

Laboratory 5: **Attacks and Defense of IP Networks with Routers**

LEARNING OUTCOMES

Upon completion of this laboratory exercise, you should be able to:

- Conduct and defend against network probing and scanning attacks
- Conduct and defend against Smurf attack
- Conduct and defend against IP fragmentation attack

REQUIRED HARDWARE

- 1 x Rack of Cisco network devices
- 1 x Box of Ethernet and console cables
- 3 x Laptops

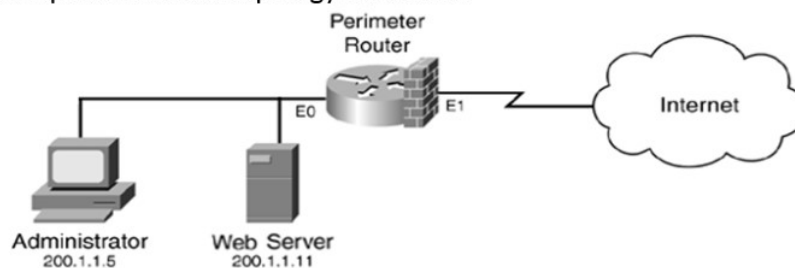
REQUIRED SOFTWARE

- Tera Term 4.106 <http://ttssh2.osdn.jp/index.html.en>
- Kali Linux Live Boot USB drive or equivalent

EXERCISE 1: CONDUCT AND DEFEND AGAINST NETWORK PROBING AND SCANNING ATTACKS

1.1: Conduct Network Probing using Nmap

1.1.1 Setup the network topology as shown:



1.1.2 Connect a PC directly to the router's interface facing the Internet to simulate the attacker's PC from the Internet and bootup in Kali Linux.

Warning: Do NOT attack over the Internet!

1.1.3 Connect the Administrator PC and Web Server PC via a switch to the router's interface facing the LAN and bootup in Windows.

- 1.1.4 Configure suitable IP addresses and subnet masks to all the PCs and router.
- 1.1.5 Verify that all PCs including attacker can ping one another to ensure that your setup is correct.
- 1.1.6 At the attacker's PC, start Wireshark to prepare capturing the network probing packets to be sent in Step 1.1.7, and responses, if any.
- 1.1.7 Refer Lab 5 Notes pg 5, commence network probing attack on the Windows PCs by launching nmap with suitable parameters, e.g.

```
(kali@kali)$ sudo nmap -sn -PE --reason 200.1.1.0/28
```

- 1.1.8 Observe your results.

1.2: Defend against Network Probing using ACL

- 1.2.1 Configure suitable ACL and apply it on appropriate interface of the router as discussed in Lab 5 Notes pg 6-9.
- 1.2.2 When done, conduct ICMP probing again as in 1.1.7.
- 1.2.3 Compare your new results with that in 1.1.8.
- 1.2.4 Do you think ACL is useful against ICMP probing?

1.3: Conduct Port Scanning using Nmap

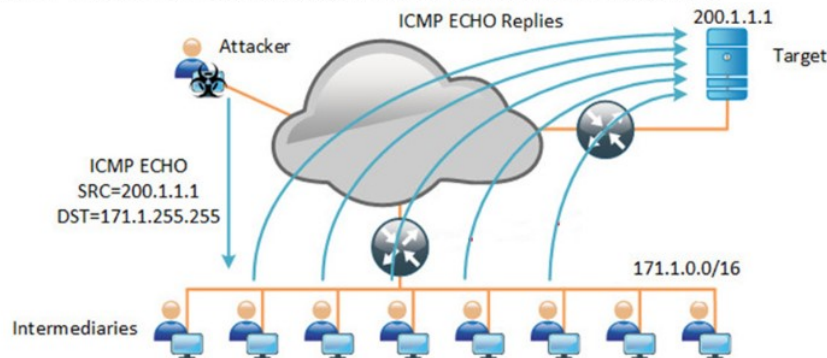
- 1.3.1 At the Web Server PC, startup a web server, e.g. Apache in XAMPP.
- 1.3.2 Configure suitable ACL and apply it on appropriate interface of the router to allow any user from the Internet to browse the website on the Web Server PC but not other services.
- 1.3.3 When done, verify that the attacker (like any user) is able to browse the website at the Web Server PC.
- 1.3.4 At the attacker's PC, re-start Wireshark to prepare capturing the port scanning packets to be sent in Step 1.3.5, and responses, if any.
- 1.3.5 Refer Lab 5 Notes pg 5, commence port scanning attack on the Web server by launching nmap with suitable parameters.
- 1.3.6 Observe your results.

