REPORT ON METASPLOITABLE2

TARGET
IP:192.168.1.78

DATE:14/05/23
TIME: 1:40 PM

SAGAR
NEPAL

TABLE OF CONTENTS:

INTRODUCTION

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. It is an intentionally vulnerable Ubuntu based Linux Virtual Machine designed to provide a test environment for performing penetration testing and security analysis.

SCANNING

Scanning can be considered a logical extension (and overlap) of active reconnaissance that helps attackers identify specific vulnerabilities. It's often that attackers use automated tools such as network scanners and war dialers to locate systems and attempt to discover vulnerabilities.

In my case the target ip address is: 192.168.1.78

NMAP SCAN

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

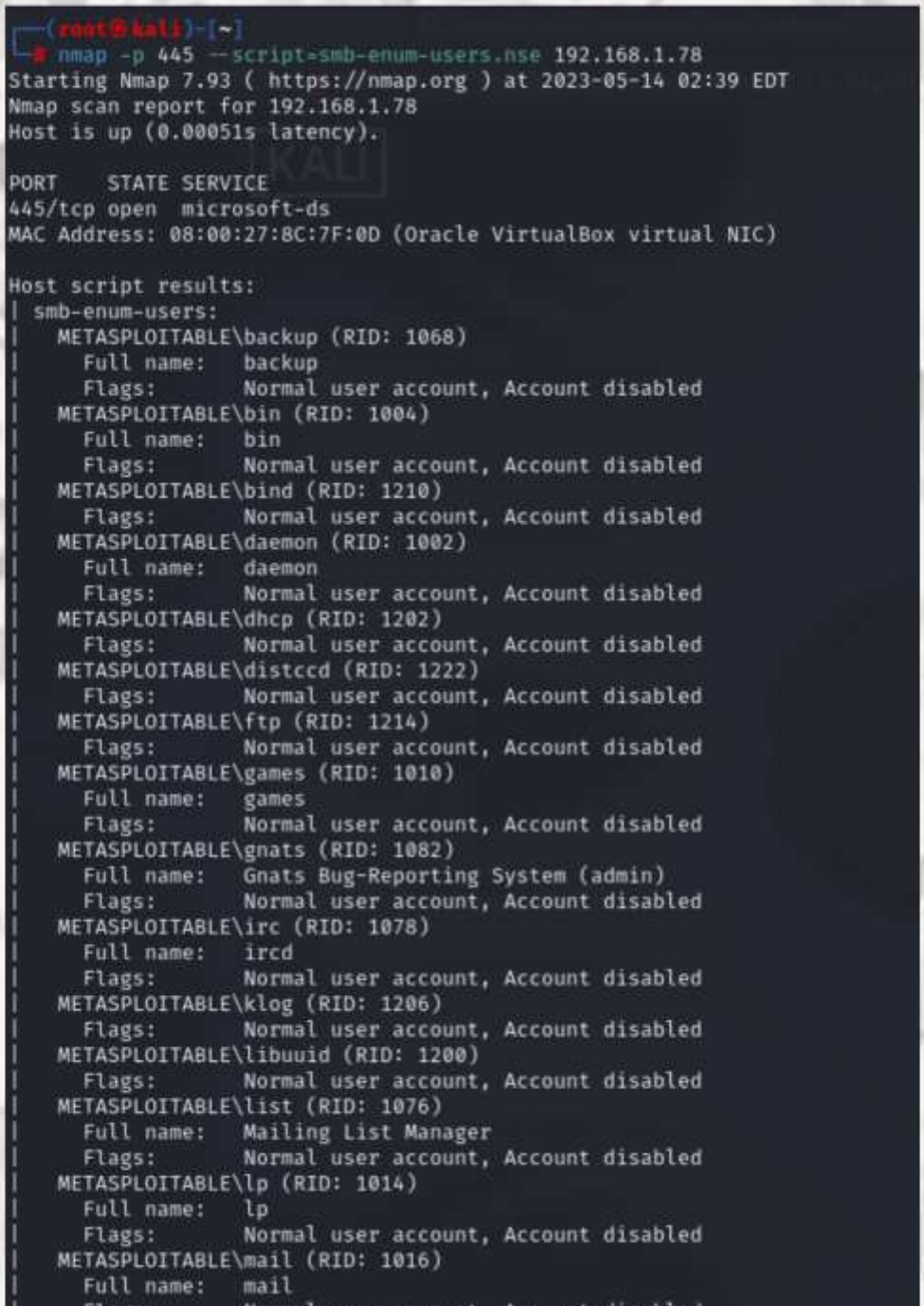
```
┌──(root㉿kali)-[~]
└─# nmap -p- 192.168.1.78
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-14 04:16 EDT
Nmap scan report for 192.168.1.78
Host is up (0.000069s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39517/tcp open  unknown
41883/tcp open  unknown
52395/tcp open  unknown
57604/tcp open  unknown
MAC Address: 08:00:27:8C:7F:0D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

I used command nmap -p- 192.168.1.78 to scan all the open ports in the given ip address.

Windows uses port 445 for file sharing across the network so I am going to enumerate it.

ENUMERATION

Enumeration in cyber security is extracting a system's valid usernames, machine names, share names, directory names, and other information. It is a key component of ethical hacking and penetration testing, as it can provide attackers with a wealth of information that can be used to exploit vulnerabilities.



