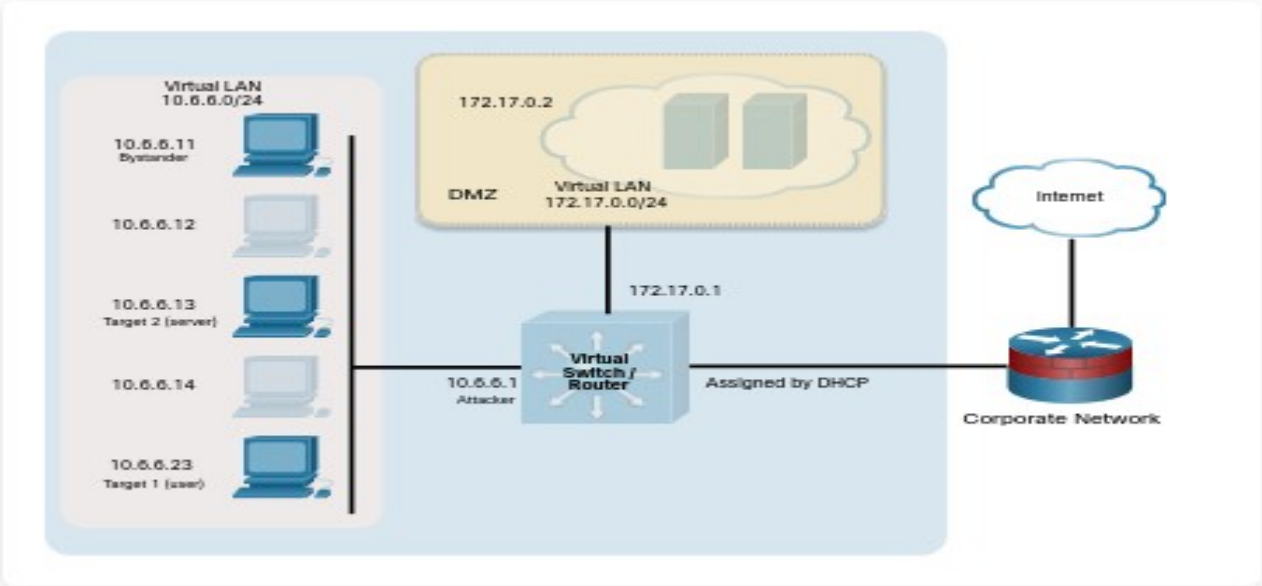
Lab - On-Path Attacks with Ettercap

Topology



Objectives

In this lab, you will complete the following objectives:

- **Part 1: Launch Ettercap and Explore Its Capabilities**
- **Part 2: Perform the On-Path (MITM) Attack**
- **Part 3: Use Wireshark to observe the ARP Spoofing Attack**

Background / Scenario

On-path attacks are very powerful ways to steal data that is travelling on a network. Without end-to-end encryption, as with much data travelling on local LANs, it is easy to capture clear text information, and even complete files, using on-path attack methods.

***Note**: **On-path** is replacing man-in-the-middle (MITM) as the name of this type of attack. The replacement process is incomplete; however, so you may still see MITM in many places, including some exam questions. Just be aware that the two terms are currently interchangeable.*

Required Resources

- Kali VM customized for the Ethical Hacker course

Instructions

Part 1: Launch Ettercap and Explore its Capabilities.

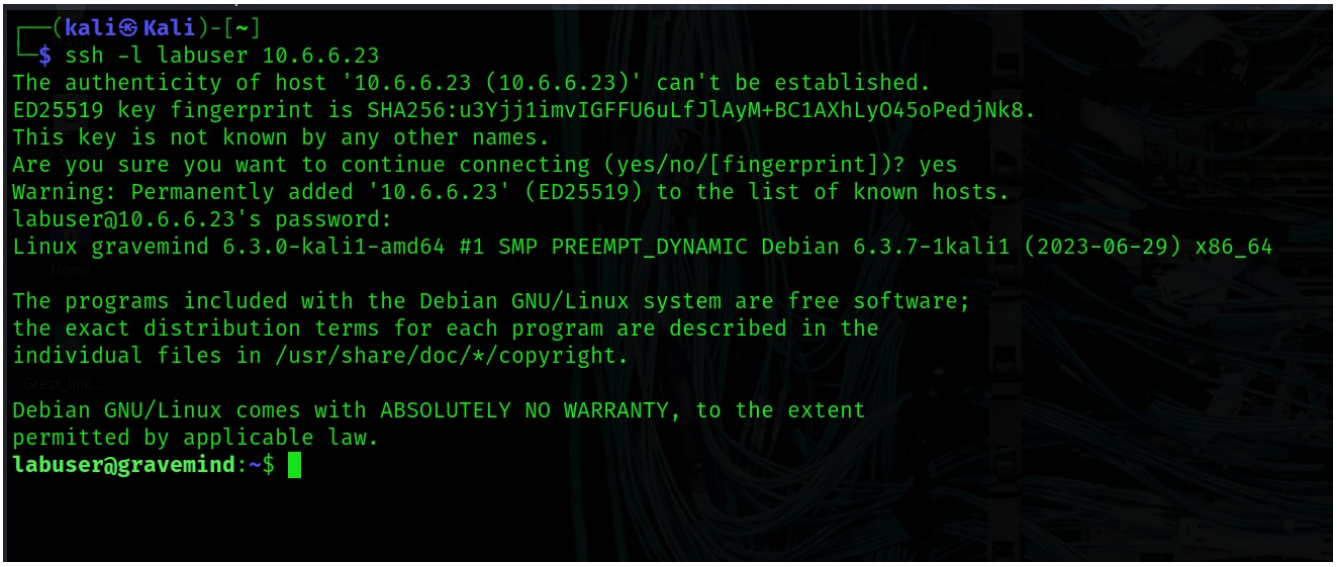
Ettercap is used to perform on-path (MITM) attacks.

The goal of an on-path attack is to intercept traffic between devices to obtain information that can be used to impersonate the target or to alter data being transmitted. The attacker is situated" between" two communicating hosts. In on-path attacks, the hacker doesn't need to compromise the target device, but can just sniff traffic passing back and forth between the target and destination. Ettercap is used as an on-path tool, and the attack machine is on the same IP network as the victim.

