Lab 3: Packet Analysis (Part 2)

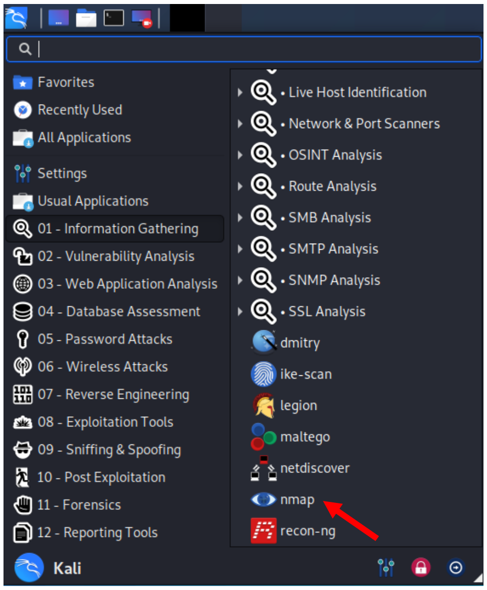
- This is an individual assignment, and worth 20 points.
- The due date is 2:30 (Sec 01) / 5:30 (Sec 76) on Friday, September 18.
- Follow the naming convention.
- You should not scan any live servers using Nmap or send malicious packets using hping3. If caught, you may be expelled from school (not a joke!).

1. Overview

- The objective of this assignment is to perform a ping sweeping and port scanning. Students also transfer files using the FileZilla client to Metasplotable and discuss security implications. Last, students perform a SYN flooding attack.
- This learning objective is measured by examining the outputs in screenshots after performing the tasks.

2. Preparation

- You can do this homework using the Proxmox server or using the two VM's you created in homework 1. I recommend doing it on your own environment for a better control of Kali screens. When you use the Proxmox server, you may want to change the screen resolution of Kali.
- If the network setting of your VMs on VirtualBox is **bridged**, please change it to **Net NAT**. This is because your Metasploitable can receive attacks.
- If you are doing this on your own Kali, you should install FileZilla. To do it, run "**apt update**" and then "**apt install filezilla**".
- Study Nmap using the following sites.
  - http://nmap.org/
  - http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
- On Kali, Nmap can be found on **01- Information Gathering** > **nmap**. Or, launch a terminal and type "nmap" on the command shell.



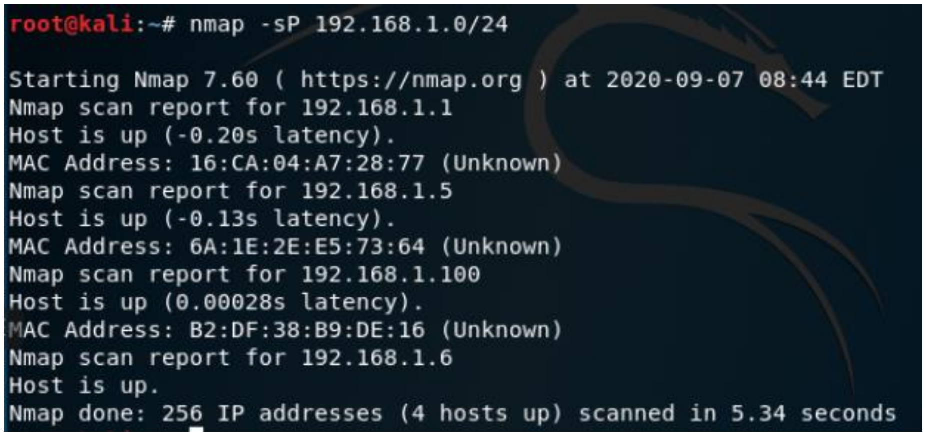
- **Power on** Kali and Metasploitable.

Task 1. Identifying the IP addresses

- Find the IP address and subnet mask of **Kali** (use ifconfig). Report the result with a screenshot.
- Find the IP address and subnet mask of **Metasploitable**. Report the result with a screenshot.

