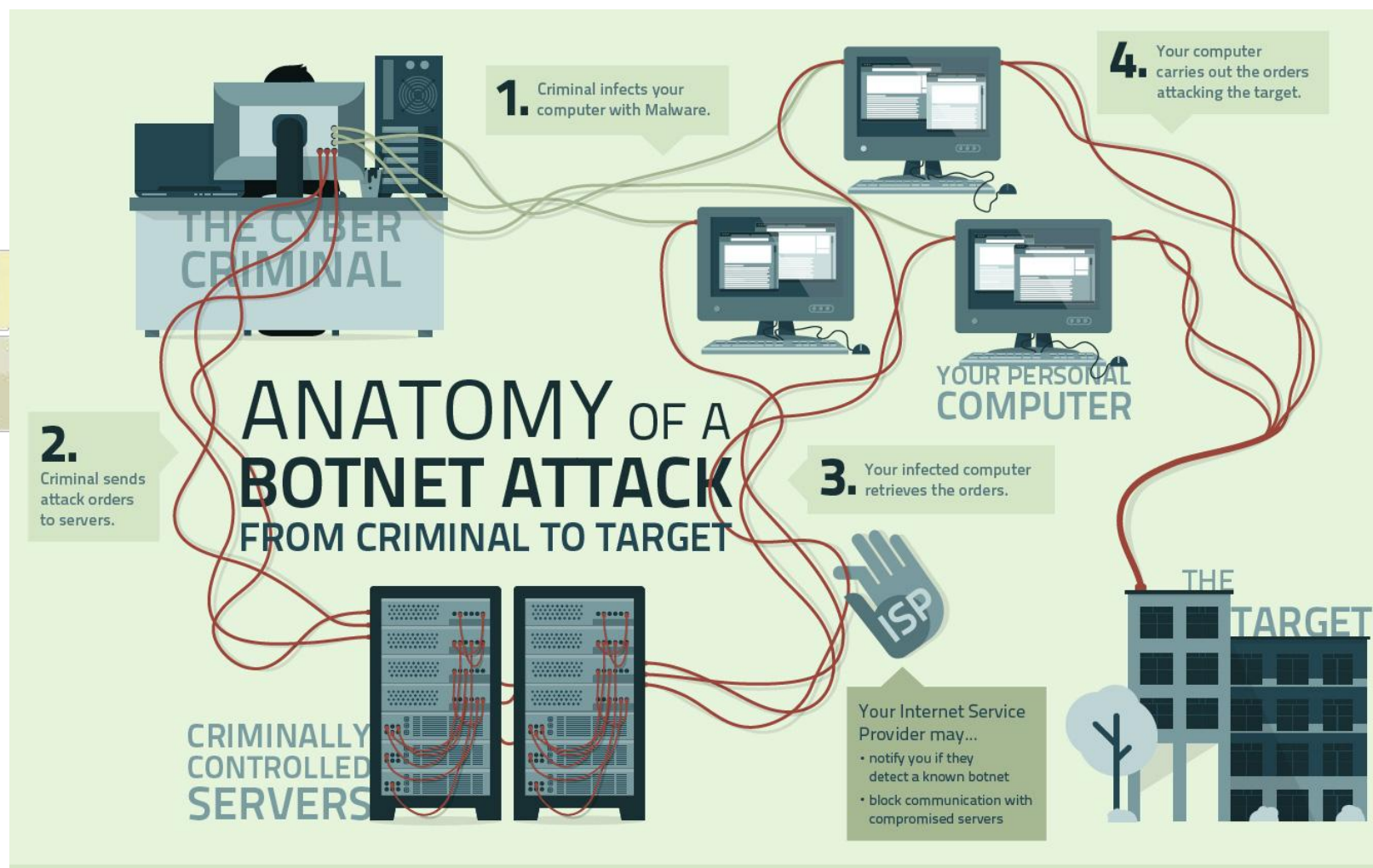
# Botnets

Red de equipos infectados (bots o zombies) controlada por el artífice de la botnet (botmaster) de forma remota, por lo general a través de servidores de Comando y Control (C&C).



