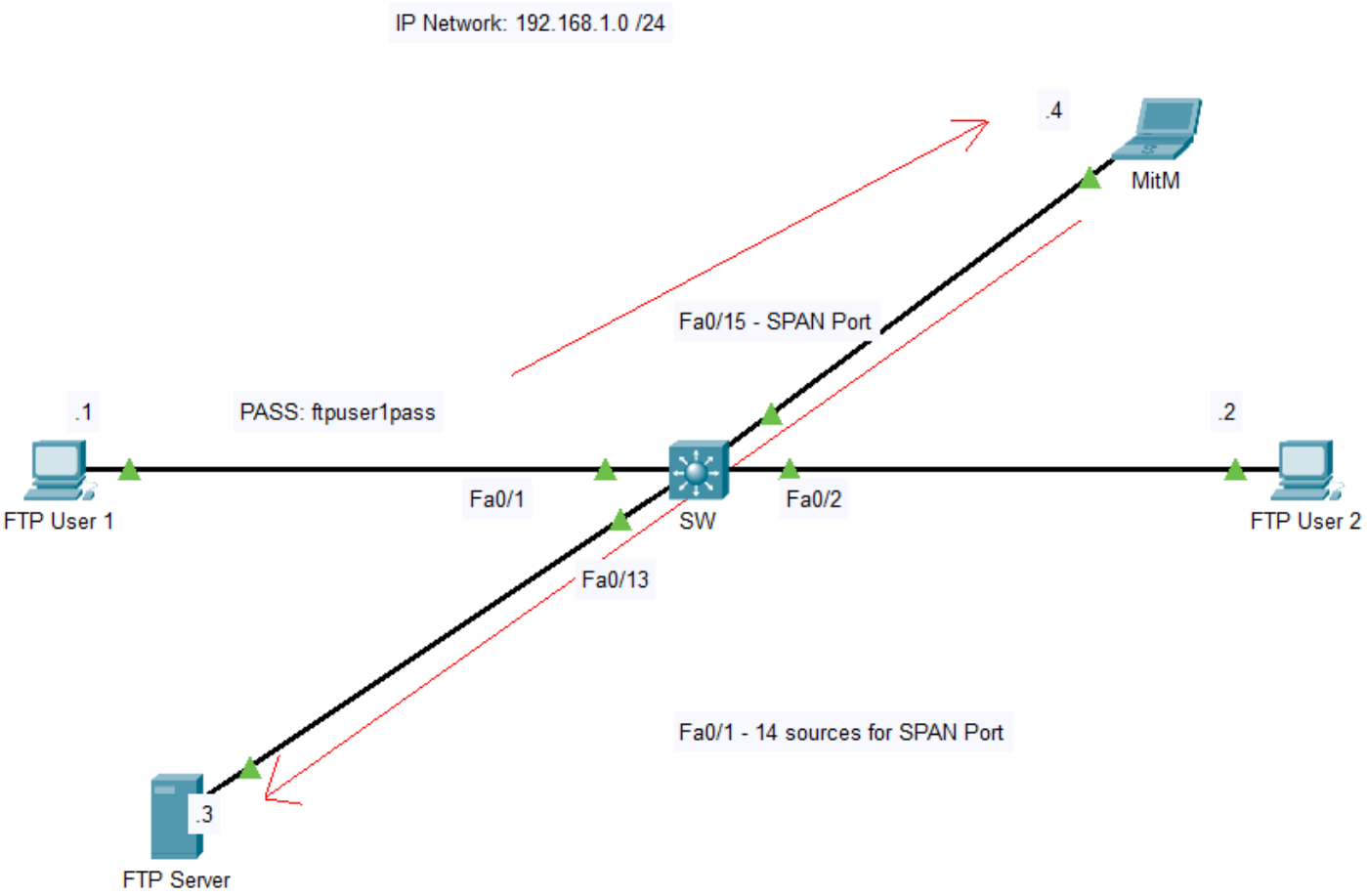
Insider Man-in-the-Middle Attack Lab: ARP Spoofing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
FTP User 1	NIC	192.168.1.1	255.255.255.0
FTP User 2	NIC	192.168.1.2	255.255.255.0
FTP Server	NIC	192.168.1.3	255.255.255.0
MitM	NIC	192.168.1.4	255.255.255.0

Account Users

Service	Username	Password	User Group
FTP	FTPUser1	<insert password>	Corporate Management Users
FTP	FTPUser2	<insert password>	Corporate Management Users

Record MitM Device MAC Address here: 0000.0000.0000

Device ARP Tables

Device	Int.	IP Address	MAC Addresses Before Attack	MAC Addresses After Attack
FTP User 1	NIC	192.168.1.2 192.168.1.3 192.168.1.4	0000.0000.0000 0000.0000.0000 0000.0000.0000	0000.0000.0000 0000.0000.0000 0000.0000.0000
FTP User 2	NIC	192.168.1.1 192.168.1.3 192.168.1.4	0000.0000.0000 0000.0000.0000 0000.0000.0000	0000.0000.0000 0000.0000.0000 0000.0000.0000
FTP Server	NIC	192.168.1.1 192.168.1.2 192.168.1.4	0000.0000.0000 0000.0000.0000 0000.0000.0000	0000.0000.0000 0000.0000.0000 0000.0000.0000

Objectives

Part 1: Build the Network Topology, Configure Basic Device Settings, and Install the FTP Server.

Part 2: Configure and use SPAN (Switched Port ANalyzer) on Cisco Catalyst series switches and using Wireshark.

Part 3: Configure Ettercap and Launch ARP Spoof attack.

Part 4: Exfiltrate FTP Credentials over the Network and use them to log in to the FTP Server.

Background

The Address Resolution Protocol is a key foundational protocol of Local Area Networks. Without it – PCs, routers, servers, and other network enabled devices would have no known standardized means of sending IP packets across wireless or wired switched networks. Its service is to resolve Layer 3 IP addresses to Layer 2 MAC addresses on the LAN for Layer 3 hosts. Layer 3 hosts then construct Ethernet frames with the correct destination MAC address for a Layer 3 IP destination before the frame is transmitted. ARP is fundamentally critical for network communications but has one unforeseen downside: ARP lacks authentication in its own IP-to-MAC address resolution process.

