

Understanding TCP/IP based Attacks

Lab Overview

The learning objective of this lab is to gain first-hand experience on TCP/IP vulnerabilities, as well as attacks against these vulnerabilities. The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol designs and implementations. They provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of cyber security and why many cyber security measures are needed. Vulnerabilities of the TCP/IP protocols occur at several layers. This lab is designed to learn them step-by-step.

Lab Environment Setup

To conduct this lab, we require all the three virtual machines: Server, Client and Attacker. The tools being used for this lab are Wireshark/Tshark, Netwox/Netwag.

Netwox/Netwag

We need tools to send out network packets of different types and with different contents. We can use Netwag to do that. However, the GUI interface of Netwag makes it difficult for us to automate our process. Therefore, we strongly suggest that you use its command-line version, the Netwox command, which is the underlying command invoked by Netwag.

Netwox consists of a suite of tools, each having a specific number. You can run the command as following (the parameters depend on which tool you are using). For some of the tools, you have to run it with the root privilege:

```
➤ netwox <number> [parameters ...]
```

If you are not sure how to set the parameters, you can look at the manual by issuing "**netwox <number> --help**". You can also learn the parameter settings by running Netwag for each command you execute from the graphic interface, Netwag actually invokes a corresponding Netwox command, and it displays the parameter settings. Therefore, you can simply copy and paste the displayed command.

Wireshark Tool.

You also need a good network-traffic sniffer tool for this lab. Although Netwox comes with a sniffer, you will find that another tool called Wireshark is a much better sniffer tool.

Both Netwox and Wireshark can be downloaded. If you are using our pre-built virtual machine, both tools are already installed. To sniff all the network traffic, both tools need to be run with root privilege.

Tshark Tool.

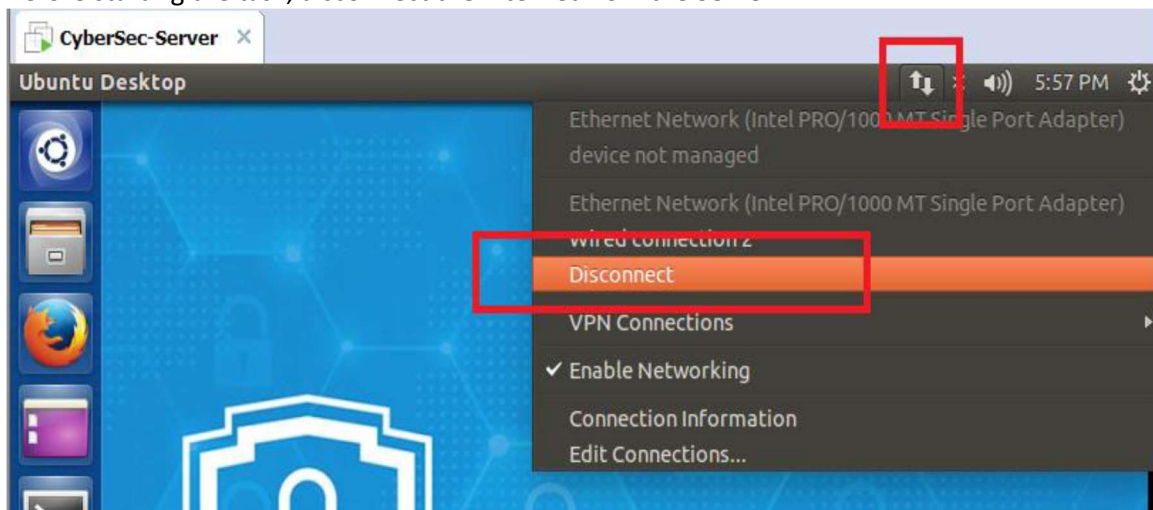
It is a terminal based network packet analyzer. You also need a good command line network-traffic sniffer tool for this lab.

Lab Tasks

In this lab, you need to conduct attacks on the TCP/IP protocols. You can use the Netwox or Netwag, Wireshark, Tshark tools in the attacks. All the attacks are performed on Linux operating systems. However, you can also conduct the same attack on the other operating system and compare the observations after lab classes. You are supposed to use all the three Virtual Machines for the experiments.

To simplify the “guess” of TCP sequence numbers and source port numbers, we assume that attacks are on the same physical network as the victims (Think of where such attacks may happen?). Therefore, you can use sniffer tools to get that information. The following is the list of attacks that need to be implemented and studied in this lab.

