SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD

TALLER PARA GERENTES DE TI

Riesgos y Amenazas

Riesgos y Amenazas (1)

TECNICAS TOP 10 - 2014:

- **Heartbleed**
- **ShellShock**
- **Poodle**
- **Rosetta Flash**
- **Residential Gateway "Misfortune Cookie"**
- **Hacking PayPal Accounts with 1 Click**
- **Google Two-Factor Authentication Bypass**
- **Apache Struts ClassLoader Manipulation Remote Code Execution and Blog Post**
- **Facebook hosted DDOS with notes app**
- **Covert Timing Channels based on HTTP Cache Headers**

Riesgos y Amenazas (2)

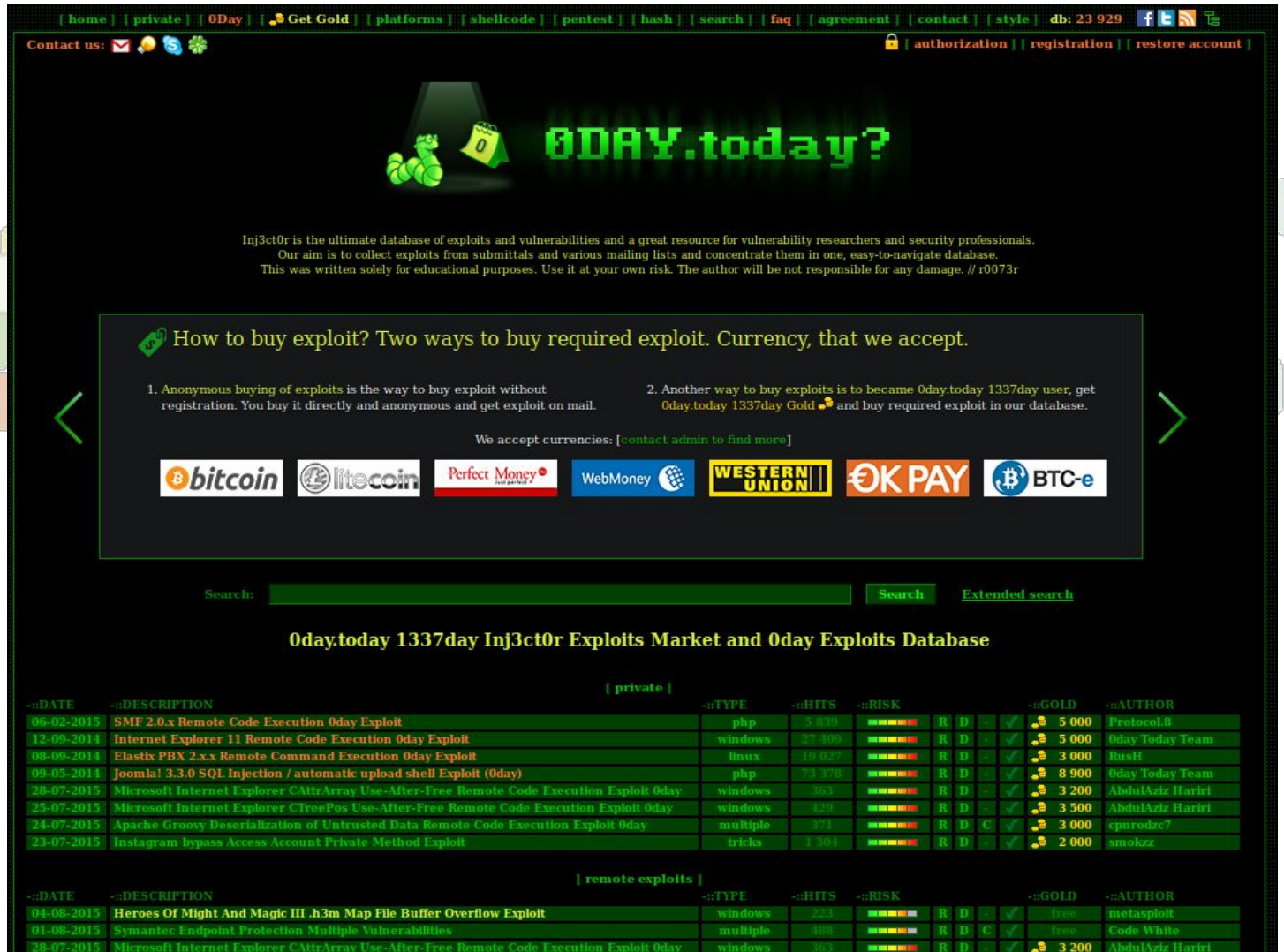
SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Actualización

¿Por qué actualizar?