Devices that require ARP maintain a table of entries called an ARP Table. This is where devices store their complete IP-to-MAC address resolutions from interactions with other hosts. Once an entry is created, the host device will always refer to it when requiring an IP's MAC until expiration. Otherwise, the device must construct and send a query asking for whichever IP address a device identifies itself with, please reply and provide your MAC address. These series of queries and responses done by ARP are called ARP requests and replies. In this process, ARP as a nonsecure protocol paves the way for ARP spoof attacks and Man-in-the-Middle.

In this lab, you are assuming the identity of a disgruntled staff member within a company who got passed up for a major promotion. To your companies' misfortune, your high administrative rights to directly access and manage their network will cost them dearly. You will build and configure the network and every necessary component within this lab to launch Man-in-the-Middle using ARP Spoofing, Wireshark, and a SPAN port. You may include a second person to set the passwords and assist you in adding a level of difficulty, requiring you to perform the attack to completion to use the credentials yourself.

Resources

- 1 Switch (Cisco Catalyst 2960, 3560, 3750, or 3650 series).
- 3 PCs (Windows 7, 8, or 10 or *nix OS with Tera Term or comparable and one Windows PC dedicated for FileZilla Server).
- 1 device running Kali Linux or comparable Linux Distro with Ettercap and Wireshark installed.
- 1 Console cable to access and configure the Switch for SPAN.
- Ethernet Cabling.
- Build the Network Topology, Configure Basic Device Settings, and Install and Setup the FTP Server

You will build the topology according to the topology image on the first page and configure the Cisco switch for SPAN in Part 2. Then configure host devices with the necessary IP configurations, test their connectivity, and install FileZilla on the designated FTP Server.

Note: **nix* encompasses Linux, Unix, and macOS operating systems.

Step 1: **Cable the network shown in the topology.**

Step 2: **Use command `ipconfig /all` (Windows) or `ifconfig` (*nix) to record the MAC address of the MitM device in the section above.**

Step 3: **After the initial boot of the switch, initialize and reload the switch as necessary.**

a. Console up to the switch, enter privilege exec-mode and enter:

```
Switch>enable
Switch#show flash
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
3 -rw- 1078 <no date> config.text
2 -rw- 736 <no date> vlan.dat

64016384 bytes total (59599649 bytes free)
Switch#
```

b. If **`config.text`** or **`vlan.dat`** is seen on the switch's flash filesystem, erase and reload.

```
Switch#erase startup-config
Switch#delete flash:/vlan.dat
Switch#reload
```

Step 4: **From the FTP Server, download, install, and configure FileZilla Server.**

a. Go to: https://filezilla-project.org/download.php?type=server

1) **Note:** FileZilla Server is only compatible with Windows computers.

2) On the "Download FileZilla Server for Windows" page, click on the "Download FileZilla Server" button under the "Windows" section. Ignore the support popup and select "Download."

b. Wait for the download to complete, then navigate to the download folder of the FTP Server and double-click "FileZilla_Server-0_9_60_2.exe."

1) **Note:** depending on when you downloaded the software, the version numbering and name may differ from the example.

2) Find and select the appropriate executable that was downloaded to your computer that came from FileZilla.

c. Accept the installation by selecting “Yes” from the UAC prompt. Read and accept the license agreement in the FileZilla Server setup window.

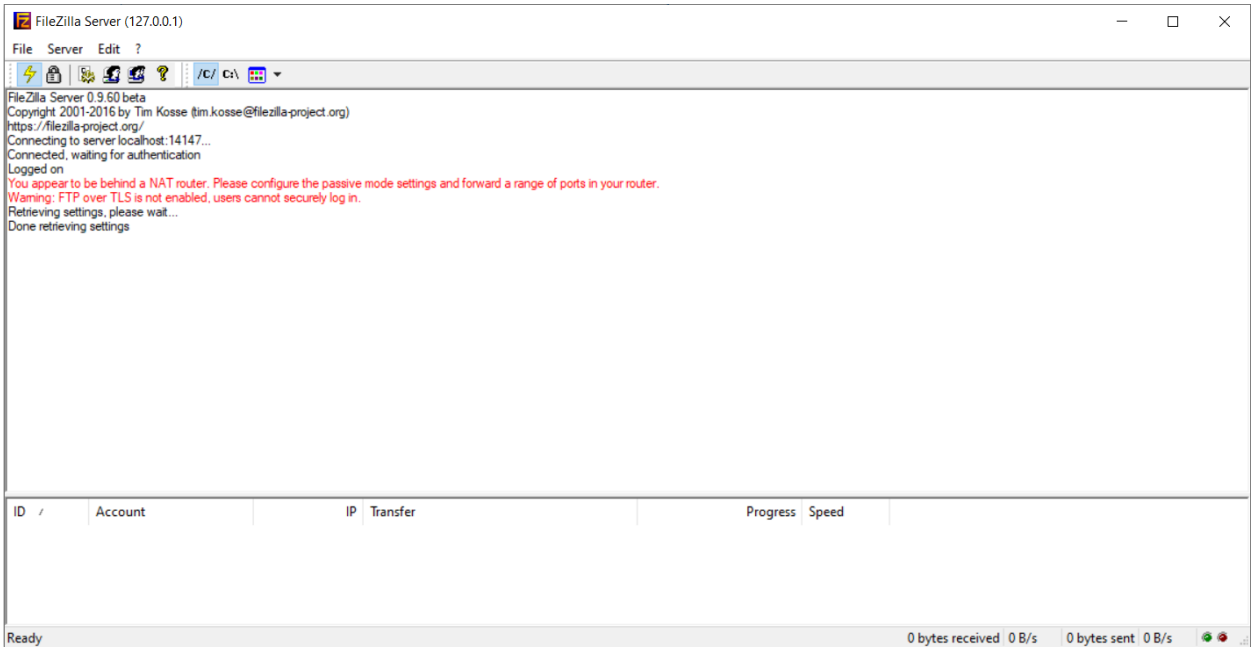
d. Keep FileZilla install type at “Standard” and select next preserve install location defaults.

