ARP SPOOFING

ARP spoofing, also known as ARP (Address Resolution Protocol) cache poisoning or ARP poisoning, is a technique used by attackers to manipulate the ARP tables on a local area network (LAN). ARP is a protocol used to map an IP address to a physical MAC (Media Access Control) address on a network.

Here's a brief overview of how ARP works:

ARP Request:

When a device on a network wants to communicate with another device, it sends out an ARP request to find the MAC address associated with a specific IP address.

ARP Reply:

The device with the corresponding IP address responds with its MAC address.
ARP spoofing involves sending fake ARP messages to link a different MAC address with an IP address.

There are two common types of ARP spoofing attacks:

Man-in-the-Middle (MITM) Attack:

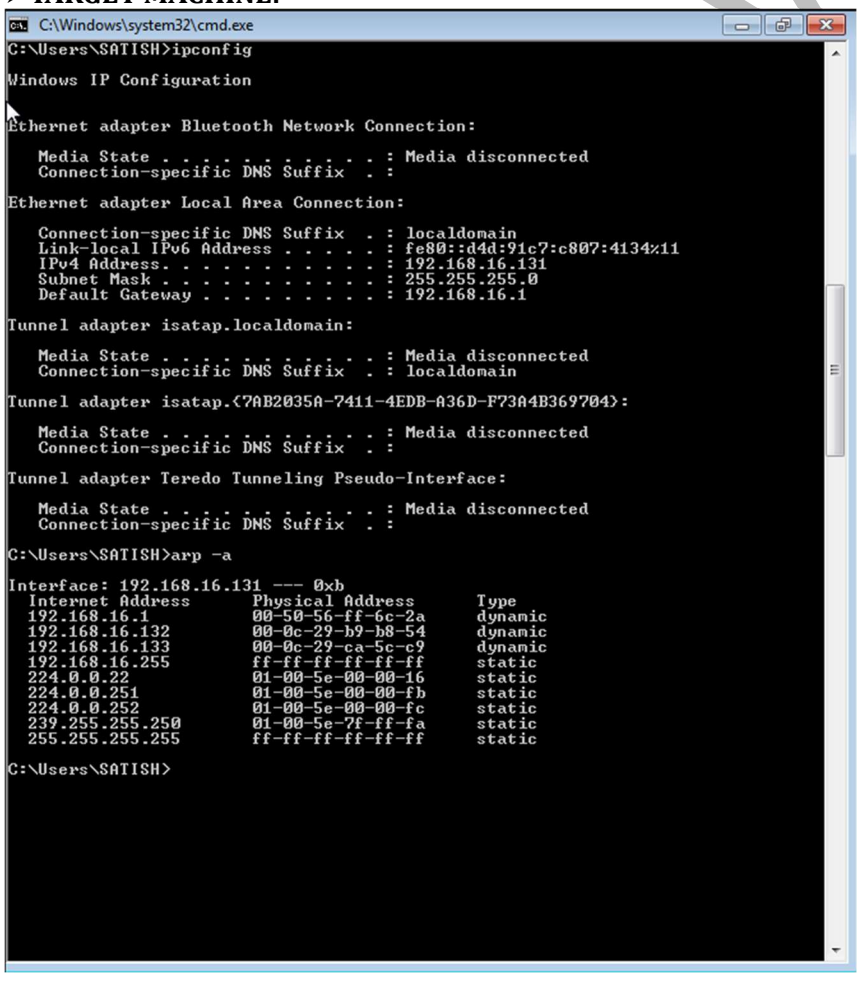
In a MITM attack using ARP spoofing, an attacker intercepts communication between two parties by placing themselves between them. The attacker sends false ARP replies to both parties, causing them to associate the attacker's MAC address with the IP address of the other party.

Denial-of-Service (DoS) Attack:

In a DoS attack using ARP spoofing, an attacker sends out fake ARP replies with incorrect MAC addresses, causing confusion in the ARP tables of the targeted devices. This can lead to network disruption and loss of connectivity.
ARP spoofing can be used for various malicious purposes, such as eavesdropping on network traffic, stealing sensitive information, or conducting other attacks like session hijacking.

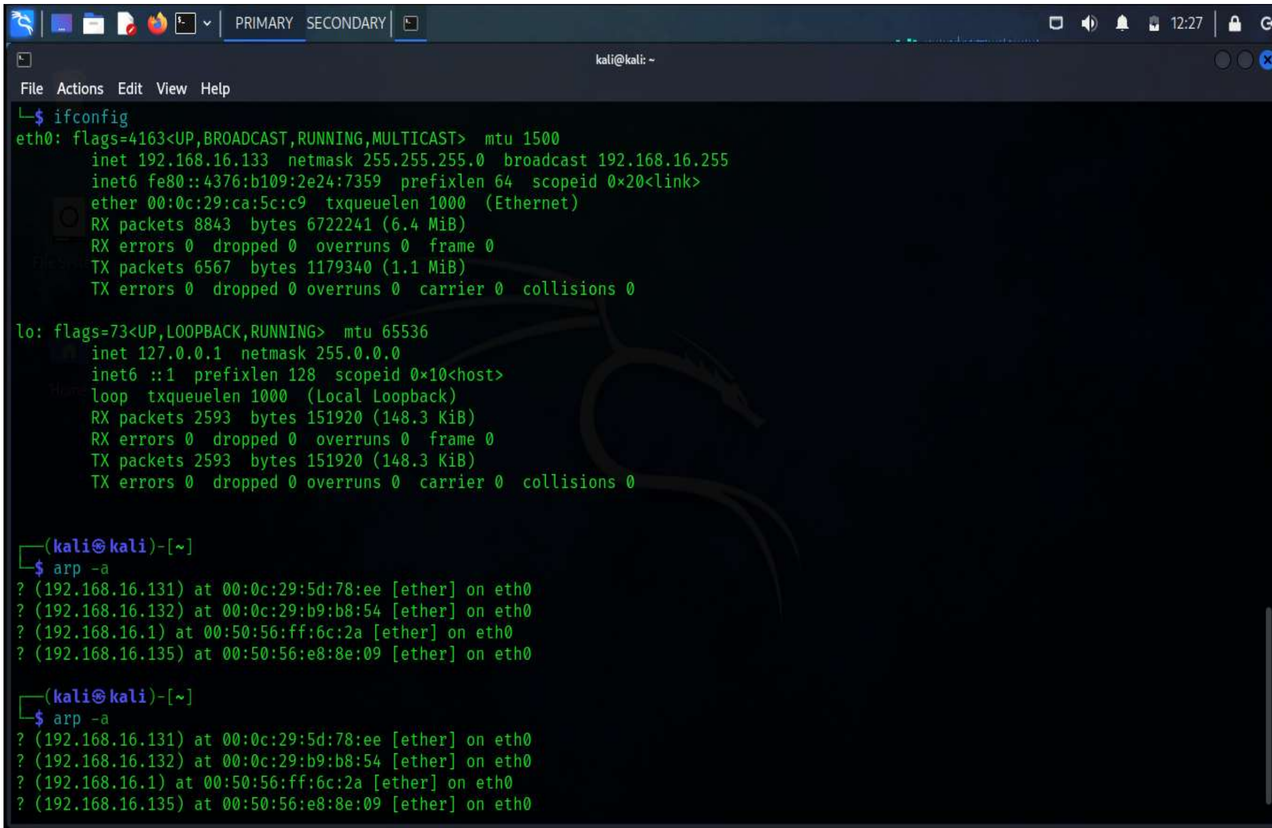
IMPLEMENTATION:

➢ **TARGET MACHINE:**



VIROTHI

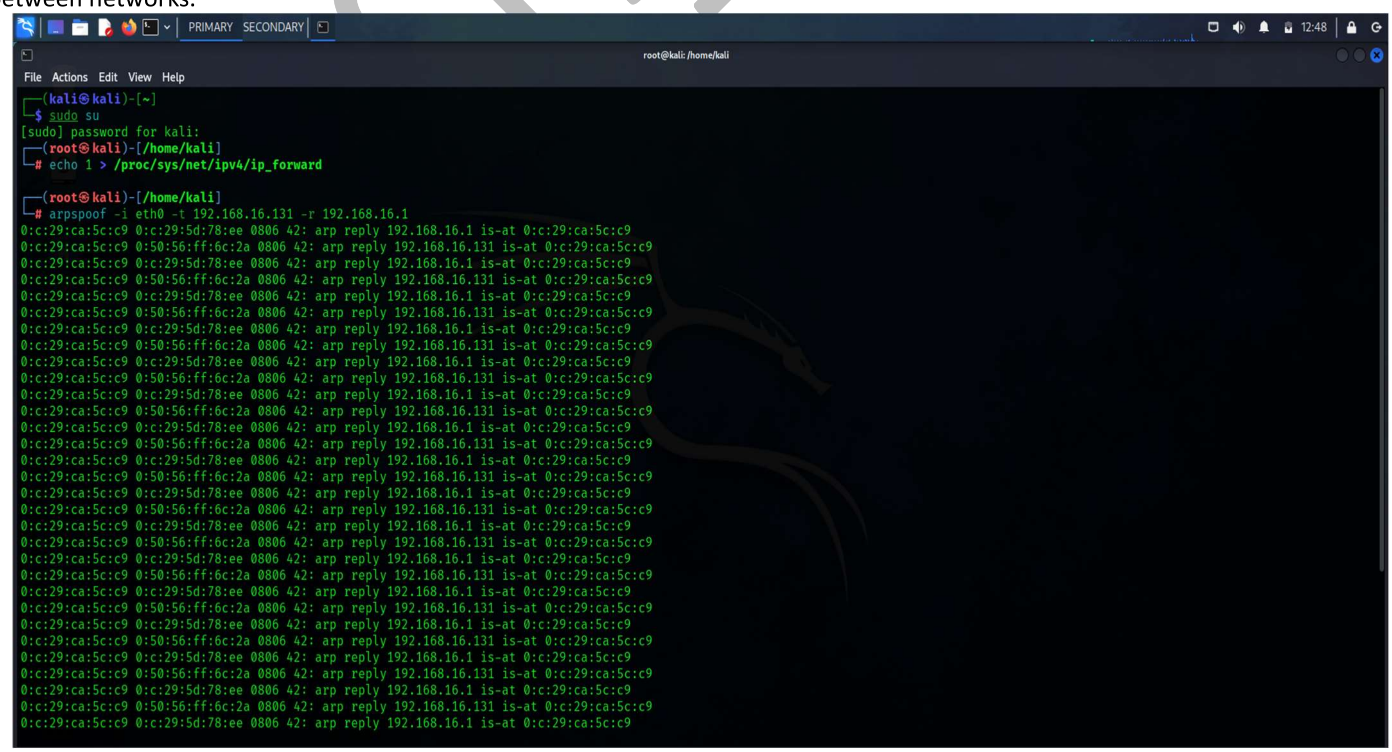
➢ATTACKER'S MACHINE:



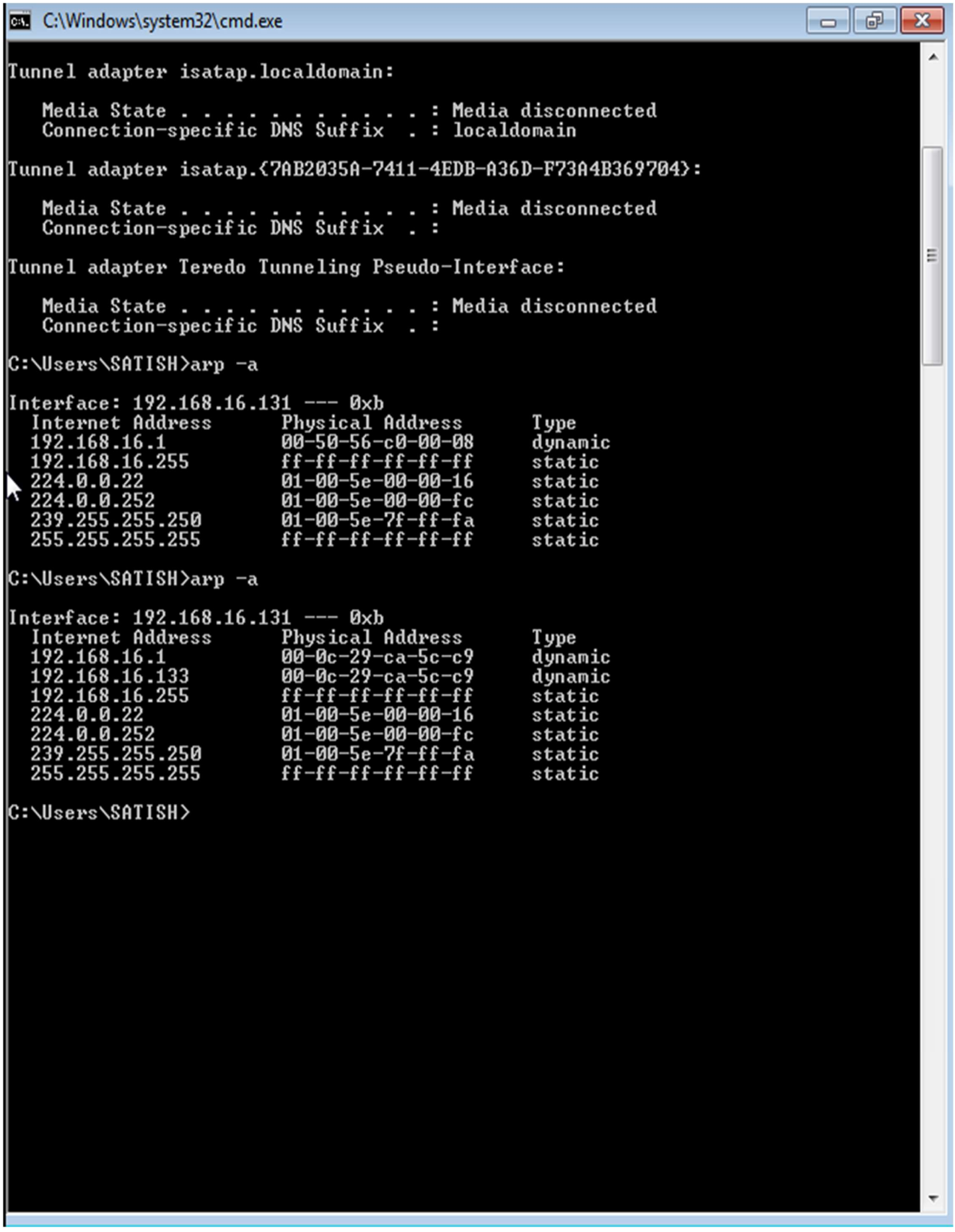
➢<u>CHANGING THE DEFAULT GATEWAY OF TARGET USING ARPSPOOF:</u>

IP Forwarding:

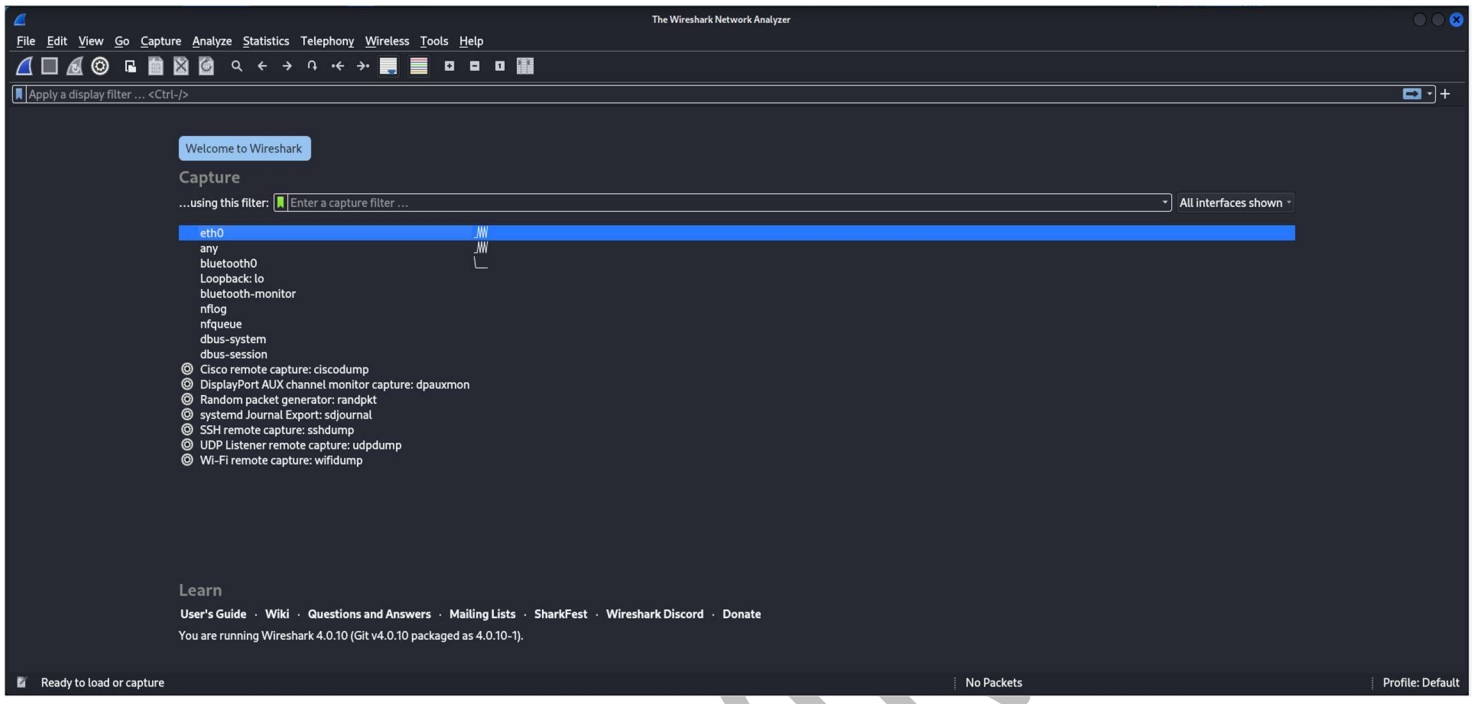
IP forwarding is a feature of a computer's network stack that allows it to pass network traffic from one network interface to another. When IP forwarding is disabled (set to 0), the system will not pass traffic between different interfaces, effectively acting as a standalone system. When IP forwarding is enabled (set to 1), the system can route packets between its network interfaces.
So, when you execute the command echo 1 > /proc/sys/net/ipv4/Ip forward, you are setting the value of Ip forward to 1, enabling IP forwarding on the system. This is commonly done when the system is functioning as a router or gateway between different networks. Enabling IP forwarding allows the system to forward packets between different network interfaces, facilitating the flow of traffic between networks.