¿Por qué actualizar? (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

¿Qué actualizar?

Equipos de usuarios:

- Sistemas operativos:
  - Windows, Mac OS X, Linux
- Software:
  - Navegadores: Chrome, Firefox, Explorer
  - Plugins: Adobe Flash Player, Shockwave, Java
  - MS Office
  - Programas en general

¿Qué actualizar? (1)

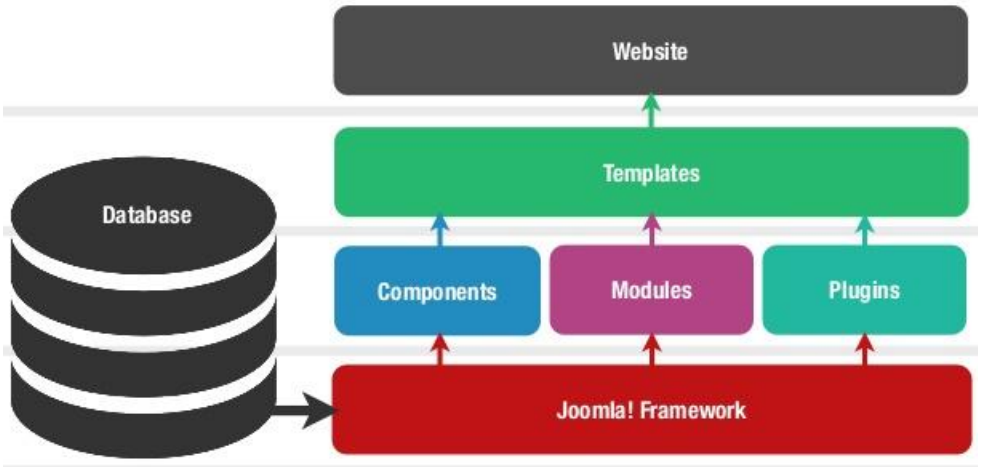
Servidores:

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

¿Qué actualizar? (2)

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



SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Control de Acceso Credenciales

Autenticación

Ataques de contraseña:

350 mil millones de contraseñas por segundo

- Fuerza Bruta
- Combinator Attack
- Rainbow Tables
- Diccionarios
- Hybrid Attack
- Técnicas personalizadas

```
b05c97fbdd6221373b029c1ce07c3d22:BNC4Life
0ed21878f91d3a6f2bb218204d2e67ba:luckiesT1!
b2fe57cda161b656aa503575cefda54b:BaldwinWallace
f7e0bc8fef87f5c174cb4de5277cc9c1:StefoN2012
24c030503e3b6760786e6fdfb8475a27:strawberryfields
90ff14b6291375639077a194a684f55d:sleepingwithsirens
3e93fb79e0970b6b8229ff8bec22d069:qeadzcwrsfxv1331
17d00e0f77a868d8fd2d97cf1ee2ce51:gonewiththewind1
9c4c082bd89ba91631e5f0c3494f9a48:courtneycunningham
21bf1514d415696c92239a49f6e2b9ac:KRAZYkat18
36d0c148d14540f451401065f04bd3bd:Mongorians.
b7d7231a77aebe9b7707f93f92408025:muffinhug92
dd44c60acc3f96076b4fe222b8678208:L!fehouse15
37f66770d185106e79096ab3e28510e2:@Oceancity12
37c8111283aa1b4ab09415104af50855:Golden.Lab
e334e65051b9a4fbb5f5c0d3c5768744:$Samuel12345
5dfa876777655b523203be54da04b030:20schuyler11
c604a5c03e3b148c7206a14992213c10:Chealsealove1
66adef2e392d0d5a4905d8be6d824e1c:$0ccerBa11
```

	Números	Minúsculas	Minúsculas + números	Minúsculas + Mayúsculas + números
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

¿Qué es una contraseña robusta?

