ICT2203/ICT2203X Network Security
2021-2022 Trimester 3

Laboratory 1:
Attacks and Defense of LAN with Switches Part 1

LEARNING OUTCOMES

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

- Conduct and defend against MAC flooding attack
- Conduct and defend against switch spoofing attack

REQUIRED HARDWARE

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

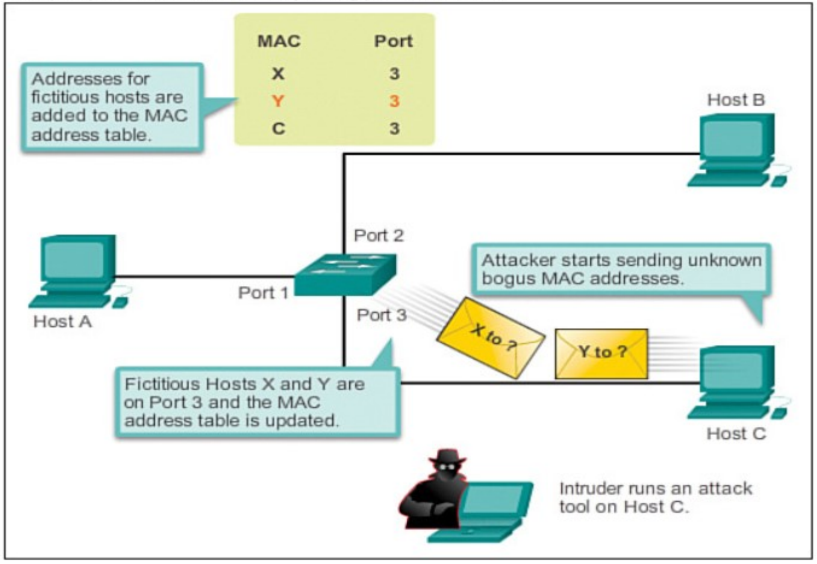
REQUIRED SOFTWARE

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

EXERCISE 1: CONDUCTING AND DEFENDING AGAINST MAC FLOODING ATTACK

1.1: Conducting MAC Flooding Attack using macof

1.1.1 Setup up the network topology as shown:

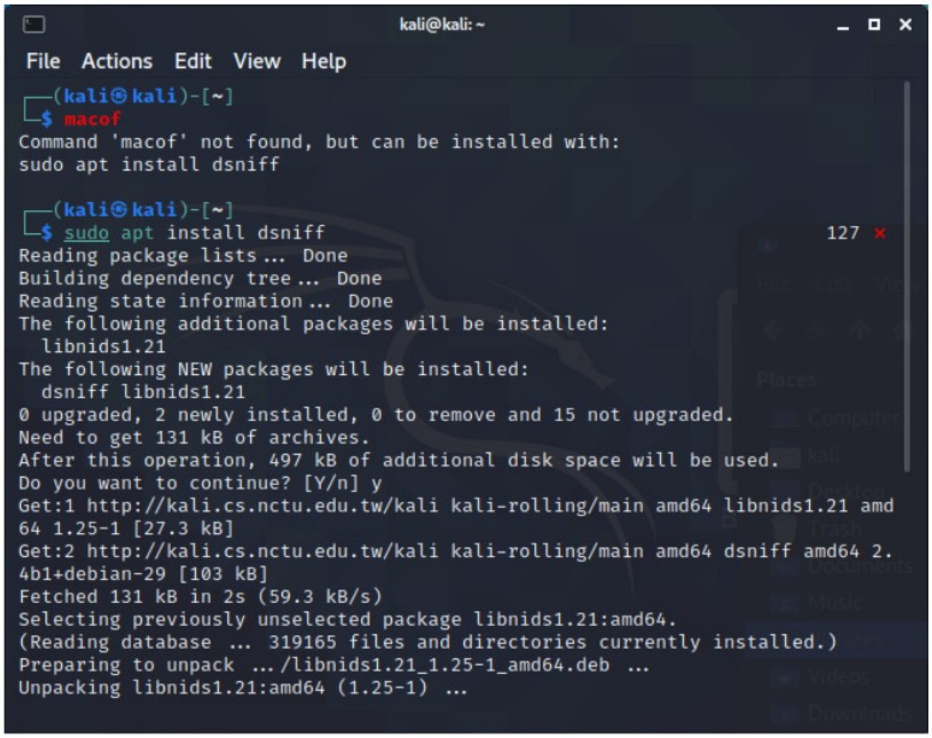

MAC
Port
X
3
Y
3
C
3
Addresses for fictitious hosts are added to the MAC address table.
Host B
Port 2
Port 1
Port 3
Host A
Attacker starts sending unknown bogus MAC addresses.
X to ?
Y to ?
Fictitious Hosts X and Y are on Port 3 and the MAC address table is updated.
Host C
Intruder runs an attack tool on Host C.

1.1.2 Boot up host A, B and C in Kali Linux and assign suitable IP addresses manually.

1.1.3 Ping host B and C from A, and vice versa, to ensure your setup is working correctly.