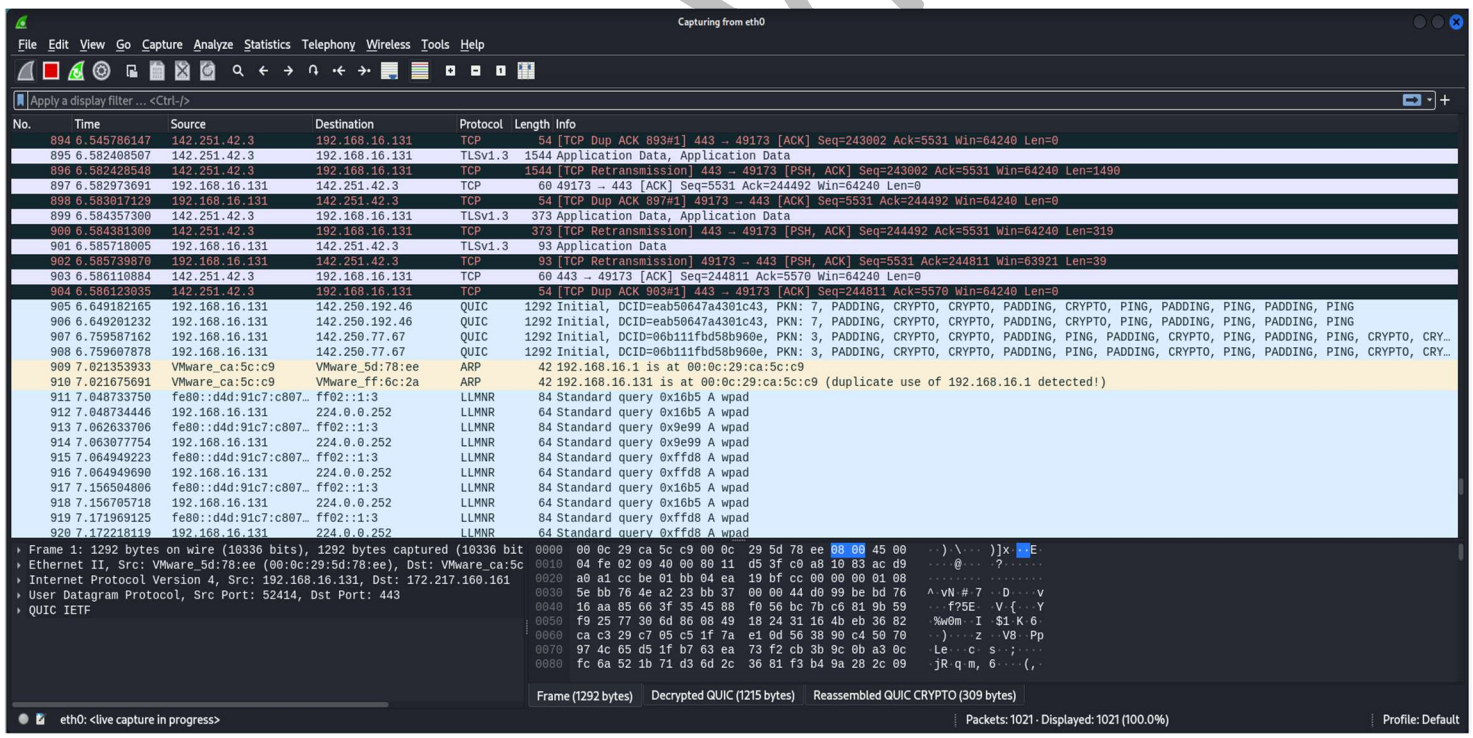


ATTACKERS ARP TABLE AFTER SPOOFING:

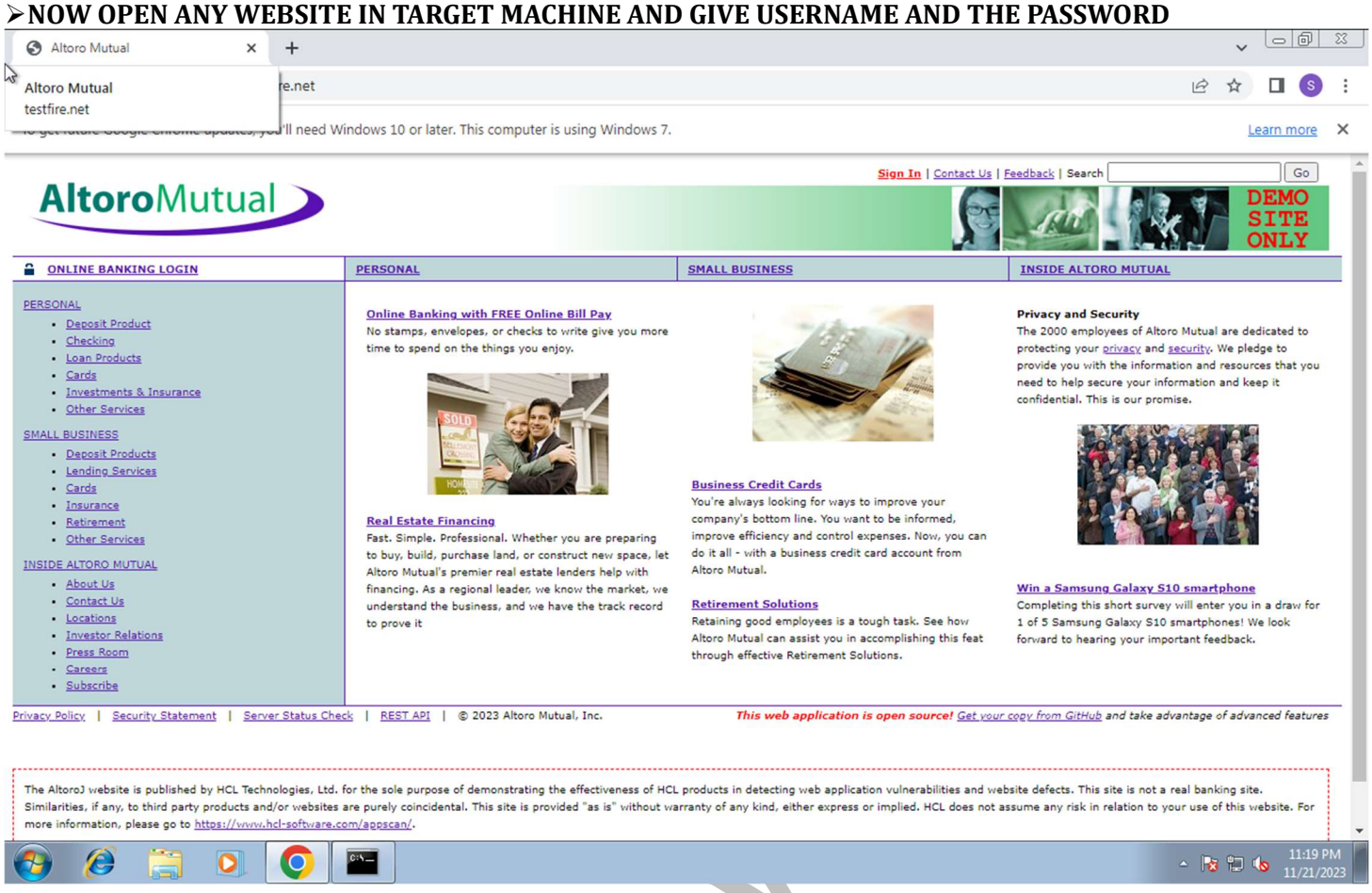


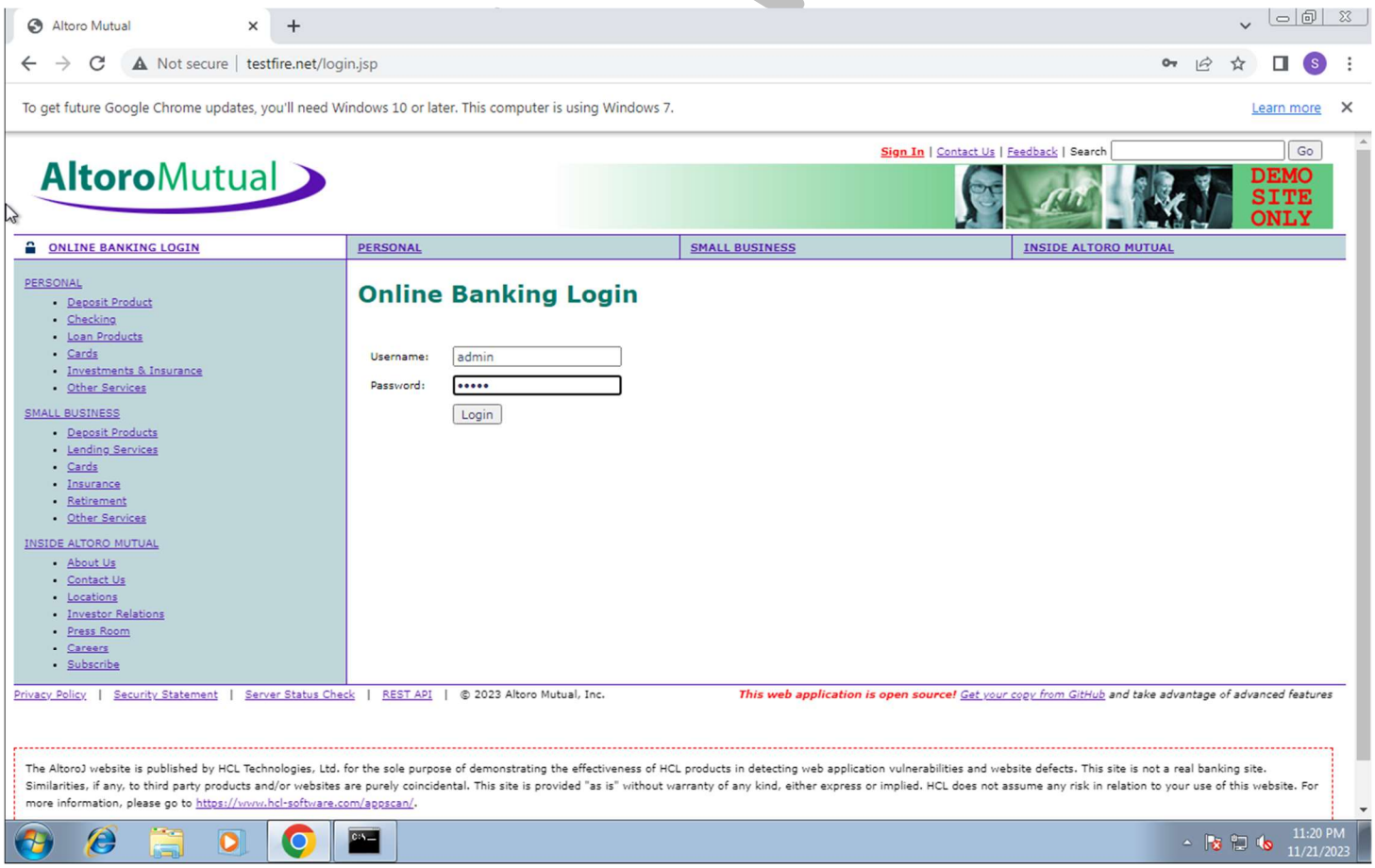
➢ **NOW ATTACKERS MACHINE IS THE DEFAULT GATEWAY. NOW OPEN THE WIRESHARK IN ATTACKERS MACHINE AND CAPTURE THE PACKETS**

