

### Laboratory 3: More Attacks and Defense of LAN with Switches

#### LEARNING OUTCOMES

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

- Conduct and defend against DHCP starvation and spoofing attacks which can lead to DNS spoofing and website spoofing attacks
- Conduct and defend against ARP poisoning attack which can lead to MitM attacks
- Conduct and defend against IP address spoofing and MAC address spoofing attacks

#### REQUIRED HARDWARE

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

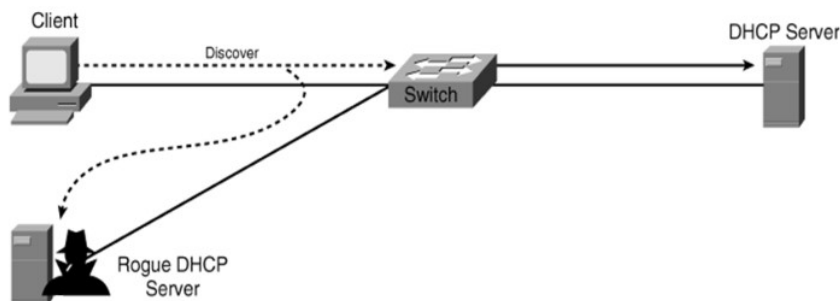
#### REQUIRED SOFTWARE

- 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 DHCP STARVATION AND SPOOFING ATTACKS

##### 1.1: Conduct DHCP Starvation Attack using Yersinia

- 1.1.1 Setup the network topology as shown. Use a router for the DHCP server, a Kali host for the rogue DHCP server and a Windows or Kali host for the client. **Do NOT connect** the client host to the switch yet.



- 1.1.2 Configure the router to function as the DHCP server and assign suitable IP address and subnet mask to its interface.

**IP address of router interface:**

**Subnet mask:**

**Note:** If you need help, refer to ICT1010 Lab on Configuring Basic DHCPv4 on a Router.

- 1.1.3 Boot up the attacker host in Kali Linux and verify that it can receive an IP address from the DHCP server successfully. Note this IP address which will be used later in Part 1.2 and 1.4.

**IP address of attacker host:**

- 1.1.4 Show the current address leases in the DHCP binding table of the router.
- 1.1.5 Start a terminal in Kali Linux and launch Yersinia to conduct DHCP starvation attack as shown in Lab 3 Notes pg 5. Stop it after a short while where all available addresses are offered by the DHCP server.
- 1.1.6 Show the current address leases in the DHCP binding table of the router again. What do you observe?

## **1.2: Conduct DHCP Server Spoofing Attack using Metasploit**

- 1.2.1 Start another terminal in Kali Linux and launch Metasploit console as shown in Lab 3 Notes pg 9.
- 1.2.2 Follow the commands as shown in Lab 3 Notes pg 9, use DHCP module in Metasploit and set the required parameters as follows:
- a. SRVHOST based on 1.1.3 because you are going to conduct DHCP server spoofing attack by running rogue DHCP server on your Kali Linux;
  - b. ROUTER and NETMASK based on 1.1.2
  - c. DHCPIPSTART and DHCPIPEND to any valid IP addresses
  - d. DNSSERVER also based on 1.1.3 because you are going to conduct DNS server spoofing attack by running rogue DNS server on your Kali Linux later in Part 1.4.
- 1.2.3 When done, perform Steps 1.2.4 and 1.2.5 below before entering the 'run' command to start the rogue DNS server.

- 1.2.4 Note that the DHCP starvation attack conducted in Part 1.1 is incomplete in the sense that only DHCPDiscover messages are sent out but not the DHCPRequest messages to confirm the lease. As a result, the offered IP addresses will be automatically recovered by the DHCP server after time-out.
- 1.2.5 Hence, re-run DHCP starvation attack in Part 1.1 again. Similarly, stop it after a short while when all available addresses are offered by the DHCP server.
- 1.2.6 Immediately after DHCP starvation attack, continue from Step 1.2.3 and enter the 'run' command in Metasploit to start the rogue DHCP server.
- 1.2.7 Now, connect the client host to the switch. What is the IP address, DHCP server address, and DNS server address of this client host?  
  
**IP address of client:**  
**DHCP server address learned from DHCP:**  
**DNS server address learned from DHCP:**
- 1.2.8 Do you think users would be able to notice that they are getting the DHCP lease from the spoofed DHCP server?