- 1.3.7 Is there any way to write ACL to prevent port scanning from discovering the Web server, and yet allowing any user to browse the website?

EXERCISE 2: CONDUCT AND DEFEND AGAINST SMURF ATTACK

2.1: Conduct Smurf Attack using hping3

- 2.1.1 Setup the network topology as shown, using one router with 3 interfaces to interconnect attacker, target, and intermediaries together.



- 2.1.2 Connect as many intermediaries as possible via a switch to the router.
- 2.1.3 Boot up the attacker and intermediaries PCs in Kali Linux. The target PC may be in Windows.
- 2.1.4 Configure suitable IP addresses and subnet masks to all the PCs and router.
- 2.1.5 Verify that all PCs - attacker, intermediaries and target - can ping one another to ensure your setup is correct.
- 2.1.6 To experience smurf attack back in the late 1990s, you'll need to intentionally disable the defenses on the router and PCs in Step 2.1.7 and 2.1.8 which are enabled by default nowadays.
- 2.1.7 At the router, enable support for directed broadcast as follows:

```
router(config): interface nnn
router(config-if): ip directed-broadcast
```

- 2.1.8 At the intermediaries, enable support for broadcast ping as follows:

```
(kali@kali)$ sudo su
(root@kali)# echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

- 2.1.9 Start Wireshark at the intermediaries and target PC.
- 2.1.10 At the attacker's PC, open a terminal and use hping3 to launch smurf attack as shown in Lab 5 Notes pg 15.
- 2.1.11 At the intermediaries, can your Wireshark capture the broadcast ping request packets sent by the attacker? If not, experiment with Step 2.1.7 on different interfaces of the router until you are able to capture.
- 2.1.12 At the target PC, can your Wireshark capture the ping reply packets reflected from the intermediaries? How many times more are there as compared with that sent by the attacker in Step 2.1.10?

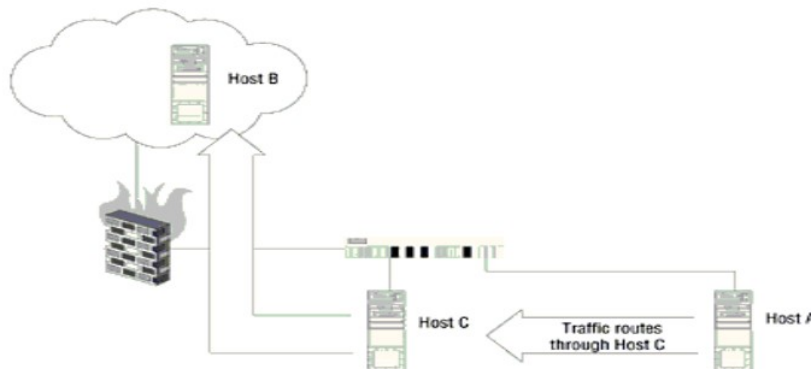
2.2: Defend against Smurf Attack

- 2.2.1 Disable support for directed broadcast in router.
- 2.2.2 Disable support for broadcast ping in the intermediaries.
- 2.2.3 When ready, use hping3 to launch smurf attack again.
- 2.2.4 At the intermediaries, can your Wireshark capture the broadcast ping request packets sent by the attacker?
- 2.2.5 At the target PC, can your Wireshark capture the ping reply packets reflected from the intermediaries?
- 2.2.6 Are the recommended defenses effective in defending against smurf attack?

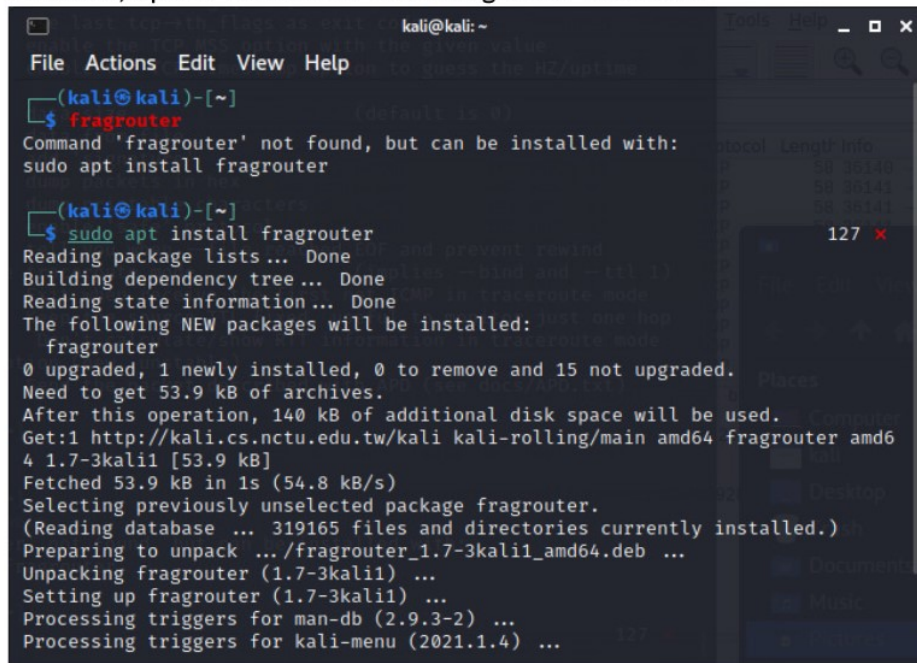
