# Network Sniffing

# Introduction :

Network sniffing is the process of capturing, analyzing, and monitoring network traffic using software or hardware tools. Sniffing tools, often referred to as packet sniffers, can intercept and log network packets in real-time. This process is widely used in both legitimate and malicious activities, making it a critical topic in cybersecurity

## Network Devices

### Hub

- Sends data to all connected devices
- Stores port number and device name
- Less secure because every device receives the same data

### Switch

- Sends data to a particular device only
- Stores port number, device name, and MAC address
- More secure than a hub but still vulnerable to attacks like MAC flooding

### Router

- Connects different networks
- Routes data based on IP addresses
- Acts as a gateway between networks

## DHCP Starvation Attack:

**DHCP (Dynamic Host Configuration Protocol)** automatically assigns IP addresses.

- Attacker floods DHCP server with fake requests
- All IP addresses get exhausted
- Legitimate users cannot obtain an IP address

**Tool Used:** Metasploit Framework (`auxiliary/server/dhcp`)

# Session Hijacking:

Session hijacking occurs when attackers steal session cookies to impersonate users.

Once stolen, attackers can access accounts without login credentials.

# DNS Poisoning :

DNS Poisoning manipulates DNS records to redirect users to malicious websites.

## Types

1. Intranet DNS Spoofing
2. Internet DNS Spoofing
3. Proxy Server DNS Poisoning
4. DNS Cache Poisoning

# OSI Model :

The **OSI (Open Systems Interconnection) Model** explains how data flows through a network:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Understanding OSI layers helps identify where attacks occur.

## OSI Layer Involvement in MITM Attack:

• **Layer 2 (Data Link Layer):**

ARP Spoofing occurs here by manipulating MAC–IP mappings.

• **Layer 3 (Network Layer):**

IP forwarding allows packets to pass between victim and router.

• **Layer 4 (Transport Layer):**

TCP/UDP sessions are intercepted and monitored.

• **Layer 7 (Application Layer):**

Credentials, cookies, and HTTP data are captured.

# MAC Address Spoofing:

MAC spoofing changes the MAC address of a device to impersonate another device.

### Tools

- Technitium MAC Address Changer
- SMAC Tool (Professional Edition)

# Sniffing Detection Techniques:

Sniffing detection identifies devices running in promiscuous mode.

### Detection Methods

- Monitor unusual network traffic
- Check ARP tables
- Use promiscuous detection tools
- Analyze latency and packet behavior

# Conclusion

Sniffing and related attacks such as ARP spoofing, DNS poisoning, DHCP starvation, and session hijacking pose serious threats to network security. Understanding how these attacks work, the tools used, and detection techniques is essential for securing modern networks. This module provides foundational knowledge required for ethical hacking and network defense

# MITM Attack

## (Man In The Middle Attack)

The purpose of this report is to document the execution and results of a Man-in-the-Middle (MITM) attack carried out within a controlled home-lab environment.
This activity was performed strictly for learning, cybersecurity research, and internal testing to better understand how network-level attacks are conducted and how to defend against them.

**Tools :**

- ARP Spoofing / Poisoning
  Used to redirect network traffic through the attacker.
- Ettercap
  Employed for ARP poisoning, traffic interception, and protocol analysis.
- Bettercap
  Used for advanced MITM attacks, network scanning, packet sniffing, and spoofing.
- Wireshark
  Used to inspect captured packets and analyze network behavior in detail.
- Kali Linux
  Operating system used on the attacker machine, providing all required networking tools.