e. At Startup settings, change how FileZilla Server should start by clicking the dropdown box and selecting “Install as service, started manually.” Leave everything else at the default setting and select “Next.”

f. Next, choose how the server interface should be started. From the dropdown menu, select “Start manually.” Keep rest of defaults and install. The program should launch the service and interface automatically after successful installation.

g. No administrative password will be set for this demo, and host/port settings will remain at defaults. Select the “Connect” button in the popup to enter the FileZilla Server Admin console.

h. If everything was installed correctly, you should be greeted by the following window:



i. **Note: If FileZilla Server is not working correctly or at all, refer to Google searching about your problem. Go to the FileZilla support page at: https://filezilla-project.org/support.php, or uninstall and reinstall the program.**

j. Go to server options from the Admin console by “Edit > Settings.” Then under “General settings > Welcome message,” append the following message to the welcome message text box:

Welcome to the Corporate FTP Server! Please enter your username and password for authentication!

k. Exit Server settings and create the FTP group the FTP Users will connect to via “Edit > Groups” then, in the Groups window, select “Add” to create a new group. In the user group creation window, name the user group “Corporate Management Users.”

l. After creation, keep the current group selected and under the “Page:” section, select “Shared folders” and add a group directory. You may select any current or create your directory as the group home directory. Once done, select OK at the bottom left corner of the Groups window to exit.

m. Finally, create and link the user accounts to log in to the server and access the Corporate Management Users Home directory. Navigate to the Users settings window by "Edit > Users" and create two new users according to the Account Users section.

n. Then once both accounts have been created, under "Account settings" on the Users setting window, click the Password check box for both and enter their corresponding password. Once finished, select OK at the bottom left corner of the Users window to exit.

Step 5: **Configure PC hosts according to the Addressing Table.**

Step 6: **Test end-to-end connectivity before continuing.**

a. Ping all hosts from each device with an IP address to ensure end-to-end connectivity.

b. Verify FTP hosts can log in to their user account. From both FTP User devices, open a web browser and in the address bar, enter: ftp://192.168.1.3 and when prompted, enter the corresponding username and password. Optionally, using the **`ftp`** (Windows and *nix) command, you can access the ftp server on the command prompt or on PowerShell from Windows or a terminal window from *nix.

c. If logging into the FTP server fails, check physical layer connections, ping from your computer to the server, and check your password spelling on both the server and at login.

Step 7: **Enter command `arp -a` (Windows and *nix) on each device specified in the "Device ARP Tables" and record the MAC addresses under "MAC Addresses Before Attack" for each IP address.**

Part 2: Configure and use SPAN (Switched Port ANalyzer) on Cisco Catalyst series switches and using Wireshark

SPAN is a feature of Cisco Catalyst series switches for network analysis. It functions by taking a range of ports configured as a source for SPAN. These source ports for SPAN essentially copy whatever is being transmitted or received on the ports and redirects them to a destination port for SPAN. This form of monitoring can be considered out-of-band (OOB) as network traffic is not directly affected as SPAN copies the PDUs and sends them to a network analyzer like the MitM host operating Wireshark at the opposite end of the SPAN port link.

Wireshark is a protocol analyzer and is quite useful on production networks. It captures packets being received on an interface and interprets them for a network admin to monitor. Wireshark has a wide variety of feature sets that gives its users the ability to track from entire multiprotocol network conversations between devices to single PDUs based on specific filtering criteria. It can even be used to identify unusual network activity. However, for your nefarious purposes, you will configure a SPAN port and install and use Wireshark.

Step 1: **Console into the switch from the MitM host or any other computer with the console cable.**

Step 2: **Create the SPAN session on the switch with the `monitor` command.**

a. Navigate to global configuration mode of the switch.

```
Switch>enable
Switch#configure terminal
Switch(config)#
```

b. Next, create the monitor session of 1 and enter the source range of ports as specified in the Topology section.

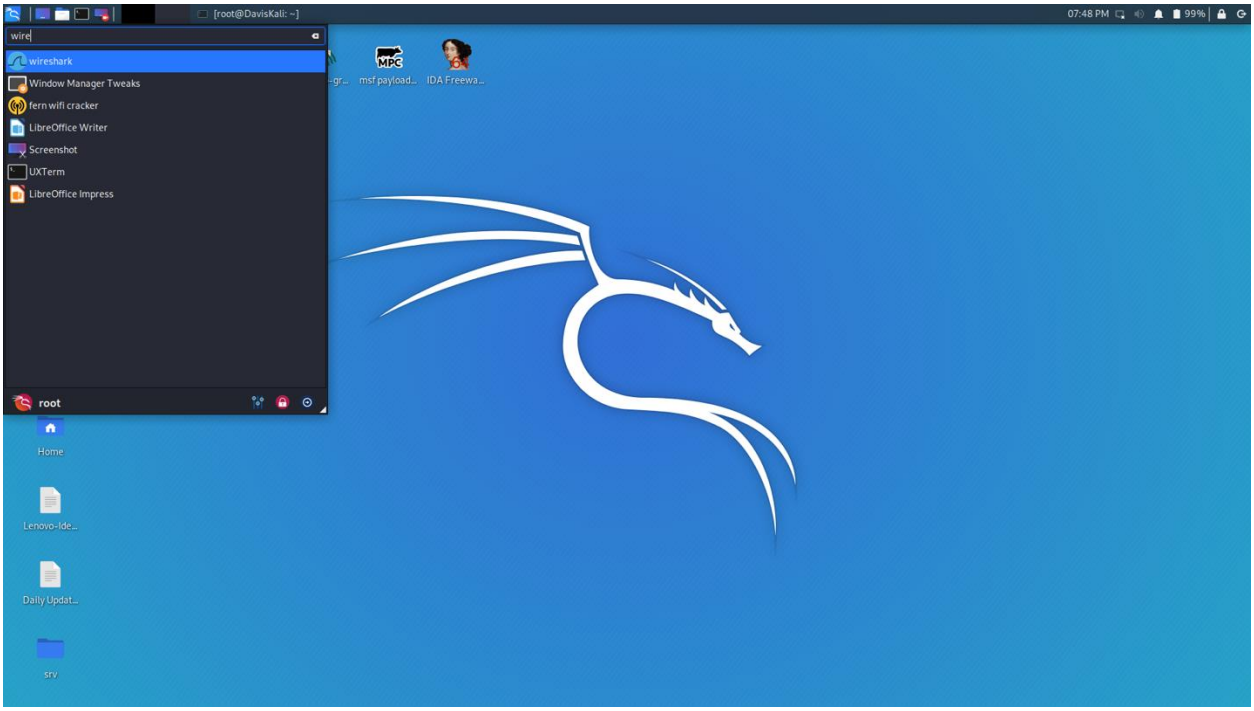
```
Switch(config)#monitor session 1 source interface Fa0/1 – 14
Switch(config)#
```