- 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

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

Tv5Monde revealed his own passwords in an interview

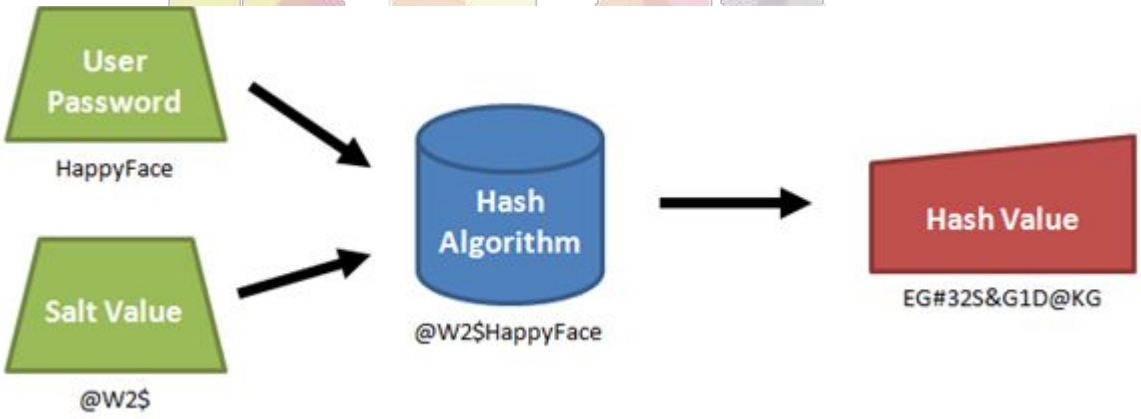
April 10, 2015 By Pierluigi Paganini

A TV5Monde staffer accidentally revealed a password used to access the social media account of the broadcaster in an interview.

Following the successful attack against the network of the TV French Channel TV5Monde, law enforcement and French Intelligence started to investigate the attach chain.

Almacenamiento de contraseñas

- No almacenar nunca en texto plano
- No usar MD5, SHA1, y otros algoritmos antiguos - Usar SHA3, Blowfish..
- Implementar Salt – usar funciones estándar de los lenguajes



Control de Accesos y Usuarios

- Evitar compartir contraseñas
- Evitar usar usuario root – Usar sudo
- Revisar regularmente los usuarios de sistema en servidores
- Establecer e implementar políticas de administración de usuarios
- Establecer e implementar políticas de contraseñas
- Otorgar los mínimos privilegios necesarios
- Implementar límites de intentos fallidos de autenticación

¿Es suficiente? ...

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Autenticación de Doble Factor

Autenticación de doble factor

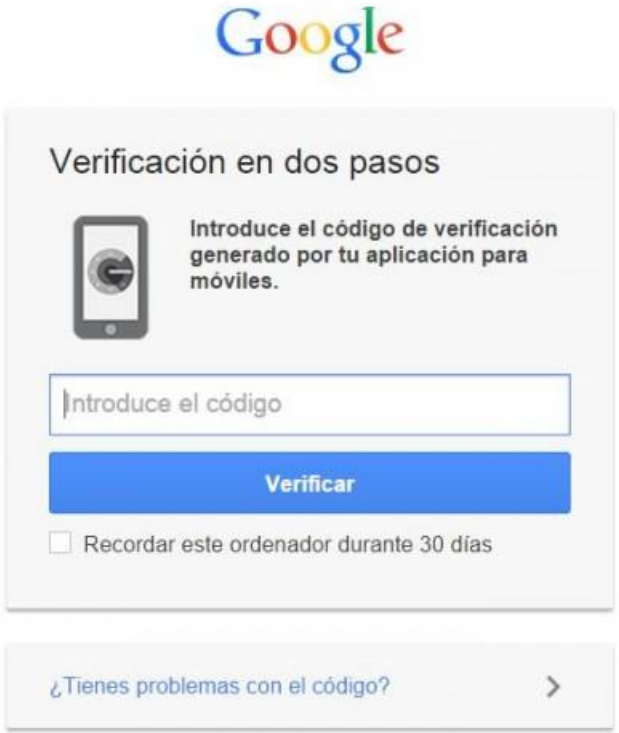
- Medida de seguridad adicional al usuario y contraseña

