**ASSIGNMENT-5**

**USING ARP SPOOFING TO POISON NETWORK AND DETECT USING WIRESHAK**

**Subject Name:** Cryptography and Network Security

**Subject Code:** CS6008

**Module:** 4

**Name:** Sreeratcha B

**Reg. No:** 2019103585

**Date:** 03-06-2022

**Aim:** Using ARP spoofing to poison network and detect using wireshark.

**Tools involved:**

* Kali linux VM
* Ettercap
* Wireshak

**Problem Description:**

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.

Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn’t know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.

The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.

**Input:** The user visits any http link and enters credentials.

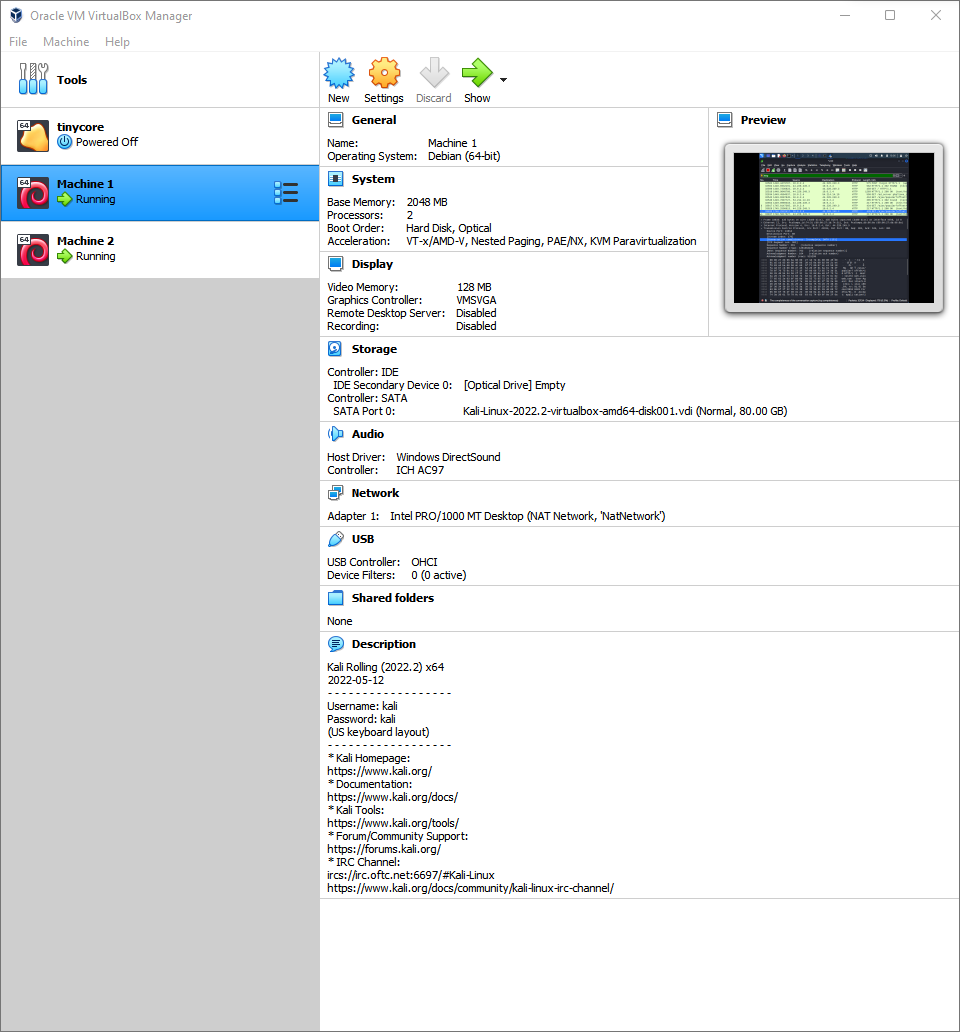
**Output:** Username and password.