Step 1: Set up an ARP spoofing attack.

In this attack, you will use ARP spoofing to redirect traffic on the local virtual network to your Kali Linux system at 10.6.6.1. ARP spoofing is often used to impersonate the default gateway router to capture all traffic entering or leaving the local IP network. Because your lab environment uses an internal virtual network, instead of spoofing the default gateway, you will use ARP spoofing to redirect traffic that is destined for a local server with the address 10.6.6.13.

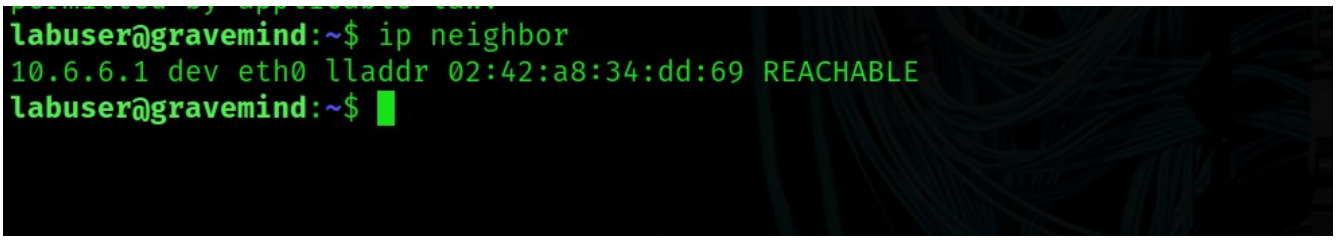
a. Load Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.
b. The target host in this lab is the Linux device at 10.6.6.23. To view the network from the target perspective, and initiate traffic between the target and the server, use SSH to log in to this host. The username is **labuser** and the password is **Cisco123**. Command: **ssh -l labuser 10.6.6.23**



The user of the 10.6.6.23 host is communicating with the server at 10.6.6.13. The on-path attacker at 10.6.6.1 (your Kali VM) will intercept and relay traffic between these hosts.

c. Because you are creating an on-path attack that uses ARP spoofing, you will be monitoring the ARP mappings on the victim host. The attack will cause changes to those mappings.

Use the command **ip neighbor** to view the current ARP cache on the target computer.



***Note**: If you are using the ARM CPUs (Apple M1/M2) version of the VM, you will need to switch to use the **root user** with the password **Cisco123** and use the command **arp -a** in place of **ip neighbor** to view the current ARP cache throughout this activity.*

How many entries are there in the current ARP cache? **1 for 10.6.6.1**
What is the MAC address of the Kali attacker machine? **02:42:a8:34:dd:69**

Step 2: Load Ettercap GUI interface to begin scanning.

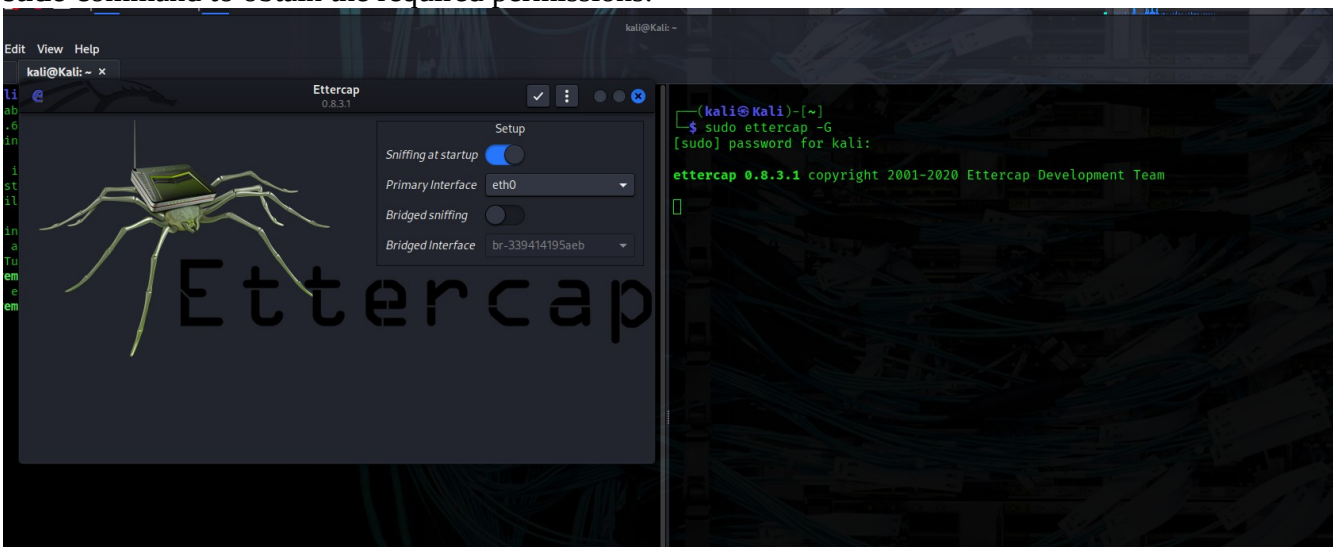
a. Open a new terminal session from the menu bar in Kali Linux. Do not close the SSH-terminal that is running the session with 10.6.6.23.
b. Use the **ettercap -h** command to view the help file for the Ettercap application.

Examine the help file content.

