M Sameer Malik

m.sameer.malik113@gmail.com

What’s inside?

This lab aims to provide information on how small misconfigurations found in most networks can empower an attacker to monitor the traffic in that network this lab also provides ways to mitigate those misconfigurations.

Cyber security lab

Network Exploitation

Table of Contents

[**Lab - On-Path Attacks with Ettercap** 2](#_Toc203501122)

[Objectives: 2](#_Toc203501123)

[Requirements: 2](#_Toc203501124)

[Procedure: 2](#_Toc203501125)

[Note: 2](#_Toc203501126)

[Disclaimer: 2](#_Toc203501127)

[Part 1- ARP Poisoning: 3](#_Toc203501128)

[Practical: 3](#_Toc203501129)

[Part 2 – Performing On-Path (MITM Attacks) 6](#_Toc203501130)

[Practical: 6](#_Toc203501131)

[Analysis- Phase: 7](#_Toc203501132)

[Mitigation: 7](#_Toc203501133)

# **Lab - On-Path Attacks with Ettercap**

## Objectives:

* Get familiarity with Ettercap.
* Realize how most networks can be exploited by On-Path Attack
* Thoroughly learn and apply the different terms such as ARP spoofing, ARP poisoning, DNS poisoning, Mac spoofing etc.
* Use Wireshark to analyze packets captured via On-Path Attacks.
* Learn the mitigations for these attacks.

## Requirements:

1. kali VM
2. Network

## Procedure:

In Part 1 use the GUI for arp poisoning. Also attach screenshot for each step.

In Part 2 use CLI for on-path attacks, intercept the traffic and inspect the packets via Wireshark also check each packet in detail for source and destination.

## Note:

Always use authorized environment for testing purposes!

## Disclaimer:

The techniques taught in this lab are for educational purposes only the author shall not be responsible for the misuse of any of the following techniques.

## Part 1- ARP Poisoning:

ARP Poising is the process of spoofing your mac address similar to that of a device with which the victim communicates in order to route the traffic via attacker machine.

## Practical:

Start Ettercap as a root user use **ettercap -G** for graphical user interface.

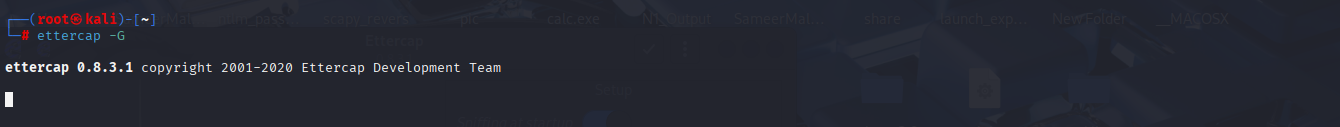


Figure 1

Select your required interface as primary interface. For this lab I am using eth0. Note I am performing this lab on an authorized live network you can also create a topology and set up devices there and then proceed accordingly.



Figure 2

Click the tick and then select the hosts/target option for setting up your required targets! All the traffic other than the compromised targets will communicate normally.



Figure 3

Click the scan button if you don’t see any targets this will refresh the targets and show you the available options. Then add the targets , these are the we victims you want to conduct On-Path Attacks on.

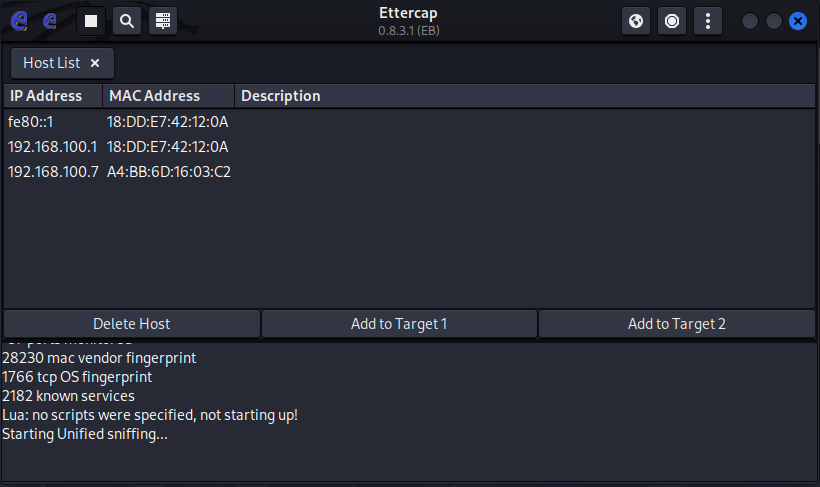


Figure 4

Click on the target before adding it to target 1 and target 2.

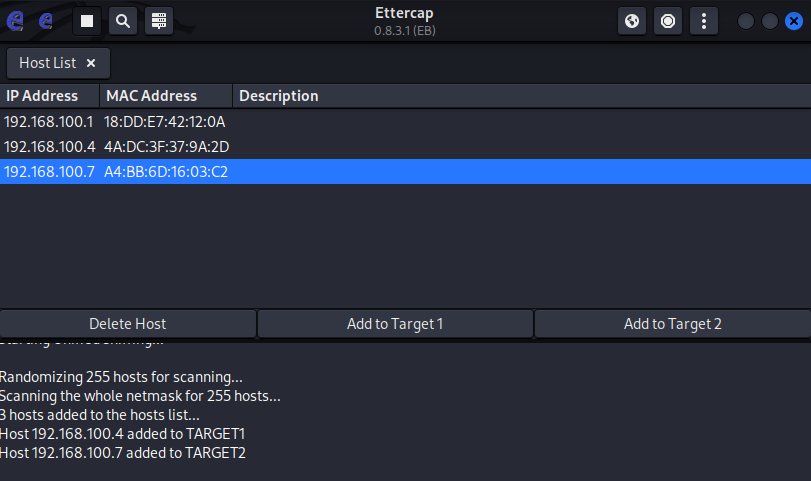


Figure 5

After that you will be prompted with something like figure 6, make sure the check the first box and click ok!