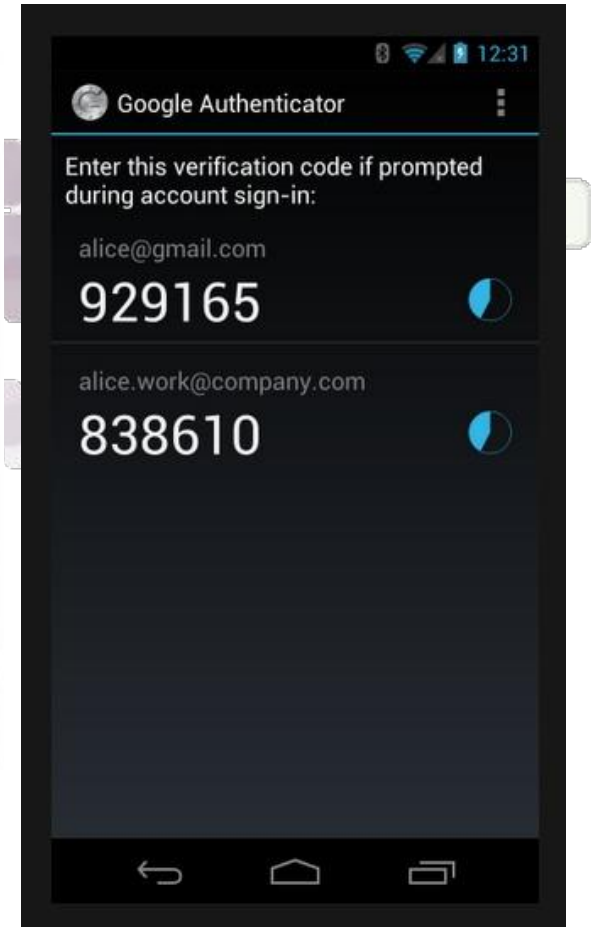
Usuario + Contraseña + CÓDIGO DE SEGURIDAD

1) Algo que el usuario sabe → contraseña
2) Algo que el usuario tiene → teléfono
3) Algo que el usuario es → huella dactilar

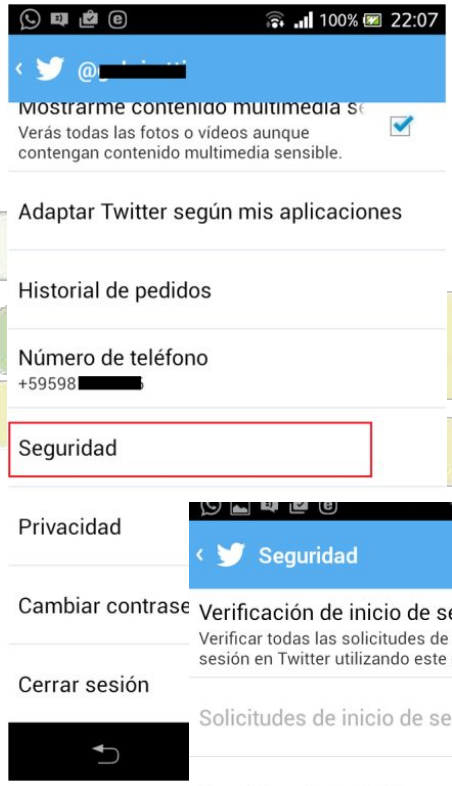
Autenticación de doble factor (1)

- Google
- Outlook
- Facebook
- Twitter
- Dropbox
- Wordpress





Autenticación de doble factor (2)



Autenticación de doble factor (3)

- Implementacion 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:~#
```

Autenticación de doble factor (4)

- Implementacion de OTP con Google Authenticator para proteger SSH

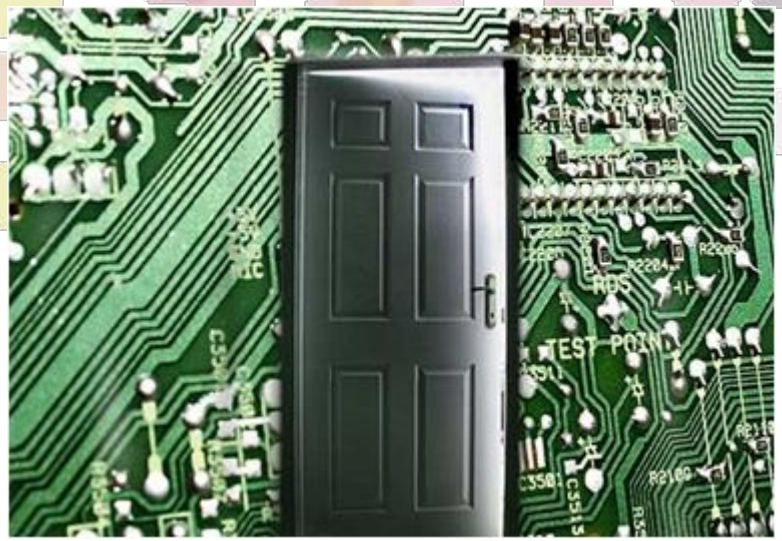
```
root@kali:~/libpam-google-authenticator-1.0#
root@kali:~/libpam-google-authenticator-1.0# google-authenticator