How many user interfaces are available for the Ettercap tool? What are the options used to specify the user interfaces? **4 types: -T, -C, -D, -G**

```
┌──(kali㉿Kali)-[~]
└─$ ettercap -h

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team


Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]

TARGET is in the format MAC/IP/IPv6/PORTs (see the man for further detail)

Sniffing and Attack options:
  -M, --mitm <METHOD:ARGS>    perform a mitm attack
  -o, --only-mitm             don't sniff, only perform the mitm attack
  -b, --broadcast             sniff packets destined to broadcast
  -B, --bridge <IFACE>        use bridged sniff (needs 2 ifaces)
  -p, --nopromisc             do not put the iface in promisc mode
  -S, --nosslmitm             do not forge SSL certificates
  -u, --unoffensive           do not forward packets
  -r, --read <file>           read data from pcapfile <file>
  -f, --pcapfilter <string>   set the pcap filter <string>
  -R, --reversed              use reversed TARGET matching
  -t, --proto <proto>         sniff only this proto (default is all)
      --certificate <file>    certificate file to use for SSL MiTM
      --private-key <file>    private key file to use for SSL MiTM

User Interface Type:
  -T, --text                  use text only GUI
       -q, --quiet                 do not display packet contents
       -s, --script <CMD>          issue these commands to the GUI
  -C, --curses                use curses GUI
  -D, --daemon                daemonize ettercap (no GUI)
  -G, --gtk                   use GTK+ GUI

Logging options:
  -w, --write <file>          write sniffed data to pcapfile <file>
  -L, --log <logfile>         log all the traffic to this <logfile>
  -l, --log-info <logfile>    log only passive infos to this <logfile>
  -m, --log-msg <logfile>     log all the messages to this <logfile>
  -c, --compress              use gzip compression on log files

Visualization options:
  -d, --dns                   resolves ip addresses into hostnames
  -V, --visual <format>       set the visualization format
  -e, --regex <regex>         visualize only packets matching this regex
  -E, --ext-headers           print extended header for every pck
  -Q, --superquiet            do not display user and password

LUA options:
      --lua-script <script1>,[<script2>, ... ]     comma-separted list of LUA scripts
      --lua-args n1=v1,[n2=v2, ... ]               comma-separated arguments to LUA script(s)
```

In this part, you will use a GUI interface to access Ettercap. Start Ettercap GTK+ graphical user interface using the **ettercap -G** command. Most Ettercap functions require root permissions, so use the **sudo** command to obtain the required permissions.



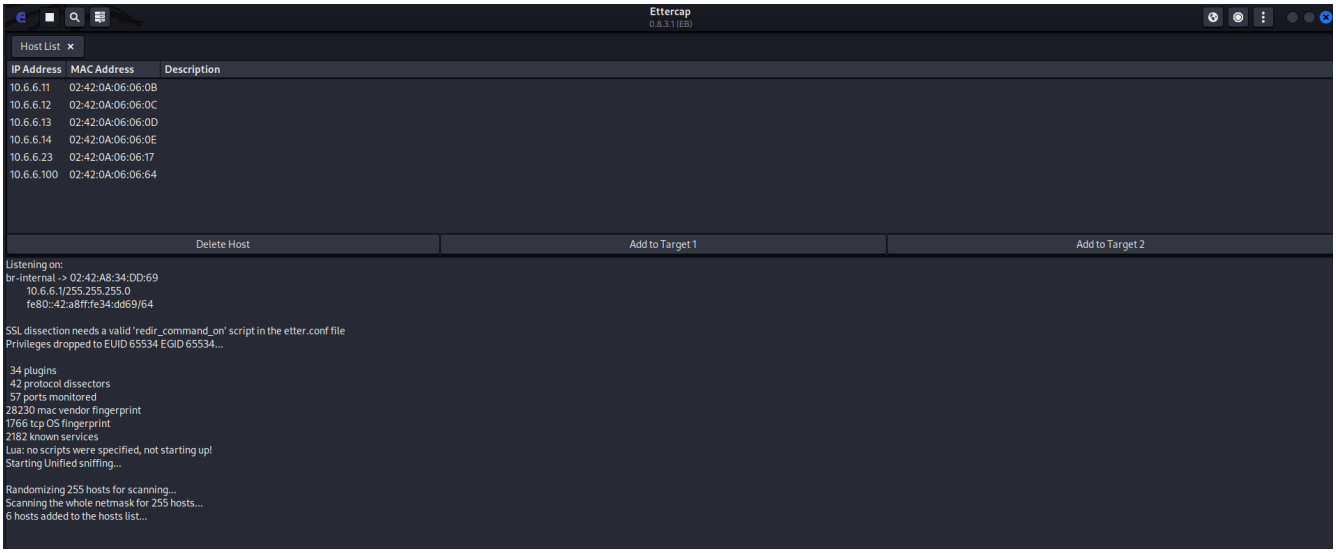
The Ettercap GUI opens in a new window. You are sniffing traffic on an internal, virtual network. The default setup is to scan using interface eth0. Change the sniffing interface to **br-internal**, which is the interface that is configured on the 10.6.6.0/24 virtual network, by changing the value in the **Setup** > **Primary Interface** dropdown.

Click the **checkbox** icon at the top right of the Ettercap screen to continue. A message appears at the bottom of the screen indicating that Unified sniffing has started.

Part 2: Perform the On-Path (MITM) Attack

Step 1: Select the Target Devices.

