

Lab #2

CECS 378 – Spring 2020 Cappel

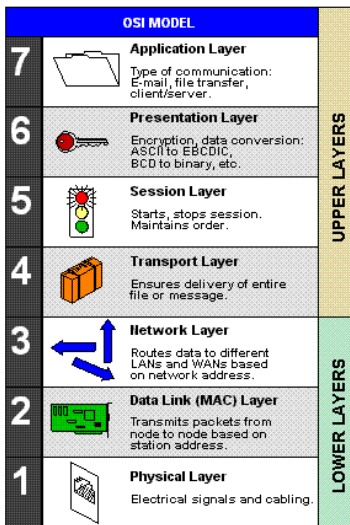
Due: Tuesday, February 25 prior to lab (6 PM)

This lab will leverage the virtual machines you built in Lab #1.

We will be using the following VM's in Lab #2: KaliLinux, SeedUbuntu1, & SeedUbuntu2 VM's.

The Open Systems Interconnect (OSI) Model

The **OSI model** is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.



We will be performing a Man-in-the-Middle (MitM) attack later in this lab which will allow us to examine all traffic passing between two devices. We will be poisoning the Address Resolution Protocol (ARP) cache of these two devices to be able to execute this MitM attack.

One of the objectives of this lab is to demonstrate that securing *ALL* layers of the OSI model is important! The hard part is having the resources (staff) to be able to understand and maintain all those security controls.

Note: Here is a simple mnemonic aid that may help you remember the 7 layers in the OSI Model – “**P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way”

OSI model			
Layer		Protocol data unit (PDU)	Function ^[6]
Host layers	7 Application	Data	High-level APIs, including resource sharing, remote file access
	6 Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5 Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4 Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3 Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2 Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1 Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

The **Internet protocol suite** is the conceptual model and set of communications protocols used on the Internet and on most internal computer networks (Intranets). It is commonly known as **TCP/IP** because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

Question 1) How does the Internet protocol suite documented in [RFC 1122](#) map to the OSI Model?

Hint: Map the relationships between the 7 layers in the OSI model to the 4 layers in the Internet protocol model.

Address Resolution Protocol (ARP)

The **Address Resolution Protocol (ARP)** is a communication protocol used for discovering the link layer address (such as a MAC address) associated with a given internet layer address (typically an IPv4 address). This mapping is a critical function in the [Internet protocol suite](#).

Here is an example of ARP at work:

Two computers in an office (Computer 1 and Computer 2) are connected to each other in a local area network by Ethernet cables and network switches, with no intervening gateways or routers. Computer 1 has a packet to send to Computer 2. Through DNS, it determines that Computer 2 has the IP address 192.168.0.55.

To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up 192.168.0.55 for any existing records of Computer 2's MAC address (00:eb:24:b2:05:ac). If the MAC address is found, it sends an Ethernet frame with destination address 00:eb:24:b2:05:ac, containing the IP packet onto the link. If the cache did not produce a result for 192.168.0.55, Computer 1 has to send a broadcast ARP request message (destination FF:FF:FF:FF:FF:FF MAC address), which is accepted by all computers on the local network, requesting an answer for 192.168.0.55.

Computer 2 responds with an ARP response message containing its MAC and IP addresses. As part of fielding the request, Computer 2 may insert an entry for Computer 1 into its ARP table for future use.

Computer 1 receives and caches the response information in its ARP table and can now send the packet.

Question 2) At what layers of the OSI Model does the ARP protocol function?

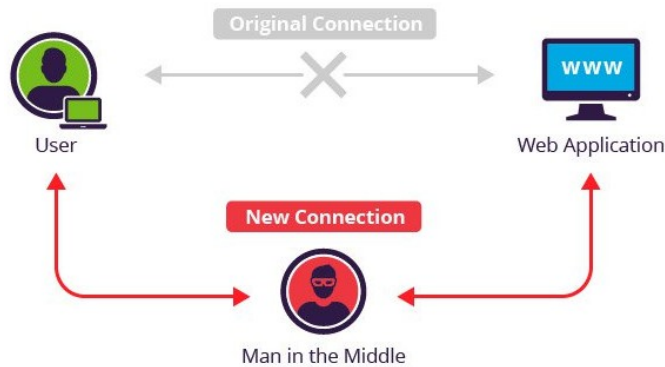
Man-in-the-Middle (MitM)

In cryptography and computer security, a **Man-in-the-Middle (MitM)** attack is an attack where the bad actor secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Please watch the following YouTube video which will discuss how to perform a MitM attack using ARP cache poisoning: <https://www.youtube.com/watch?v=2MBnX9-KIVU>

Question 3) What tool did he leverage on the Windows device to perform the MitM attack?