Do you want authentication tokens to be time-based (y/n) y
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/root
@kali%3Fsecret%3DWKHM6UVJNTPYSPTQ
Your new secret key is: WKHM6UVJNTPYSPTQ
Your verification code is 434260
Your emergency scratch codes are:
  30287010
  70585905
  68748337
  15176712
  38041521

Do you want me to update your "/root/.google_authenticator" file (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 seconds and in order to compensate for
possible time-skew between the client and the server, we allow an extra
token before and after the current time. If you experience problems with poor
time synchronization, you can increase the window from its default
size of 1:30min to about 4min. Do you want to do so (y/n) y
```

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

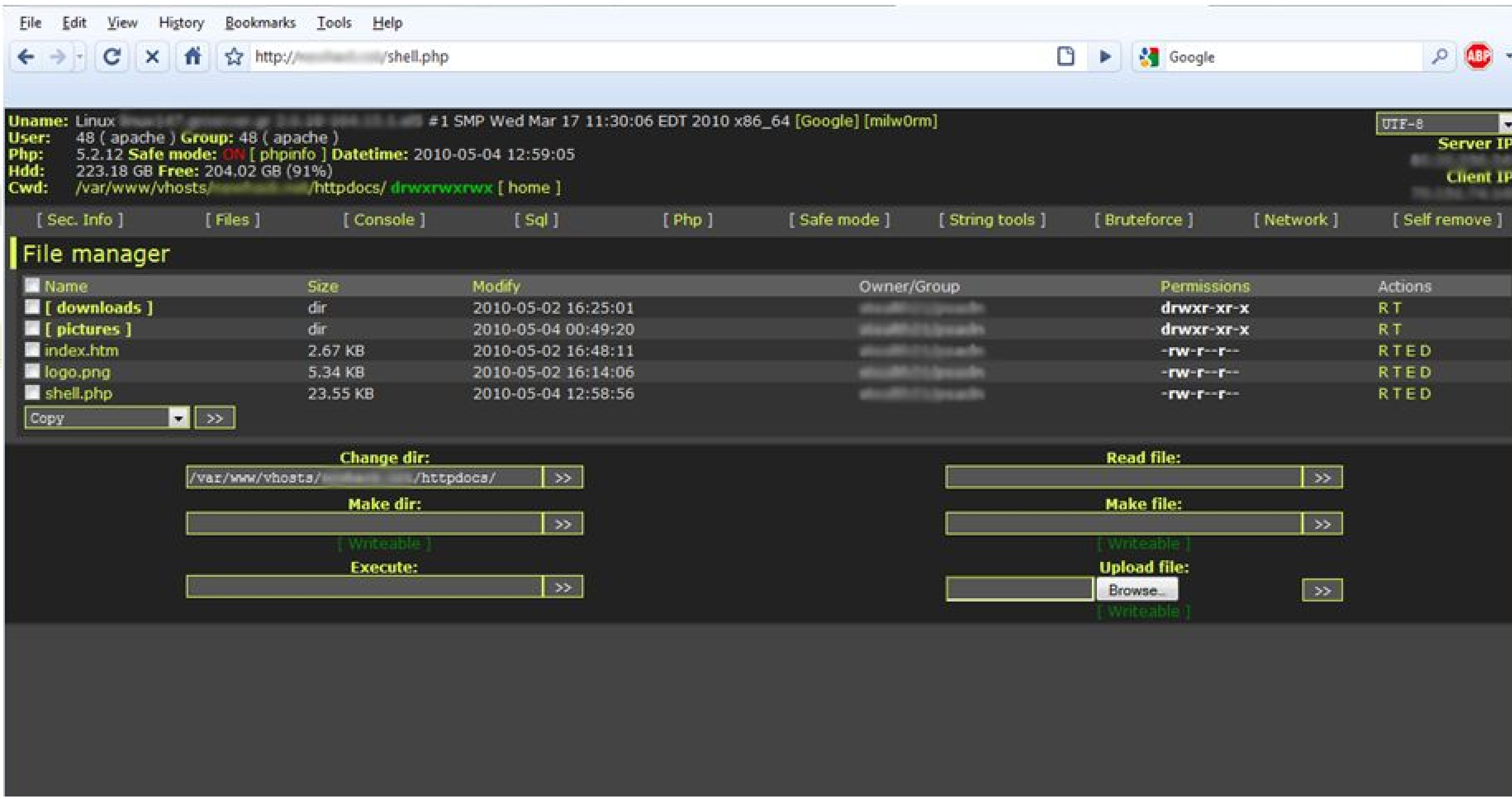
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Webshell y Backdoors



Webshells


File Edit View History Bookmarks Tools Help
http:// /shell.php
Google
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]
UTF-8
Server IP:
Client IP:
[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 drwxr-xr-x R T
[pictures] dir 2010-05-04 00:49:20 drwxr-xr-x R T
index.htm 2.67 KB 2010-05-02 16:48:11 -rw-r--r-- R T E D
logo.png 5.34 KB 2010-05-02 16:14:06 -rw-r--r-- R T E D
shell.php 23.55 KB 2010-05-04 12:58:56 -rw-r--r-- R T E D
Copy
Change dir:
/var/www/vhosts/ /httpdocs/
Read file:
Make dir:
Make file:
[Writeable]
Execute:
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@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:*
```

