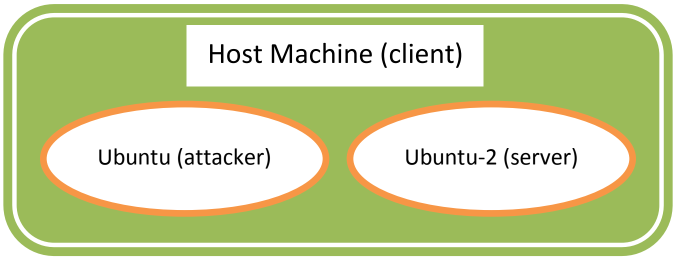
Lab Assignment 3: due 10/26 Monday

Preparation

1. **Network Setup:** To conduct this lab, you need to have 3 machines (for task 1). One computer is used for attacking, the second computer is used as the victim client, and the third computer is used as a server. The host machine and the virtual machine 'Ubuntu' can be regarded as two machines. You need to create another VM by cloning the current VM to be the third one ('Ubuntu-2').



2. **Install Apache Web Server on 'Ubuntu-2' (optional):** You can install apache2 package by executing the following command:

```
$sudo apt-get install apache2
```

   Change the default web page as you want and try to access this web server from the host machine.

3. **Install Netwox/Netwag Tools on 'Ubuntu' (optional):** Netwox consists of a suite of network tools. You will use it to launch attacks. Netwag is a GUI version of Netwox.

```
$sudo apt-get install netwox
```

   Take a brief look at the manual at
   http://www.cis.syr.edu/~wedu/seed/Labs/Lab_Setup/netw522/netwox-doc_html/tools/index.html

4. **Install Ettercap on 'Ubuntu':** Ettercap is another powerful tool often used for man-in-the-middle attacks.

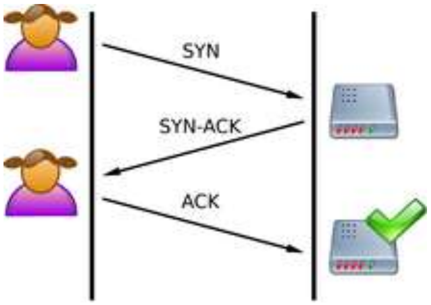
```
$sudo apt-get install ettercap-graphical
```

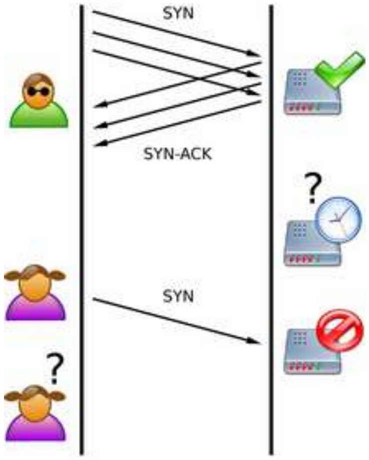
Submission

1. Use **scp** to download the lab report file at /home/shengbo/it443/lab3.txt (optional)
   $scp userid@linux1.cs.umb.edu:/home/shengbo/it443/lab3.txt .
2. Write all the answers in the file.
3. Rename the file to **lab3_firstname1_firstname2.txt**. E.g., if Alice and Bob form a team, the file name should be **lab3_alice_bob.txt**
4. Email the lab report to the TA (Jiayin.Wang001@umb.edu) and CC the instructor (shengbo@cs.umb.edu)

Task 1: SYN Flood Attack

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim's TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP address or do not continue the procedure. Through this attack, attackers can flood the victim's queue that is used for half-opened connections, i.e. the connections that has finished SYN, SYN-ACK, but has not yet got a final ACK back. When this queue is full, the victim cannot take any more connection.





The size of the queue has a system-wide setting. In Linux, we can check the system queue size setting using the following command:

```
$sysctl -q net.ipv4.tcp_max_syn_backlog
```

We can use command "`netstat -na`" to check the usage of the queue, i.e., the number of half opened connection associated with a listening port. The state for such connections is SYN-RECV. If the 3-way handshake is finished, the state of the connections will be ESTABLISHED.

In this task, we will use three machines, the host machine as a **client**, 'Ubuntu-2' as a web **server** running Apache, and 'Ubuntu' as the **attacker**.

Step 1: Start wireshark at 'Ubuntu-2' to monitor the server traffic. Open the web browser at the client side (host machine) and access the web server ('Ubuntu-2'). Identify a regular 3-way handshake in the wireshark trace. What are the packet sizes of SYN, SYN-ACK and ACK? How long does the process take?
Use "`netstat -na`" command to identify the client's access and check the stat of that connection.