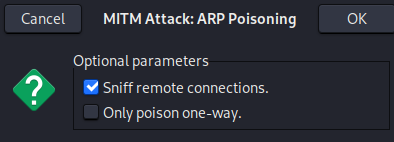


Figure 6

This concludes the part 1 of our lab now if we check the ip of connected devices in the kali cli using the **ip neighbour** commandwe will see the repeated mac address this verifies that our attack is working successfully and now we are spoofing the mac address of client which the victim intending to communicate with now we can intercept the traffic using the On-path attack. Check the figure 7 for seeing ip neighbour command in action.



Figure 7

## Part 2 – Performing On-Path (MITM Attacks)

These types of attacks involve intercepting the traffic b/w victim and default gateway.

## Practical:

First of use Ettercap with root privileges use the command shown in the screenshot below.

**ettercap -T -q -i eth0 –-write <file name> arp /<ip>//**

The breakdown of this command is:

-T = terminal

-q = quiet

-i = interface

--write = for writing the output

arp/<ip>// = specify the ip

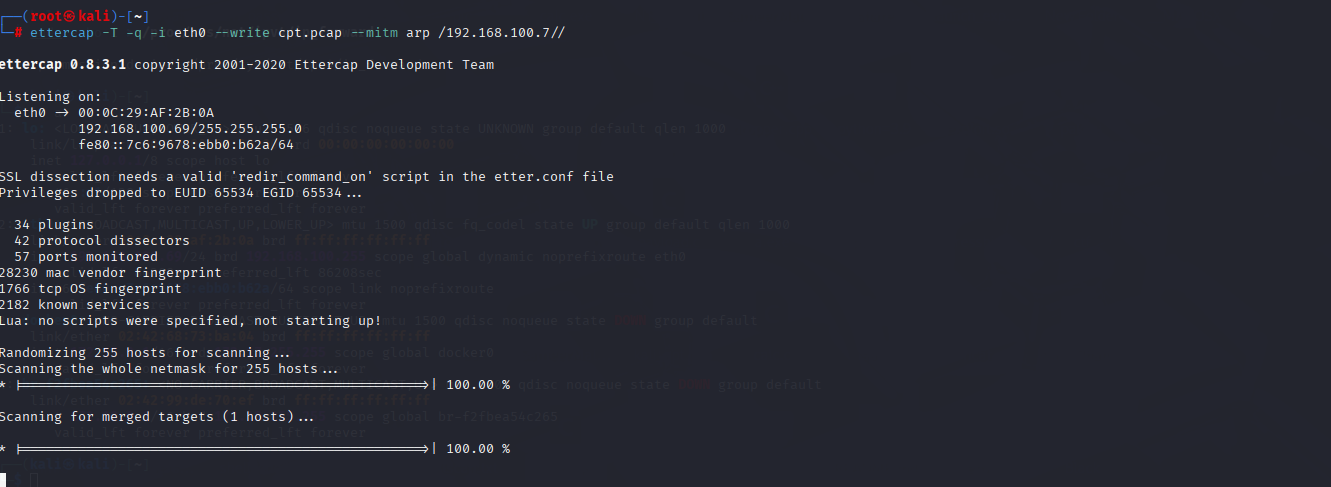


Figure 8

After capturing the packets for a while hit ctrl c. This will stop the packet capture and save the output to a file in present working directory.

## Analysis- Phase:

In this phase we will Analyze the traffic captured by On-Path Attack.

Use the **wireshark <file name>** to open the captured traffic in wireshark as demonstrated in figure 9.



Figure 9

Click specific packets in wireshark for thoroughly inspecting them observe how these packets are being intercepted by attacker machine!

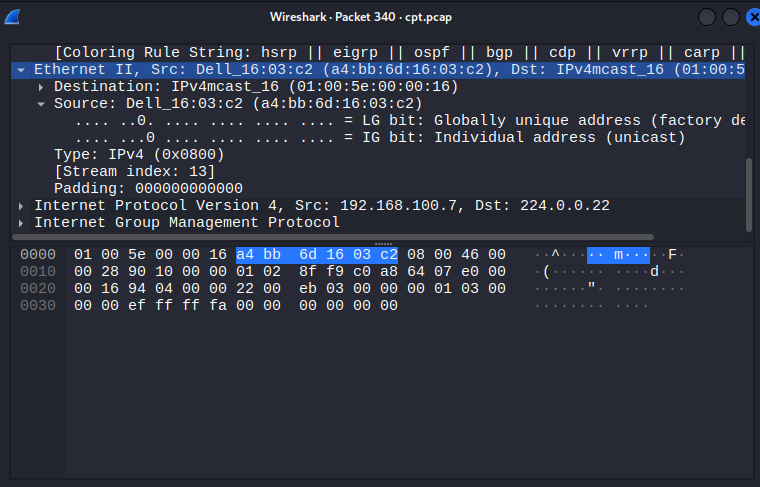


Figure 10

## Mitigation:

Most networks are vulnerable to this type of attacks thus it is important to correctly configure this misconfiguration by adding rules such as:

* Dynamic ARP resolution.
* Not allowing duplicate mac and ip’s to prevent Mac spoofing and Ip spoofing.