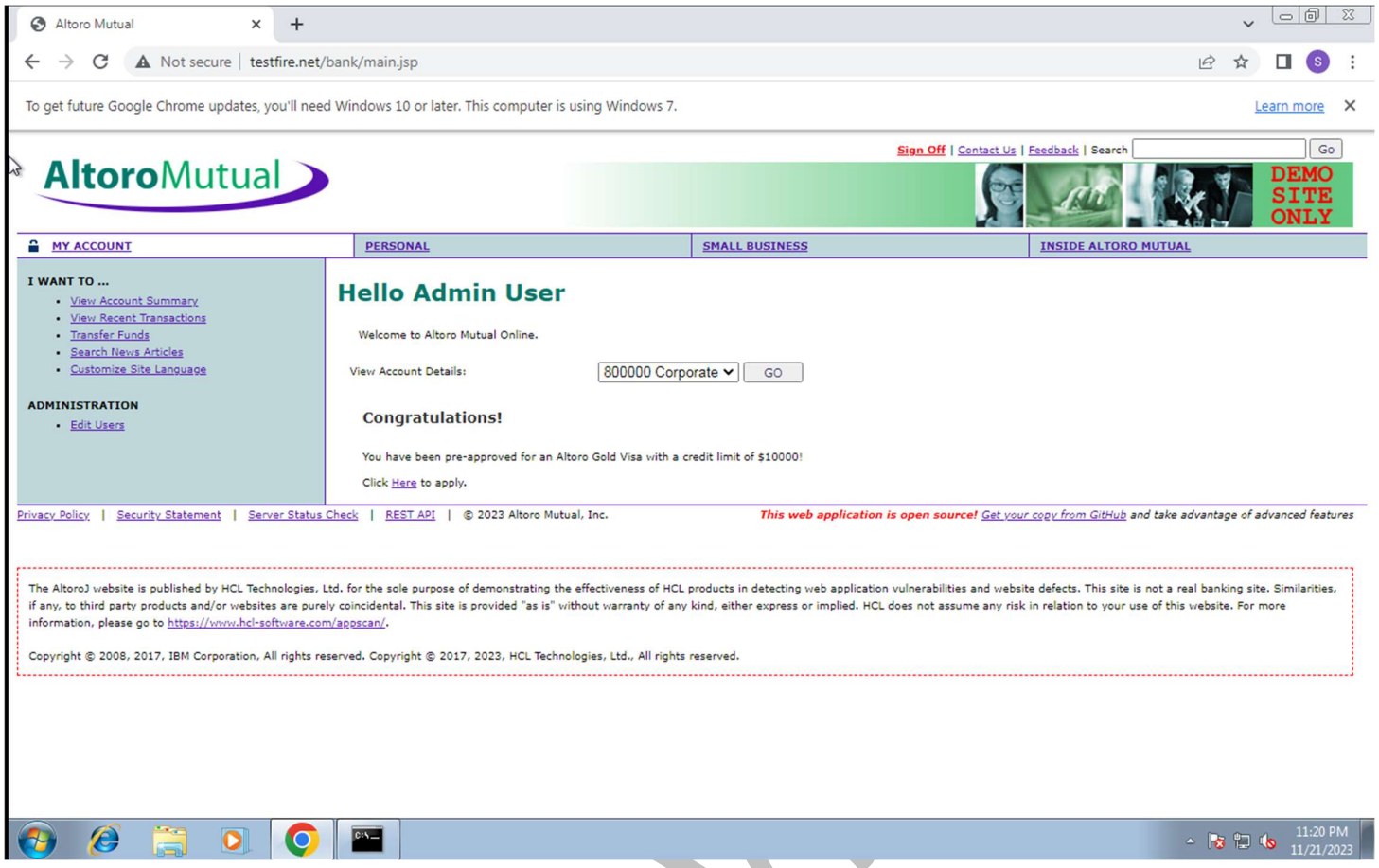




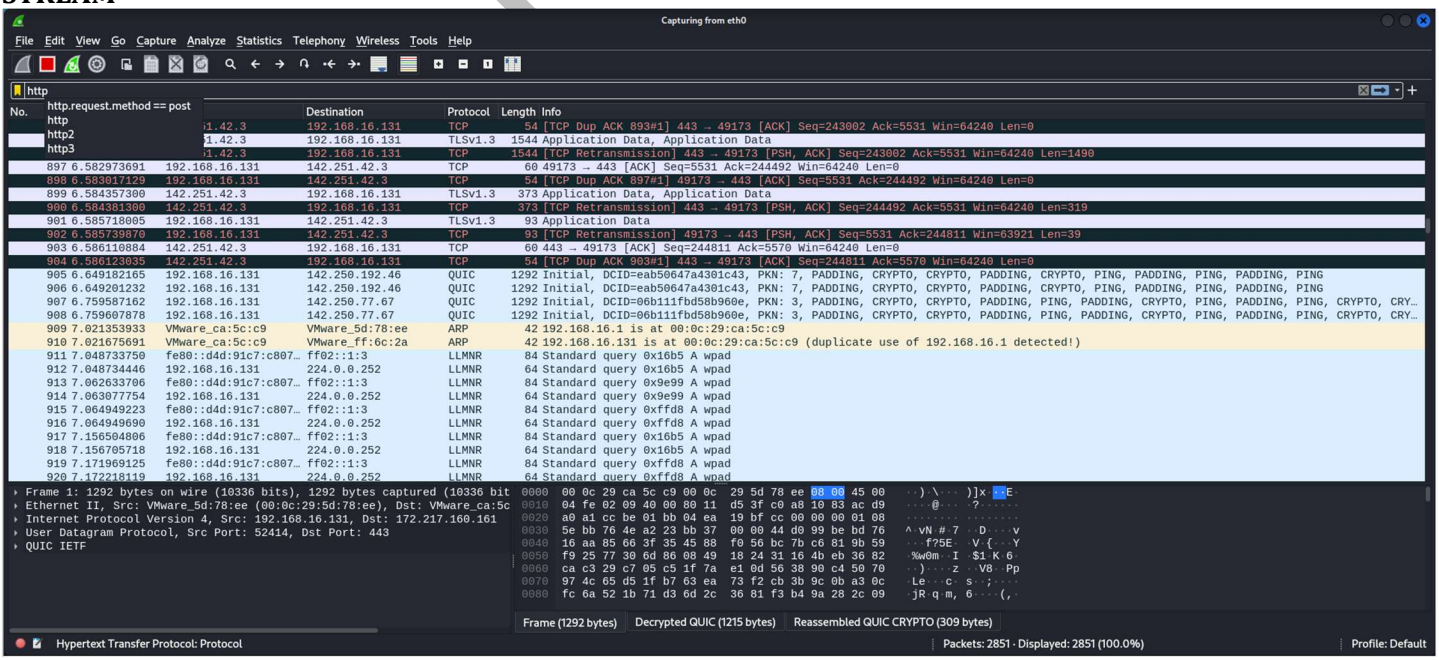
➢**NOW OPEN ANY WEBSITE IN TARGET MACHINE AND GIVE USERNAME AND THE PASSWORD**

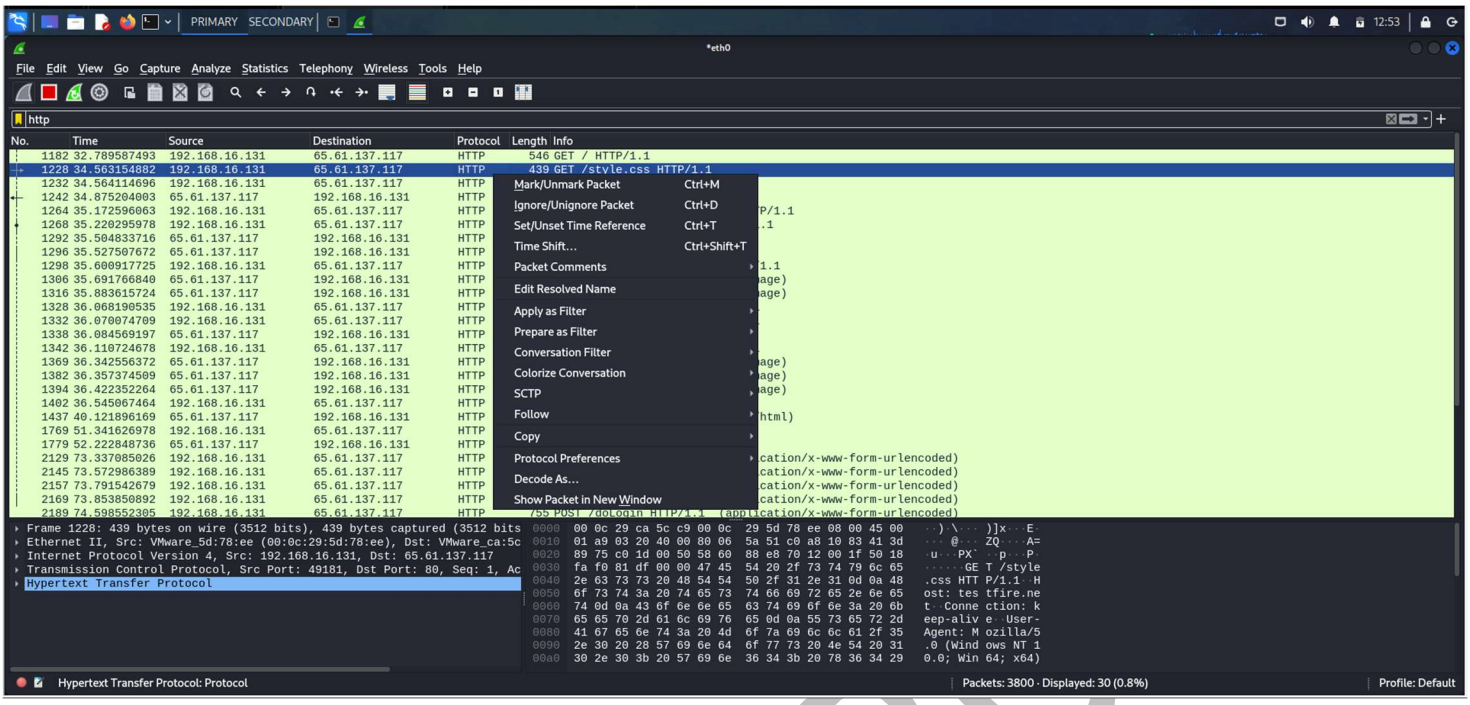


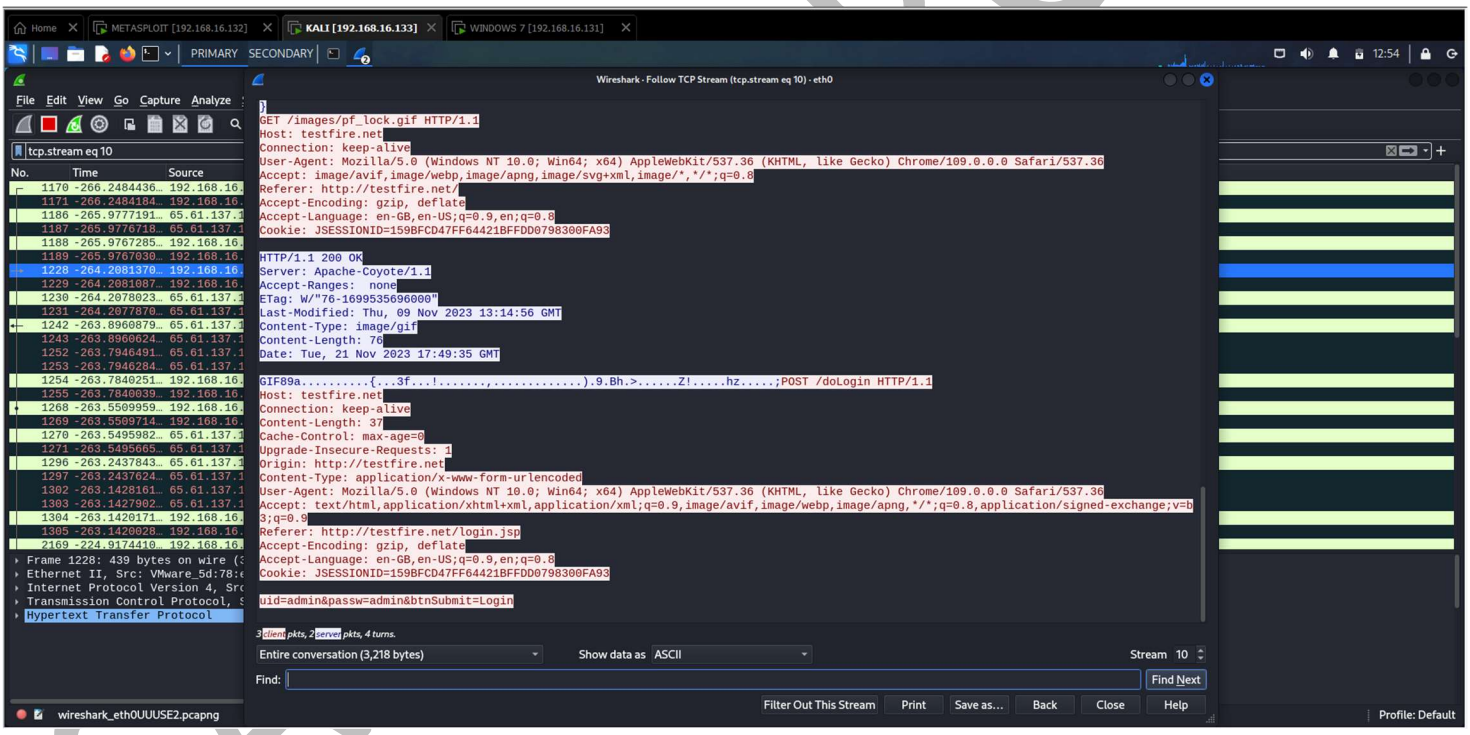




➢ **NOW COME BACK TO ATTACKERS MACHINE AND CAPTURE THE HTTP PACKETS AND FOLLOW THE TCP STREAM**



