Lab 3.1.4 Network Enumeration

Tuesday, July 11, 2023 9:09 PM

PART A:
#Telnet Probing

172.20.50.10
Vulnerable *
Web Server:
Microsoft IIS httpd 10.0

172.20.50.54
Vulnerable *
Web Server:
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
Note Worthy:
Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>

2 Hosts Vulnerable…

PART B:
#smb_enumshares exploit SMB scan with Metasploit

Rhost set to 172.20.50.10 for the Windows server

Scan results:

[-] 172.20.50.10:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[*] 172.20.50.10:445 - Windows 2019 (Unknown)
[*] 172.20.50.10:445 - No shares collected
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

SMB User credentials set to:
Username: SWilson
Password: OnYourLeft!

Scan results after credentials:

[-] 172.20.50.10:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[*] 172.20.50.10:445 - Windows 2019 (Unknown)
[+] 172.20.50.10:445 - ADMIN$ - (DISK) Remote Admin
[+] 172.20.50.10:445 - C$ - (DISK) Default share
[+] 172.20.50.10:445 - IPC$ - (IPC) Remote IPC
[+] 172.20.50.10:445 - NETLOGON - (DISK) Logon server share
[+] 172.20.50.10:445 - Private - (DISK)
[+] 172.20.50.10:445 - Public - (DISK) Public
[+] 172.20.50.10:445 - SYSVOL - (DISK) Logon server share
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

#smb_enumusers exploit SMB scan with Metasploit

Rhost set to 172.20.50.10

Scan results:

[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Note Insufficient results. Proceeding with providing a valid account.

SMB User credentials set to:
Username: SWilson
Password: OnYourLeft!

Scan results after credentials:

[+] 172.20.50.10:445 - HACKME [Administrator, Guest, krbtgt, dev, NRomanoff, PPotts, SWilson, WMaximoff, BBanner, SRogers, WWilson, SLee, PBlart, SLang, TStark, SStrange, JHammer, CJanssen, PPhillips] (LockoutTries=0 PasswordMin=7)
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Note New account user names discovered as well as Lockout tries is 0 and Passwordmin is set to 7.

PART C:

#Use nmap script to scan for SMB-related info on Metasploitable host:

Note Syntax used in nmap:
Nmap -script=smb-enum-shares 172.20.50.54

Scan results:

Nmap scan report for 172.20.50.54
Host is up (0.0023s latency).
Not shown: 978 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
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

Host script results:
| smb-enum-shares:
| account_used: <blank>
| \\172.20.50.54\ADMIN$:
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\172.20.50.54\IPC$:
| 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
| \\172.20.50.54\opt:
| Type: STYPE_DISKTREE
| Comment:
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\172.20.50.54\print$:
| Type: STYPE_DISKTREE
| Comment: Printer Drivers
| Users: 1
| Max Users: <unlimited>
| Path: C:\var\lib\samba\printers
| Anonymous access: <none>
| \\172.20.50.54\tmp:
| Type: STYPE_DISKTREE
| Comment: oh noes!
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_   Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 17.55 seconds

Recorded for comment in share \tmp:

\172.20.50.54\tmp:

| Type: STYPE_DISKTREE
| Comment: oh noes!
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_ Anonymous access: READ/WRITE

#Nmap script smb-enum-users.nse

Results of script scan smb-enum-users.nse

Starting Nmap 7.91 (https://nmap.org) at 2023-07-12 00:55 CDT
Nmap scan report for 172.20.50.54
Host is up (0.0046s latency).
Not shown: 978 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
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

Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
| Full name: backup
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1004)
| Full name: bin
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bind (RID: 1210)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\daemon (RID: 1002)
| Full name: daemon
| Flags: Account disabled, Normal user account

| METASPLOITABLE\dhcp (RID: 1202)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\distccd (RID: 1222)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\ftp (RID: 1214)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\games (RID: 1010)
| Full name: games
| Flags: Account disabled, Normal user account
| METASPLOITABLE\gnats (RID: 1082)
| Full name: Gnats Bug-Reporting System (admin)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\irc (RID: 1078)
| Full name: ircd
| Flags: Account disabled, Normal user account
| METASPLOITABLE\klog (RID: 1206)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\libuuid (RID: 1200)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\list (RID: 1076)
| Full name: Mailing List Manager
| Flags: Account disabled, Normal user account
| METASPLOITABLE\lp (RID: 1014)
| Full name: lp
| Flags: Account disabled, Normal user account
| METASPLOITABLE\mail (RID: 1016)
| Full name: mail
| Flags: Account disabled, Normal user account
| METASPLOITABLE\man (RID: 1012)
| Full name: man
| Flags: Account disabled, Normal user account
| METASPLOITABLE\msfadmin (RID: 3000)
| Full name: msfadmin,,,
| Flags: Normal user account
| METASPLOITABLE\mysql (RID: 1218)
| Full name: MySQL Server,,,
| Flags: Account disabled, Normal user account
| METASPLOITABLE\news (RID: 1018)
| Full name: news
| Flags: Account disabled, Normal user account
| METASPLOITABLE\nobody (RID: 501)
| Full name: nobody
| Flags: Account disabled, Normal user account
| METASPLOITABLE\postfix (RID: 1212)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\postgres (RID: 1216)
| Full name: PostgreSQL administrator,,,
| Flags: Account disabled, Normal user account
| METASPLOITABLE\proftpd (RID: 1226)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\proxy (RID: 1026)
| Full name: proxy
| Flags: Account disabled, Normal user account

```
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Account disabled, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

#Questions in #4 of part C:

Recorded results:

A. Yes, there is an account named "nobody"
B. Yes, there is an account named "www-data"
C. No, there is NOT an account name "1337"