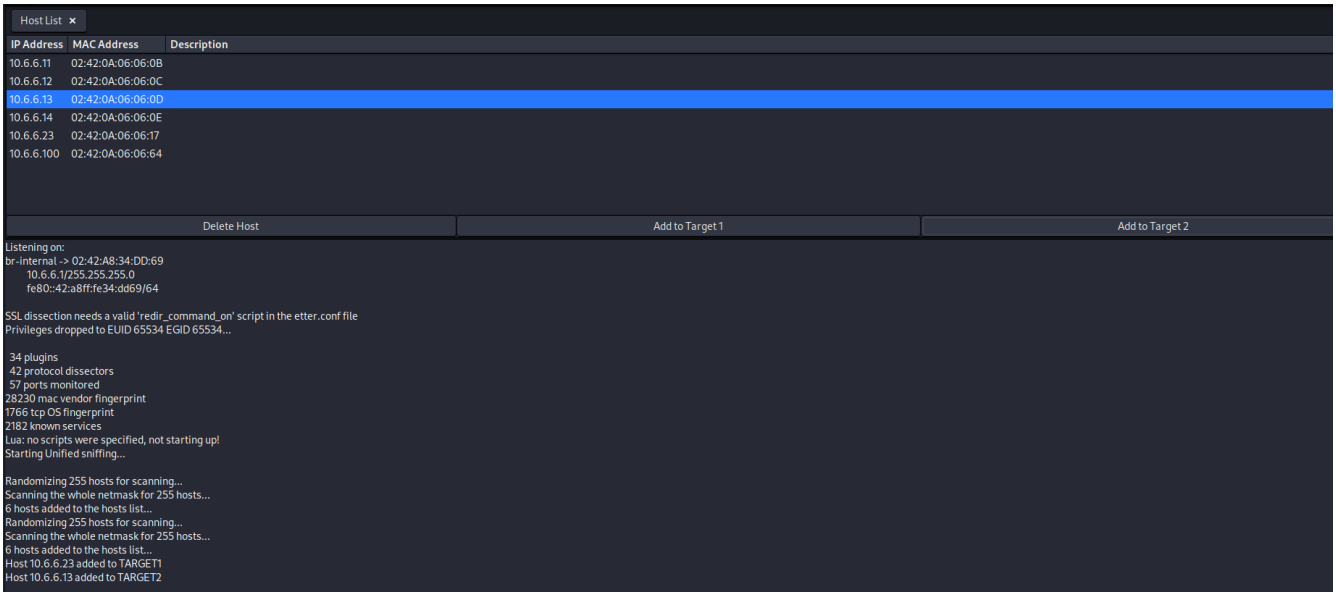
a. In the Ettercap GUI window, open the Hosts List window by clicking the Ettercap menu (three dots icon). Select the **Hosts** entry and then **Hosts List**. Click the **Scan for Hosts** icon (magnifying glass) at top left in the menu bar. A list of the hosts that were discovered on the 10.6.6.0/24 network appears in the Host List window.



How many hosts were discovered? **6**

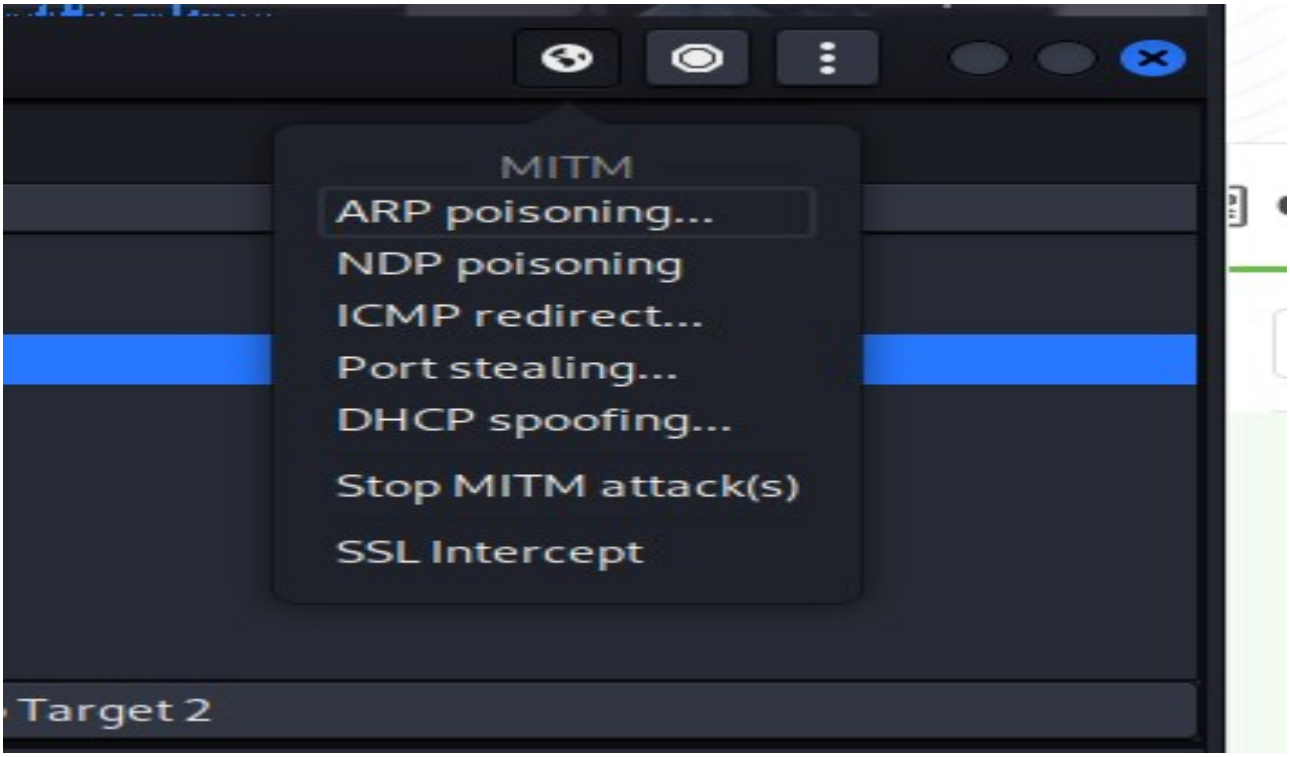
Define the source and destination devices for the attack. To do so, click the IP address **10.6.6.23** in the window to highlight the target user host. Click the **Add to Target 1** button at the bottom of the Host List window. This defines the user's host as Target 1.

Click the IP address of the destination web server at **10.6.6.13** to highlight the line. Click the **Add to Target 2** button at the bottom of the host window.