Cómo detectarlos?

Herramientas y técnicas:

- Findbot: http://cbl.abuseat.org/findbot.pl
- Shelldetect: http://shelldetector.com/
- img-analize.sh: script desarrollado por el CERT-PY
- Comandos útiles: grep, find, locate, ps, netstat

Posibles indicadores:

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

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Malware y Rootkits

Malware

- Virus
- Gusanos
- Spyware
- Troyanos
- Ransomware

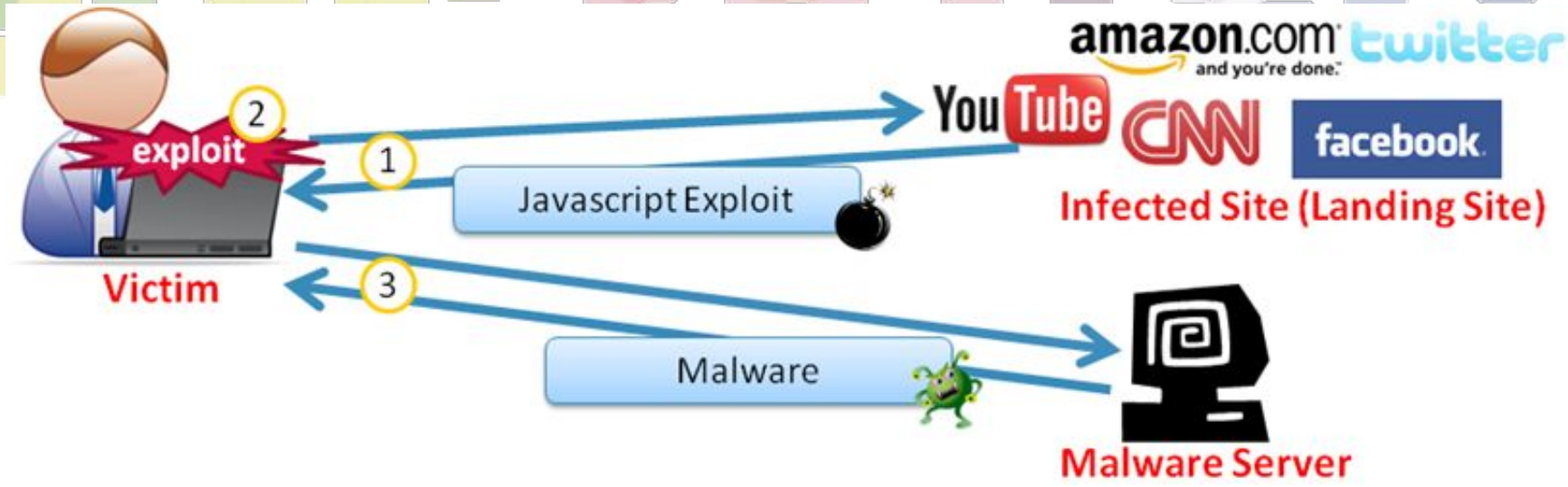
¿Cómo entran? ...