# 1. ARP Spoofing / Poisoning : (Address Resolution Protocol)

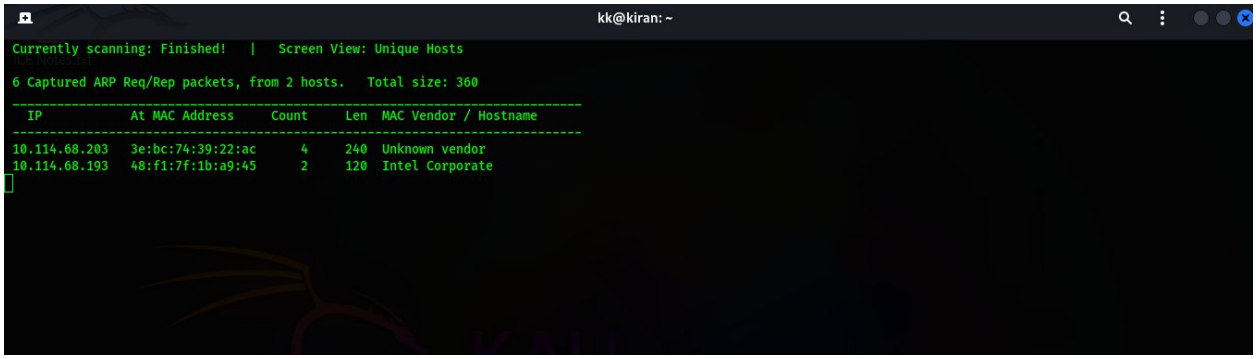
ARP Spoofing (also called ARP Poisoning) is a technique used to manipulate the Address Resolution Protocol (ARP) within a local network.

**This allows the attacker to:**

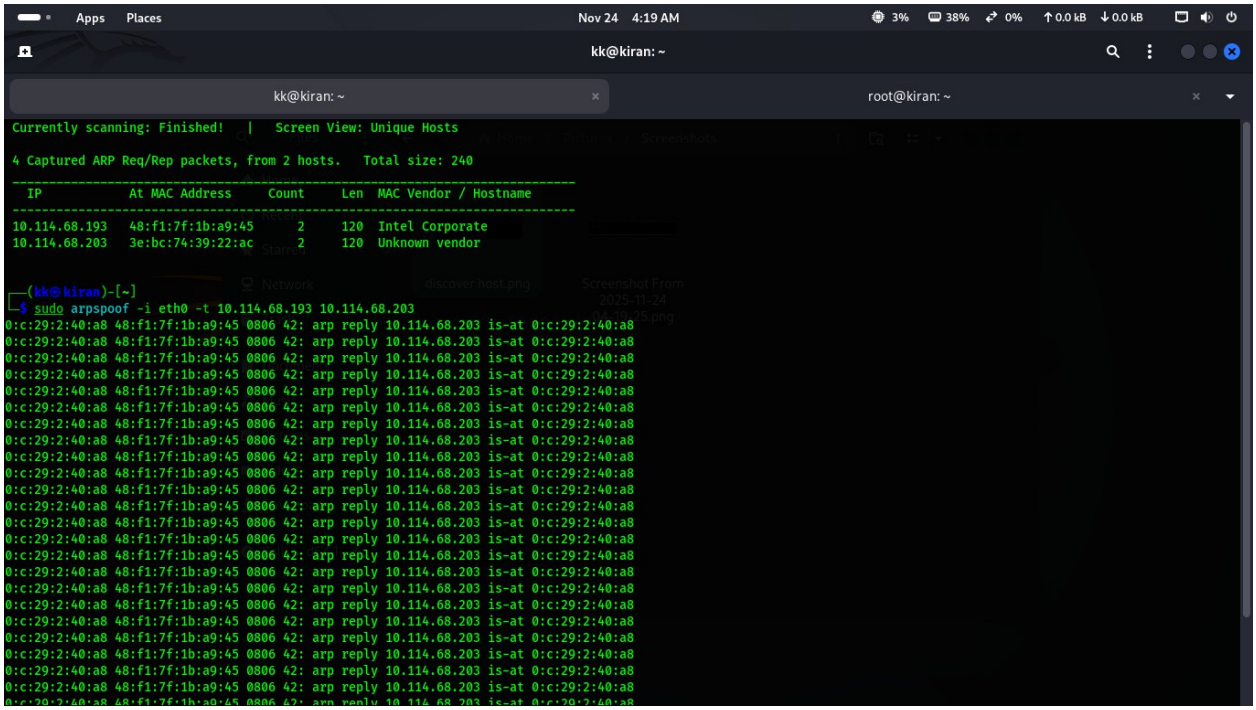
- Intercept packets
- Capture credentials from unencrypted sessions
- Perform further MITM attacks such as DNS spoofing or session hijacking