c. Finally, declare the destination port for SPAN to that declared in the Topology section.

```
Switch(conifg)#interface Fa0/15
Switch(config-if)#shutdown
Switch(config-if)#monitor session 1 destination interface Fa0/15
ingress untagged vlan 1
Switch(config)#interface Fa0/15
Switch(config-if)#no shutdown
```

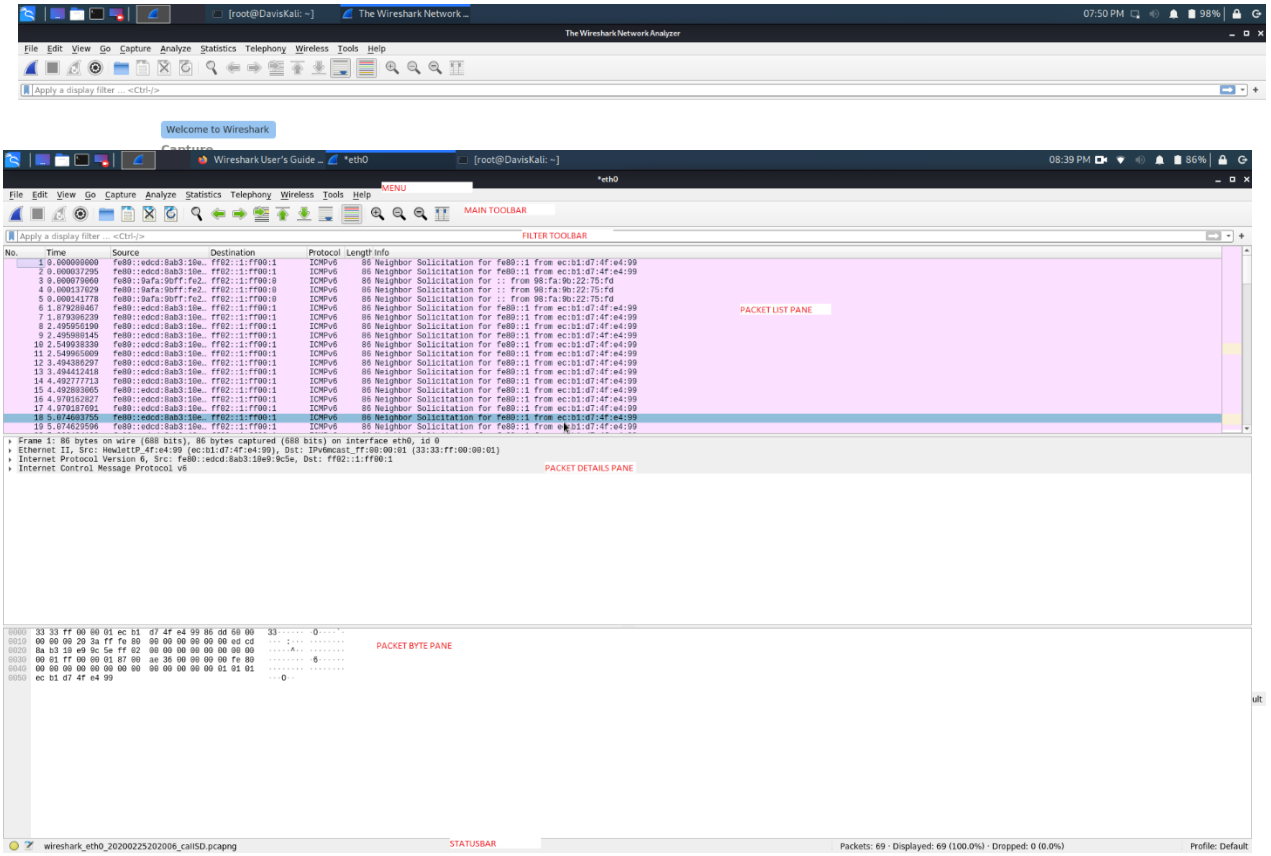
Step 3: **Open Wireshark from MitM host and verify SPAN port functionality.**

a. Navigate to and open Wireshark. An example from Kali is shown.



b. By default, Wireshark will display a list of network interfaces on the device to choose from. For this demonstration, wired Ethernet interfaces are being used. Typically, on Linux machines, the