Vulnerabilidades

- Sistema operativo:
  - Windows
  - Linux
  - OS X
  - Android
- Programas o aplicaciones:
  - Office
  - Java
  - Navegadores

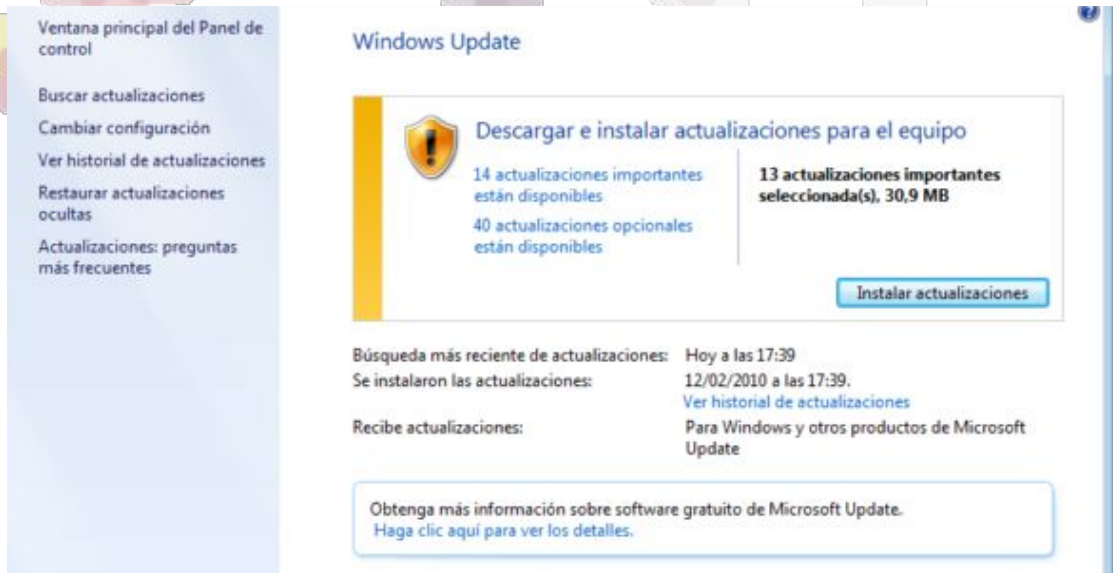
Drive by Download

- Sólo se requiere que un usuario abra una página web en el navegador para infectarlo.
- El payload malicioso explota una vulnerabilidad y se ejecuta