**ARP Spoofing works only on local networks where ARP is used.**

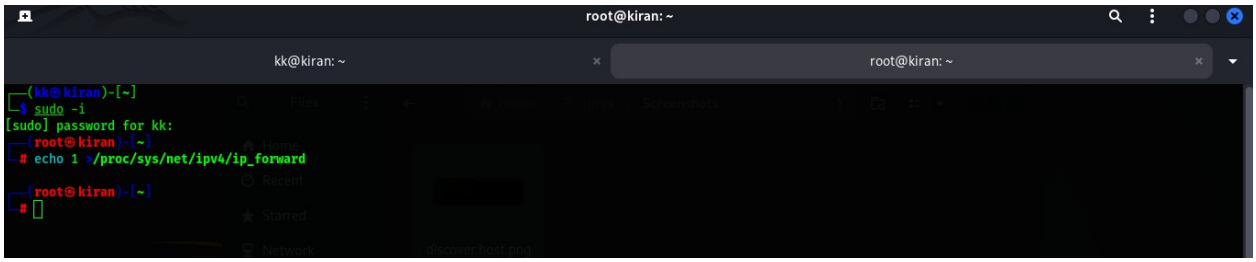
**Host Discovery on the network -**



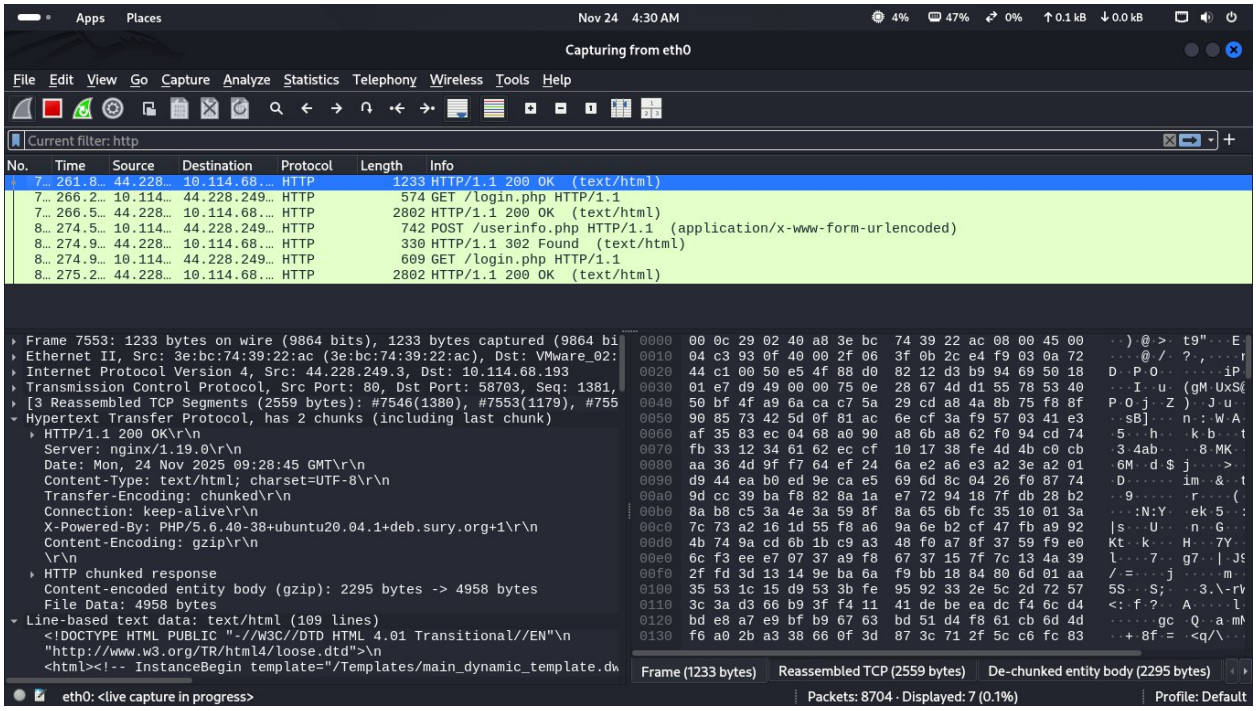

**Start ARP spoof -**



## Ip Forwarding -




## Wireshark Capture -



## 2) Ettercap :

Ettercap is a powerful network security tool designed specifically for Man-in-the-Middle attacks on LAN networks. It supports ARP poisoning, traffic interception, protocol analysis, and packet manipulation.