Step 2: Next, you will demonstrate the SYN flooding attack. The Linux kernel has a built-in SYN cookies option which protects the system from SYN flooding attack. You need to first disable SYN cookie. You can use the sysctl command to turn on/off the SYN cookie mechanism:

```
$sysctl -a | grep cookie (Display the SYN cookie flag)
$sudo sysctl -w net.ipv4.tcp_syncookies=0 (turn off SYN cookie)
$sudo sysctl -w net.ipv4.tcp_syncookies=1 (turn on SYN cookie)
```

Now you can use the Netwox tool to conduct the attack, and then use wireshark to capture the attacking packets at the server (set a limit to stop wireshark as the server will receive a large amount of packets). The attacker (‘Ubuntu’) can use the following command to launch the attack:

```
$sudo netwox 76 -i IP_of_server -p 80
```

While the attack is ongoing, try to access the web server from the client again. Describe the observation. Run the "**`netstat -na`**" command on the server machine, and compare the result with that before the attack. Find out how many open TCP connections there are on the server (you need to show how you get the number in the report). Compare to the backlog queue length and try to explain your observation.

Check the packets caught by wireshark and describe how the attack works.

Step 3: Finally, turn on SYN cookie option on the server and launch the attack again. The client should be able to access the server now. Run "**`netstat -na`**" on the server again and compare to the previous results.

Questions:

1. Identify a regular 3-way handshake in the wireshark trace. What are the packet sizes of SYN, SYN-ACK and ACK? How long does the process take? (step 1)

2. In Step 2:
    a. While the attack is ongoing, try to access the web server from the client again. Describe the observation.

    b. Run the "**`netstat -na`**" command on the server machine, and compare the result with that before the attack.

    c. Find out how many open TCP connections there are on the server (you need to show how you get the number in the report). Compare to the backlog queue length and try to explain your observation.

    d. Check the packets caught by wireshark and describe how the attack works

Task 2: ARP Poisoning Attack

The ARP cache is an important part of the ARP protocol. Once a mapping between a MAC address and an IP address is resolved as the result of executing the ARP protocol, the mapping will be cached. Therefore, there is no need to repeat the ARP protocol if the mapping is already in the cache. However, because the ARP protocol is stateless, the cache can be easily poisoned by maliciously crafted ARP messages. Such an attack is called the ARP cache poisoning attack.

Fundamentally, there is no built-in form of authentication in ARP, therefore replies can be easily spoofed. By sending false ARP replies, it is easy to redirect traffic from a victim to yourself. At this point you can perform several attacks. You could drop the traffic, effectively performing a denial-of-service. You could listen to the traffic and forward it, sniffing the entire victim's traffic. You could also modify the traffic before sending it.

In this task, you will use ettercap to perform an ARP poisoning. Review the man page on ettercap and become familiar with the options. You will use the GUI interface of ettercap. In this task, you need two machines, one as the victim client ('Ubuntu-2'), and the other as the attacker ('Ubuntu').

Step 1: On the client machine ('Ubuntu-2'), ping the host machine and the attacker. Then use "`arp -n`" command to check the current ARP table and confirm the MAC addresses.

Step 2: On the attacker machine, you need to first enable IP forwarding so that the attacker machine will act as the intermediary between the victim and the intended destination. Login as the root and execute

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

Then, you need to modify the ettercap configuration file. Open /etc/etter.conf , find the "Linux" section, and uncomment the 4 lines there. Now run "`sudo ettercap -G`" to start ettercap program.

1. Select "Sniff → Unified sniffing", and set the network interface (usually eth0 or eth1)
2. Select "Hosts → Scan for hosts", then "Hosts → Host List". Click on the victim client's IP address and click "Add to Target 1".
3. Select "Mitm → Arp poisoning", then check "Sniff remote connections".
4. Select "Start → Start sniffing"

Step 3: Check the ARP table on the client machine and describe your observation. Start wireshark on the client machine and set filters to display only ARP packets. Stop wireshark on the client side and start another wireshark monitoring on the attacker machine. Open the web browser on the client machine and visit http://www.cs.umb.edu. Type in some keywords in the search field and press "Go".

Step 4: Go back to the attacker machine and check the wireshark window to to see if the keywords are captured.

Step 5: Select "Mitm → Stop mitm attack", and "Start → Stop sniffing". Then quit ettercap program.

Questions:

1. In Step 3, check the ARP table on the client machine and describe your observation.
2. Observe the packets caught by wireshark in step 3 and answer the following questions:
   a. Are there ARP requests from the client?
   b. For a particular ARP request, how many replies did the client receive?
   c. Are there spoofed replies? Are there valid replies? How do you identify them?
   d. According to the trace, describe how this attack works.