### **1.3: Host a Spoofed Website using XAMPP**

- 1.3.1 Connect a new host in Windows to the switch which will be used to host the spoofed website. Note this IP address which will be used in Part 1.4.  
  
**IP address of web server:**
- 1.3.2 Recall ICT1004 labs, launch XAMPP and start the Apache web server. For simplicity, you may just use the default web page as the phishing website, or any web page developed by you in ICT1004.
- 1.3.3 Start a web browser in the local host to verify that your web server is running properly.

### **1.4: Conduct DNS Server Spoofing Attack using DNSChuf**

- 1.4.1 Start a third terminal in Kali Linux.
- 1.4.2 Launch DNSChuf as shown in Lab 3 Notes pg 11, specifying it to listen to your Kali Linux interface IP address in 1.1.3, and for simplicity, to fake all DNS replies to point to your spoofed web server IP address in 1.3.1.

- 1.4.3 When done, start a browser in the victim client host and key in any URL, e.g. ***http://demo.testfire.net***. Are you redirected to the spoofed website?

**Note:** If unsuccessful, you may need to flush the DNS cache at the victim host using the following command in Windows prompt:

```
> ipconfig /flushdns
```

- 1.4.4 If an attacker were to spend time to touch-up the spoofed website to imitate the real look-and-feel of the authentic website, do you think users will get spoofed?
- 1.4.5 You may have heard about the security advice to verify the URL to avoid visiting a spoofed website. Do you think this advice is foolproof?

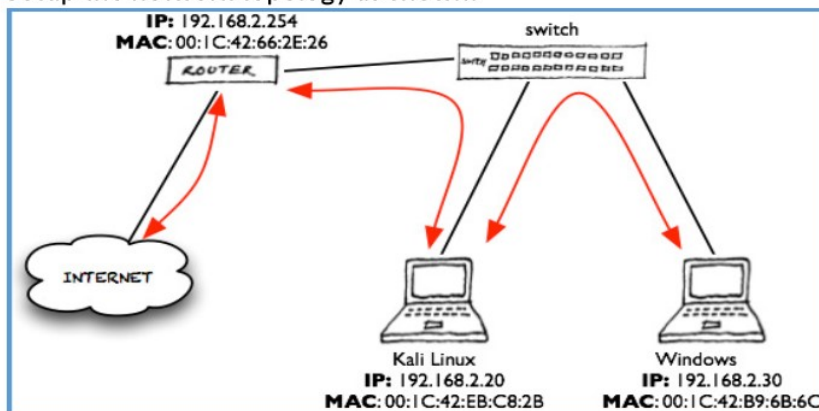
### 1.5: Defend DHCP Starvation and Server Spoofing Attacks using DHCP Snooping

- 1.5.1 Implement DHCP snooping as discussed in Lab 3 Notes pg 12-18.
- 1.5.2 When done, launch DHCP starvation and server spoofing attacks again and observe what happens.
- 1.5.3 Do you think DHCP snooping is effective against DHCP starvation and server spoofing attacks?

## EXERCISE 2: CONDUCT AND DEFEND AGAINST ARP POISONING AND MITM ATTACKS

### 2.1: Setup Network with Internet Access

- 2.1.1 Setup the network topology as shown:



- 2.1.2 Configure the router, Kali Linux and Windows hosts with suitable subnet mask and IP addresses as shown.



- 2.1.3 In addition, configure Kali Linux and Windows hosts to use Google public DNS at IP addresses 8.8.8.8 and 8.8.4.4 as alternate if needed.
- 2.1.4 Verify that the router, Kali Linux and Windows hosts can ping one another to ensure that your setup is correct.
- 2.1.5 To connect to the Internet, open up the removable floorboard covering nearest to your network rack and look up for odd-numbered Ethernet port marked NL1-BS<sub>xx</sub> or NL2-BS<sub>xx</sub>, where <sub>xx</sub> ranges from 1 to 56, and connect it to your router using the 5m light-blue Ethernet cable.

**Note:** Most racks may already have the 5m light-blue Ethernet cable connected to the Ethernet port on the floor. **Do NOT remove** them after your lab exercises.