Task 2. Performing a Ping Sweeping

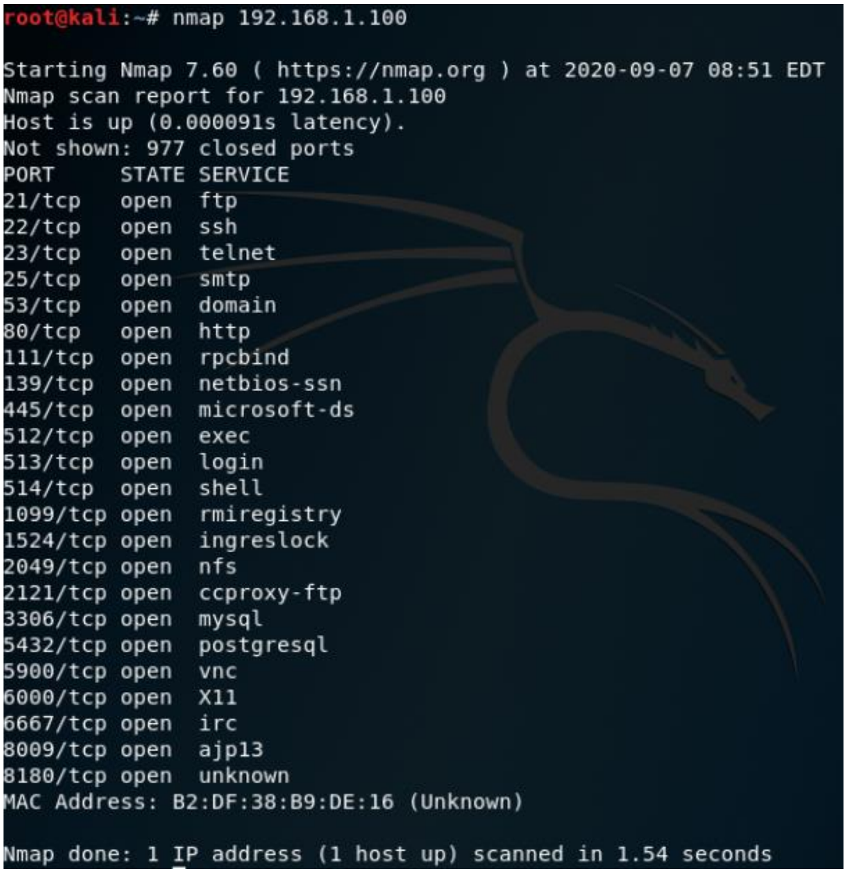
- Perform a ping sweeping with Nmap on the network in your VLAN. For ping sweeping, use **-sP** flag of Nmap and provide the network address and subnet mask.
- Ping sweeping can be performed as follows (sample output below).
  - **# nmap -sP x.x.x.0/24** where x.x.x.0 is a network address.
- Report the result with a screenshot.



```
root@kali:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-07 08:44 EDT
Nmap scan report for 192.168.1.1
Host is up (-0.20s latency).
MAC Address: 16:CA:04:A7:28:77 (Unknown)
Nmap scan report for 192.168.1.5
Host is up (-0.13s latency).
MAC Address: 6A:1E:2E:E5:73:64 (Unknown)
Nmap scan report for 192.168.1.100
Host is up (0.00028s latency).
MAC Address: B2:DF:38:B9:DE:16 (Unknown)
Nmap scan report for 192.168.1.6
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.34 seconds
```

Task 3. Performing a Port Scanning

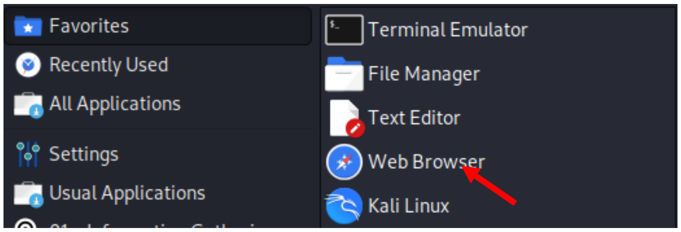
- Port scanning is an attempt to figure out whether any ports on a host are open and listening.
- Scan **Metasploitable** using **Kali**.
- Port scanning can be performed as follows (sample output below).
  - **# nmap IP-of-the-target**
  - You should replace **IP-of-the-target** with your target's.
- Report the result with a screenshot.