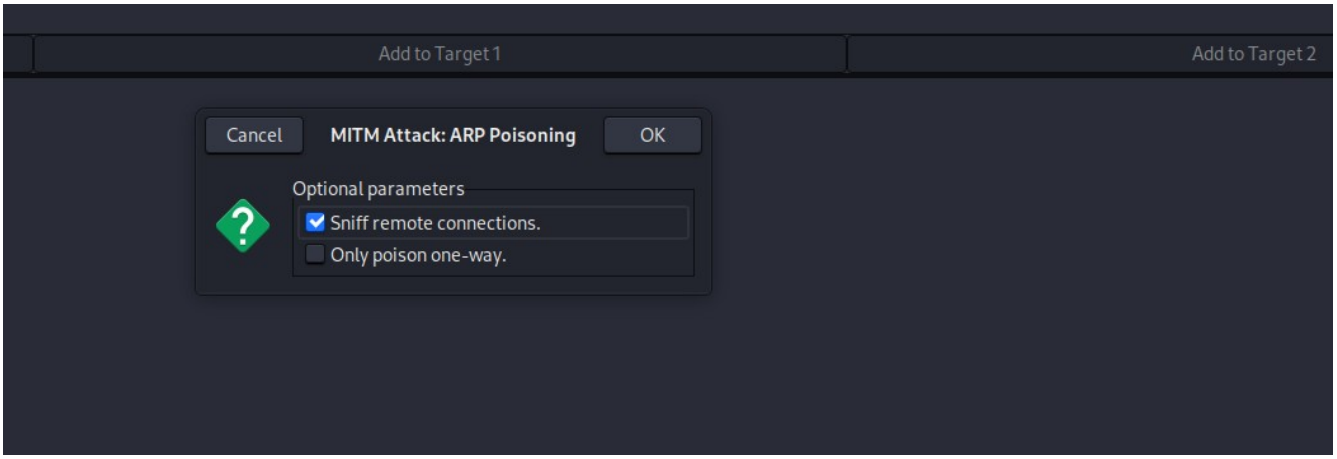


Any IP/MAC address specified as a Target 1 will have all its traffic diverted through the attacking computer that is running Ettercap. In this lab, the attacking computer is the Kali Linux machine at 10.6.6.1. All other computers on the subnet, other than the targets, will communicate normally.

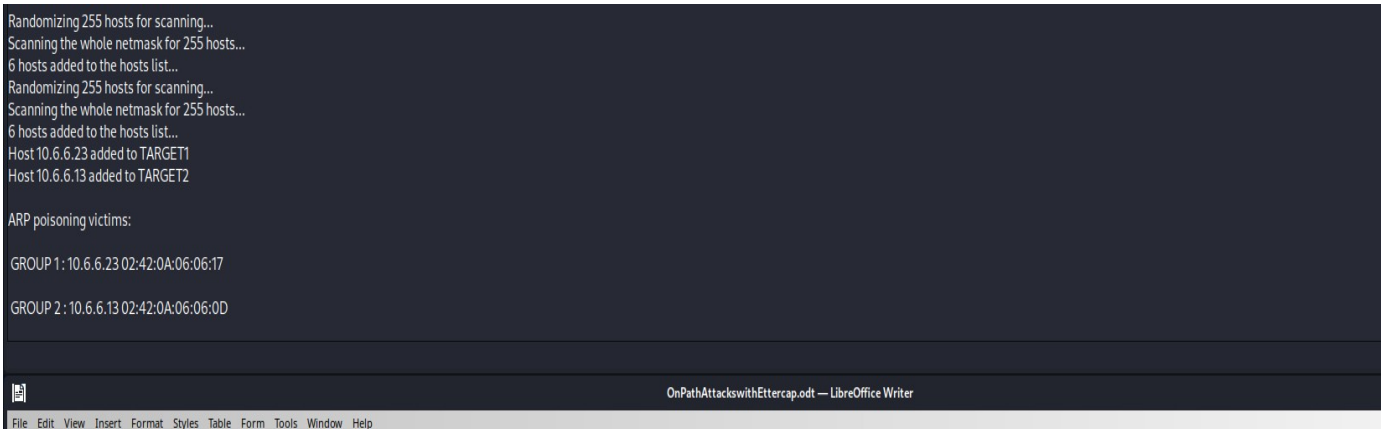
Click the MITM icon on the menu bar (the first circular icon on top right). Select **ARP Poisoning…** from the dropdown menu.



Verify that **Sniff remote connections** is selected. Click **OK**.



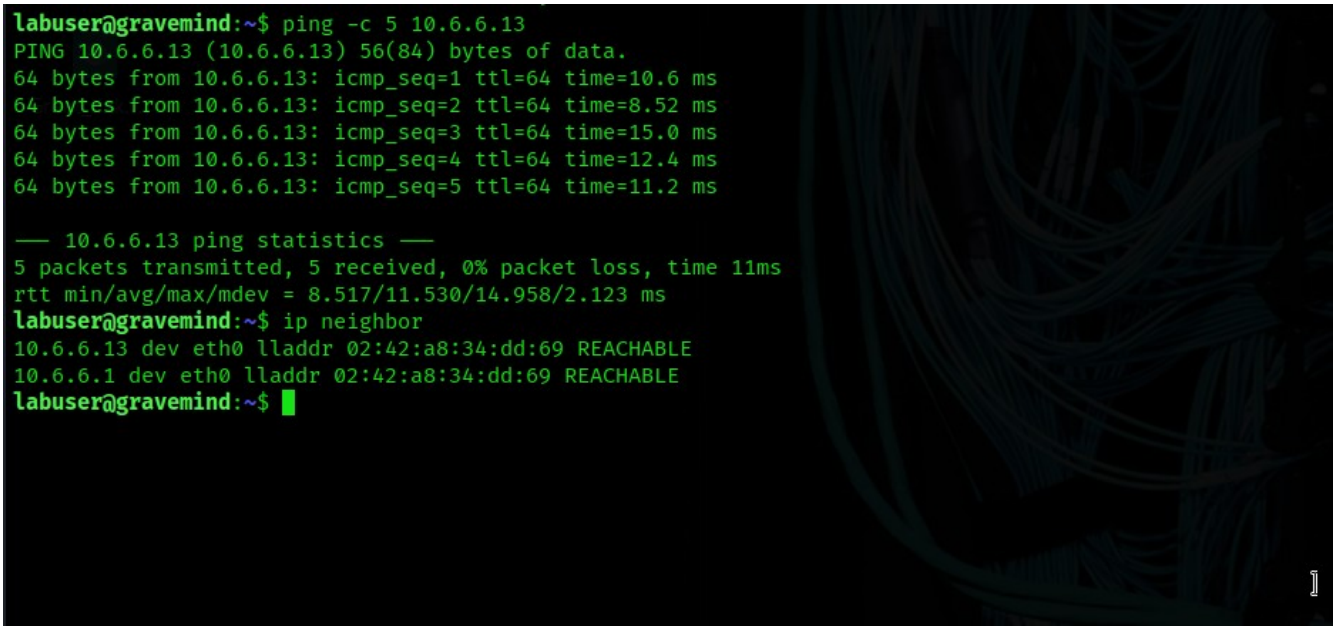
The MITM exploit is started. If sniffing does not start immediately, click the **Start** option (play button) at left in the top menu.