**Screenshots:**

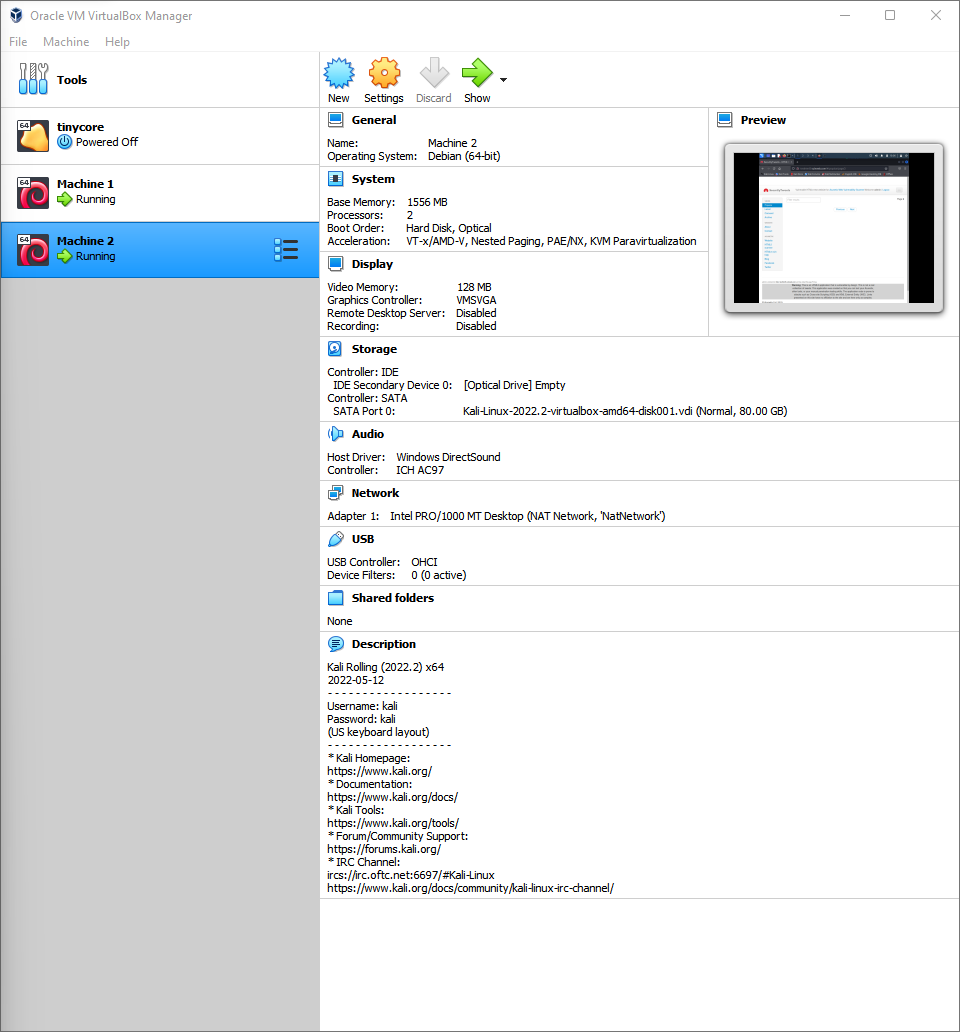
Two Kali Linux machines are used to do ARP spoofing.

One machine act as the attacker and the other one is the user.

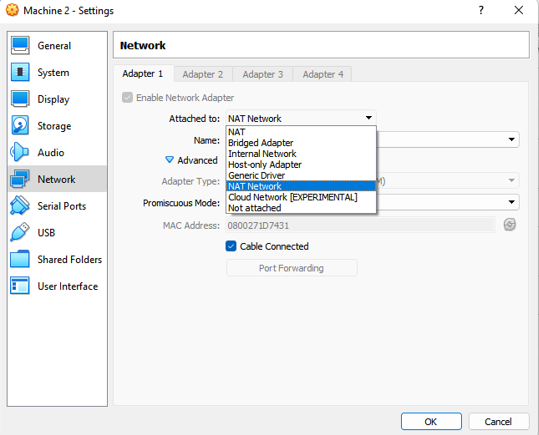
Attacker (Machine-1)



User (Machine-2)

