Lab 3

Scanning & Lab Quiz

1. Turn on **Kali** and **Metasploitable2** VM.

   Kali and **Metasploitable2** ("Meta") will be used as an attacker's machine and a target machine, respectively. **Metasploitable2** is purposely set up as vulnerable.

   Kali Username:kali
   Kali Password: kali
   Meta Username: msfadmin
   Meta Password:msfadmin

   Check the connections between two VMs. You can use `ifconfig` to check the IP addresses and use `ping` to check the connectivity.
   (a) What is the IP address of your Metasploitable machine? 10.0.2.4
   (b) What is the IP address of your Kali Linux? 10.0.2.15

2. `fping` is a tool for ping sweep. You will be using your Kali machine to scan your Meta VM.

   (a) Run `fping -h` or `fping -h|less` to know about available options. What is "-g" option for?

   (b) Run `fping -g <IPADDR1> <IPADDR2>`
   (change the range between IPADDR1 and IPADDR2 to include the Meta VM IP address)

   (c) Run `fping -g <IPADDR3>/28`
   (change IPADDR3 to include the Meta VM IP address)

3. Nmap is the most popular scanning tool. This exercise is to familiarize yourself with `nmap` commands. Use `-v` to get more detailed results.
   To view the help page of nmap, type `nmap -h`
   To view it page by page run `nmap -h | less`

   (a) Go to **Kali**. Run `nmap` against the **Meta.**
   `nmap <Meta IPADDR>.`
   What is a default scanning method? TCP SYN (-sS)

   (b) Run nmap to scan specific ports:
   `nmap -p 80-100 <Meta IPADDR>`

   (c) Run nmap to scan the Use `--top-ports N` option with FIN (-sF) and Xmas (-sX) scans.

   Are there any differences in the scan?

Are there any differences in the scan results?

(d) Where is nmap-services file located?
How many entries are there in the file?

(e) 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 much time so that you have to stop it using `ctrl+c`.

(f) Save your result to a text file. Use `-oN file1.txt`

4. On your **Meta VM,** enable the firewall to block all ports.

(a) Set the default rule of firewall is DENY
```
$ sudo ufw default DENY
```

Turn on the firewall
```
$ sudo ufw enable
```

Check firewall status
```
$ sudo ufw status
```

(b) On your **Kali VM**, run
```
nmap -sA -v <Meta IPADDR>
```

What are the results of your scan?
What does `-sA` mean?

TCP ACK port scan

(c) On your **Meta VM**, turn off the firewall.
```
sudo ufw disable
sudo ufw status
```

(d) On your **Kali VM**.
Try TCP Ack Scan against Meta VM again.
Is the firewall working? What are the difference in the output?

(e) On your **Meta VM**, enable the firewall, but allow port 80.
```
$ sudo ufw enable
$ sudo ufw allow 80
$ sudo ufw status
```

Additionally, you can check the port 80 by browsing to `http://<Meta IP address>` from **Kali**

Block port 80
```
$ sudo ufw deny 80
```

Can you still connect to http://<Meta IPADDR> from your **Kali VM**?

On your Meta VM, disable the firewall after you are done.
```
sudo ufw disable
sudo ufw status
```

5. OS fingerprinting (Remote OS Detection)

OS finger printing is when attacker sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After the test, the results are compared against the general behaviour of operating systems for a match.
Nmap is the most popular active OS detection tool. *Nmap* probes a target with large number of well-crafted packets and the results are compared against Nmap's database of OS fingerprints (nmap-os-db).
Where is this file?

Try to find the version of your **Metasploitable2** using *Nmap*.
```
nmap -v -O <Meta IPADDR>
```

Confirm your result on your **Meta VM**.
```
uname –a
```

6. Scanning with *Scapy*

We can use Scapy to create our own "ad-hoc" scanning tool. We send crafted packets and displaying their responses from the target, **Metasploitable2**.
Issue `scapy` at the terminal to do the following.

(a) (Recap) We can create and test TCP packet with various flags.
Examples: (let the IP address of Metasploitable VM is 10.0.2.5)

i. Crafting a TCP packet with a SYN flag
```
a=IP(dst="<Meta IPADDR>")/TCP(dport=80,flags="S")
sr1(a)
```
ii. Crafting a TCP packet for NULL flag
```
sr1(IP(dst="Meta IPADDR")/TCP(dport=80,flags=0x00))
```
iii. Compare the above results.

(b) The hexadecimal number is useful to set the flags. The first number represents the first 4 bits and the second number represents the next 4 bits. For example, in Xmas scan fin, psh and urg have to be set.

```
[cwr|ece|urg|ack|psh|rst|syn|fin]
[ 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 ]  → 0x29
```

i. Craft a TCP packet with the flag 0x29
```
>>>sr1(IP(dst="10.0.2.5")/TCP(dport=80,flags=0x29))
```
ii. What is the hexadecimal equivalent of a TCP SYN flag in scapy?
iii. Reconstruct (6ai) with a hexadecimal equivalent of SYN flag. Verify your results.

(c) Run multiple ports scan using Scapy

i. Configuring multiple ports using a range ()

```
>>> ans, unans =
sr(IP(dst="10.0.2.5")/TCP(dport=(80,84),flags=0x02))
>>> ans.summary()
```

ii. Passing multiple ports as a list parameter []

```
>>>
sr(IP(dst="10.0.2.5")/TCP(dport=[80,81,83],flags=0x02)
)
```