- 2.1.6 Ensure that you are connected to the odd-numbered ports of NL1-BS<sub>xx</sub> or NL2-BS<sub>xx</sub>:
  - a. Configure your router port connected to the Ethernet port on the floor the IP address  $172.27.47.8(y - 1) + 1/29$ , where  $y$  ranges from 1 to 20 corresponding to your rack number; e.g. rack 1 will be  $8(1 - 1) + 1 = 1$ , i.e. 172.27.47.1, and so on.
  - b. In addition, configure default route on the router and make sure you can ping the 'ISP' serving your rack at IP address  $172.27.47.8(y - 1) + 2/29$ , where  $y$  ranges from 1 to 20 corresponding to your rack number; e.g. rack 1 will be  $8(1 - 1) + 2 = 2$ , i.e. 172.27.47.2, and so on.

**Note:** If you need help, refer to ICT1010 Lab on Configuring IPv4 Static and Default Routes.

- c. Next, configure NAT on your router using the assigned public IP address block  $129.126.164.8(y - 1)/29$ , where  $y$  ranges from 1 to 20 corresponding to your rack number; e.g. rack 20 will be  $8(20 - 1) = 152$ , i.e. 129.126.164.152/29.

**Note:** If you need help, refer ICT1010 Lab on Configuring NAT Pool Overload and PAT.

- 2.1.7 Now, you should be able to access the Internet from your rack. Launch web browser in Windows and Kali Linux hosts to verify it. If not successful, happy trouble-shooting! 😊

## 2.2: Conduct ARP Poisoning Attack using Bettercap

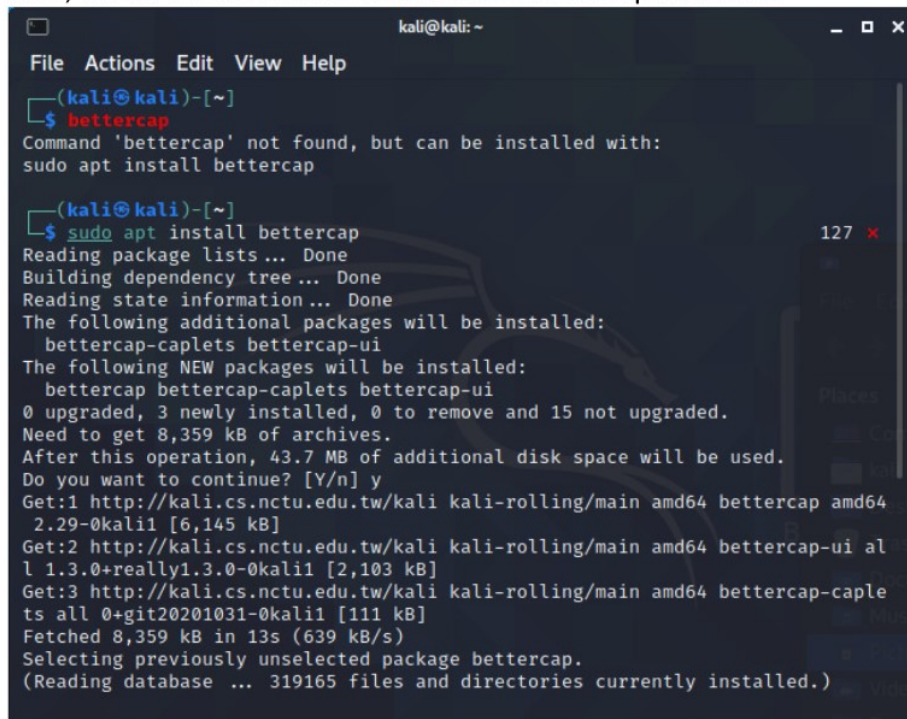
- 2.2.1 Open a command prompt terminal in the Windows host and show the ARP cache. What are the cache entries for default gateway and Kali Linux host?

ARP cache before attack	
Internet Address	Physical Address

- 2.2.2 Similarly, go to the console terminal of the router and show the ARP cache using the command '**show arp**'. What are the cache entries for Windows and Kali Linux hosts?

ARP cache before attack	
Internet Address	Physical Address

- 2.2.3 Now, start a terminal Kali Linux and install Bettercap as shown:



```

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

(kali@kali)-[~]
$ sudo apt install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bettercap-caplets bettercap-ui
The following NEW packages will be installed:
  bettercap bettercap-caplets bettercap-ui
0 upgraded, 3 newly installed, 0 to remove and 15 not upgraded.
Need to get 8,359 kB of archives.
After this operation, 43.7 MB 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 bettercap amd64
  2.29-0kali1 [6,145 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 bettercap-ui al
  l 1.3.0+really1.3.0-0kali1 [2,103 kB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 bettercap-caple
  ts all 0+git20201031-0kali1 [111 kB]
Fetched 8,359 kB in 13s (639 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 319165 files and directories currently installed.)