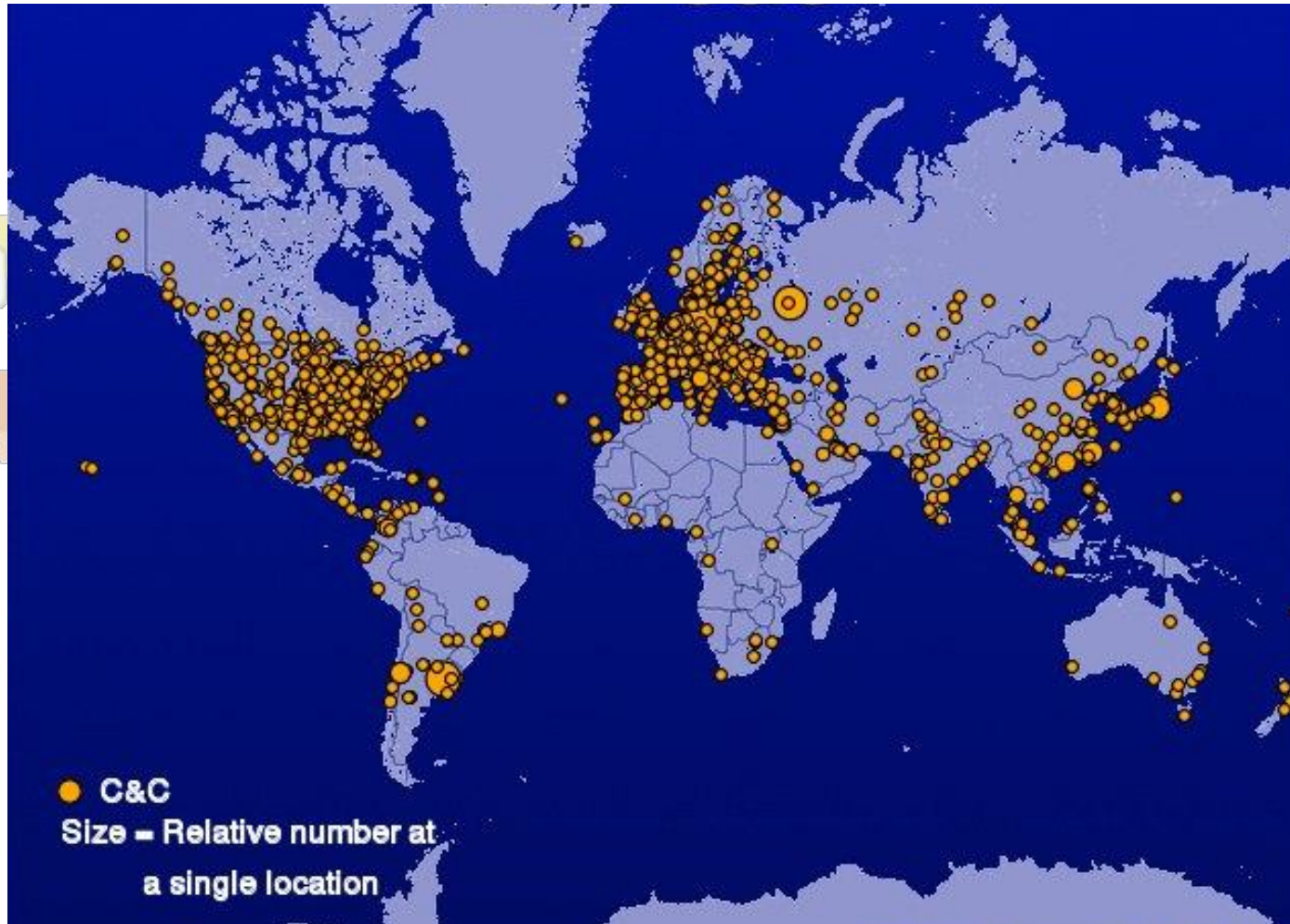


# Botnets (1)





## Estadísticas C&C





## ¿Por qué servidores?

- Mayor ancho de banda
- Mayor capacidad de procesamiento
- Uptime 24x7x365
- Poca interacción con el usuario
- Mayor exposición desde Internet





## ¿Para qué servidores?

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

*¿Cómo entran? ...*





# Webshell y Backdoors







# Webshells

File Edit View History Bookmarks Tools Help

← → ↻ × 🏠 ☆ http://.../shell.php

Google

UTF-8

Server IP: ...  
Client IP: ...