Here is a simple graphic depicting a typical Man-in-the-Middle attack:



Step 1 – MitM Attack using ARP Cache Poisoning (command line with arpspoof & tcpdump)

Complete the following steps to perform a MitM attack using the command line:

1. Turn on your KaliLinux, SeedUbuntu1, & SeedUbuntu2 virtual machines in VirtualBox.
Note: The KaliLinux device will represent the bad actor, the SEED vm's represent the innocent users.
2. On each of the 3 virtual machines, open a command prompt (terminal emulator) and run *ifconfig*.
3. Document the IP address and MAC address of the three virtual machines as you will need that info.
Note: The MAC addresses should all begin with 08:00:27. Funny how this organizationally unique identifier belongs to Cadmus Computer Systems. <https://www.macvendorlookup.com/browse/17160>
First 24 bits of the MAC address is supposed to belong to the hypervisor vendor – Oracle going cheap!
4. On the SEEDUbuntu1 vm, type *arp* at the command prompt (this displays the local arp cache).
Note: You probably don't see the SEEDUbuntu2 IP address and MAC address listed in the arp cache.
5. On the SEEDUbuntu1 vm, *ping* the SEEDUbuntu2 vm and then stop the pings by using *Ctrl^C*.
6. On the SEEDUbuntu1 vm, re-run the *arp* command and verify you now see SEEDUbuntu2 information.
Note: When pinging SEEDUbuntu2, an ARP request was performed to find SEEDUbuntu2's MAC address then the received information was placed in the arp cache and then the ping was successful.
7. On the SEEDUbuntu2 vm, type *arp* at the command prompt.
Note: You probably see the SEEDUbuntu1 IP address and MAC address listed in the arp cache due to the ping performed earlier between the two SEED vm's.
8. On the KaliLinux vm, type *arp* at the command prompt.
Note: You probably don't see either SEEDUbuntu IP addresses & MAC address in the arp cache.
9. On the KaliLinux vm, *ping* both the SEEDUbuntu1 & SEEDUbuntu2 vm's.
10. On the KaliLinux vm, re-run the *arp* command and verify you now see IP & MAC information for both.
11. On the KaliLinux vm, type the *sudo apt-get install dsniff* command.

Note: This will download a set of network traffic analysis tools and it contains the arpspoof tool.

12. On the KaliLinux vm, type *arpspoof -help* and examine the -i, -t, and -r switches.

13. On the KaliLinux vm, type *clear* to create some real estate on the screen.

Note: This command will come in handy many times during the lab.

14. On the KaliLinux vm, type *arpspoof -i eth0 -t <SEEDUbuntu1 IP> -r <SEEDUbuntu2 IP>*.

Note: Let this command continue to run as we want to continue the spoofing for a while.

This command is telling SEEDUbuntu1 that SEEDUbuntu2's MAC address is the KaliLinux MAC.

15. On the KaliLinux vm, open another command prompt window and type the following command:

arpspoof -i eth0 -t <SEEDUbuntu2 IP> -r <SEEDUbuntu1 IP>.

Note: Let this command continue to run as we want to continue the spoofing for a while.

This command is telling SEEDUbuntu2 that SEEDUbuntu1's MAC address is the KaliLinux MAC.

16. On the SEEDUbuntu1 vm, type *arp*. Do you see anything interesting in the arp cache?

Note: You should notice that the bad actor's MAC address is listed twice!

17. On the SEEDUbuntu2 vm, type *arp*. Verify the arp cache looks similar on the SEEDUbuntu2 vm.

18. On the SEEDUbuntu2 vm, *ping* the SEEDUbuntu1 vm. Did you get a response?

Note: Traffic is being sent to the bad actor's device. **However:** We forgot to setup one very important thing so let's fix things in the next step!!