```

- 2.2.4 Before running Bettercap, run Wireshark to prepare capturing the gratuitous ARP replies to be sent out by Bettercap upon initiating ARP poisoning attack; e.g. as shown in Lab 3 Notes pg 24.
- 2.2.5 Next, run Bettercap as shown in Lab 3 Notes pg 23.

- 2.2.6 Now, show the ARP caches at Windows host and router again. Do you observe any difference as compared to 2.2.1 and 2.2.2 before the attack?

Windows host:

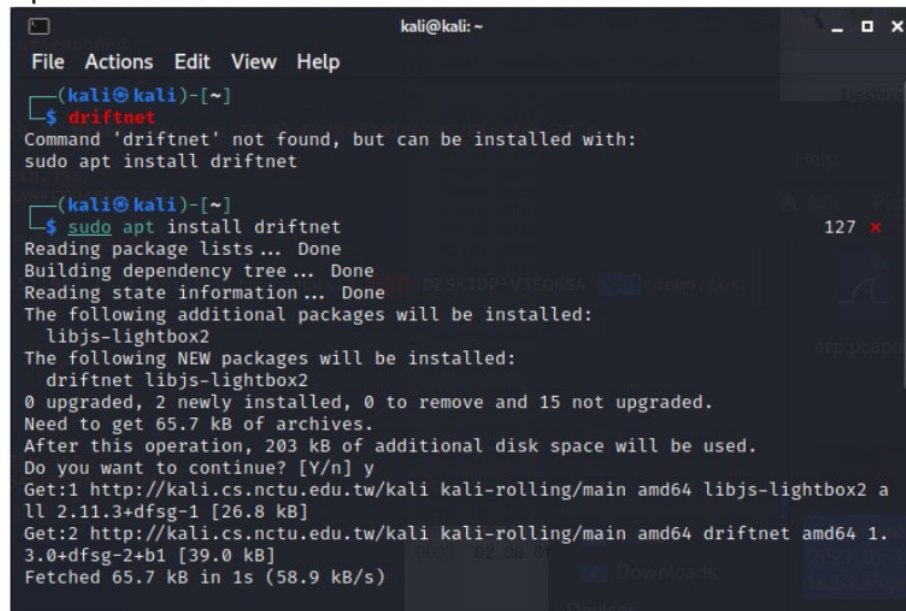
ARP cache after attack	
Internet Address	Physical Address

Router:

ARP cache after attack	
Internet Address	Physical Address

### 2.3: Conduct MitM Eavesdropping Attack using Bettercap and Driftnet

- 2.3.1 Open a terminal in Kali Linux to install Driftnet as shown:



```

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

(kali@kali)-[~]
$ sudo apt install driftnet
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libjs-lightbox2
The following NEW packages will be installed:
  driftnet libjs-lightbox2
0 upgraded, 2 newly installed, 0 to remove and 15 not upgraded.
Need to get 65.7 kB of archives.
After this operation, 203 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 libjs-lightbox2 a
ll 2.11.3+dfsg-1 [26.8 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 driftnet amd64 1.
3.0+dfsg-2+b1 [39.0 kB]
Fetched 65.7 kB in 1s (58.9 kB/s)

```

- 2.3.2 When done, run driftnet as shown in Lab 3 Notes pg 26.
- 2.3.3 Back to the same terminal running Bettercap in Kali Linux, enable sniffing as shown in Lab 3 Notes pg 25.
- 2.3.4 Now ask your victim at the Windows host to visit any http website; e.g. ***http://demo.testfire.net/login.jsp***

- 2.3.5 At the attacker Kali Linux host, are you able to capture the URL and the images that the victim is visiting?

**Note:** If not successful, you may try manually enabling forwarding mode in Kali Linux as follows and try again:

```
(kali@kali)$ sudo su
(root@kali)# echo "1" > /proc/sys/net/ipv4/ip_forward
```

- 2.3.6 Next, ask your victim to login using any username and password.
- 2.3.7 Are you able to capture the victim's username and password at the attacker Kali Linux host?
- 2.3.8 Do you think the victim at the Windows host would be able to notice that he/she is under attack?