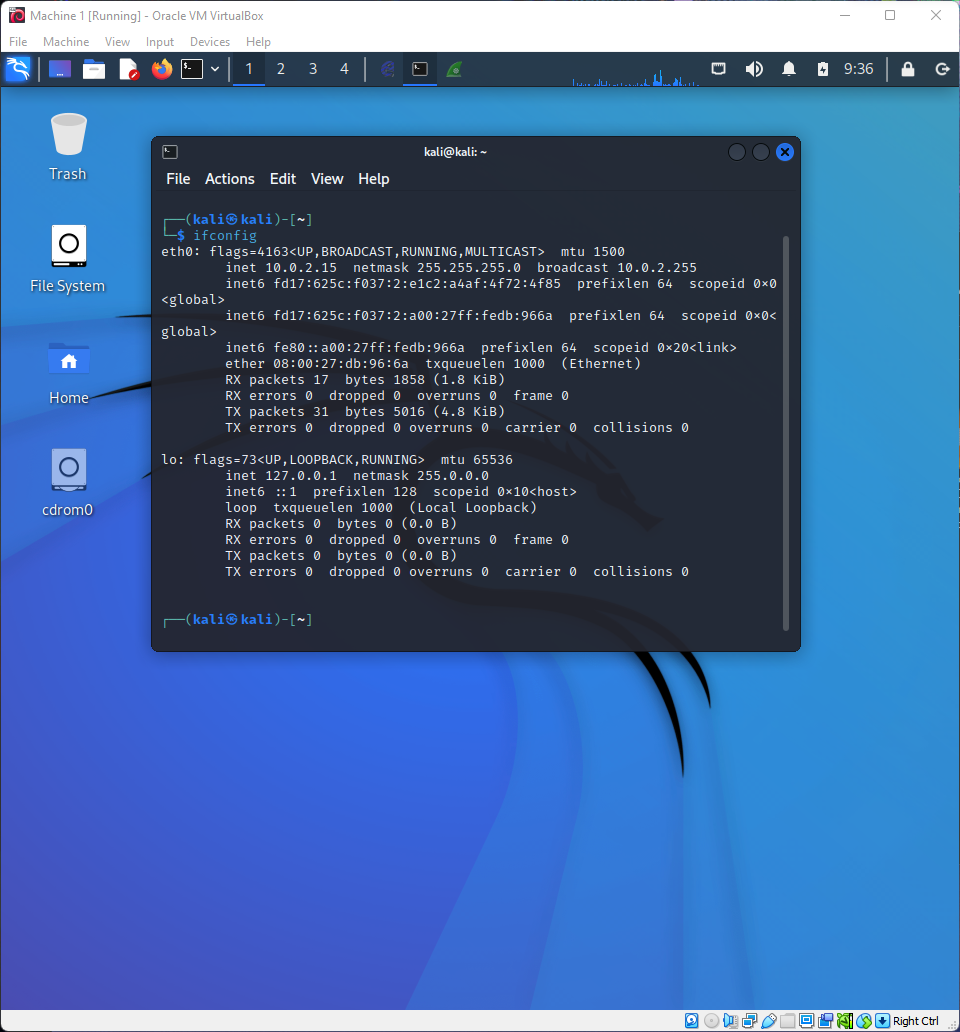


NAT network is used.

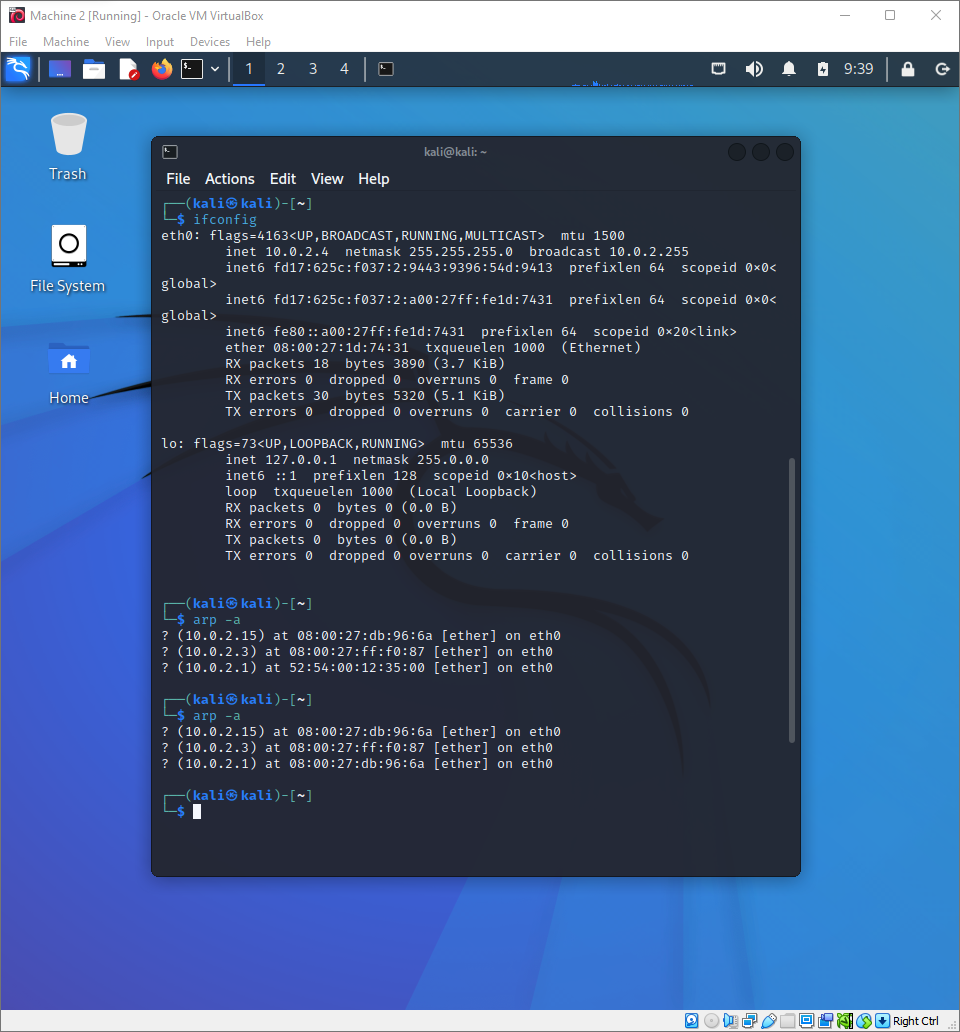


Using the ifconfig command we can view the IP address, mac address and default gateway.