19. On the KaliLinux vm, open a third command prompt and type the following command:

sysctl -w net.ipv4.ip_forward=1

Note: This will allow IP forwarding on the bad actor device. This is required to forward the traffic between the two user devices, otherwise when the traffic gets to the bad actor it is dropped.

20. On the SEEDUbuntu2 vm, type *ping <SEEDUbuntu1 IP>*. Did you get a response now?

Note: We are now passing traffic thru the bad actor device and the users are oblivious!

21. On the KaliLinux vm, on the last command prompt window opened, type *tcpdump -help*.

Note: The tcpdump command allows you to sniff and display all the traffic to the screen.

22. On the KaliLinux vm, type *tcpdump -i eth0*.

Note: You should see all the traffic passing thru the bad actor's ethernet interface (including those ARP requests you keep sending both user devices).

23. On the SEEDUbuntu1 vm, type *ftp <SEEDUbuntu2 IP>*. Enter the username (seed) and password (dees) to establish an FTP session on SEEDUbuntu2.

24. On the KaliLinux vm, stop the tcpdump by typing *Ctrl/C*. Now scroll up thru the tcpdump data and see if you find anything interesting...

Note: You should have been able to sniff the user and password used to establish that FTP session.

Screen Shot 1) [Take a snip of the screen to show you found the password used to FTP using tcpdump.](#)

25. On the KaliLinux vm, close the command prompt where the tcpdump was performed.
26. On the KaliLinux vm, stop both arpspoof commands by using *Ctrl/C* & close cmd prompt windows.
- Note:** When stopping each arpspoof, you will see it cleaning up & re-arping. Wait for the cmd prompt.
27. On the SEEDUbuntu1 vm, type arp and make sure the SEEDUbuntu2 vm is back to original information.
28. On the SEEDUbuntu1 vm, close all command prompt windows.
29. On the SEEDUbuntu2 vm, type arp and make sure the SEEDUbuntu1 vm is back to original information.
30. On the SEEDUbuntu2 vm, close all command prompt windows.

Imagine other types of data that could have been captured...Now let's try some graphical tools!!

Step 2 – Check to see if you have the Ettercap 0.8.2 known issue occurring in Kali 2019.4

Perform the following steps to determine if you need to upgrade your Ettercap software:

1. On your KaliLinux vm, open a command prompt and type the following command:
`cat /etc/*{release,version}` **Note:** Make a note of the KaliLinux version (i.e., 2019.4)
If you are running version 2020.1 of Kali Linux you may skip this step and go to Step 3 below.
2. On your KaliLinux vm, type *ettercap -Tqslq* and hit Enter.
Note: If you receive a message stating “0 hosts added to the hosts list...” then you will need to fix the version of Ettercap currently installed in your KaliLinux vm. If your hosts list populates with devices on your network, you are in luck and can continue to Step 3 below.
3. On your KaliLinux vm, type *ettercap --version* **Note:** Make a note of the Ettercap version (i.e., 0.8.2)
4. If you are running version 0.8.2, type *apt install ettercap-common ettercap-graphical* and hit Enter.
5. On your KaliLinux vm, type *ettercap --version* **Note:** Ensure you are now on Ettercap version (i.e., 0.8.3)
6. On your KaliLinux vm, re-run the *ettercap -Tqslq* command and hit Enter.
Note: Your hosts list should now populate with devices on your network, you can continue to Step 3.

Step 3 – MitM Attack using ARP Cache Poisoning (graphical with ettercap & wireshark)

Perform the following steps to perform a MitM attack using graphical tools:

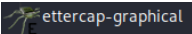
7. Turn on your KaliLinux, SeedUbuntu1, & SeedUbuntu2 virtual machines in VirtualBox (If needed).
8. The IP addresses and MAC addresses of the 3 devices should remain static (same as in Step 1 above).
9. On the KaliLinux vm, open a command prompt and type the following command:

`sysctl -w net.ipv4.ip_forward=1`

Note: This will ensure IP Forwarding is ON.