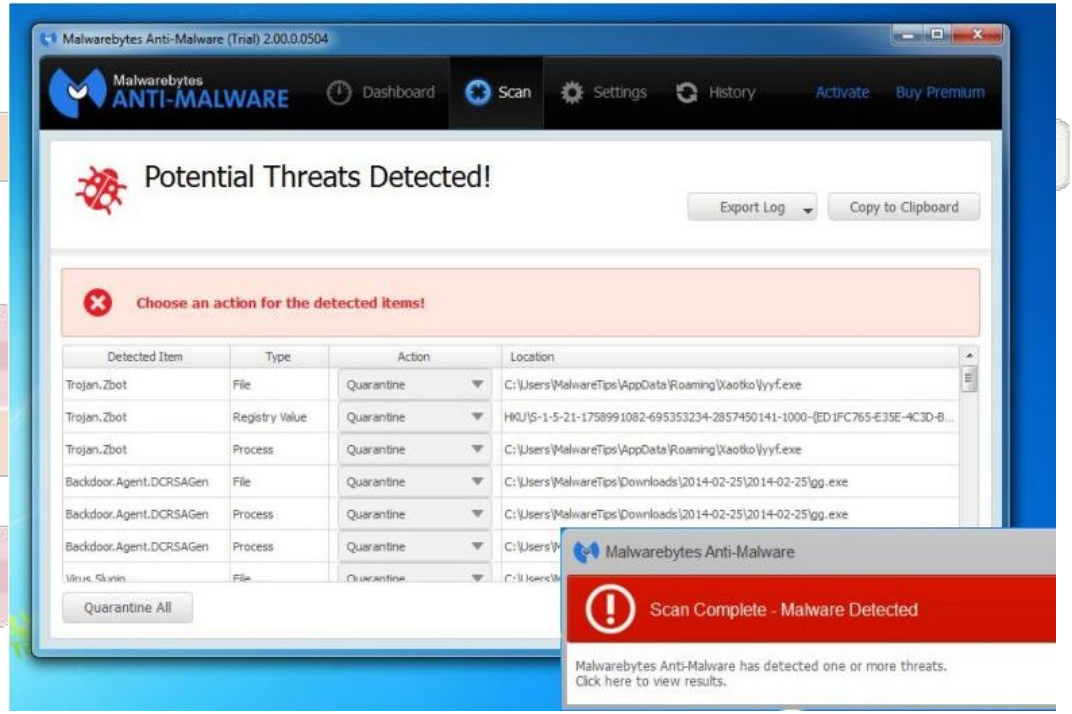
¿Cómo protegernos del malware?

- Actualización permanente del sistema operativo y aplicaciones
- Usar software legal
- No descargar programas de dudosa reputación
- Deshabilitar la ejecución automática de dispositivos USB
- Contar con software de seguridad



Software de seguridad

- Antivirus
- Antimalware
- Antirootkit



Free vs. Premium

Malwarebytes Anti-Malware Key Features	Free	Premium
REAL-TIME PROTECTION	✗	✓
MALICIOUS WEBSITE BLOCKING	✗	✓
AUTOMATIC UPDATES	✗	✓
FAST HYPER SCANS	✗	✓
SCHEDULED SCANS	✗	✓
ADVANCED MALWARE DETECTION	✓	✓
ADVANCED MALWARE REMOVAL	✓	✓

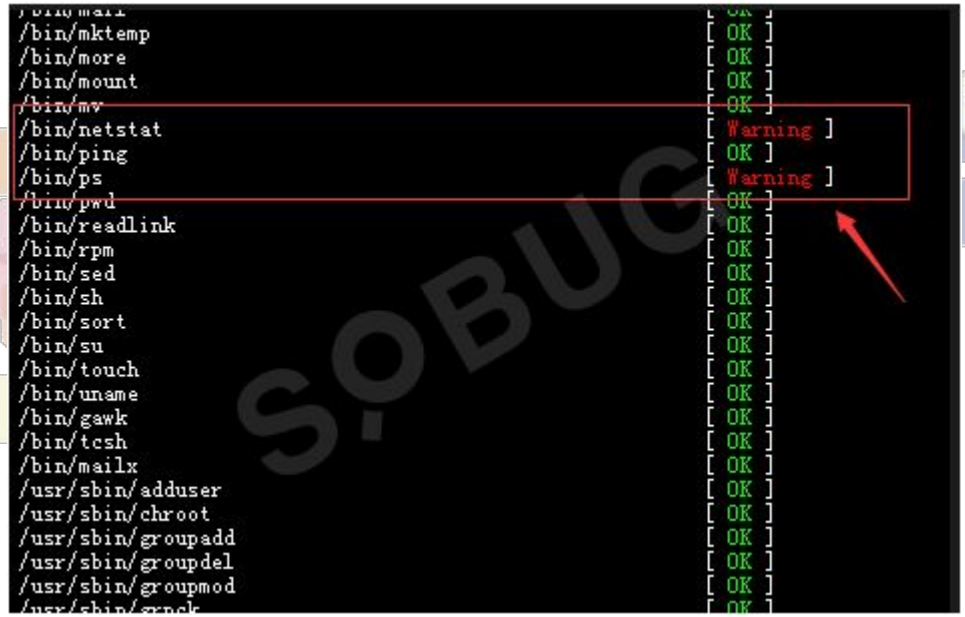
Rootkit

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.

Software de seguridad (1)

En servidores Linux:

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



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