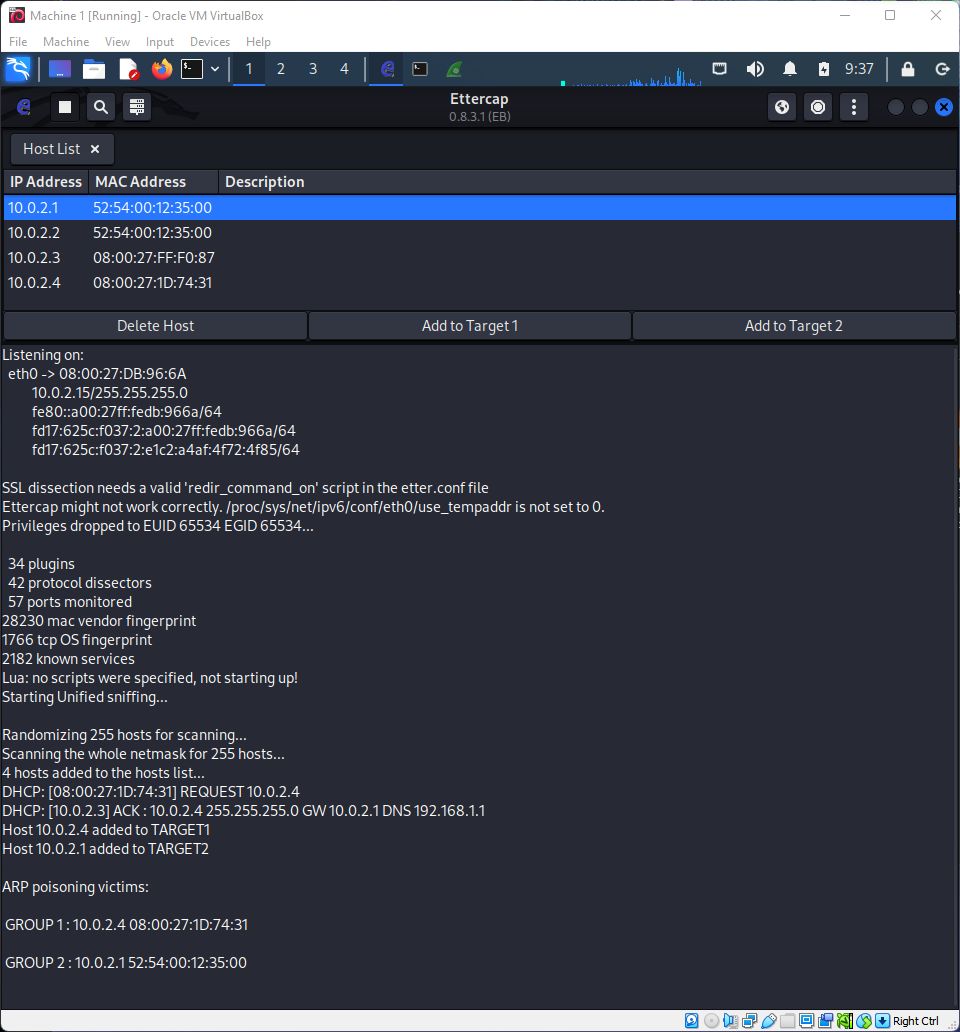
Machine-1



Machine-2



Ettercap software is used to do ARP Spoofing. This software is used to scan and display the list of hosts and perform poisoning.