```
METASPLOITABLE\man (RID: 1012)
  Full name:   man
  Flags:       Normal user account, Account disabled
METASPLOITABLE\msfadmin (RID: 3000)
  Full name:   msfadmin,,,
  Flags:       Normal user account
METASPLOITABLE\mysql (RID: 1218)
  Full name:   MySQL Server,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\news (RID: 1018)
  Full name:   news
  Flags:       Normal user account, Account disabled
METASPLOITABLE\nobody (RID: 501)
  Full name:   nobody
  Flags:       Normal user account, Account disabled
METASPLOITABLE\postfix (RID: 1212)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\postgres (RID: 1216)
  Full name:   PostgreSQL administrator,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\proftpd (RID: 1226)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\proxy (RID: 1026)
  Full name:   proxy
  Flags:       Normal user account, Account disabled
METASPLOITABLE\root (RID: 1000)
  Full name:   root
  Flags:       Normal user account, Account disabled
METASPLOITABLE\service (RID: 3004)
  Full name:   ,,,
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sshd (RID: 1208)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sync (RID: 1008)
  Full name:   sync
  Flags:       Normal user account, Account disabled
METASPLOITABLE\sys (RID: 1006)
  Full name:   sys
  Flags:       Normal user account, Account disabled
METASPLOITABLE\syslog (RID: 1204)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\telnetd (RID: 1224)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\tomcat55 (RID: 1220)
  Flags:       Normal user account, Account disabled
METASPLOITABLE\user (RID: 3002)
  Full name:   just a user,111,,
  Flags:       Normal user account
METASPLOITABLE\uucp (RID: 1020)
  Full name:   uucp
  Flags:       Normal user account, Account disabled
METASPLOITABLE\www-data (RID: 1066)
  Full name:   www-data
```

We can see only msfadmin and user account are enabled in the given port 445 where all the other account are disabled.

So I am using smbclient -U username -L ip address to gain access in WORKGROUP of both of them using the default password i.e user.

```
┌──(root㉿kali)-[~]
└─# smbclient -U msfadmin -L 192.168.1.78
Password for [WORKGROUP\msfadmin]:

        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))
        msfadmin        Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

┌──(root㉿kali)-[~]
└─# smbclient -U user -L 192.168.1.78
Password for [WORKGROUP\user]:

        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))
        user            Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

Then I Tried To ENUMERATE all the SHARE FILE Inside the USER one by one by using SMBCLIENT //IP ADDRESS/FILENAME and got the following output where I got the Anonymous login successful for TMP and IPC$.

```
┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun May 14 02:42:11 2023
  ..                                 DR        0  Sun May 20 14:36:12 2012
  .ICE-unix                          DH        0  Sun May 14 02:36:43 2023
  .X11-unix                          DH        0  Sun May 14 02:36:52 2023
  .X0-lock                           HR       11  Sun May 14 02:36:52 2023
  4571.jsvc_up                        R        0  Sun May 14 02:36:59 2023

                7282168 blocks of size 1024. 5427160 blocks available
smb: \> pwd
Current directory is \\192.168.1.78\tmp\
smb: \> cd ..
smb: \> ls
  .                                   D        0  Sun May 14 02:42:11 2023
  ..                                 DR        0  Sun May 20 14:36:12 2012
  .ICE-unix                          DH        0  Sun May 14 02:36:43 2023
  .X11-unix                          DH        0  Sun May 14 02:36:52 2023
  .X0-lock                           HR       11  Sun May 14 02:36:52 2023
  4571.jsvc_up                        R        0  Sun May 14 02:36:59 2023

                7282168 blocks of size 1024. 5427160 blocks available
smb: \> exit
```

```
┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/user
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/opt
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/print$
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/IPC$
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> cd ..
smb: \> pwd
Current directory is \\192.168.1.78\IPC$\
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> exit

┌──(root㉿kali)-[~]
└─# smbclient //192.168.1.78/ADMIN$
Password for [WORKGROUP\root]:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
```

THE ANONYMOUS LOGIN FOR REST OF THE OTHER FILES WERE DENIED.

CONCLUSION

So in this way attackers will scan networks to discover live hosts and open port. They will then enumerate the live hosts and ports to discover services, machine names, and other network resources.