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: Browse... >>

[ Writeable ]



# 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@IBTeam:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.1.33: inverse host lookup failed: Unknown server error : Connection
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.33] 1057
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
[root@dwa ~]# netstat -ntlp
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	LISTEN	3146/mysql
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	1798/sshd
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN	999/sendmail
tcp	0	0	0.0.0.0:4444	0.0.0.0:*	LISTEN	3473/nc
tcp	0	0	:::80	:::*	LISTEN	2743/httpd
tcp	0	0	:::22	:::*	LISTEN	1798/sshd



# Cuando la webshell no es suficiente..





# Vulnerabilidades y exploits

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

Contact us:
[ 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.**

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. 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	rpmrodzc7	
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	



## 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
# █
```

WELCOME TO  
HACKER-DEMO



# 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.





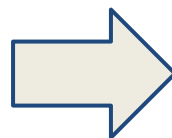


## Detectando Rootkits

En servidores Linux:

- ClamAV
- unhide.rb / unhide
- Rkhunter
- Chkrootkit
- Volatility

```
/bin/mktemp [OK]
/bin/more [OK]
/bin/mount [OK]
/bin/mv [OK]
/bin/netstat [Warning]
/bin/ping [OK]
/bin/ps [Warning]
/bin/pwd [OK]
/bin/readlink [OK]
/bin/rpm [OK]
/bin/sed [OK]
/bin/sh [OK]
/bin/sort [OK]
/bin/su [OK]
/bin/touch [OK]
/bin/uname [OK]
/bin/gawk [OK]
/bin/tesh [OK]
/bin/mailx [OK]
/usr/sbin/adduser [OK]
/usr/sbin/chroot [OK]
/usr/sbin/groupadd [OK]
/usr/sbin/groupdel [OK]
/usr/sbin/groupmod [OK]
/usr/sbin/grpck [OK]
```



**REINSTALACIÓN DE S.O.**



# Cómo protegernos?





# Actualización

- **Sistema Operativo:**
  - Linux, Windows Server
- **Software:**
  - MySQL, PHP, Apache, BIND
  - Zimbra
  - Librerías: OpenSSL, glibC, etc.
  - Paquetes adicionales
- **Aplicaciones Web:**
  - CMS, Plugins, Plantillas





# Contraseña robustas y Buenas prácticas

- Longitud: mínimo 12 caracteres
- 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**





# Autenticación de doble factor

Medida de seguridad adicional al usuario y contraseña

**Usuario + Contraseña + CÓDIGO DE SEGURIDAD**

➤ Implementación de OTP con Google Authenticator para proteger SSH