IP address of machine-1: 10.0.1.15

MAC address: Ends with 6a

IP address of machine-2: 10.0.2.4

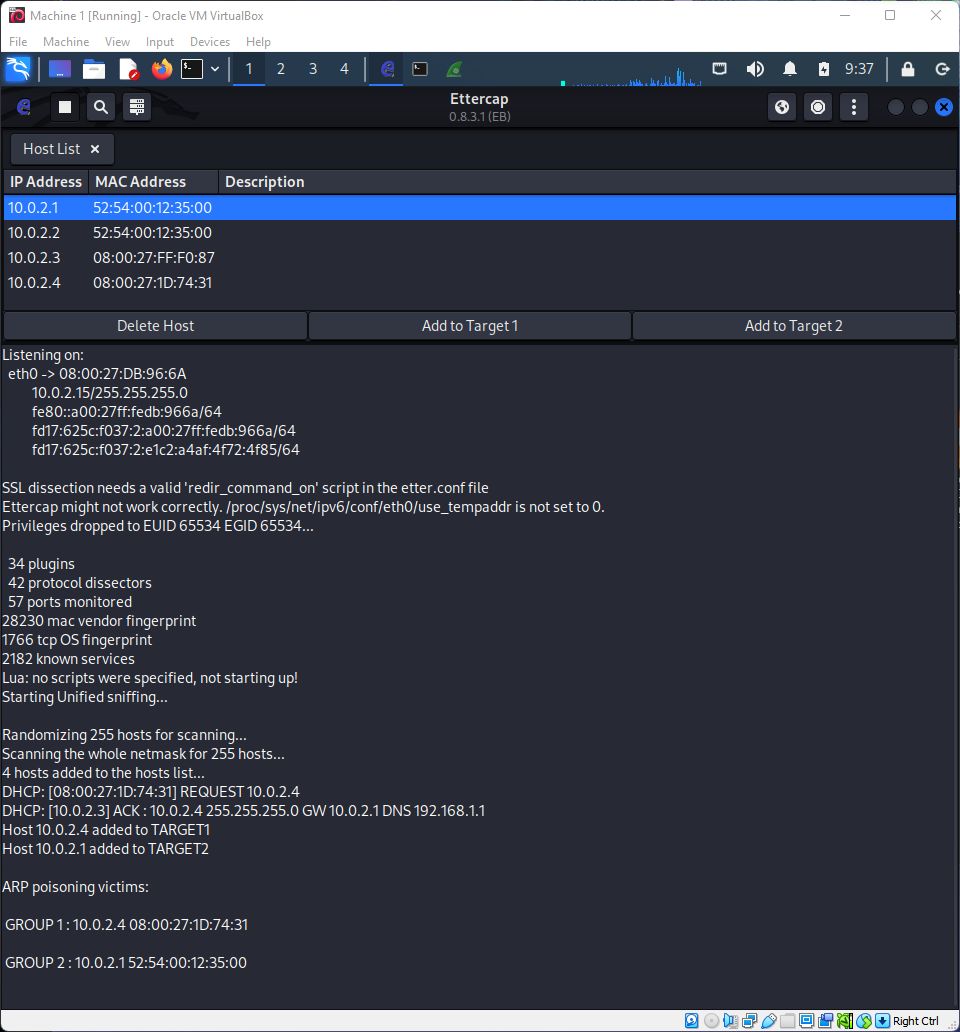
MAC address: Ends with 31

IP address of router: 10.0.2.1

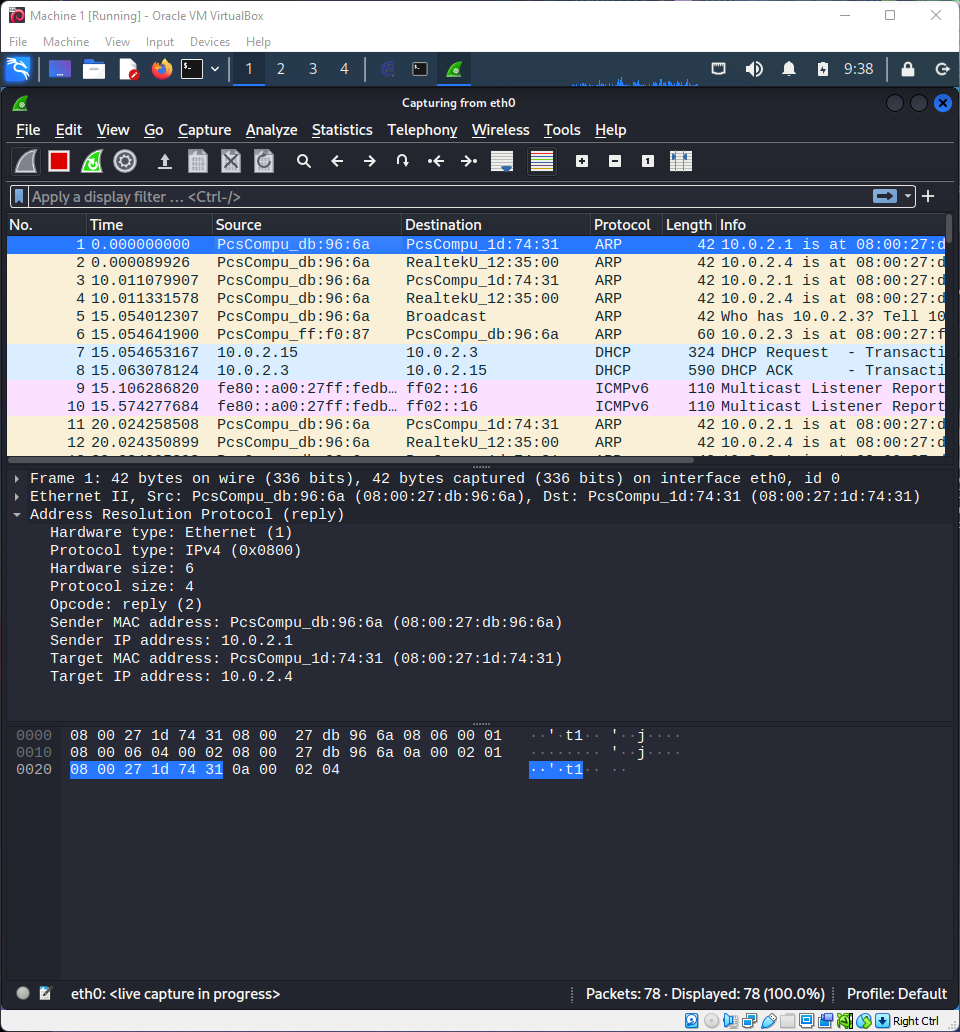
MAC address: Ends with 00

In the Ettercap the user on which attack is performed is added to target-1 and the router is added to target-2.