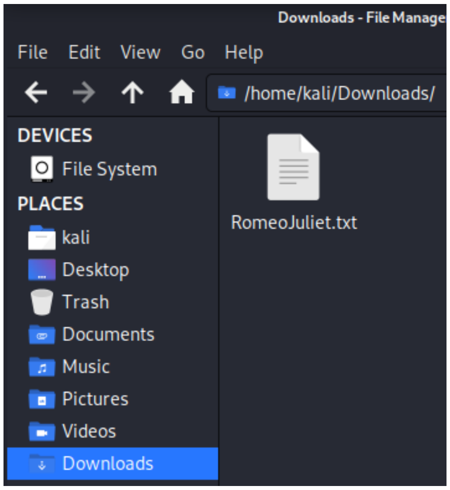
```
root@kali:~# nmap 192.168.1.100

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-07 08:51 EDT
Nmap scan report for 192.168.1.100
Host is up (0.000091s 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: B2:DF:38:B9:DE:16 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
```

Task 4. Analyzing FTP Signatures

- Open a web browser on Kali and go to the class webpage on BB. Locate Homework 3 and download the text file "RomeoJuliet.txt."



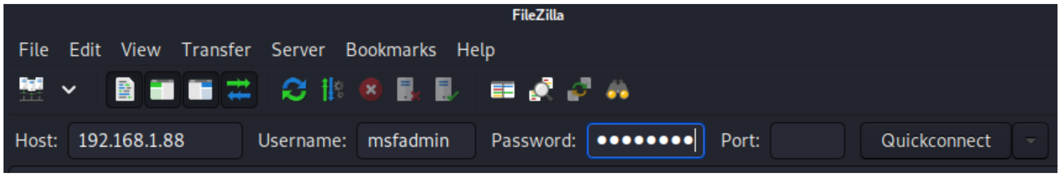
- Check the location of the downloaded text file.