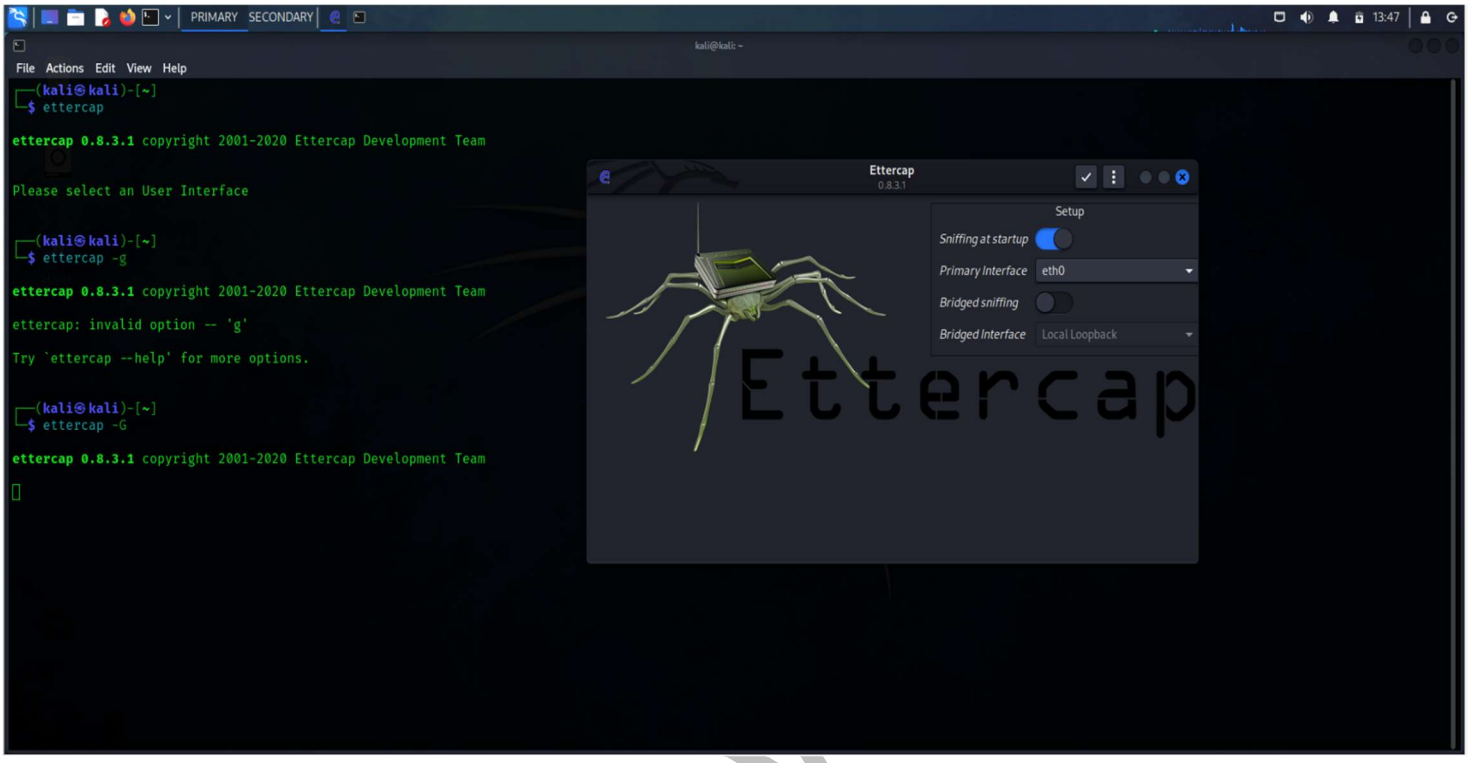


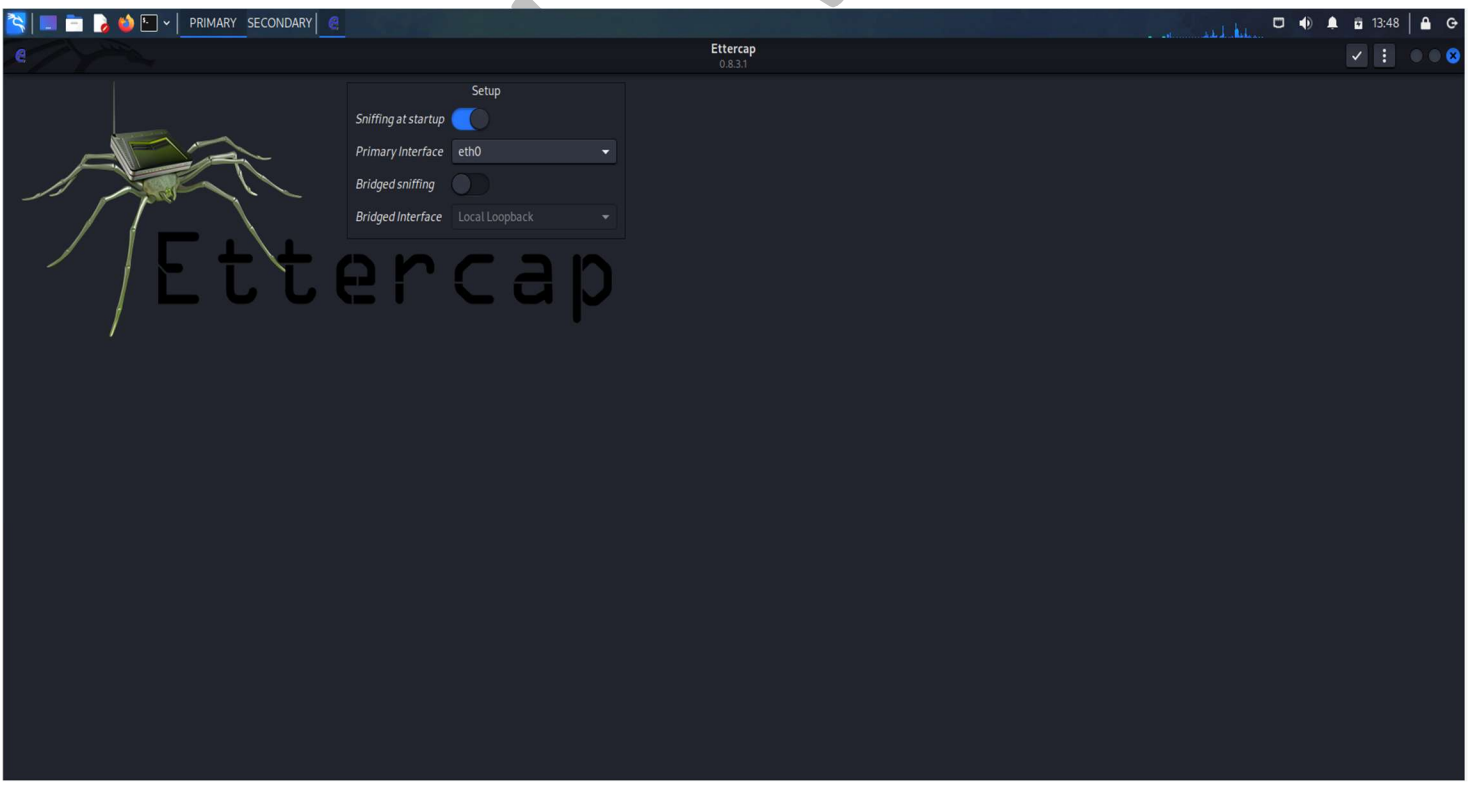


➢ **HERE WE CAN OBSERVE THE USER NAME AND THE PASSWORD IN THE PLAIN TEXT THAT HAS BEEN SUBMITTED BY THE TARGET**

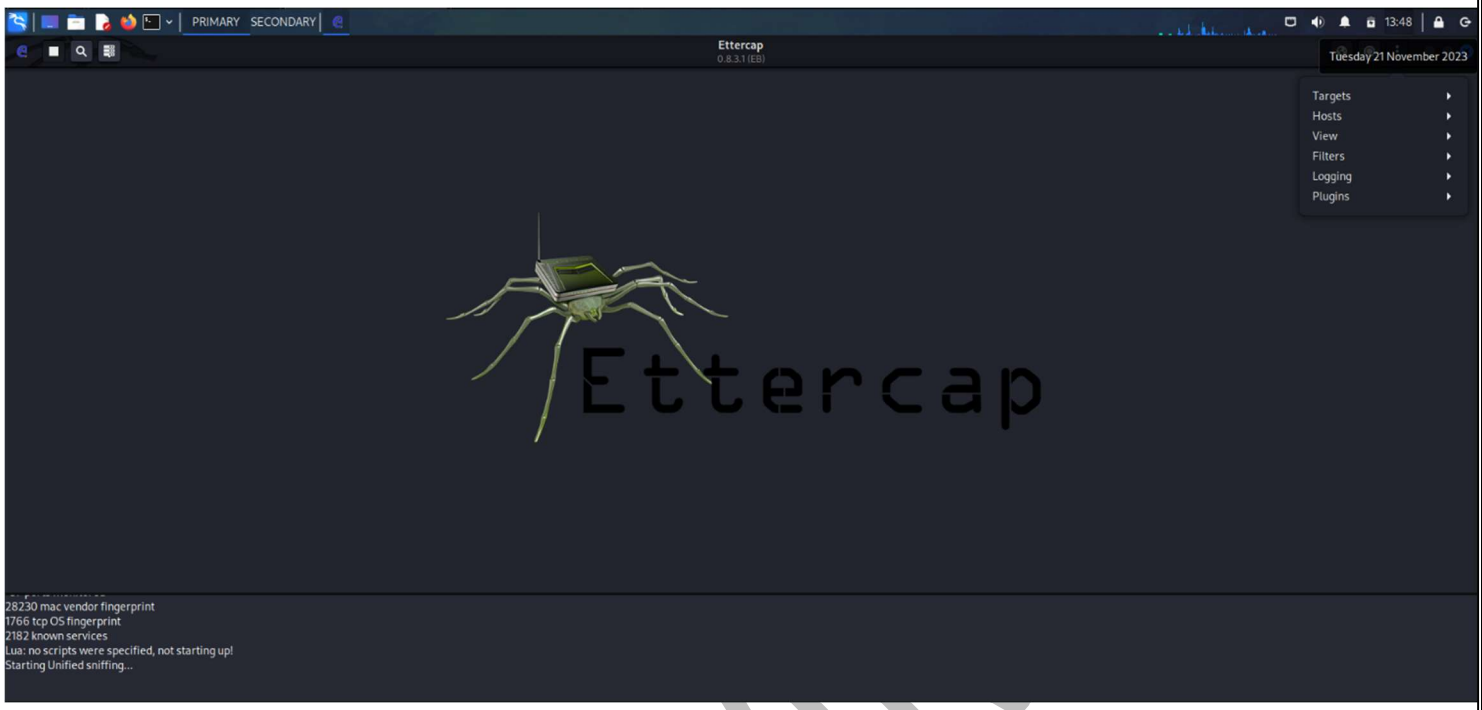
ETTERCAP:

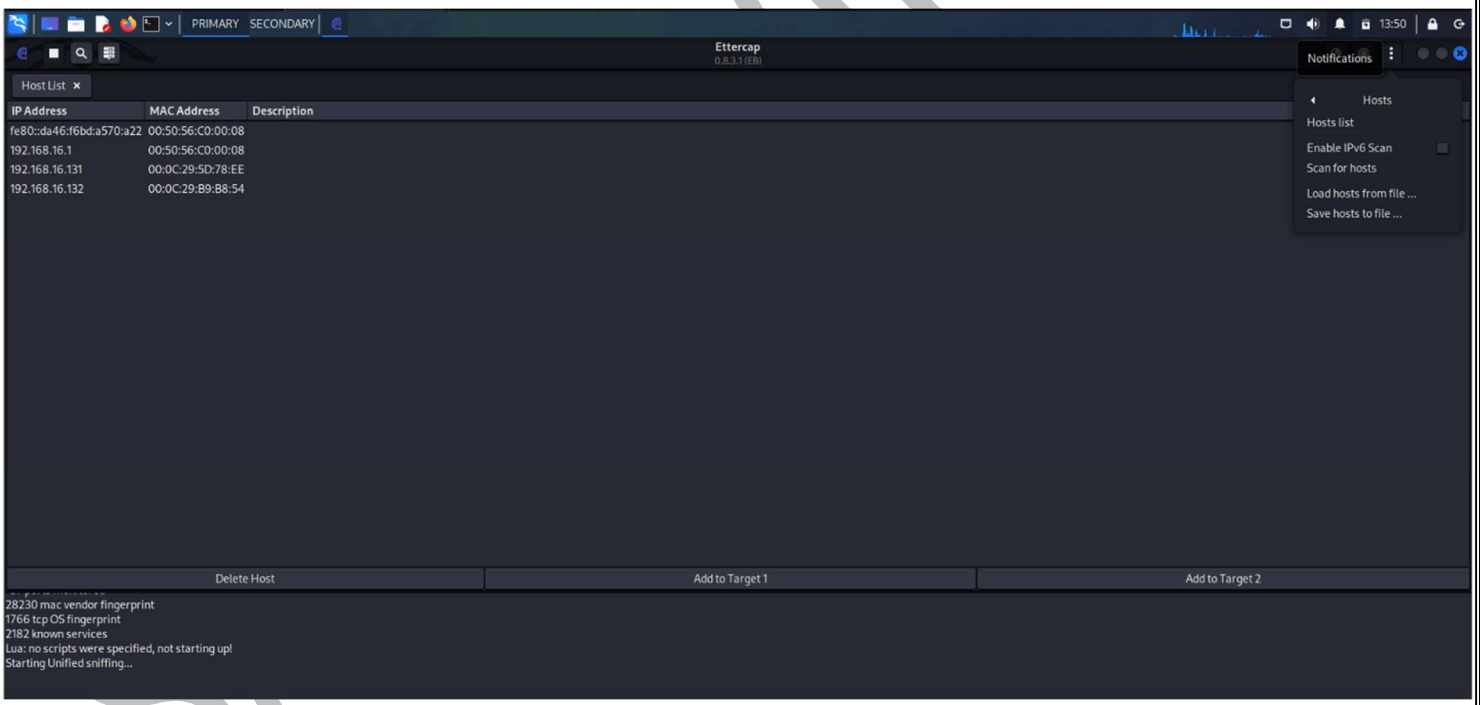
Ettercap is commonly used for ARP spoofing, which is a type of man-in-the-middle attack. ARP spoofing involves sending fake Address Resolution Protocol (ARP) messages on a local area network. The goal is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing network traffic to be sent to the attacker instead of the legitimate destination.