ARP poisoning can be performed on a button click using Ettercap.

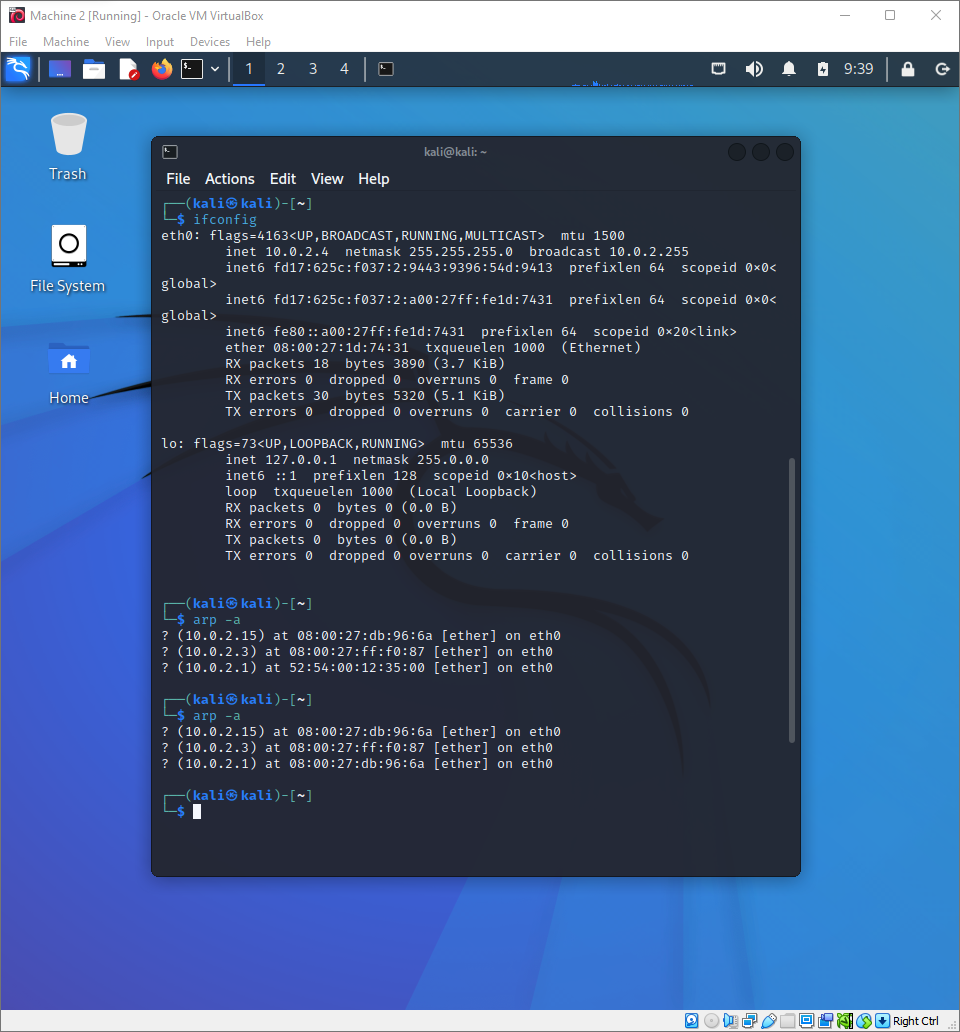


We can see the traffic getting directed to attacker’s machine.