1.1.4 Before commencing MAC flooding attack, connect any laptop to the console port of the switch to observe the MAC address table. Refer Lab 1 Notes pg 11 and 14.

1.1.5 Start a terminal in Kali Linux at host C to install macof as shown:



```
┌──(kali㉿kali)-[~]
└─$ macof
Command 'macof' not found, but can be installed with:
sudo apt install dsniff

┌──(kali㉿kali)-[~]
└─$ sudo apt install dsniff                                          127 ✗
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnids1.21
The following NEW packages will be installed:
  dsniff libnids1.21
0 upgraded, 2 newly installed, 0 to remove and 15 not upgraded.
Need to get 131 kB of archives.
After this operation, 497 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 libnids1.21 amd
64 1.25-1 [27.3 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 dsniff amd64 2.
4b1+debian-29 [103 kB]
Fetched 131 kB in 2s (59.3 kB/s)
Selecting previously unselected package libnids1.21:amd64.
(Reading database ... 319165 files and directories currently installed.)
Preparing to unpack .../libnids1.21_1.25-1_amd64.deb ...
Unpacking libnids1.21:amd64 (1.25-1) ...
```

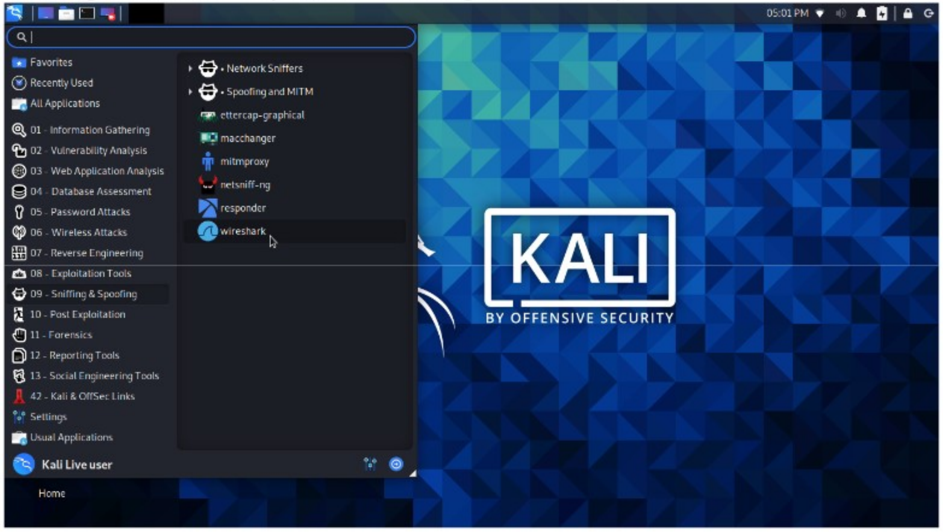
1.1.6 For testing purpose, launch macof to send 5 Ethernet frames with random source MAC addresses as shown in Lab 1 Notes pg 10.