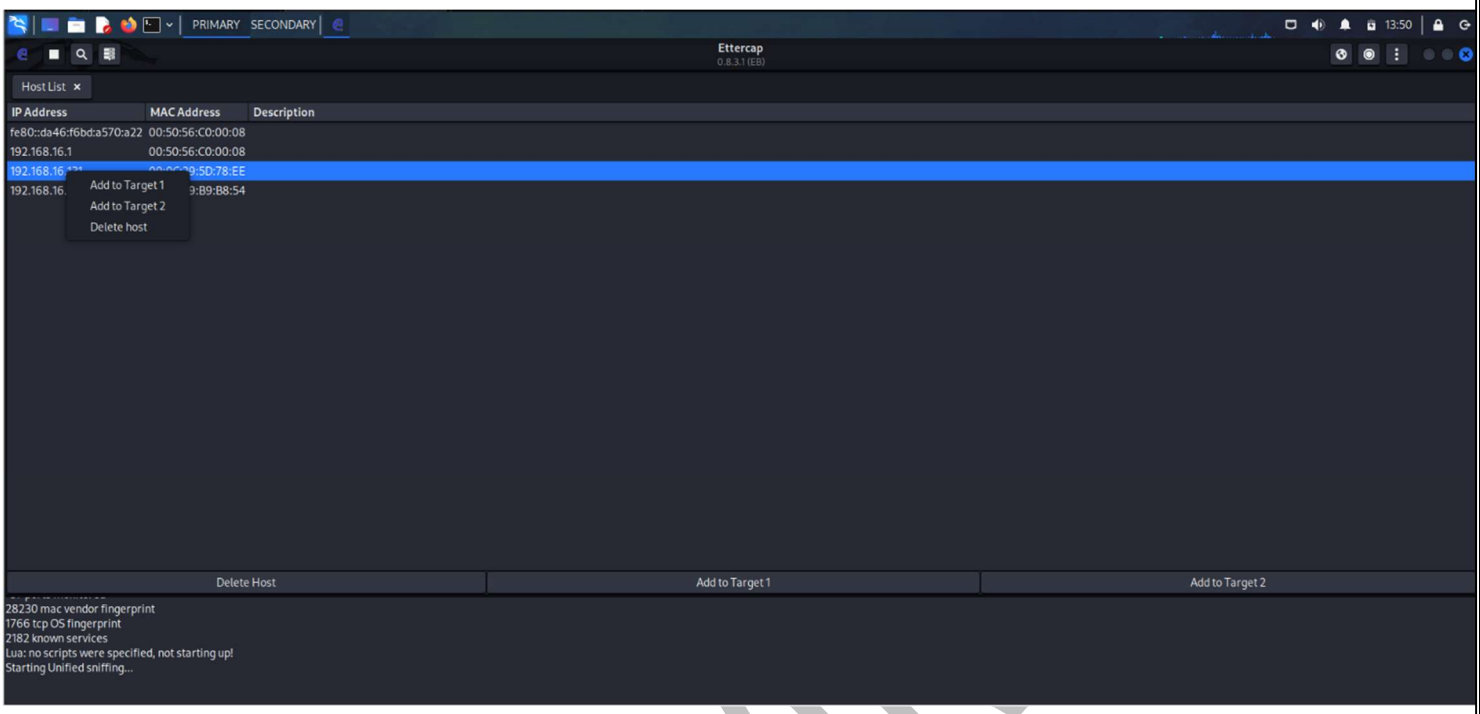


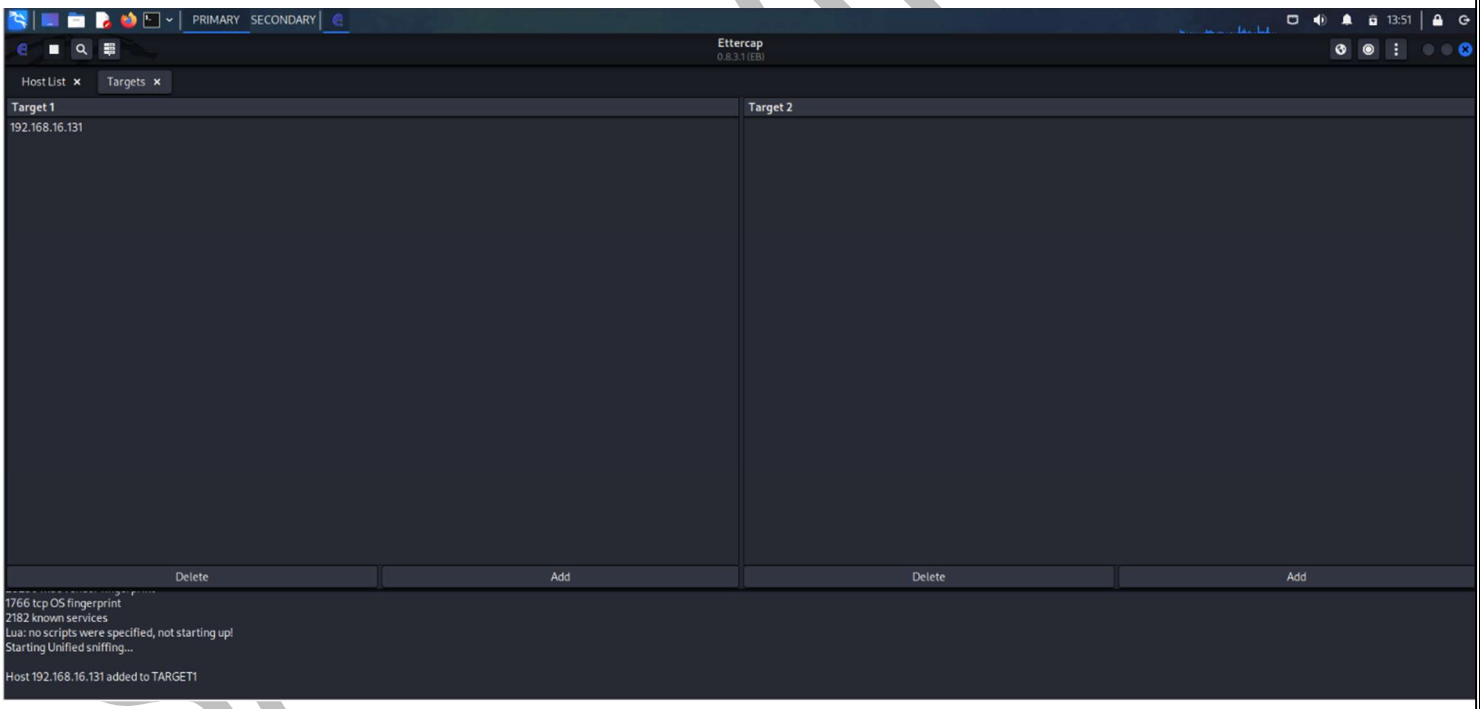
➢TO VIEW THE LIVE HOSTS IN THE NETWORK:



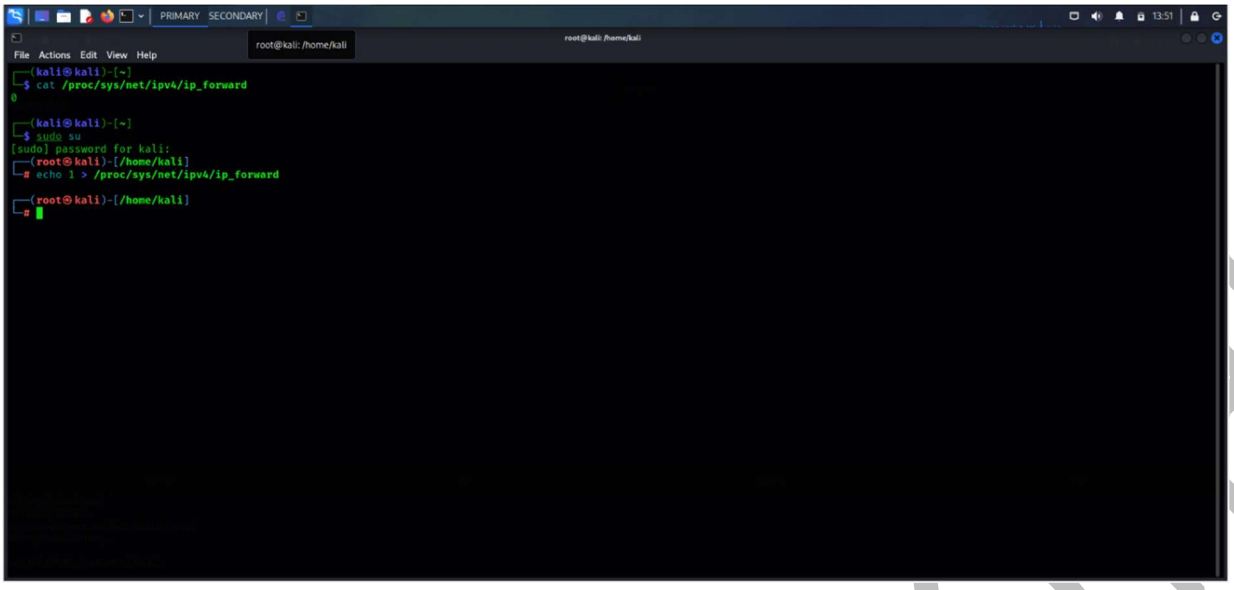


➢ADDING THE WINDOWS MACHINE AS TARGET:

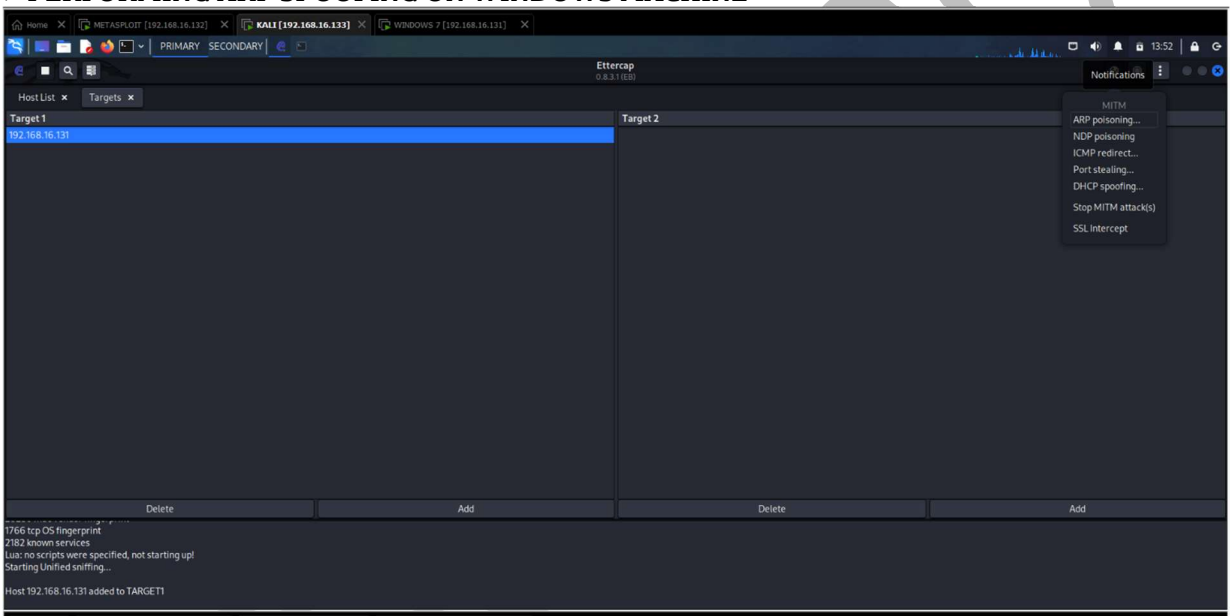


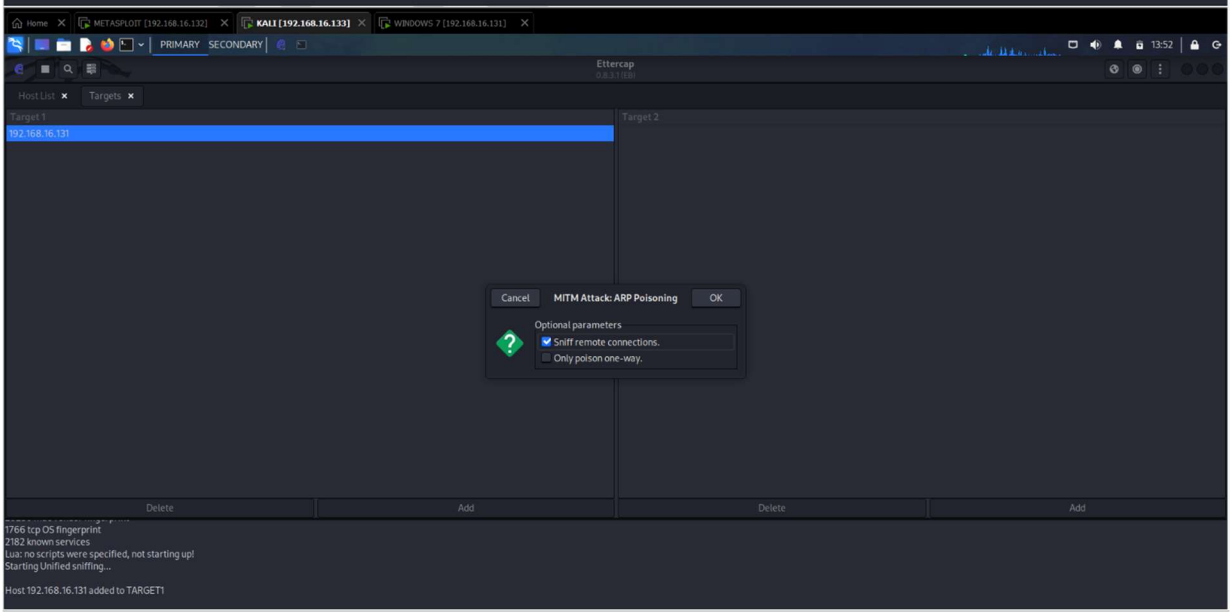


➢ENABLING IP FORWARDING

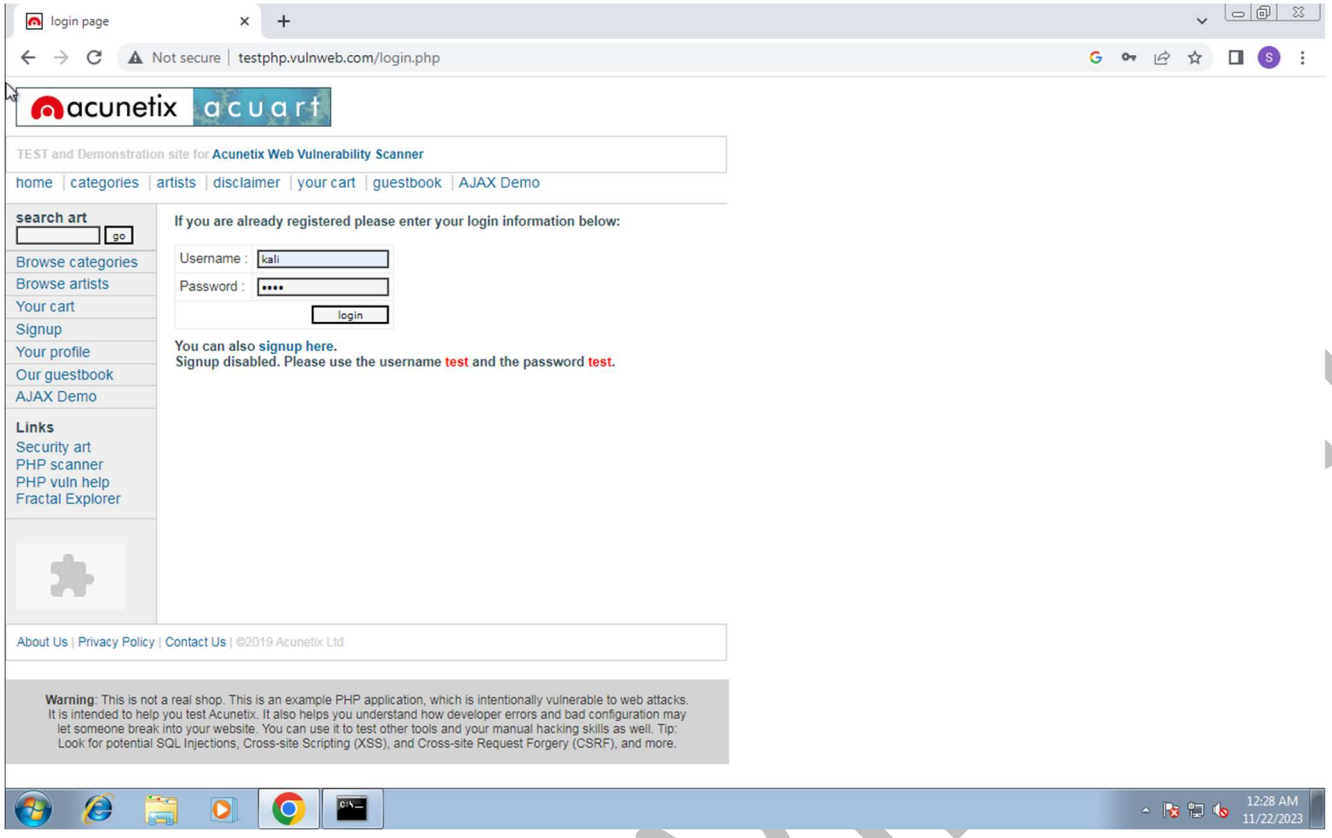


➢PERFORMING ARP SPOOFING ON WINDOWS MACHINE



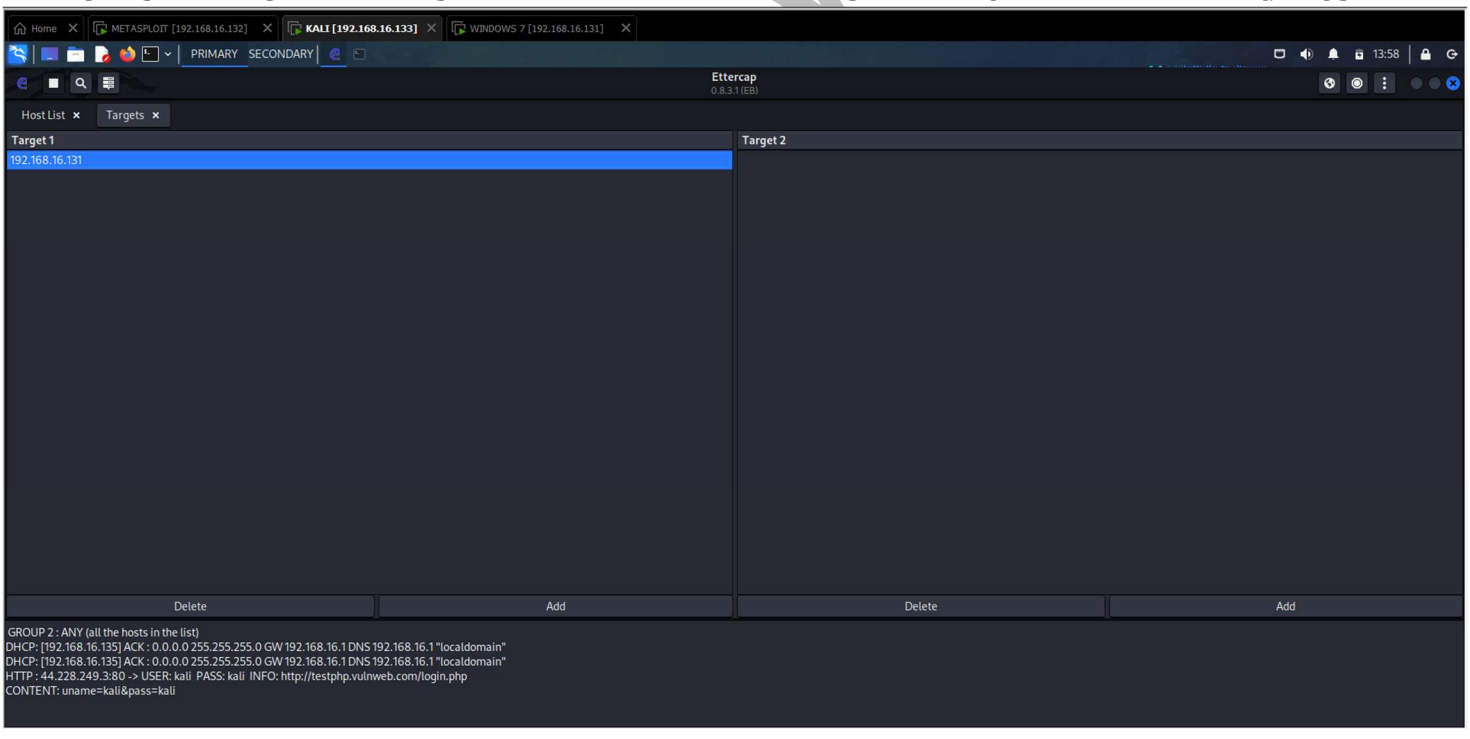


➢**OPEN THE TARGET AND OPEN ANY WEBSITE AND PROVIDE THE USER CREDENTIALS**



➢**NOW COME BACK TO ATTACKERS MACHINE.**

➢**WE CAN SEE THE CREDENTIALS IN THE PLAIN TEXT THAT HAS BEEN PROVIDED BY THE TARGET USER**



➢ **ETTERCAP TERMINAL :**

```
Listening on:
  eth0 -> 00:0C:29:CA:5C:C9
          192.168.16.133/255.255.255.0
          fe80::4376:b109:2e24:7359/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Host 192.168.16.131 added to TARGET1

ARP poisoning victims:

 GROUP 1 : 192.168.16.131 00:0C:29:5D:78:EE

 GROUP 2 : ANY (all the hosts in the list)
DHCP: [192.168.16.135] ACK : 0.0.0.0 255.255.255.0 GW 192.168.16.1 DNS 192.168.16.1 "localdomain"
DHCP: [192.168.16.135] ACK : 0.0.0.0 255.255.255.0 GW 192.168.16.1 DNS 192.168.16.1 "localdomain"
HTTP : 44.228.249.3:80 -> USER: kali  PASS: kali  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=kali&pass=kali
```

Mitigation techniques:

- Use ARP Spoofing Detection Tools.
- Configure Static ARP Entries.
- Enable Port Security on Network Switches.
- Implement Network Segmentation.
- Use DHCP Snooping to Validate DHCP Messages.
- Deploy Dynamic ARP Inspection (DAI).
- Utilize VLANs to Isolate Network Segments.
- Encrypt Network Traffic with Protocols like WPA2/WPA3.
- Regularly Monitor Network Activity for Anomalies.
- Provide Security Awareness Training for Users.

SATISH_V