- ✓ **ARP Spoofing & MITM Attacks -**

Ettercap automatically poisons ARP tables between chosen hosts, placing the attacker between two communicating devices.

- ✓ **Packet Sniffing -**

Ettercap can capture network traffic and display credentials, visited URLs, cookies, and protocol data.

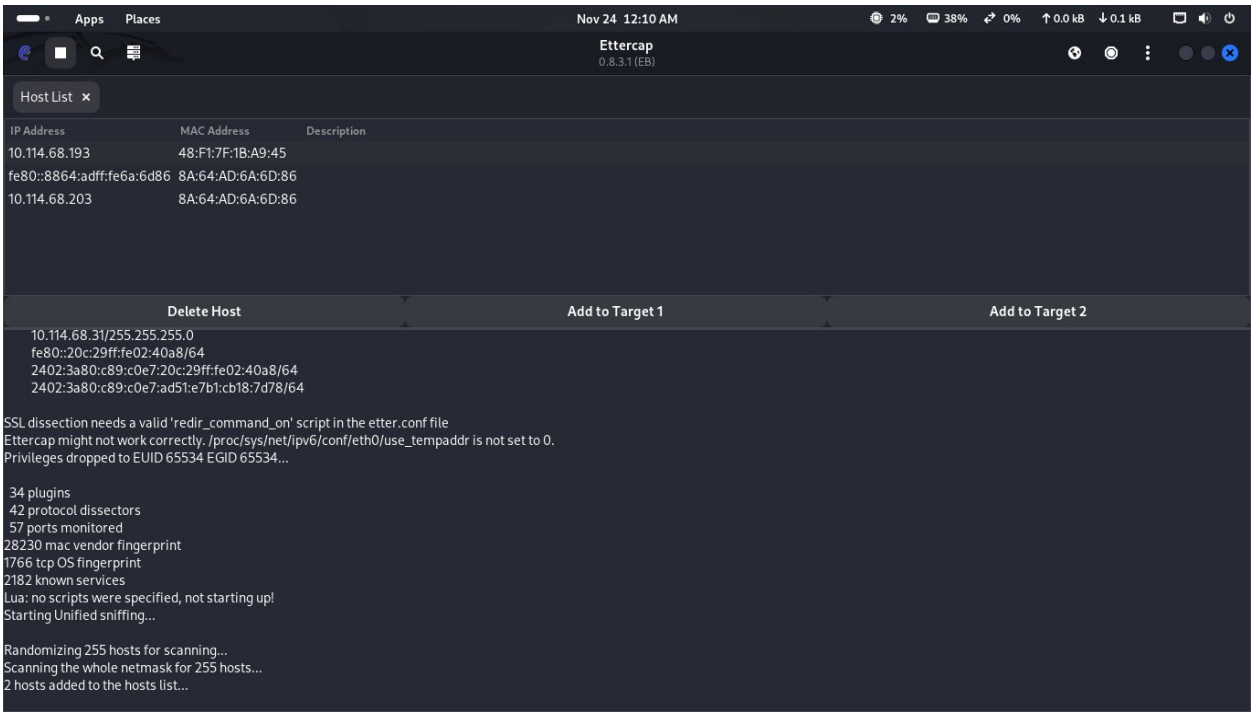
- ✓ **GUI and CLI Support**

The graphical interface makes host discovery and MITM setup simple, while the command-line version is ideal for automation.