Step 2: Perform the ARP spoofing attack.

a. Return to the terminal window that is running the SSH session with the target user host at 10.6.6.23. Repeat the ping to 10.6.6.13

b. Use the **ip neighbor** command to view the ARP table on 10.6.6.23 again. Note the MAC address listed for 10.6.6.13.



Is the MAC address associated with 10.6.6.13 the same as the one you recorded in Part 1, Step 1e?
YES

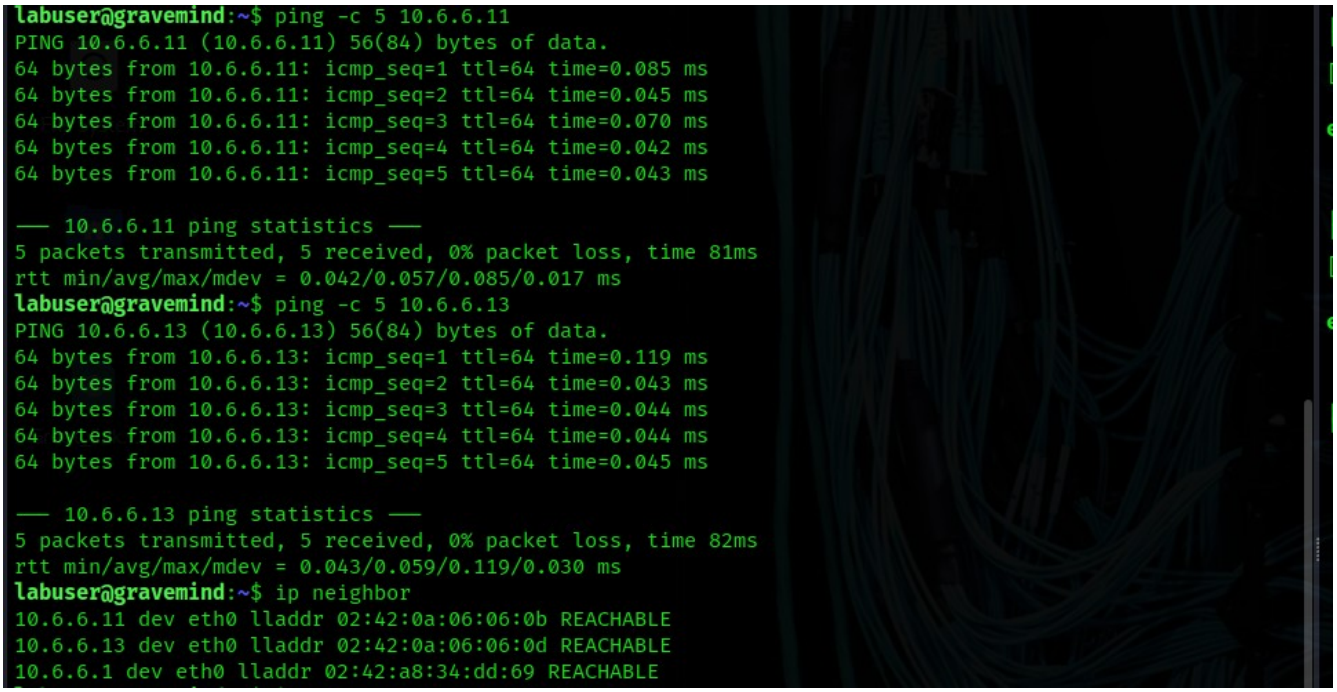
What is strange about this? **MAC addresses are supposed to be globally unique, so it is strange that two devices have the same MAC address.**
What is the effect of this change? **Packets that are sent on the LAN to 10.6.6.13 will be received by both the intended host and the Kali VM attacker.**
Close the Ettercap graphical user interface. Leave the SSH connection to 10.6.6.23 active.

Part 3: Use Wireshark to Observe the ARP Spoofing Attack

Step 1: Select the Target Devices and Perform the MITM attack using the CLI

In this step, you will use the command line interface in Ettercap to perform ARP spoofing and write a .pcap file that can be opened in Wireshark. Refer to the help information for Ettercap to interpret the options used in the commands.

a. Return to the terminal session that is connected via SSH to 10.6.6.23. Ping the IP addresses 10.6.6.11 and 10.6.6.13. 10.6.6.11 is another host on the LAN that we will verify is unaffected by the attack. Then, use the **ip neighbor** command to find the MAC addresses associated with the IP addresses of the two systems.



Complete the table:

***Note**: To find the MAC of 10.6.6.23, go to the SSH session terminal and enter the **ip address** command. Determine the MAC address of the interface that is addressed on the 10.6.6.0/24 network.*

IP Address	MAC Address
10.6.6.1	Answer Area: 02:42:a8:34:dd:69
10.6.6.11	Answer Area: 02:42:0a:06:06:0b
10.6.6.13	Answer Area: 02:42:0a:06:06:0d
10.6.6.23	Answer Area: 02:42:0a:06:06:17