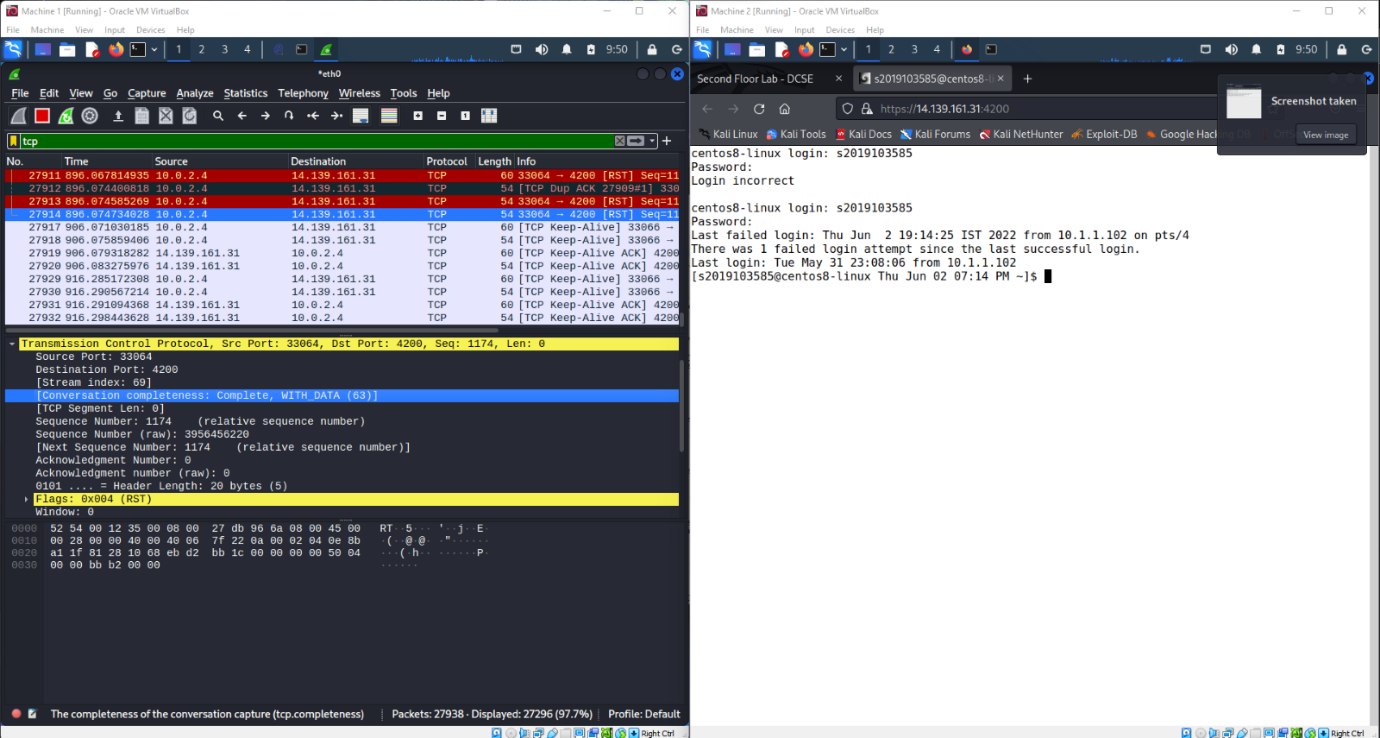
After poisoning we can observe that the ARP cache has mapped the router’s IP address with the MAC address of the attacker’s machine.

In this way the ARP cache is poisoned.



Example-1

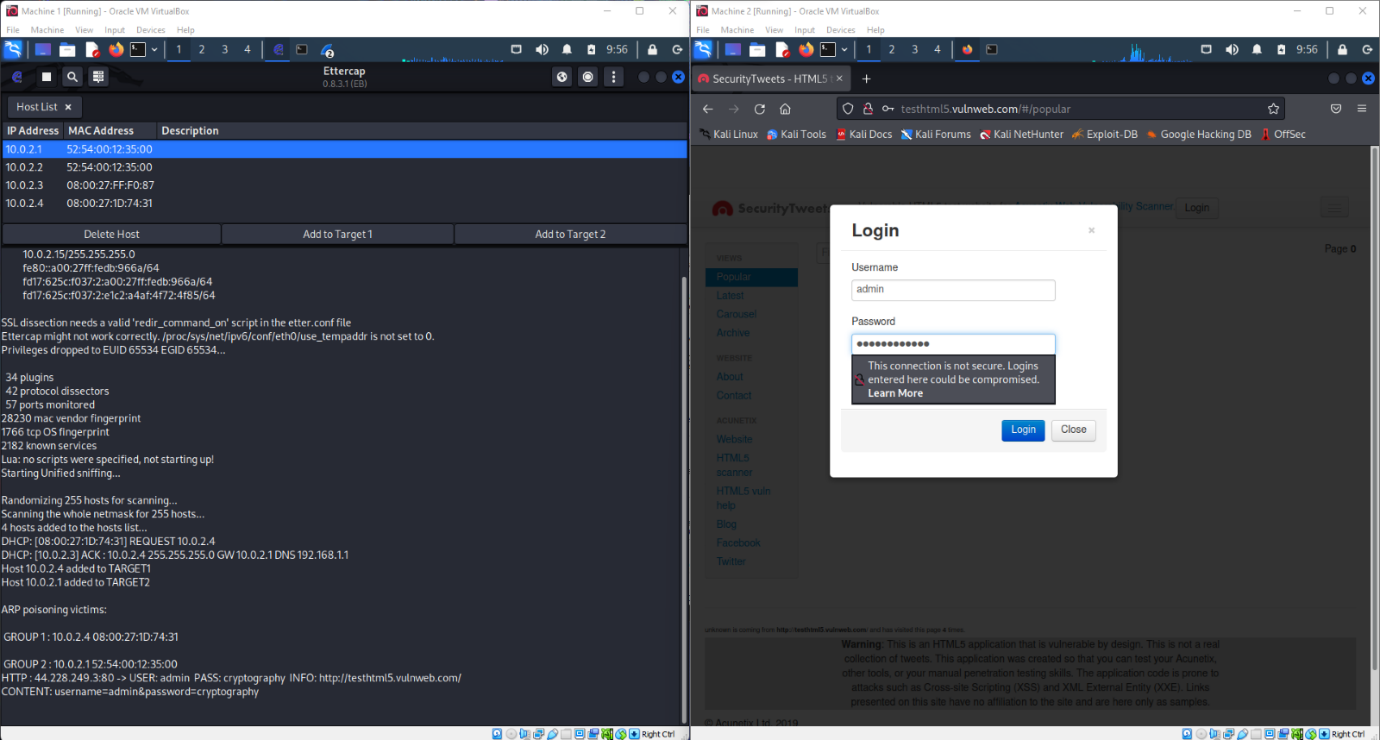
We can see the user accessing the server in their machine. Since it’s a https link we can’t read the username and password.