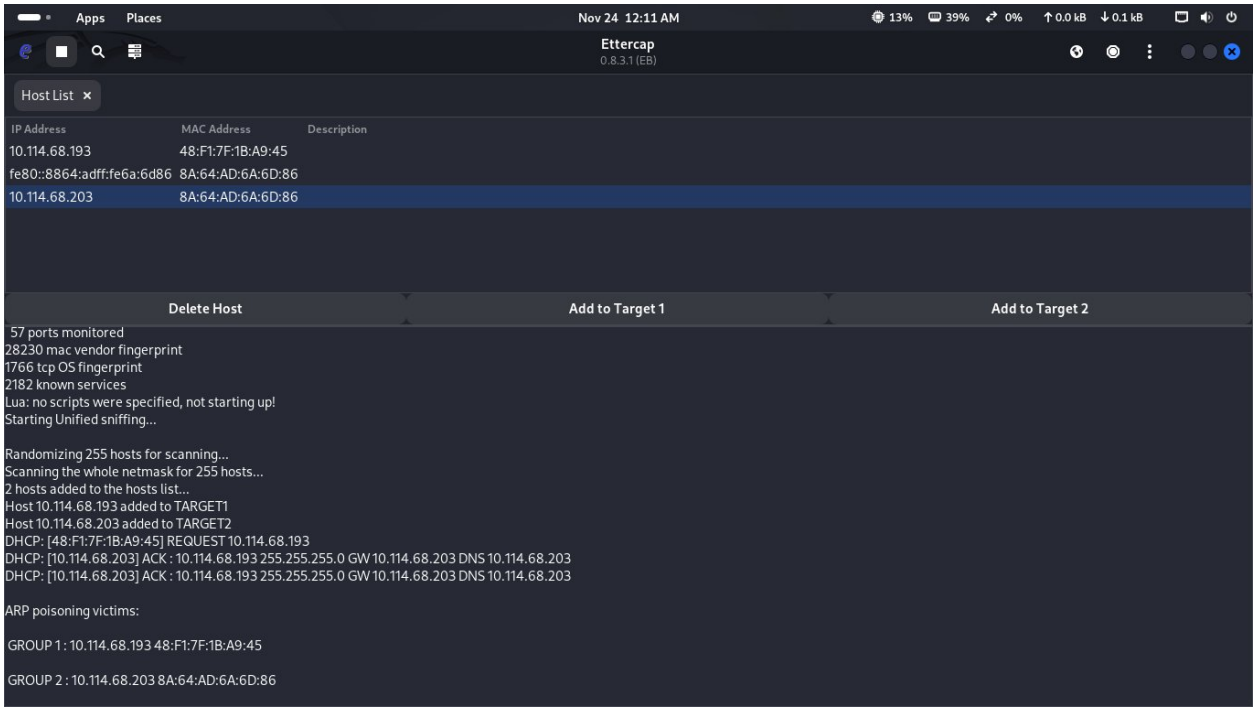
**Ettercap is one of the most commonly used MITM tools in penetration testing and network auditing.**