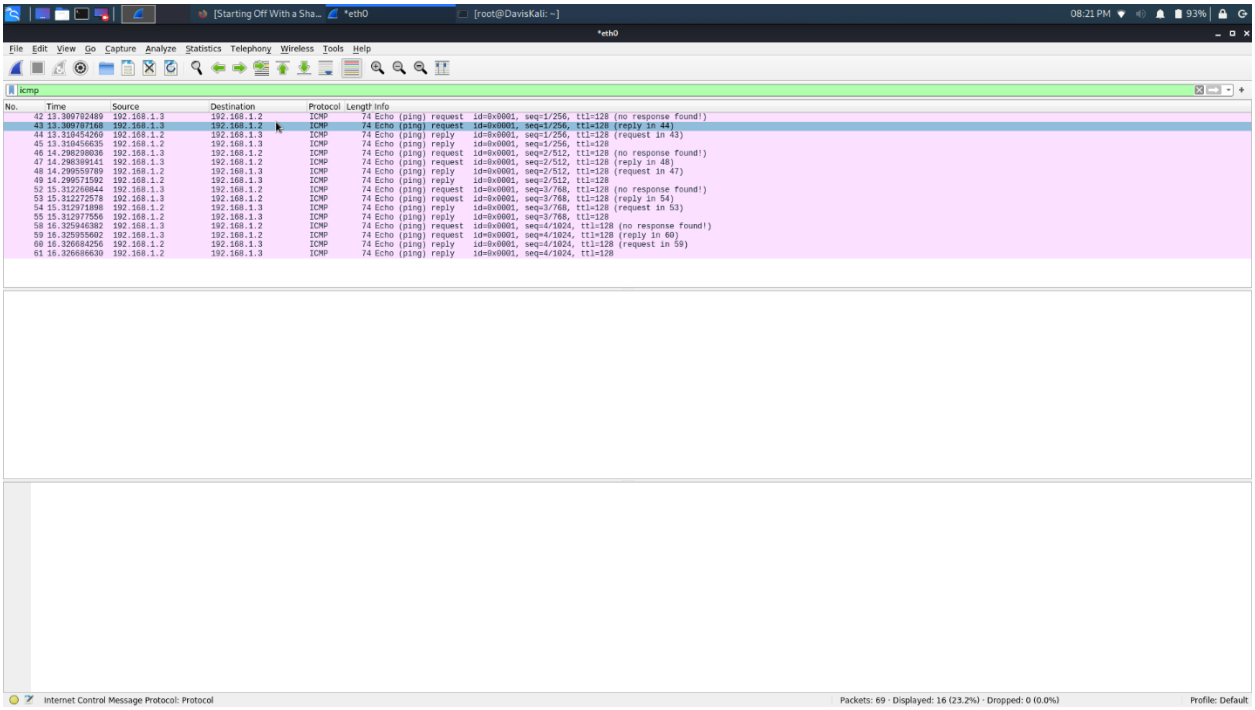
default wired Ethernet interface is named **`eth0`**. Select the eth0 or the Ethernet interface on the list with network activity. An example is shown below.



c. Now, you should be in the main window. From this window, any packet that arrives the MitM's NIC will be detected and displayed in the packet list pane. The packet list pane is located near the top of the main window underneath the menu, main toolbar, and filter toolbar. If the switch and MitM host are configured correctly, you should see PDUs populating the topmost pane – the packet list pane. Here is a dissection of the Wireshark main window for reference.

d. From the filter toolbar, type **`icmp`** and hit enter. Any packets in the list pane before should now be gone. The purpose of the filter toolbar is to filter by packet type i.e. return only packets of the Internet Control Message Protocol (ICMP) or by more specific parameters relating to the packet type. For the moment, no ICMP packets have been captured by Wireshark.

e. From the FTP Client 1 or 2, ping the IP address of the FTP Server. Then return to Wireshark to examine the packet list pane on MitM host. The packet list pane should now be populated with ICMP echo requests and replies sourced from either client destined to the FTP Server and back respectively.



f. This should not be possible under normal circumstances because (1) the ARP Spoof attack has not taken place yet and (2) the packets are addressed to either one of the clients or the server and not the MitM host. However, because we configured SPAN on the switch and are getting this output in the packet list pane, the SPAN port is functioning correctly. Another indicator is the doubles of the same packet indicating SPAN is capturing ingress (receiving) and egress (transmitting) traffic from the switch.

Now that SPAN and Wireshark are working as expected, the real core of the attack can be done – ARP Spoofing.

Note: Leave Wireshark running and capturing packets. If stopped or closed, repeat the steps above to reopen the packet capture window.

Part 3: Configure Ettercap and Launch ARP Spoof attack.

Ettercap is the *"swiss army knife"* of MitM LAN attacks, including ARP spoofing. With Ettercap, ARP spoofing is not the be-all-end-all tool because ARP spoofing itself is often the foundation of other LAN attacks. These include DNS poisoning, HTTP injection attacks, and if ARP spoofing cannot be done, there is a port stealing attack to achieve the same effect. However, the usage of Ettercap for this lab will be just for ARP spoofing to redirect traffic between the FTP Server and clients to the MitM host machine. First, more on ARP Spoofing.

As said in the background, ARP IP-to-MAC translations are maintained in the table on a device. To obtain those translations, the device that wants the MAC address of an IP address – of another computer – must ask for it. So, it constructs an ARP request or "Who is `IP address`? Please give me your MAC address." Then when the 'proper' device with that IP address receives this request, it replies with an ARP reply or "Hi, I am `IP address`, here is my MAC address." When the requesting device sends the request, the destination address of the frame encapsulating it is a broadcast address of `FF-FF-FF-FF-FF-FF` (`FFFF.FFFF.FFFF` or `FF:FF:FF:FF:FF:FF` are acceptable formats for a MAC address too).

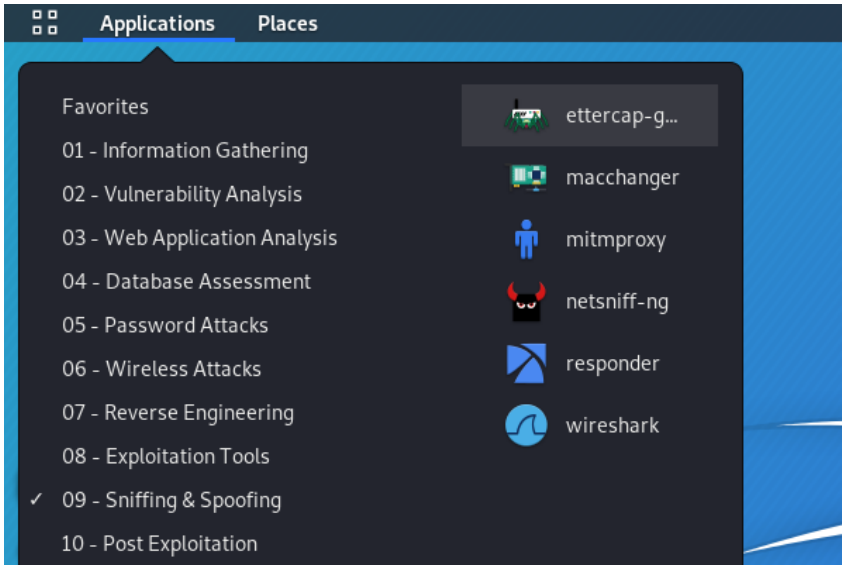
To the switch that receives it, it interprets this as send this frame out of every active switch port except the port that originally received it. Every active device in the broadcast domain will receive and process the ARP request, and it is up to them to determine if the ARP request is meant for them or not. This process is done purely on 'good faith' of other devices in the broadcast domain to drop the ARP request when it is not addressed to them. More importantly, if a device on the network gets this

request and answers back with their MAC address, even though they are not the IP address that has to answer this ARP request, nothing can be done. No detection, no authentication. A ‘forged’ ARP reply is as good as the ‘authentic’ one as no means exist in ARP itself to distinguish forged replies from real replies.