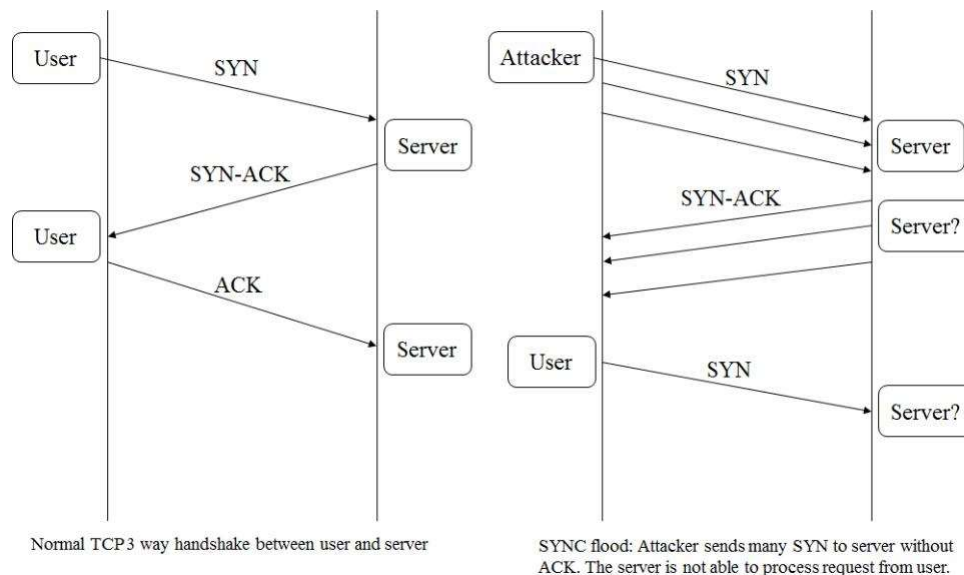
Before starting the task, disconnect the internet from the Server VM.



Task 1: SYN Flooding 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. Following figure illustrates the attack.

48730-32548, Cyber Security Week-5



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

➤ **`sysctl -q net.ipv4.tcp_max_syn_backlog`**

You 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.

For this task, **Netwag Tool 76** will be used to conduct the attack, and **tshark** tool to capture the packets.

Steps:

1. As SYN flood produces a lot of traffic in the VM due to high speed, Wireshark might crash. It is recommended to use "tshark" by entering "sudo tshark" on Terminal of the Client VM.

```
cybersec-client@ubuntu:~$ sudo tshark
[sudo] password for cybersec-client:
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to
/wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wires
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
```

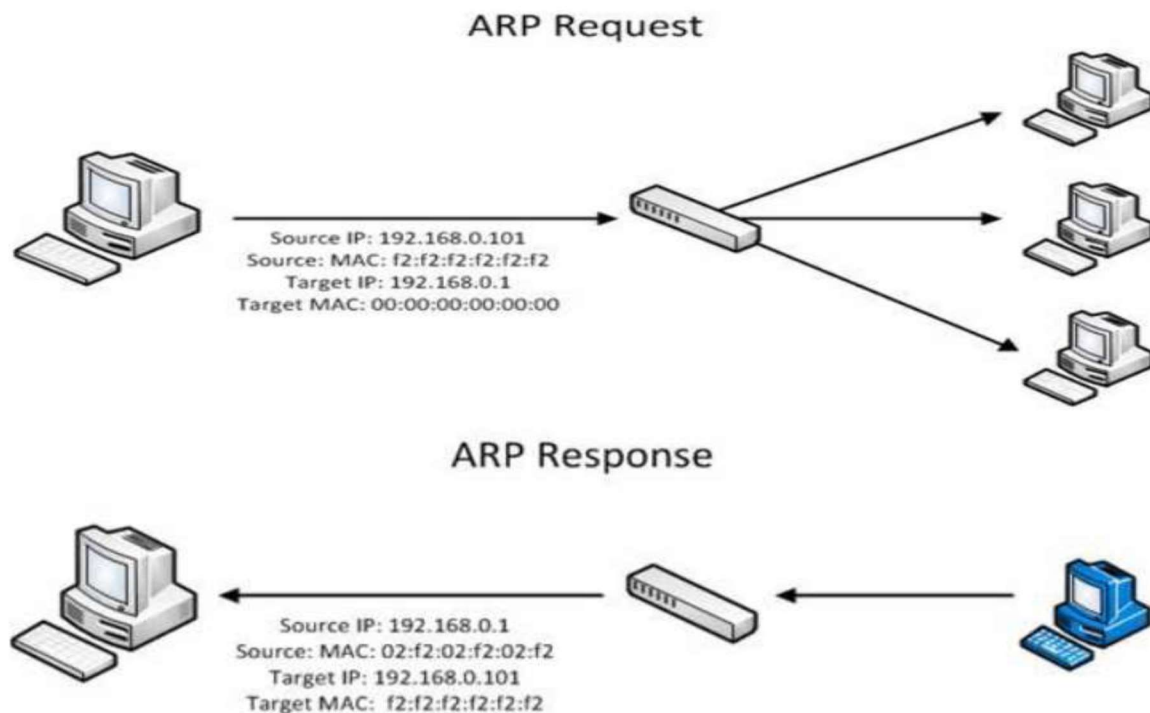
2. Then go to Attacker VM and start Netwag by entering "sudo netwag" on the Terminal.
3. Select **76: Synflood**.
4. Enter the details and click run it. **(Screenshot required)**
5. Observe the captured packets on Client VM. **(Screenshot required)**