EXERCISE 3: CONDUCT AND DEFEND AGAINST IP FRAGMENTATION ATTACK

3.1: Conduct Tiny Fragment Attack using fragrouter

- 3.1.1 Setup the network topology as shown:



- 3.1.2 Boot up host C in Kali Linux, and the rest may be in Kali Linux or Windows.
- 3.1.3 Configure suitable subnet and IP addresses at host A, B and C.
- 3.1.4 At host A, configure its default gateway to IP address of host C instead.
- 3.1.5 At host C, open a terminal to install fragrouter as shown:



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ fragrouter
Command 'fragrouter' not found, but can be installed with:
sudo apt install fragrouter

(kali@kali)-[~]
$ sudo apt install fragrouter
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
fragrouter
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 53.9 kB of archives.
After this operation, 140 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 fragrouter amd64 1.7-3kali1 [53.9 kB]
Fetched 53.9 kB in 1s (54.8 kB/s)
Selecting previously unselected package fragrouter.
(Reading database ... 319165 files and directories currently installed.)
Preparing to unpack .../fragrouter_1.7-3kali1_amd64.deb ...
Unpacking fragrouter (1.7-3kali1) ...
Setting up fragrouter (1.7-3kali1) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...
```

- 3.1.6 Once installed successfully, run fragrouter as shown in Lab 5 Notes pg 28.
- 3.1.6 Verify that all hosts A, B and C can ping one another to ensure that your setup is correct.
- 3.1.7 Startup Wireshark to capture packets at host A and B.
- 3.1.8 At host B, startup a web server, e.g. Apache in XAMPP.
- 3.1.9 At host A, startup a web browser to visit the web server at host B.
- 3.1.10 Stop Wireshark and observe the TCP packets at host A and B. What do you notice?

3.2: Defend against Tiny Fragmentation Attack with ACL

- 3.2.1 Configure ACL as shown in Lab 5 Notes pg 29 on appropriate interface of the router.
- 3.2.2 Re-start Wireshark to capture packets at host B again.

- 3.2.3 At host A, are you able to visit web server at host B again? Why?
- 3.2.4 Stop Wireshark and observe the TCP packets at host B. Is there any difference as compared to 3.1.10?

3.3: Defend against Tiny Fragmentation Attack with 'fragments' in ACL

- 3.3.1 Add ACL with 'fragments' parameter as shown in Lab 5 Notes pg 30.
- 3.3.2 Re-start Wireshark to capture packets at host B again.
- 3.3.3 At host A, are you able to visit web server at host B? Why?
- 3.3.4 Stop Wireshark and observe the TCP packets at host B. Do you notice any differences as compared to 3.1.10 and 3.2.4?