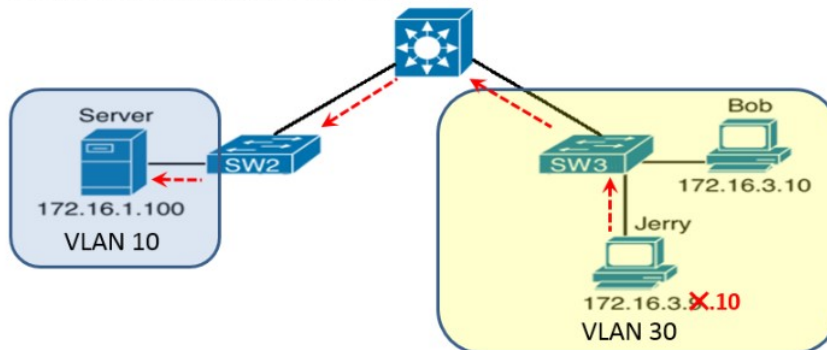
#### 2.4: Defend ARP Poisoning and MitM Attacks using DHCP Snooping and DAI

- 2.4.1 Implement DAI (Dynamic ARP Inspection) as discussed in Lab 3 Notes pg 28-32.
- 2.4.2 When done, launch ARP Poisoning attack again and observe what happens.
- 2.4.3 Do you think DAI is an effective defense against ARP poisoning attack?

### EXERCISE 3: CONDUCT AND DEFEND AGAINST IP AND MAC ADDRESS SPOOFING ATTACKS

#### 3.1: Setup Network with ACL to Filter Inter-VLAN Routing

- 3.1.1 Setup the network topology as shown:



- 3.1.2 Boot up Server and host Bob in Kali Linux and configure them with suitable subnet mask and IP addresses as shown.



3.1.3 Boot up host Jerry in Kali Linux and configure it with the original IP address 172.16.3.9 initially.

3.1.4 Configure the layer 3 switch with suitable IP addresses and enable inter-VLAN routing.

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

3.1.5 Verify that both Bob and Jerry are able to ping the Server to ensure your setup is correct.

3.1.6 Next, implement the ACL on layer 3 switch as shown in Lab 3 Notes pg 34.

3.1.7 When done, verify that Bob is still able to ping the Server but not Jerry now.

3.1.8 Show the arp cache of the layer 3 switch. What are the cache entries for Bob and Jerry?

ARP cache before attack	
Internet Address	Physical Address

### **3.2: Conduct IP Address Spoofing Attack**

3.2.1 Spoof the IP address of attacker's host Jerry to that of Bob.

3.2.2 Now, is Jerry able to ping the Server?

3.2.3 Show the arp cache of the layer 3 switch again. Do you observe any difference as compared to 3.1.8?

ARP cache after attack	
Internet Address	Physical Address

### **3.3: Conduct IP and MAC Address Spoofing Attack**

3.3.1 Verify that Bob is still able to ping the Server successfully.

- 3.3.2 Observe the MAC address table at switch SW2. What is the interface associated with the MAC address of Server?

MAC address table before attack	
Address	Interface

- 3.3.3 Now, disconnect attacker's host Jerry from SW3 and connect it to the same VLAN 10 as Server at SW2.

- 3.3.4 Spoof the IP address of Jerry to that of the Server.

- 3.3.5 In addition, spoof the MAC address of Jerry to MAC address of Server by entering the following command at the terminal in Kali Linux (use colon hexadecimal format xx:xx:xx:xx:xx:xx for MAC address):

```
(kali@kali)$ sudo su
(root@kali)# ifconfig eth0 hw ether spoof-mac-address
```

- 3.3.6 Verify that both the IP and MAC addresses of Jerry have been changed successfully.

- 3.3.7 From attacker's host Jerry, ping an unused IP address, e.g. 172.16.1.10 to poison the MAC address table.

- 3.3.8 Observe the MAC address table at switch SW2 again. What is the interface associated with the MAC address of Server now?

MAC address table after attack	
Address	Interface

- 3.3.9 Start Wireshark at the Server and attacker's host Jerry.

- 3.3.10 From host Bob, ping the Server IP address.

- 3.3.11 Stop Wireshark and find the ping messages at the Server and host Jerry.

- 3.3.12 Where did Bob's ping messages go to? Why?

**3.4: Defend IP and MAC Address Spoofing Attacks using DHCP Snooping and IP Source Guard**

- 3.4.1 Implement IPSG (IP Source Guard) as discussed in Lab 3 Notes pg 36-39.
- 3.4.2 When done, launch IP and MAC address spoofing attacks again and observe what happens.
- 3.4.3 Do you think IPSG is an effective defense against IP and MAC address spoofing attacks?