```
root@kali:~#  
root@kali:~# apt-get install libpam0g-dev make  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
make is already the newest version.  
make set to manually installed  
The following NEW packages will be installed:  
libpam0g-dev  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 191 kB of archives.  
After this operation, 401 kB of additional disk space will be used.  
Do you want to continue [Y/n]? Y  
Get:1 http://http.kali.org/kali/ kali/main libpam0g-dev amd64 1.1.3-7.1 [191 kB]  
Fetched 191 kB in 5s (36.2 kB/s)  
Selecting previously unselected package libpam0g-dev:amd64.  
(Reading database ... 370322 files and directories currently installed.)  
Unpacking libpam0g-dev:amd64 (from .../libpam0g-dev_1.1.3-7.1_amd64.deb) ...  
Processing triggers for man-db ...  
Setting up libpam0g-dev:amd64 (1.1.3-7.1) ...  
root@kali:~#
```



# Hardening de SO y aplicaciones

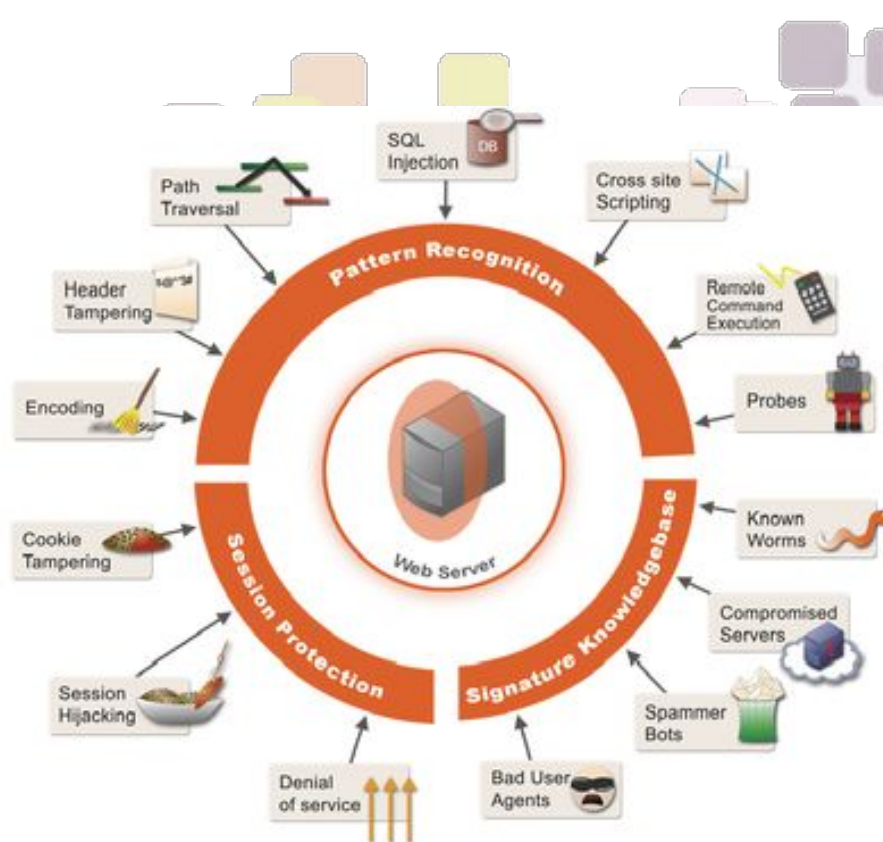
## *Haciéndole la vida difícil al atacante*

- 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

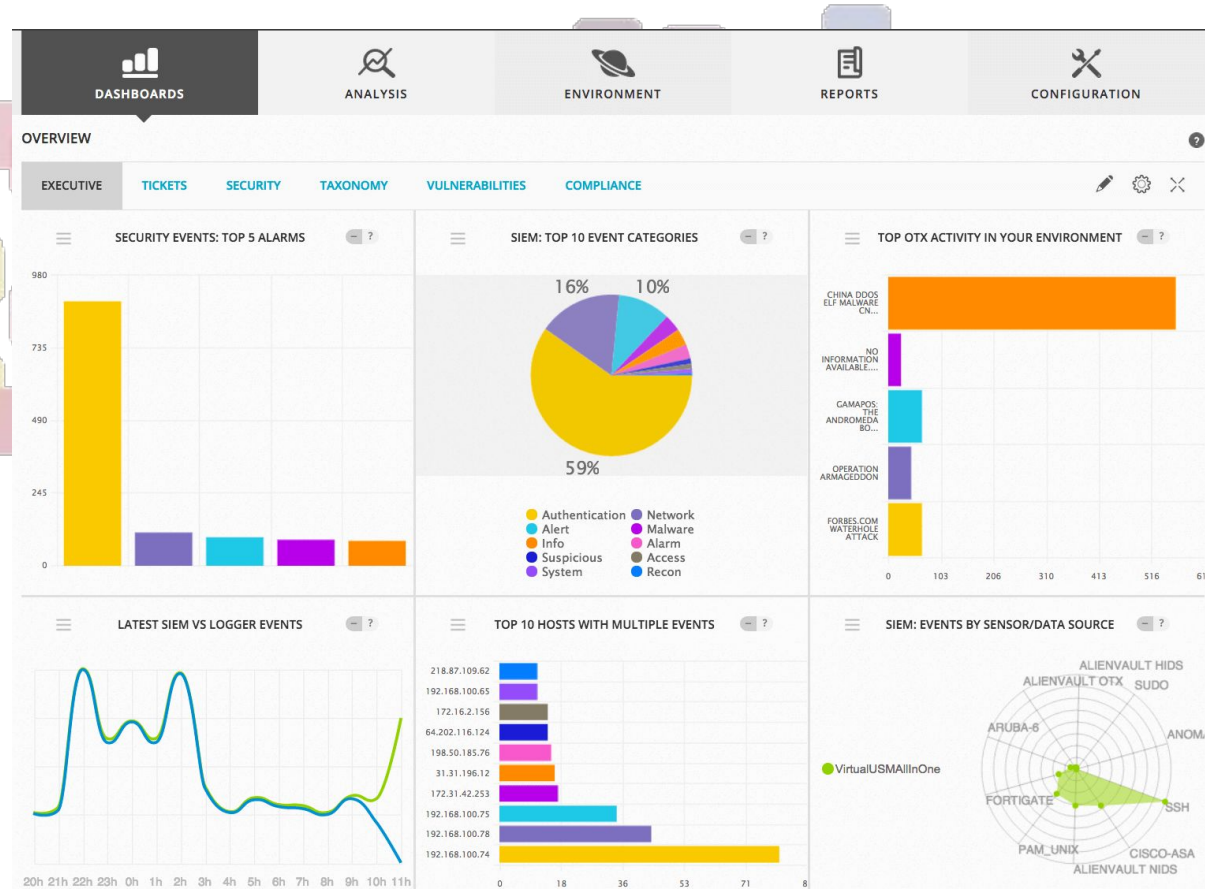




# Seguridad Perimetral

## Firewall + IDS/IPS + SIEM

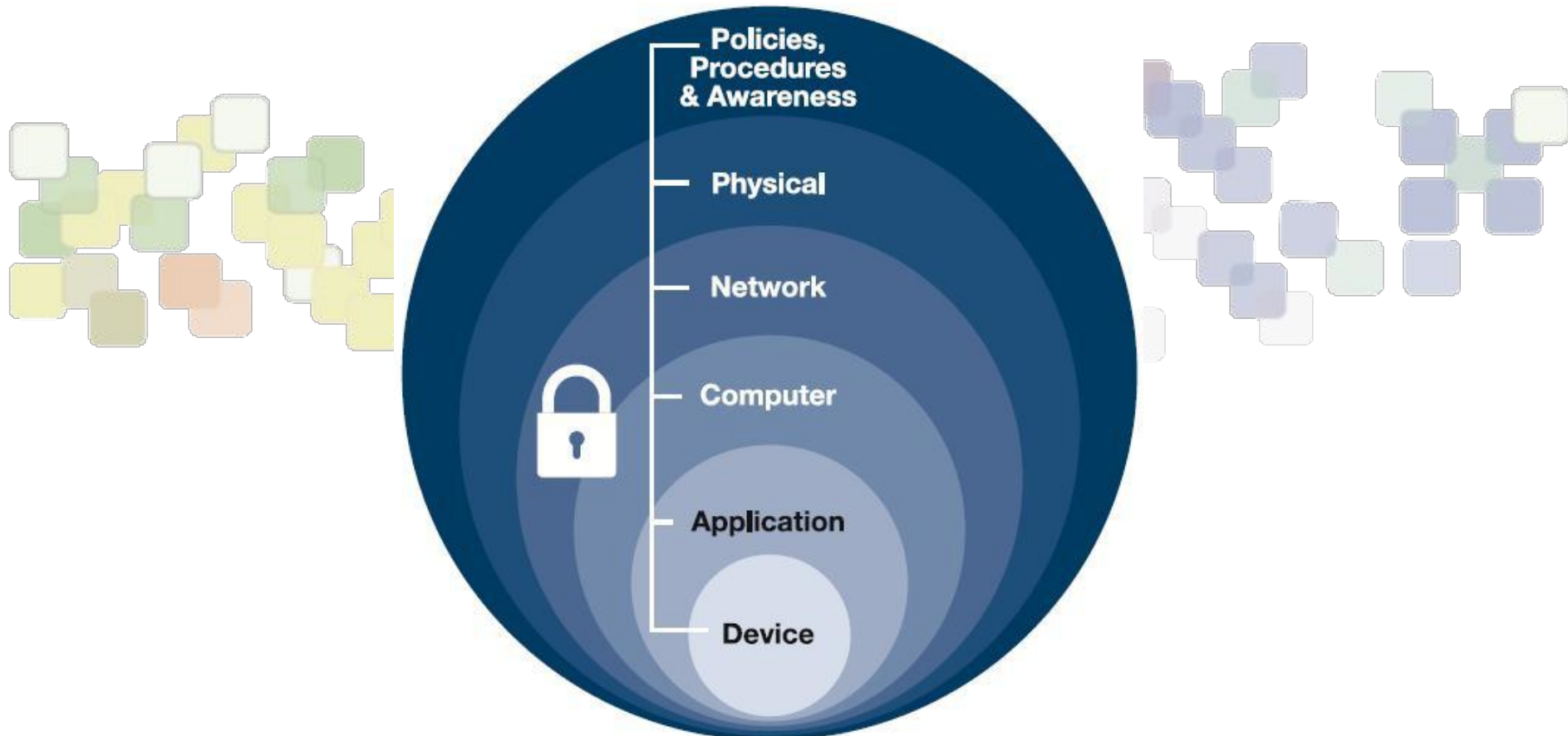
- Iptables
- CSF
- Snort
- Suricata
- Pfsense
- OSSIM







# 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)