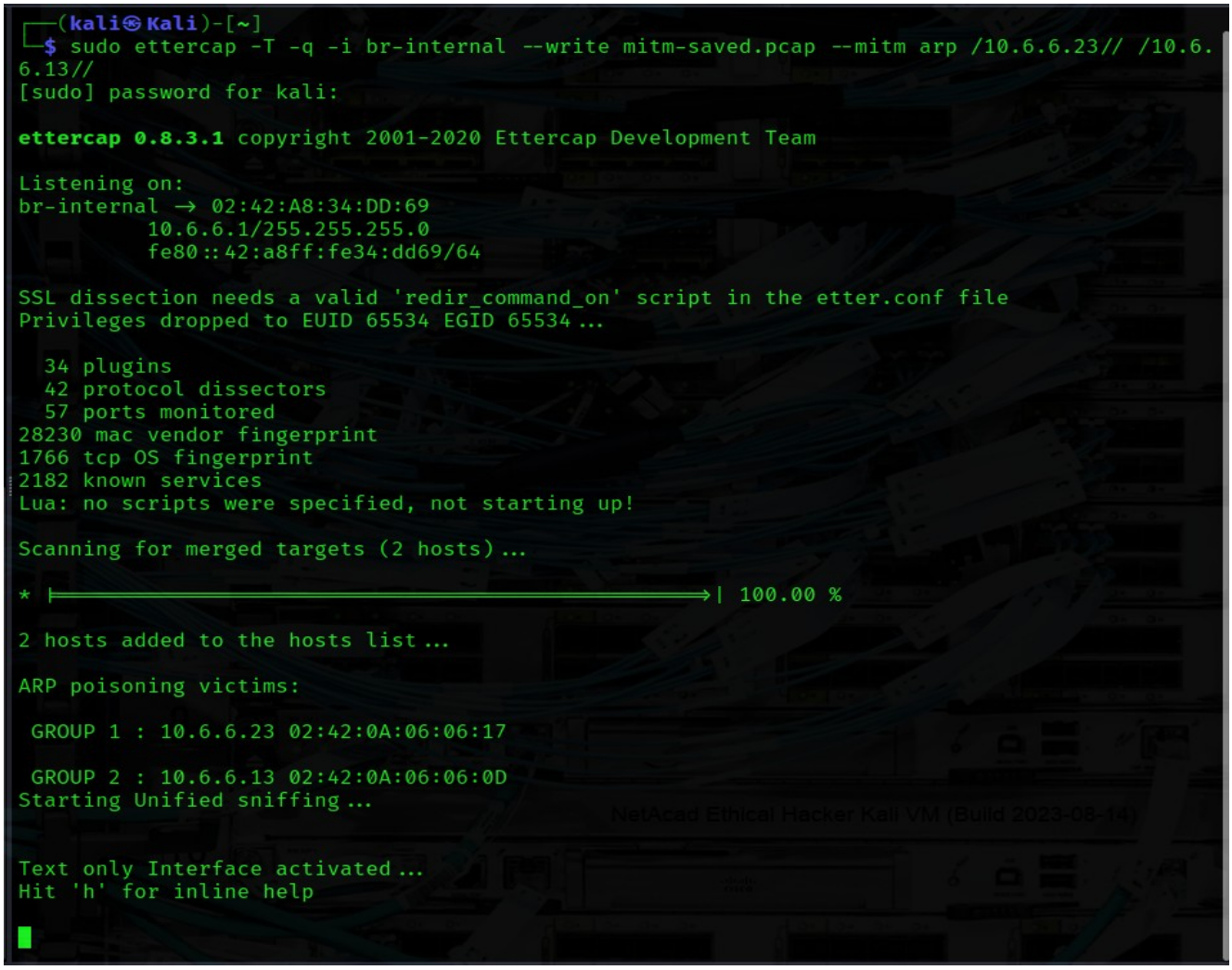
The **ettercap -T** command runs Ettercap in text mode, instead of using the GUI interface. The syntax to start Ettercap and specify the targets is: **sudo ettercap -T [*options*] -q -i [*interface*] --write [*file name*] -- mitm arp /[*target 1*]// /[*target 2*]//.

Open a new terminal window as necessary.

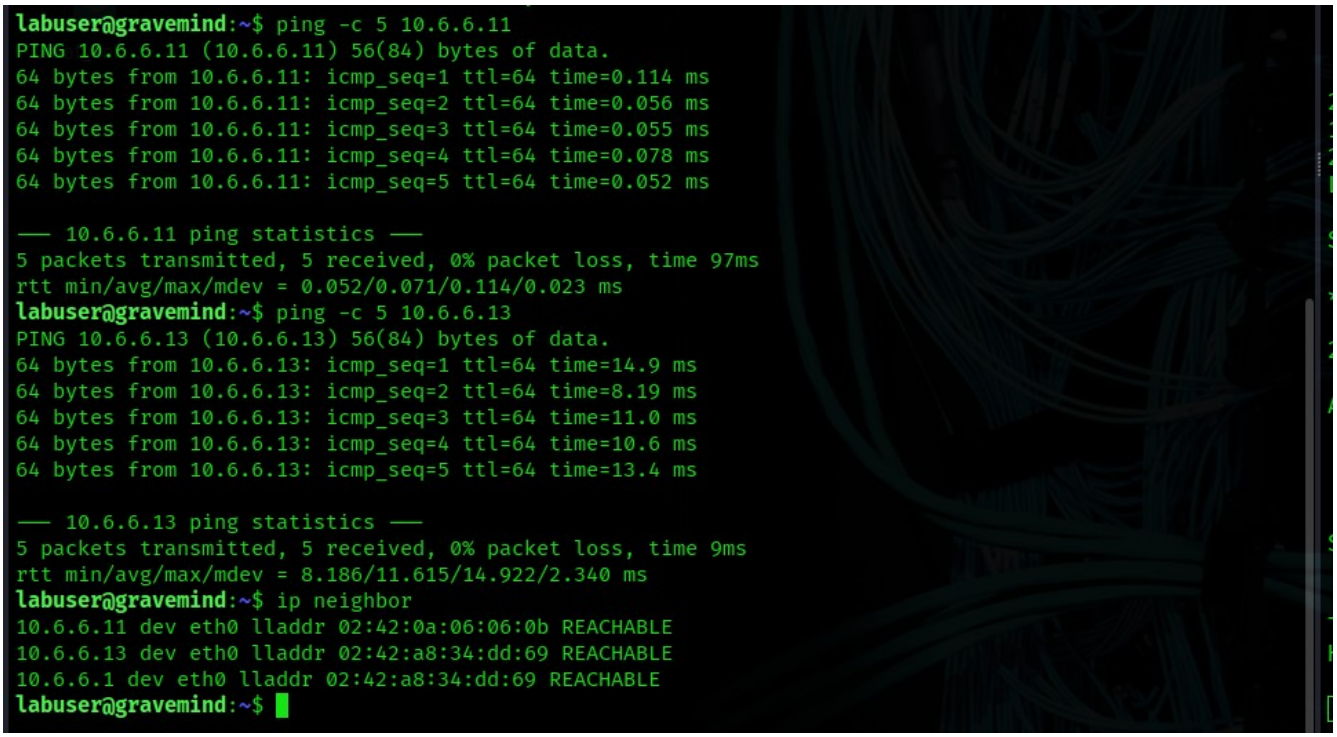
Use the man page for Ettercap and complete the table below: **man ettercap**