Questions:

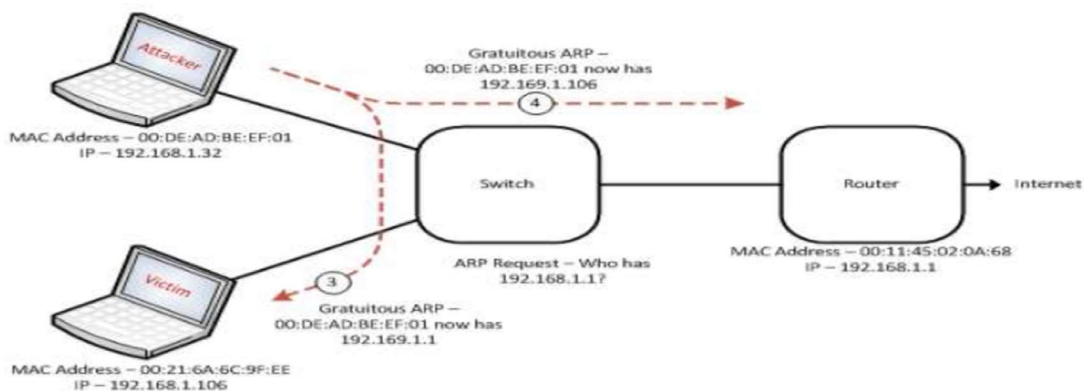
1. Observe the attack and take screenshots of the attack scenario.
2. Comment on your observation.
3. Categorize this attack in terms of severity and how it is linked to the DoS attack

Task 2: ARP cache poisoning

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.

Normal Scenario:

Attackers may use spoofed ARP messages to trick the victim to accept an invalid MAC-to IP mapping, and store the mapping in its cache. There can be various types of consequences depending on the motives of the attackers. For example, attackers can launch a DoS attack against a victim by associating a non-existent MAC address to the IP address of the victim's default gateway; attackers can also redirect the traffic to and from the victim to another machine, etc.

Attack Scenario:

48730-32548, Cyber Security Week-5

For this task, **Netwag Tool 80** is required to conduct the attack, and **wireshark** tool to capture the packets.

HINTS: In this task, you need to demonstrate how the ARP cache poisoning attack work. In Linux we can use the command **arp -a** to check the current mapping between IP address and MAC address.

Steps:

1. In Server VM, run “arp -a” on terminal to get the ARP Information (MAC Table). **(Screenshot Required)**
2. Open Netwag on Attacker VM by entering “sudo netwag” on the Terminal.
3. Select **Tool 80: Periodically Send ARP Replies**.
4. Add the fake MAC address and IP address and select the interface. **(Screenshot Required)**
5. Click “Run It”.
6. Check the MAC Table on Server VM and look for the change in MAC address for IP address provided in the Netwag tool 80. **(Screenshot required)**

Questions:

1. Observe the attack and take screenshots of the attack scenario.
2. Comment on your observation.
3. Briefly describe how you can mitigate this attack.

Task 3: ICMP Redirect Attack

The ICMP redirect message is used by routers to provide the up-to-date routing information to hosts, which initially have minimal routing information. When a host receives an ICMP redirect message, it will modify its routing table according to the message.

Because of the lack of validation, if attackers want the victim to set its routing information in a particular way, they can send spoofed ICMP redirect messages to the victim and trick the victim to modify its routing table.

For this task, **Netwag Tool 86** is required to conduct the attack, and **wireshark** tool to capture the packets.

HINTS: In this task, you should demonstrate how the ICMP redirect attack works, and describe the observed consequence. To check the routing information in Linux, you can use the command **route**

Steps:

1. Open Wireshark on Client VM by entering “sudo wireshark” in the terminal.
2. Select the interface and set “icmp” as filter and click “Apply”.
3. Open a new terminal on Client VM and ping the server. **(Screenshot required)**
4. Go to Attacker VM, run Netwag using the terminal.
5. Select the interface and “spoofip: IP spoof initialization type”. Input the required IP address into “gw: new gateway” and “src-ip: source IP address”. **(Screenshot Required)**
6. Click “Run It”.
7. Go back to Client VM, check the Wireshark output. **(Screenshot Required)**

48730-32548, Cyber Security Week-5

Questions:

1. Observe the attack and take screenshots of the attack scenario.
2. Comment on your observation.
3. Briefly describe how you can mitigate this attack.