1.1.7 Show the MAC address table again. What do you observe?

1.1.8 Now, modify the parameters of macof to conduct MAC flooding attack. Refer to http://linux.die.net/man/8/macof on the use of macof.

1.1.9 Show the MAC address table again. What do you observe?

1.1.10 Start Wireshark in Kali Linux at host C. (You are advised to stop macof before starting Wireshark to prevent crashing Wireshark.)



1.1.11 Ping host B from A, and vice versa. Can your Wireshark capture the ping packets? Why or why not? Explain.

1.1.12 If you could not capture the ping packets in 1.1.11, find out the problem and resolve it so that you are able to demonstrate successfully the conduct of MAC flooding attack and the capture of ping packets.

1.2: Defending MAC Flooding Attack using Port Security

1.2.1 Try enabling different options of Port Security as discussed in Lab 1 Notes pg 16-20.

1.2.2 When done, show the MAC address table before MAC flooding attack.

1.2.3 Launch macof to conduct MAC flooding attack again.

1.2.4 What happen to the port connected to host C now after MAC flooding attack?

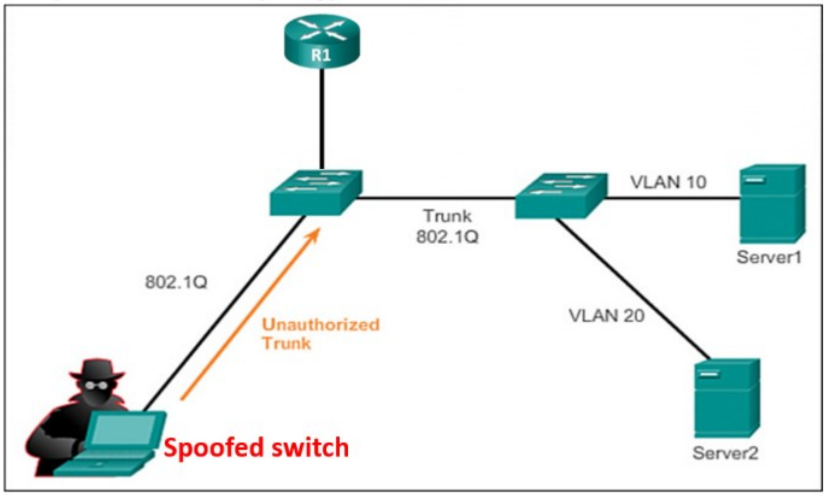
1.2.5 Show the MAC address table again. What do you observe?

1.2.6 Do you think Port Security is a good defense against MAC flooding attack? Briefly explain.

EXERCISE 2: CONDUCTING AND DEFENDING AGAINST SWITCH SPOOFING ATTACK

2.1: Conducting Switch Spoofing Attack using Yersinia

2.1.1 Setup the network topology as shown:



2.1.2 Configure the switch ports connected to Server 1 in VLAN 10, Server 2 in VLAN 20, and 802.1Q trunk between the two switches as shown in the diagram. Leave all other switch ports in default VLAN 1 dynamic auto mode.

Note: If you need help, refer to ICT1010 Lab on Configuring VLANs and Trunking.

2.1.3 Configure the router to support inter-VLAN routing, specifically router-on-a-stick.

Note: If you need help, refer to ICT1010 Lab on Configuring Routers and Layer-3 Switch for Inter-VLAN Routing.

