Lab 3

Scanning & Quiz 1

1. Turn on Kali and Meta2 VM.

   Kali and Meta2 VMs will be used as an attacker's machine and a target machine, respectively.

   Check the connections between two VMs. You can use `ifconfig` to check the IP addresses and use ping to check the connectivity.

2. Using *fping*
   fping is a tool for ping sweep.

   (a) Run `fping -h` or `fping -h|less` to know about available options.

   (b) Run `fping -g <Kali IP> <Meta2 IP>`
   (change the range to include the Meta and Kali VM's IP addresses)

   (c) Run `fping -g 10.0.2.1/27` (on Virtual Box) or `192.168.64.1/27` (on UTM)
   (change the range to include the Meta and Kali VM's IP addresses using netmask)

3. Recap of some useful Linux commands
   - sudo: $sudo <command> : Execute your command with admin privilege
   - Searching and filtering texts
     - grep: `$grep [options] [pattern] [file name]`
       - Example 1) `$ grep -irl 'password' /etc`
       - This will search for the word password in all the files starting from the etc directory in the root system (/)
       - -i : To ignore case and include all the uppercase/lowercase letters; -r : To search recursively inside subfolders; -l : To print the filenames where the filter matches
       - Open one of the files listed by the grep command using Mousepad (mousepad <filename>) and see there is a string "password" in the file.
       - Example 2) `$ sudo cat /etc/shadow | grep 'kali'`
       - We use the cat command to open the shadow file; then we use the grep command to filter out the root account and its hashed password.
     -

4. Introduction to *Nmap*

   Nmap is the most popular scanning tool. This exercise is to familiarize yourself with nmap commands. Use `–v` to get more detailed results.

(a) To view the help page of nmap, type nmap –h
To view it page by page run `nmap –h | less`

(b) Go to Kali. Let us try nmap against the Meta2 VM.

a. What is a default scanning method?
b. Give a port range. For example, nmap -p 80-100 <Meta IP>
c. Use `--top-ports N` option with FIN (`-sF`) and Xmas (`-sX`) scans. What are the results?

5. Additional *Nmap* options

(a) Say, you want to adjust timing for your scanning. What option would you use? Try to give some values for your mode: `-T0` or `–T1`. You may realize that mode 0 and 1 will take too long. In this case, you can stop it using ctrl+c.

(b) If you put `-sn` (n means "no port") as an option, nmap will behave like the Ping scan, but it will perform the following additional steps:

a. It will send an ICMP echo request and get the response (from the target host).
b. It will send an ICMP time stamp request.

Try `nmap -sn 10.0.2.1/25` (on Virtual Box) or `192.168.64.1/25` (on UTM) to see what results you get.

(c) If you want to save your result to a text file, use `–oN file1.txt` at the end of the nmap command.

6. Ack scan using *Nmap (Find filtering examples)*

(a) Log in Meta2 VM and get its IP address.

d. Set the default firewall mode as deny
```
$ sudo ufw default deny
```
e. Turn on the firewall
```
$ sudo ufw enable
```
f. Check whether the firewall is working or not
```
$ sudo ufw status
```

(b) Go to Kali. Then run `sudo nmap –sA -v <Meta2 IP >` What are the results of your scan? What does `–sA` mean? Try to run nmap again with a port option, for example, `sudo nmap –sA -v -p 80 <Meta IP>`

(c) Go to Meta2 again. Turn off the firewall.

g. Turn off the firewall
```
$ sudo ufw disable
```
h. Check whether firewall is working or not
```
$ sudo ufw status
```

(c) Go to Kali. Try TCP Ack Scan on the Meta2 VM again. What are the results of your scan? What is the different from previous scan?

(d) Go to Metasploitable. Enable the firewall but allow port 80.

a. Set the firewall up
```
$ sudo ufw enable
```
b. Add rule to allow port 80 and check the status of the firewall
```
$ sudo ufw allow 80
$ sudo ufw status
```
c. Additionally, you can check the port 80 by browsing http://<Meta IP address> from Kali

d. Now, block port 80 using the following command:
```
$ sudo ufw deny 80
```
Then, try to connect to Meta2 VM’s website again to see what happens.

e. Go to Kali and run the following command:
```
$ sudo nmap -sA -v -p 80 <Meta2 IP>
```

(e) Go to Meta2 VM again. Turn off the firewall. (Otherwise, Meta2 VM will not work for other exercises we will do later.)
```
$sudo ufw disable
```