**Ettercap -**

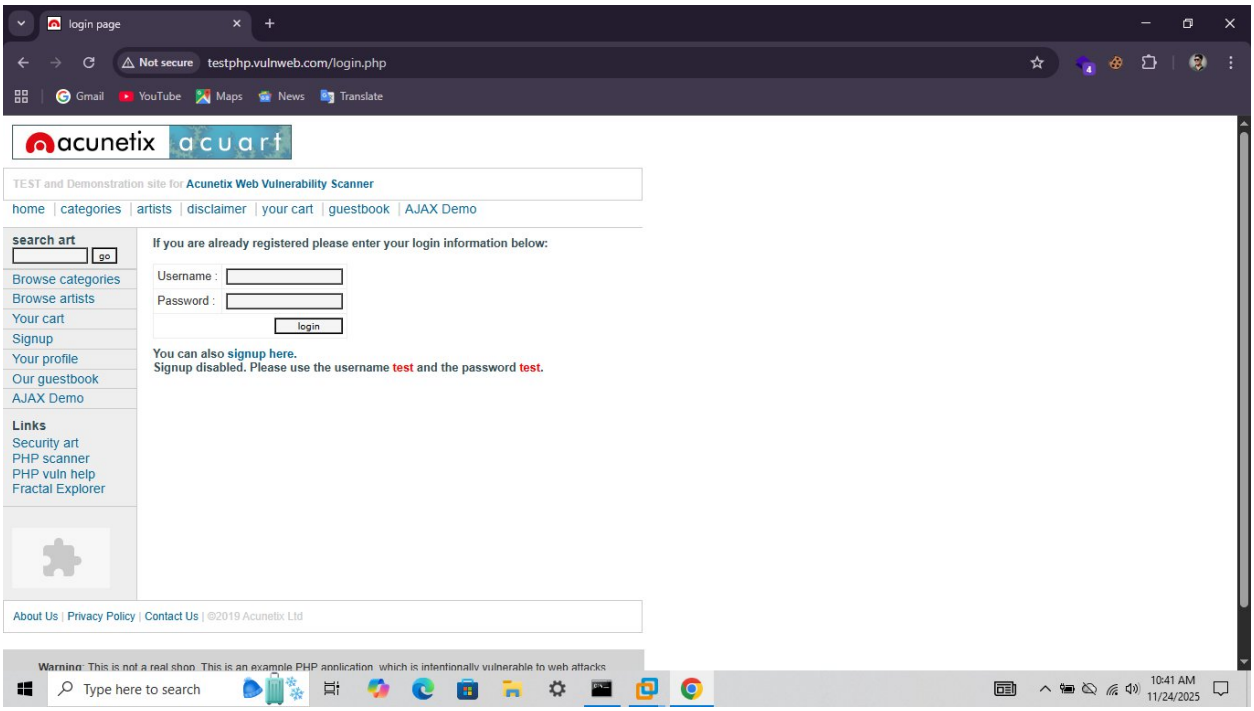
## Host Scan & List -



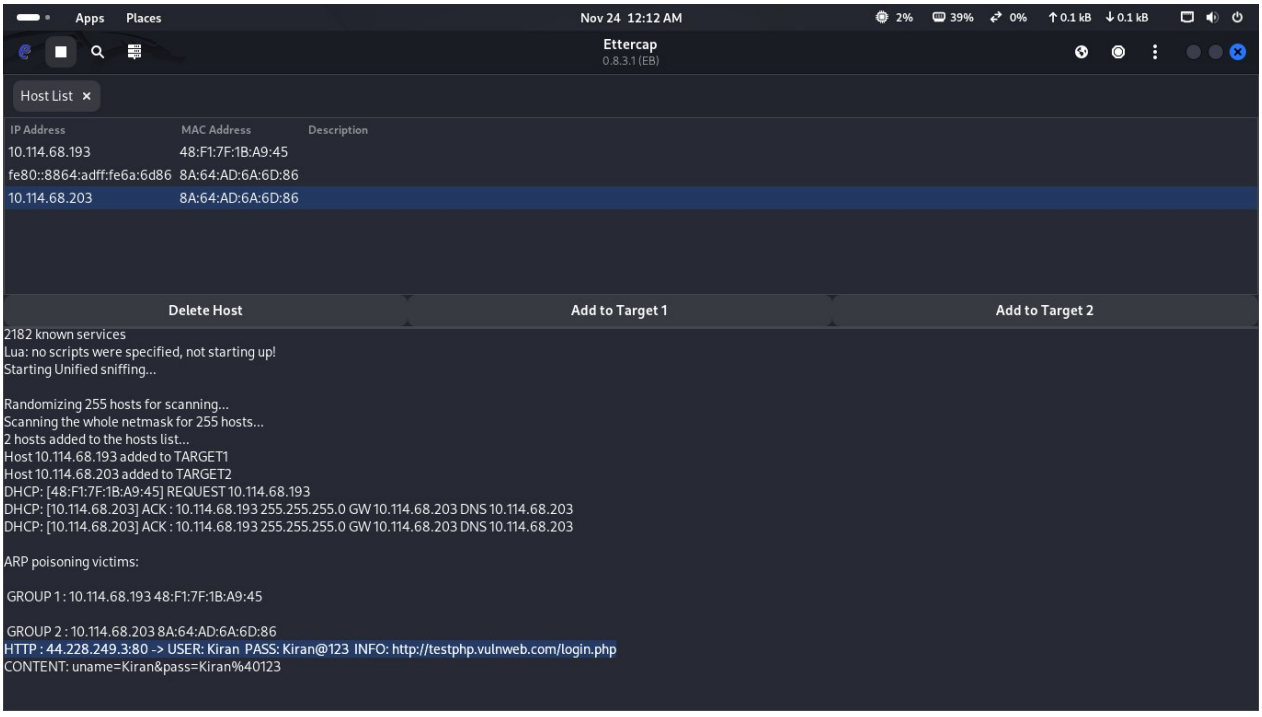

## ARP Spoofing -



## Test Website -




## Capture username & Password –



## 3) Bettercap :

Bettercap is an advanced, modern, and more powerful MITM toolset compared to Ettercap. It is designed for real-time network monitoring, manipulation, and exploitation.

