

Lab 8.2.1 - ARP Spoofing for DoS & AiTM Attacks

Objective: Investigate the methods of using Arp Poisoning to affect the CIA of network devices and data.

Part 1

Watch this video demonstration of a working attack that uses ARP Spoofing to perform a DoS attack.

<https://vimeo.com/904151265>

Part 2

Using the CYBER.ORG Range, follow instructions below to try ARP Spoofing and examine how it is stopped by network security.

Instructions:

- Go to CYBER.ORG Range (<https://apps.cyber.org>)
- Click on the **Range tab**, then launch **Kali, Ubuntu, Windows7**
- Once the status changes to booted, open **Windows 7**.
- In the bottom left, click the Start button and search for Network and Sharing Center.
- In the pop-up window, select the Public Network and change it to Home.

Examine normal communications in the network.

1. In Kali, open a terminal by clicking the black icon on the top toolbar.

Gather MAC address information for all devices in the network:

- Type **ping** <Ubuntu IP Address> **-c 5**
- Type **ping** <Windows 7 IP Address> **-c 5**
- Type **arp -a**
- Type **ifconfig**

From the results, fill in the chart below

OS Name	IP Address	MAC Address
Ubuntu		
Windows 7		
Kali		

2. Move to **Ubuntu**. Open a terminal and use the command **sudo wireshark**.

In the Wireshark top toolbar, click the “blue fin icon” to begin capturing.

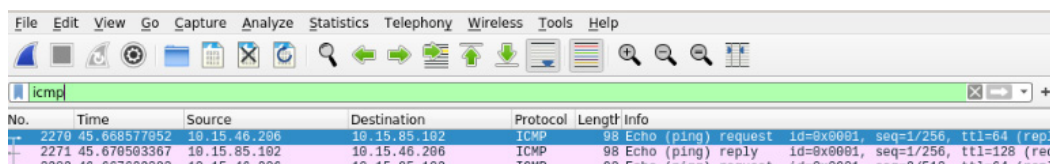


3. Open a terminal by clicking the black icon on the left desktop toolbar.

Type **ping** <Windows 7 IP Address> **-c 5**

4. When the ping is completed, go to Wireshark and stop the capture by clicking the red box in the top toolbar. Important: there will be a lot of packets that are not relevant. These come from basic network activity and from being connected to the Internet.

Examine the packets to observe normal ICMP packet delivery for the ping. To see only the ICMP packets, in the Wireshark filter bar type: **icmp**



Important – clear the filter by clicking the X in the right corner of the filter bar.

Setup ARP spoofing

Arpspoof is an ARP poisoning tool. Syntax:

arpspoof -i <interface on your device> **-t** <ip address of target host you want to poison> <ip address you want to intercept packets for>

1. START Wireshark again on Ubuntu by clicking the blue fin and then select “Continue without Saving”.
2. START Wireshark on Kali with this command in Terminal:
 - **sudo wireshark**
 - Leave this terminal window open while using Wireshark
 - Once Wireshark is open, click the blue fin to begin capturing packets
3. Use **arpspoof** on Kali to poison the Ubuntu arp cache. This will send ARP packets telling the Ubuntu device that packets for the Windows 7 device should go to Kali instead.
 - In Kali open a second Terminal and type:
sudo arpspoof -i eth0 -t <Ubuntu IP address> <Windows 7 IP Address>
 - Let the program run until you have about 10-12 packet sent. Stop arpspoof by clicking **CTRL+C**.
4. STOP Wireshark on both Ubuntu and Kali.
5. In the Kali Wireshark filter bar type **arp**. Paste a screenshot below of the ARP reply packets produced by arpspoof with false MAC address information.

6. In the Ubuntu Wireshark filter bar type **arp**. Paste a screenshot below of any ARP packets.

7. In Ubuntu open a Terminal to examine the arp cache:

Type: **arp**

Are there any IP addresses that have the same MAC address?

Attempt to send packets between the Ubuntu and Windows7 devices

1. Move to Ubuntu to ping the Windows 7 machine:

- Type **ping <Windows 7 IP Address> -c 5**
- Notice that the ping succeeds. Security on the network switches keeps track of MAC and IP addresses for all connected devices. It blocks any packets that contain incorrect or duplicated addresses.

Close all terminal and Wireshark windows.

Part 3

Analyze a Wireshark capture of an ARP Poisoning attack. Use the information in this table about network devices:

OS Name	IP Address	MAC Address
Windows 7	192.168.100.101	00:50:56:8f:62:8a
Ubuntu	192.168.100.102	00:50:56:8f:48:b0
Metasploitable	192.168.100.200	00:50:56:8f:18:6b
Kali	192.168.100.103	00:50:56:bd:1d:d5

On the Kali device open a Terminal and use these commands:

- **sudo wireshark**
- In Wireshark in the top toolbar click **File | Open** and navigate to:
/home/kali/CourseFiles/IntroCybersecurity/
- Select **ARP.pcapng** and click Open

Questions – for each answer provide packet info to support your answer:

1. Which device is the attacker?
2. Which devices are the two victims?
3. What are the username and password that were intercepted?
4. Bonus: why is it NOT possible to perform an ARP poisoning attack from this network to a device with IP address 172.1.2.3?

Closure

1. **Spoofing as a DoS:** With ARP Poisoning, packets from the Ubuntu device that are intended for the Windows 7 device would instead be delivered to the Ubuntu device. This would create a DoS between Ubuntu and Windows 7 because the Kali device is not forwarding the packets after receipt. It would be as if Kali had put up a wall between Ubuntu and Windows 7 so there wouldn't be any successful packet exchange.
 - What does DoS stand for?
2. **Spoofing as an AiTM to steal or modify data:** The Kali device can capture packets sent by Ubuntu to Windows 7. After reading or modifying the data, Kali can then use IP forwarding to send the packets on to Windows 7. Using these tools, the Ubuntu device could intercept and forward packets back and forth between the two devices.
 - What does AiTM stand for?