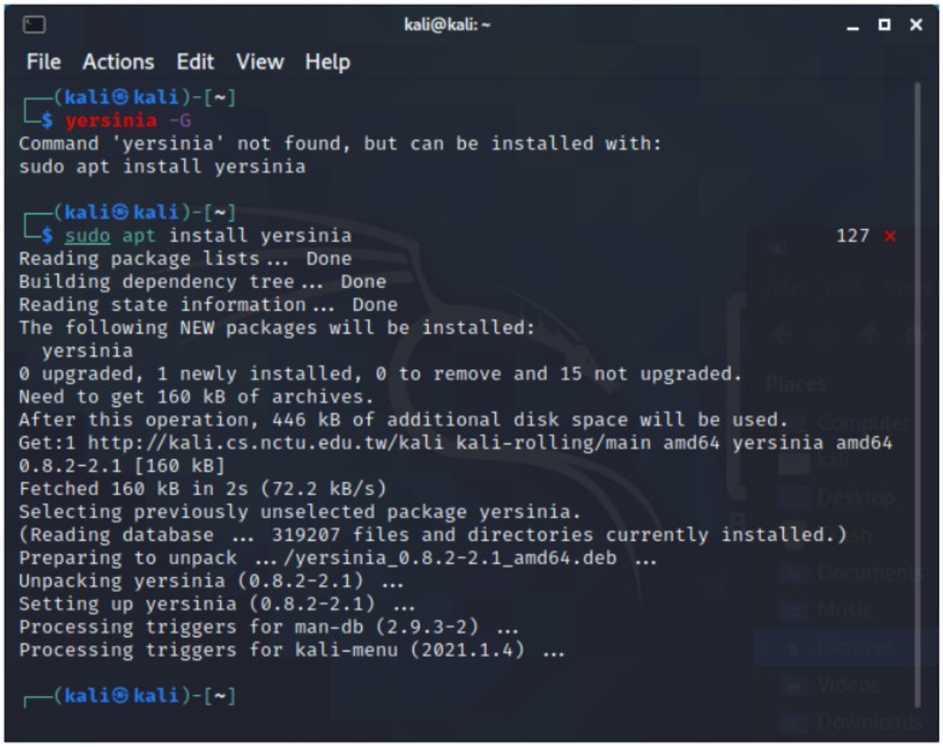
2.1.4 Boot up Server 1, Server 2 and attacker's host in Kali Linux.

2.1.5 Assign suitable IP addresses to Server 1 and 2 manually.

2.1.6 Ping Server 2 from Server 1, and vice versa, to ensure your setup is working correctly.

2.1.7 Before commencing switch spoofing attack, show the mode of the interface connected to the attacker's host as shown in Lab 1 Notes pg 27.

2.1.8 Start a terminal in Kali Linux at attacker's host to install Yersinia as shown:



```
┌──(kali㉿kali)-[~]
└─$ yersinia -G
Command 'yersinia' not found, but can be installed with:
sudo apt install yersinia

┌──(kali㉿kali)-[~]
└─$ sudo apt install yersinia                                           127 ×
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  yersinia
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 160 kB of archives.
After this operation, 446 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 yersinia amd64
0.8.2-2.1 [160 kB]
Fetched 160 kB in 2s (72.2 kB/s)
Selecting previously unselected package yersinia.
(Reading database ... 319207 files and directories currently installed.)
Preparing to unpack .../yersinia_0.8.2-2.1_amd64.deb ...
Unpacking yersinia (0.8.2-2.1) ...
Setting up yersinia (0.8.2-2.1) ...
Processing triggers for man-db (2.9.3-2) ...
Processing triggers for kali-menu (2021.1.4) ...

┌──(kali㉿kali)-[~]
```

2.1.9 Launch Yersinia in interactive or graphical mode as shown in Lab 1 Notes pg 25-26 to conduct switch spoofing attack.

2.1.10 Show the mode of the interface connected to the attacker's host again after switch spoofing attack. What do you observe?

2.1.11 Start Wireshark in Kali Linux at attacker's host.

2.1.12 Ping Server 2 from Server 1, and vice versa. Can your Wireshark capture the ping packets? Why or why not? Explain.

2.1.13 If you could not capture the ping packets in 2.1.12, find out the problem and resolve it so that you are able to successfully capture at least one ping packet.

2.2: Defending against Switch Spoofing Attack

2.2.1 Implement defense against switch spoofing attack as discussed in Lab 1 Notes pg 28-29.

2.2.2 Launch Yersinia to conduct switch spoofing attack again.

2.2.3 Show the mode of the interface connected to the attacker's host after the switch spoofing attack. What do you observe?

2.2.4 Do you think the recommended defenses are effective against switch spoofing attack? Briefly explain.