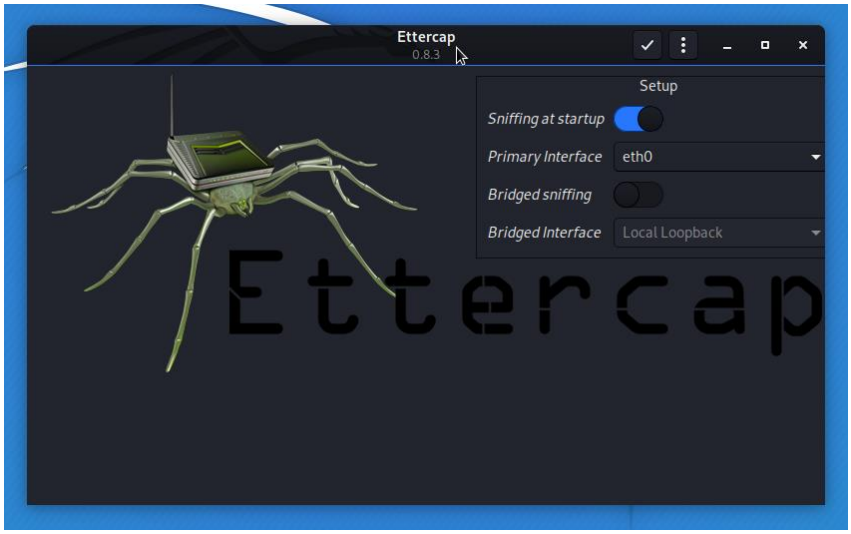
With Ettercap, launch the ARP spoof attack and forge the MitM host as the MAC address of the FTP Server and the clients, making the other think the MitM host is their intended destination.

Step 1: **Open Ettercap to run on uplinked interface.**

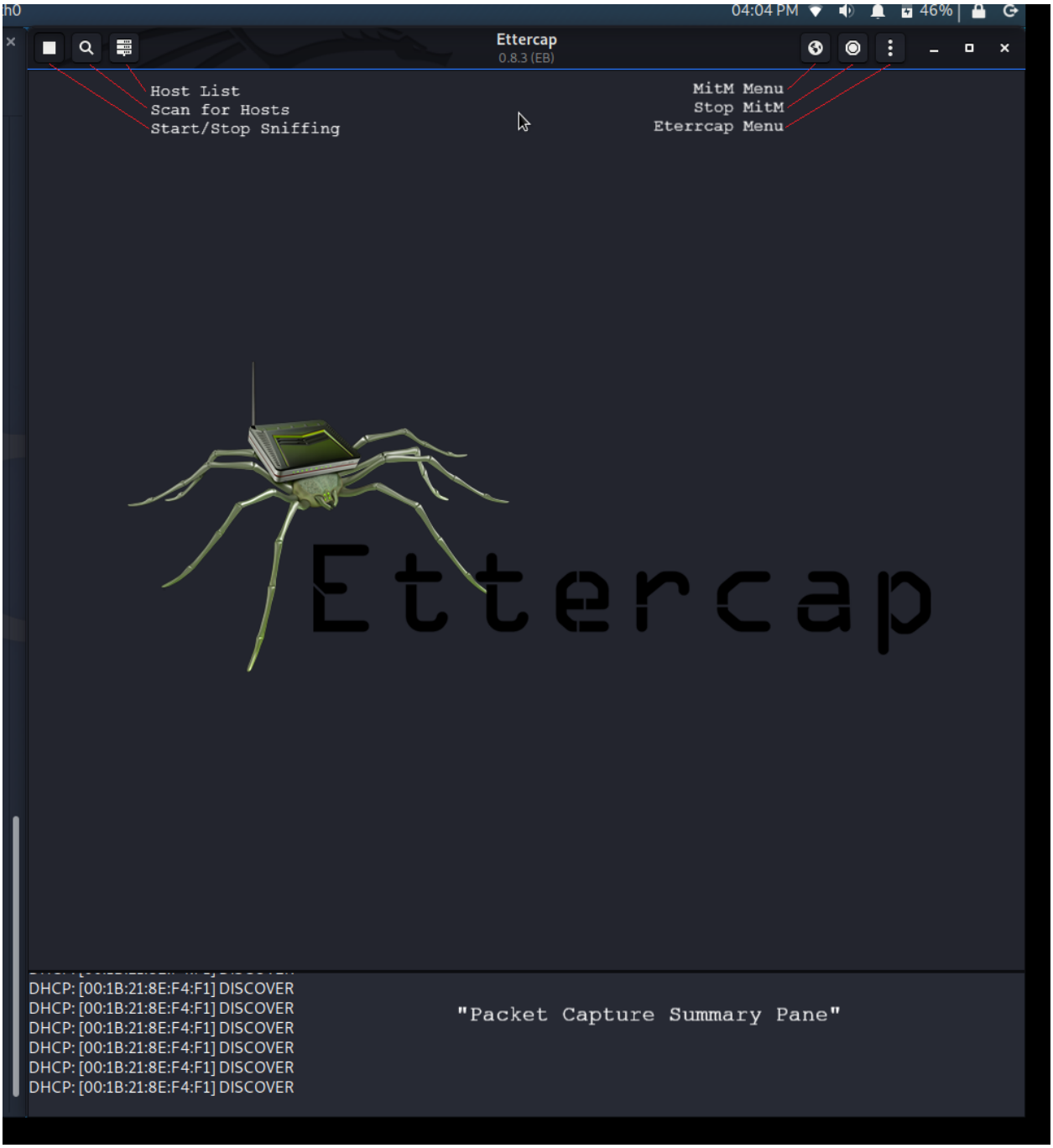
a. Ettercap functions by selecting a specific network interface to listen on and launch MitM attacks. A target list consists of 2 specified IP addresses. These addresses can be single, multiple separated by commas, or an address range of IPv4 or IPv6 addresses. To begin, open Ettercap from the Kali drop down menu up at the top right corner for “09 – Sniffing & Spoofing > Ettercap.”



b. Upon opening Ettercap, you should be greeted by the interface options window. Select the interface currently uplinked to the topology and choose the checkmark up at the top-right of the window.