/home/kali/Downloads/

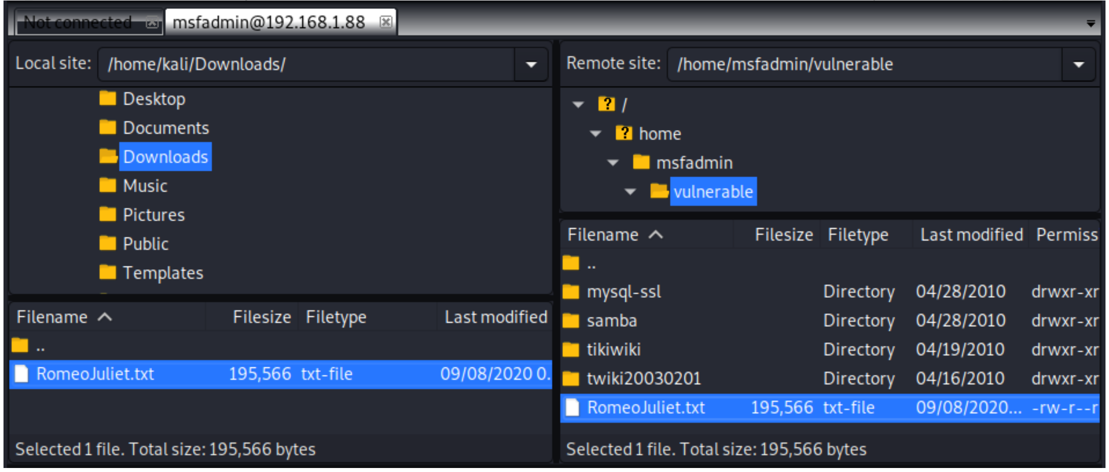
RomeoJuliet.txt

- Open a terminal and run FileZilla by typing "**filezilla**" command. For this, you do not switch into a super user. Check that you are directed to **home** directory (Figure below). If you run it as a super user, you are directed to the **root**.
- Open another terminal and switch into a super user. Type **wireshark** to launch the application. **Start** Wireshark by following Capture > Options > Input > Select Interface (eth0) > Start.
- On **FileZilla**, log in to the ftp server running on **Metasploitable**. Use "**msfadmin/msfadmin**" for ID/pwd. You should provide the IP address of your target.



Host: 192.168.1.88 Username: msfadmin Password: •••••••• Port:

- **Upload** the text file you downloaded on Kali to the "**vulnerable**" directory on Metasploitable.



Local site: /home/kali/Downloads/

Filename	Filesize	Filetype	Last modified
..			
RomeoJuliet.txt	195,566	txt-file	09/08/2020 0.

Selected 1 file. Total size: 195,566 bytes

Remote site: /home/msfadmin/vulnerable

Filename	Filesize	Filetype	Last modified	Permiss
..				
mysql-ssl		Directory	04/28/2010	drwxr-xr
samba		Directory	04/28/2010	drwxr-xr
tikiwiki		Directory	04/19/2010	drwxr-xr
twiki20030201		Directory	04/16/2010	drwxr-xr
RomeoJuliet.txt	195,566	txt-file	09/08/2020...	-rw-r--r

Selected 1 file. Total size: 195,566 bytes

- On Wireshark, **stop** capturing the packets and **save** the data. The pcap file goes to **Downloads** directory. If you don't capture the traffic on Wireshark, it is possible that you have not selected the right interface.
- **Stop** the connection to the FTP server and **close** FileZilla.
- Run **Wireshark as a super user**. **Open** the saved pcap file with Wireshark. For this, follow File > Open > locate the pcap file.

- Task

1) Identify the TCP packets used for the initial three-way handshake for the connection to the ftp server. Take a screenshot of those TCP packets. Those packets are placed right before the first ftp packet.
2) Identify the TCP stream used for the authentication of the client to the FTP server. Take a screenshot of the TCP stream.
3) Identify the first and last FTP-DATA packets used for the uploading of the text file. Take a screenshot for each (two required).
4) Discuss security implications of this transfer.

Task 5. SYN Flooding Attack

- Perform a SYN flooding attack using **hping3 against Metasploitable from your Kali**. The detailed info of Hping3 can be found here: http://linux.die.net/man/8/hping3.

- **Steps**

  1) Start Wireshark on **Kali** as a super user.
  2) Open a terminal and run a command for a SYN flooding attack using the following template (you should type the command on the command shell. No copying and pasting!):

```
hping3  -S  target_ip_addr  -a  spoofed_ip_addr  --flood
```

-S --syn	set SYN flag
-a --spoof	spoofed source address (use a private IP address: 192.168.x.x)
-p --destport	destination port (default 0)
-i --interval	wait (uX for X microseconds, for example -i u1000)
--fast	alias for -i u10000 (10 packets for second)
--faster	alias for -i u1000 (100 packets for second)
--flood	send packets as fast as possible. Don't show replies. (usage: -i flood, or --flood)

target_ip_addr: provide the IP address of Metasploitable
spoofed_ip_addr: provide an arbitrary private IP address

  3) Run the above command for 10 seconds only. Stop the attack by pressing CNTL+C to prevent the crash of the host. If you are doing it with your own host (not on Proxmox)

and want to experiment, run it for several minutes to see whether the attack really crashes the host.

- Task

1) Report your Wireshark capture in a screenshot. Show only SYN packets.