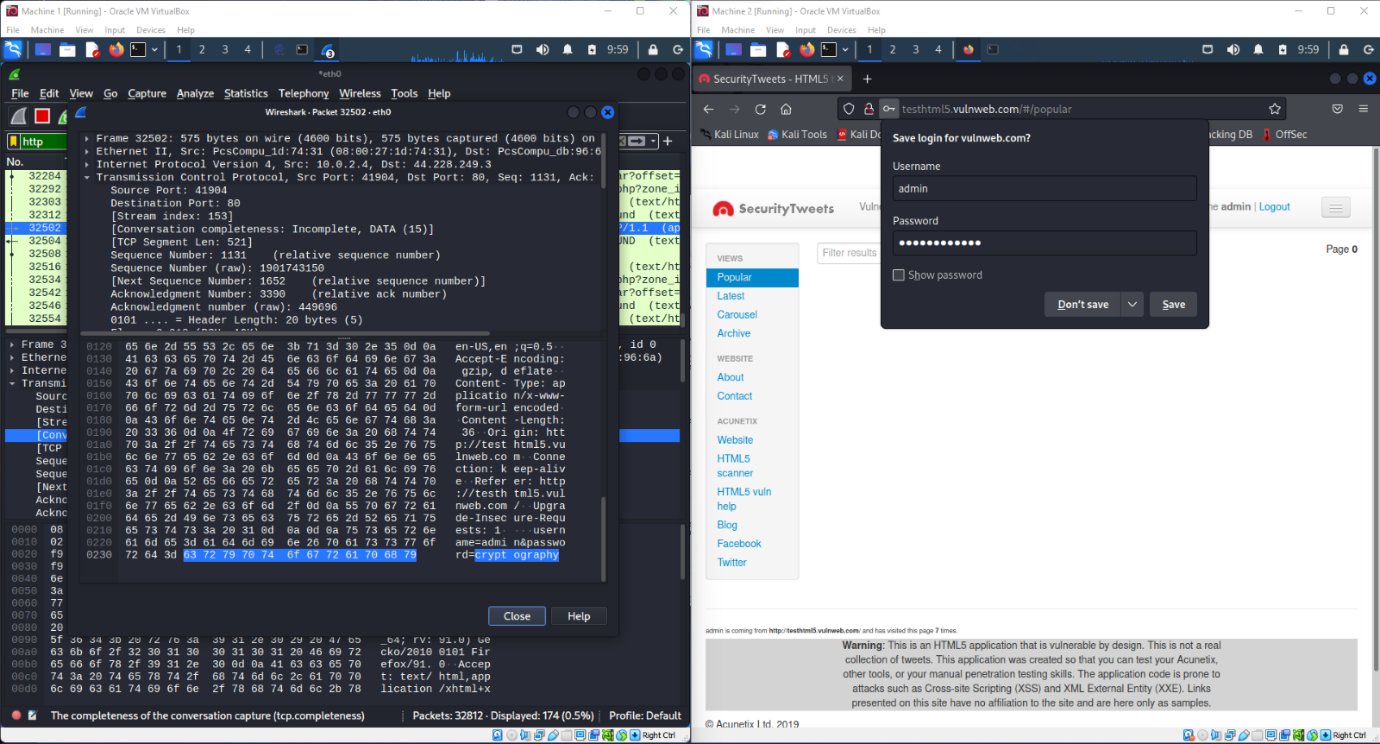
Example-2

In this example a http site is accessed and the username and password are entered. The attacker can access those since http is not secure.

Ettercap:



Wireshak output:



Username: admin

Password: cryptography

These are the credentials obtained through poisoning.