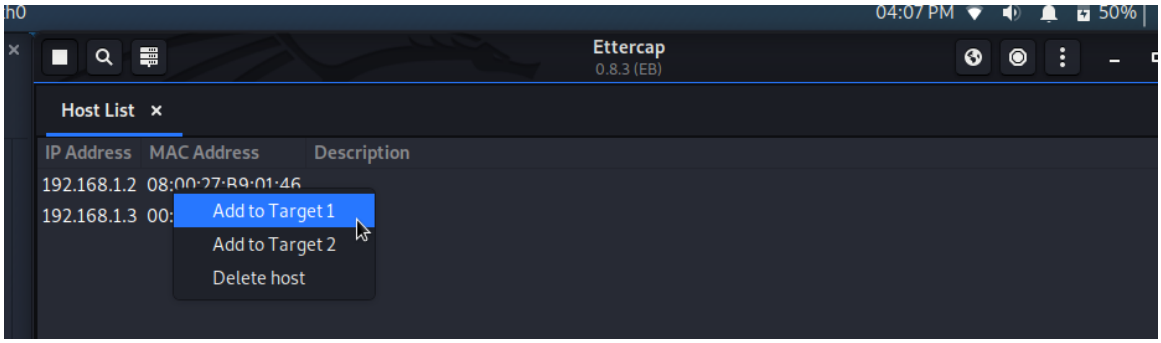


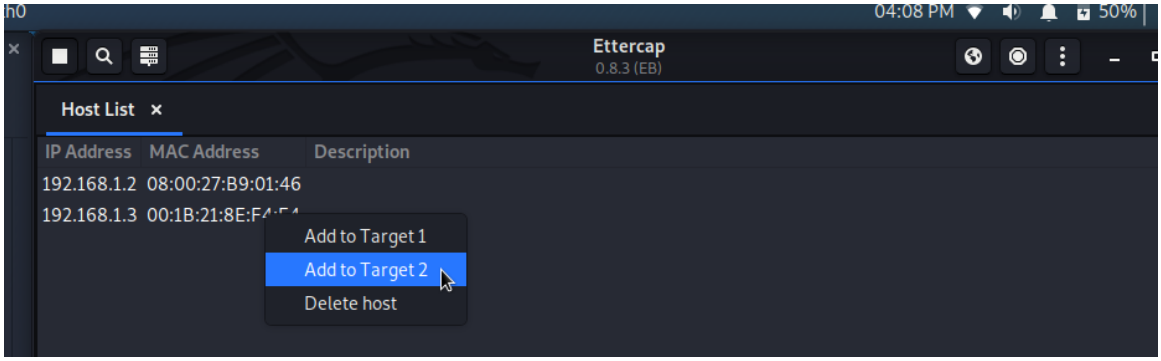
c. Now, you are in Ettercap's main window. Use this below as a reference to navigate the Ettercap GUI.



Step 2: **Enter and add IP targets to host list.**

a. Enter the host list and add the FTP Client's 1 and 2 to Target 1 and FTP Server to Target 2 by right-clicking on each list entry, adding them to the appropriate target.

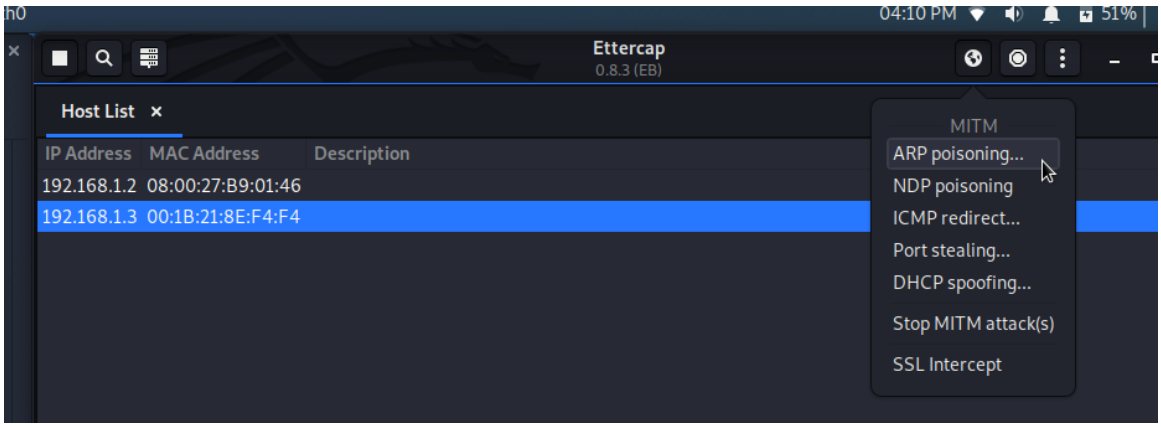




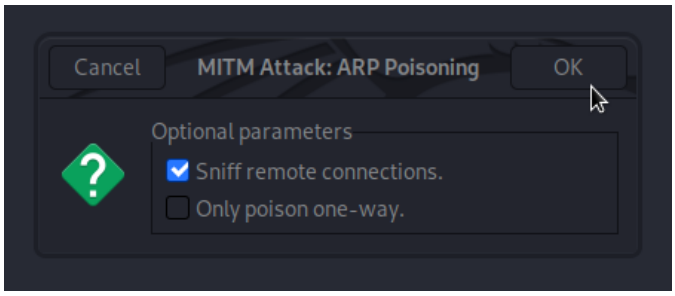
b. **Note:** If the 2 clients and server do not all show up on the host list, use the "Scan for Hosts" option to populate the list. If that does not work, verify network connectivity by checking physical layer connections and pinging each host on each device in the topology with an IP address and troubleshoot as required before attempting again.