Options and Values	Meaning
-T	user the text only interface
-q	run the command in quiet mode to simplify output
-i	specify the sniffing/attacking network interface
--write	Write packets to a .pcap file that can be opened in Wireshark. Specify the name for the file
--mitm arp	Conduct the ARP poisoning MITM attack
/target1//	the IP address of the target user host
/target2//	the IP address of the target server

In a terminal window, enter the command as follows to save the pcap file in the current working directory:



Return to the SSH terminal session to 10.6.6.23. Ping the two IP addresses, 10.6.6.11 and 10.6.6.13, again. Use the **ip neighbor** command to view the associated MAC addresses.



Are the MAC addresses that are associated with the IP addresses the same as you recorded in substep a? **No, 10.6.6.13 now has the same MAC as 10.6.6.1. The MAC for 10.6.6.11 is unchanged because it is not a target in the attack.**

Close the SSH terminal session that is connected to 10.6.6.23 and return to the terminal session running Ettercap in text mode. Enter **q** to quit Ettercap.

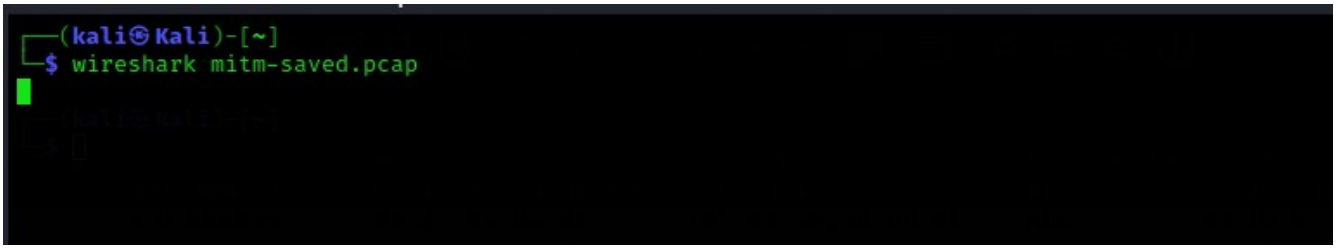
Step 2: Open Wireshark to view the Saved PCAP file.

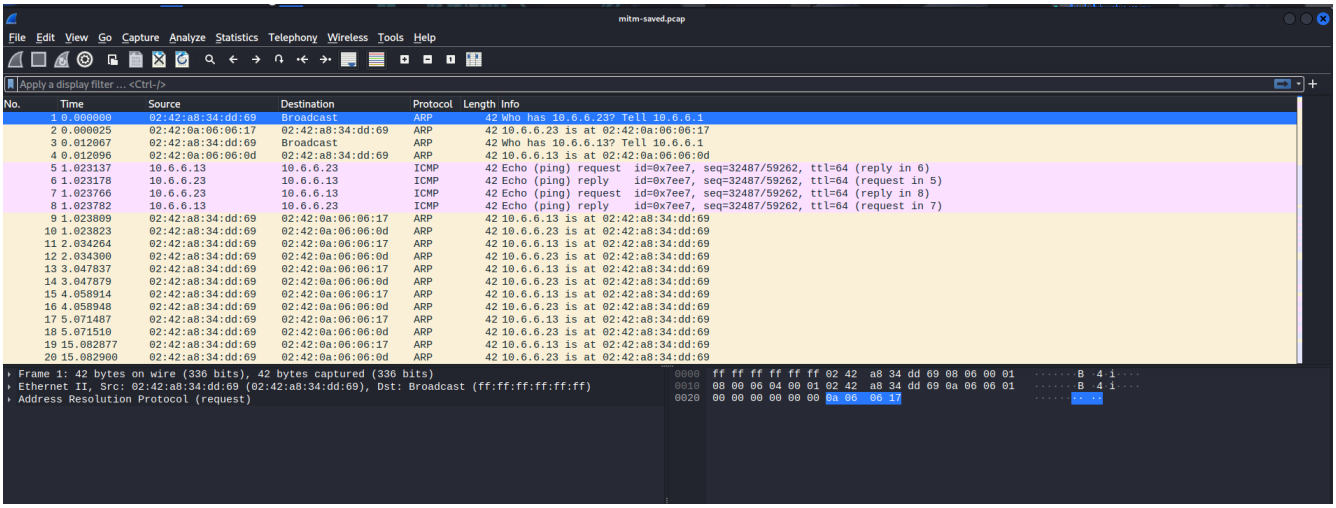
In this step, you will examine the .pcap file that Ettercap created.

a. Review the MAC addresses that you recorded in Step 1c. The MAC address for 10.6.6.23 can be found in the output of the Ettercap text interface in Target Group 1.

What is now true of the MAC addresses of these three systems? **The 10.6.6.23 (target user) and 10.6.6.1 (attacker) have the same MAC address. The MAC address for 10.6.6.11 (bystander) remains the same because it is not the target in the attack.**

In the Kali terminal window, start Wireshark with the mitm-saved.pcap file that you created with Ettercap.





The Ettercap attack computer first broadcasts ARP requests to obtain the actual MAC addresses for the two target hosts, 10.6.6.23 and 10.6.6.11. The attacking machine then begins to send ARP responses to both target hosts using its own MAC for both IP addresses. This causes the two target hosts to address the Ethernet frames to the attacker's computer, which enables it to collect data as an on-path attacker.

Why must the computer executing the Ettercap attack be located on the same IP network as the target system? **Because ARP protocol uses Layer 2 broadcasts to obtain the destination MAC associated with the target IP address. Broadcasts and Layer 2 ARP information are not forwarded beyond the local network.**