10. On the KaliLinux vm, close the command prompt as this step in the lab will use the graphical interface.

11. On the KaliLinux vm, Select the Kali icon in the upper left corner. 

12. On the KaliLinux vm, Select the Ettercap-Graphical tool in the Sniffing & Spoofing folder. 

13. On the KaliLinux vm, Select the check mark in the upper right corner to accept the settings.

Note: Unified sniffing should begin in the lower window of the Ettercap tool.

14. On the KaliLinux vm, Select the Ettercap menu (three dots), Select Hosts, and Select Scan for hosts.

Note: A number of hosts should have been added to the hosts list.

15. On the KaliLinux vm, Select the Ettercap menu (three dots), Select Hosts, and Select Hosts list.

16. On the KaliLinux vm, Right-click the SEEDUbuntu1 IP in the hosts list and Select Add to Target 1.

Note: You should see that IP added to Target 1 in the lower window.

17. On the KaliLinux vm, Right-click the SEEDUbuntu2 IP in the hosts list and Select Add to Target 2.

Note: You should see that IP added to Target 2 in the lower window.

18. On the KaliLinux vm, Select the MitM menu (Globe Icon), Select ARP Poisoning, ensure sniff remote connections is checked and Click OK.

Note: You should see the ARP poisoning happening now in the lower window.

19. On the SEEDUbuntu2 vm, type *arp*.

Note: You should notice that the bad actor's MAC address is listed twice!


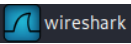
20. On the SEEDUbuntu1 vm, type *arp*. Verify the arp cache looks similar on the SEEDUbuntu2 vm.

21. On the SEEDUbuntu1 vm, type *ftp <SEEDUbuntu2 IP>*. Enter the username (seed) and password (dees) to establish an FTP session on SEEDUbuntu2.

22. On the KaliLinux vm, watch the window at the bottom of the Ettercap tool.

Note: You should see the user and password used to establish that FTP session right on the screen.

Screen Shot 2) Take a snip of the screen to show you found the password for the FTP session using ettercap.

23. On the KaliLinux vm, Select the Kali icon in the upper left corner. 
24. On the KaliLinux vm, Select the Wireshark tool in the Sniffing and Spoofing folder. 
25. On the KaliLinux vm, Start the Wireshark capture by selecting the Blue Shark fin on the toolbar.
26. On the SEEDUbuntu1 vm, type *ftp <SEEDUbuntu2 IP>*. Enter the username (seed) and password (dees) to establish an FTP session on SEEDUbuntu2.
27. On the KaliLinux vm, Stop the Wireshark capture by selecting the Red Box on the toolbar.
28. On the KaliLinux vm, examine the data in the Wireshark capture and see what you find.

Note: You should see the user and password used to establish that FTP session.

Screen Shot 3) Take a snip of the screen to show you found the password used to FTP using Wireshark.

29. On the KaliLinux vm, Start the Wireshark capture by selecting the Blue Shark fin on the toolbar. Select Continue without saving so the previous capture is deleted.
30. On the SEEDUbuntu2 vm, type *telnet <SEEDUbuntu1 IP>*. Enter the username (seed) and password (dees) to establish a telnet session on SEEDUbuntu1.
31. On the KaliLinux vm, Stop the Wireshark capture by selecting the Red Box on the toolbar.
32. On the KaliLinux vm, examine the data in the Wireshark capture and see what you find.

Note: You should see the user and password used to establish that telnet session.

Question 4) Why was the telnet password harder to obtain in the Wireshark data?

Conclusion

As you can see, it is not very difficult to perform a MitM attack by poisoning the ARP cache. This should show you how important it is to ensure all sensitive information is encrypted in transit while on the network. This MitM approach can work on any wireless network; hence, the need to keep your router secure and the encryption used to connect devices to your home wireless network at the highest level available. This also shows you why you should NOT use those public wireless networks or hotel networks unless you are sure your communication is encrypted!

Now just a few more questions and you are all done...

Question 5) Can you perform a MitM Attack using the APR Cache Poisoning approach if the devices are on separate networks (separated by a router)?

Question 6) Can you poison the ARP cache using IPv6? Why?

Question 7) List two ways to prevent the MitM Attack using ARP Cache Poisoning?