Step 3: **Start the ARP poisoning (spoofing) attack.**

a. Now, choose the MitM attack options. From the drop-down menu, select ARP poisoning.



b. Upon selection, a small popup window will appear, leave it at its default settings and select OK.



Step 4: **Verify ARP spoofing has affected the specified targets.**

Step 5: **Go Back to the "Device ARP Tables" and repeat the same process specified in Part 1, step 7 except do it for "MAC Addresses After Attack" column.**

Part 4: Exfiltrate FTP Credentials over the Network and use them to login to the FTP Server.

FTP is an application layer protocol apart of the TCP/IP protocols suite. FTP utilizes Transport Control Protocol (TCP) as the underlying transport mechanism for carrying commands and data between a client and server. Two TCP ports are used in original FTP: port no. 20 and 21 – data and control connections respectively.

The control connection (port no. 21) is used to connect to the FTP server initially and pass on server responses and client commands. One prime example of using control connection between FTP client and server is the transmission of user credentials consisting of the username and password for a specific user. This is often required for FTP servers that service multiple users and groups, whom have files that belong to the user or for a specific group that others should not be permitted access to.

The data connection (port no. 20) is used to upload files from or download files to the FTP client on the server. What a client (user) can do depends on what specific permissions they have. If a user can only read (download) files from FTP server for their specific group, then they cannot upload files (write) to the server. The FTP server software running the service is often managed by a network or systems administrator on production networks and will configure the appropriate permissions per user/group accordingly for what access they have.

Both aspects of requiring user authentication and restricting permissions to only the bare minimum for users and groups is based on the principles of security hardening. A securely configured server with these basic implementations should be enough at deterring individual users from accessing and modifying files of other users on the server. However, as you are about to demonstrate, there is an aspect of the FTP Server's configuration that has been overlooked and will allow another user to access and modify files of another user regardless.

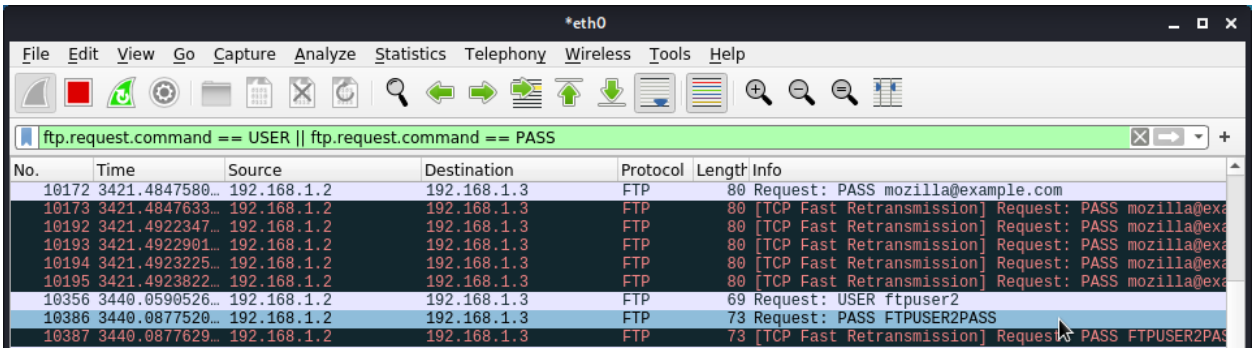
Step 1: **Login to the FTP Server from both FTP User 1 and User 2 using the appropriate user credentials.**

Step 2: **Go back to Wireshark and enter the following filter into the filter toolbar:**

```
ftp.request.command eq USER || ftp.request.command eq PASS
```

Step 3: **From the packet list pane, identify the user credentials of both clients.**

a. If no output is shown in the pane, check your spelling and syntax entered on the filter toolbar to that of step 3's.



Step 4: **Verify Ettercap has also exfiltrated the user credentials of both clients.**

a. Ettercap should also have received the user credentials as well. If they do not appear, do not worry. Sometimes Ettercap will not capture credentials in time.

```
Host 192.168.1.2 added to TARGET1
Host 192.168.1.3 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.1.2 08:00:27:B9:01:46

 GROUP 2 : 192.168.1.3 00:1B:21:8E:F4:F4
FTP : 192.168.1.3:21 -> USER: anonymous  PASS: mozilla@example.com
FTP : 192.168.1.3:21 -> USER: ftpuser2  PASS: FTPUSER2PASS
FTP : 192.168.1.3:21 -> USER: anonymous  PASS: mozilla@example.com
FTP : 192.168.1.3:21 -> USER: ftpuser2  PASS: ftpuser2pass
```

Step 5: **With exfiltrated user credentials, from the MitM host, login to the FTP Server with credentials stolen off the network.**

Conclusion

As the inside attacker, you now have unfettered access to 2 FTP user accounts. This attack was successful because of your authorized access to your company's switched network and the leveraging of ARP spoofing to perform a man-in-the-middle. You also exploited a weakly configured FTP server that transmits and receives all responses, commands, and data unencrypted. So, even if the business properly controls access for users and groups on the server, an attacker that can listen to network activity will gain access to multiple user accounts simultaneously.

By setting up a SPAN port on the switch, you were able to passively listen to network conversations to ascertain victims. Using ARP spoofing you redirected FTP conversations between the FTP clients and server to pass through the MitM host machine. Finally, you exfiltrated the unencrypted user credentials being sent across the network to gain privileged access.

The software and tools you learned to use was configuration of an FTP server with FileZilla, SPAN on Cisco Catalyst series switches for passive interception, Wireshark for network monitoring, and Ettercap for active interception and manipulation of a TCP/IP protocol. You also learned about how ARP and FTP fundamentally works and how to exploit its operation (lack of authentication and encryption).