### ✓ ARP Spoofing

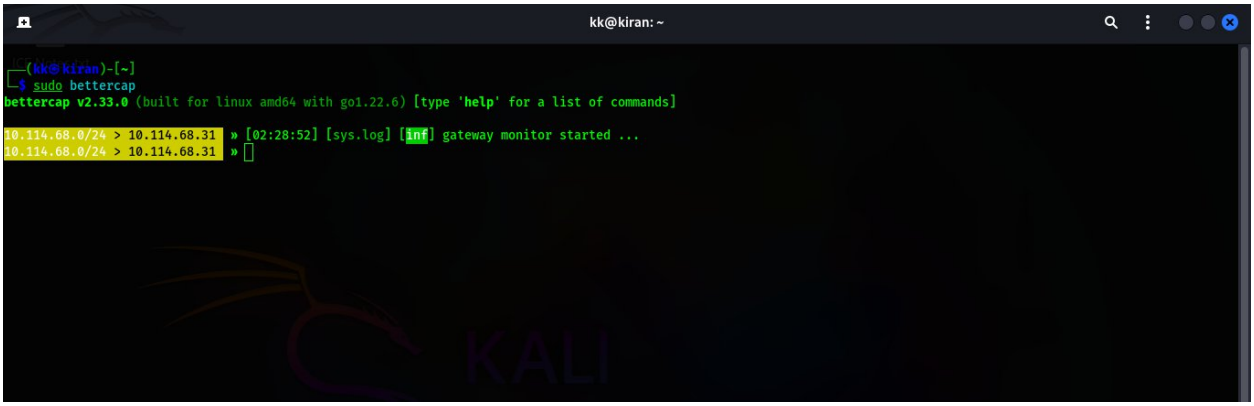
Bettercap can quickly discover hosts and automatically poison ARP tables to intercept traffic.

### ✓ Lightweight & Fast

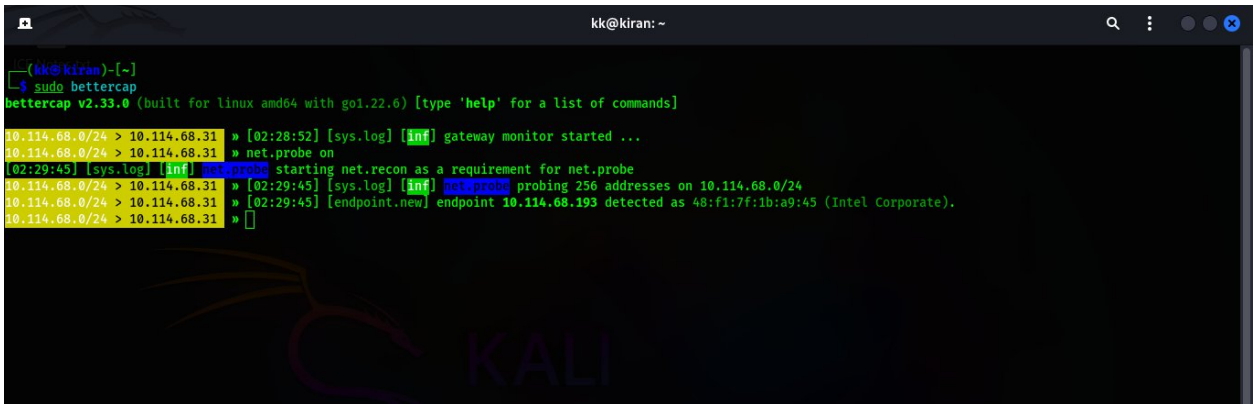
Bettercap is built in Go, making it more efficient and more stable than older MITM tools.

Bettercap is widely regarded as one of the most powerful tools for local network attacks, monitoring, and red-team scenarios.

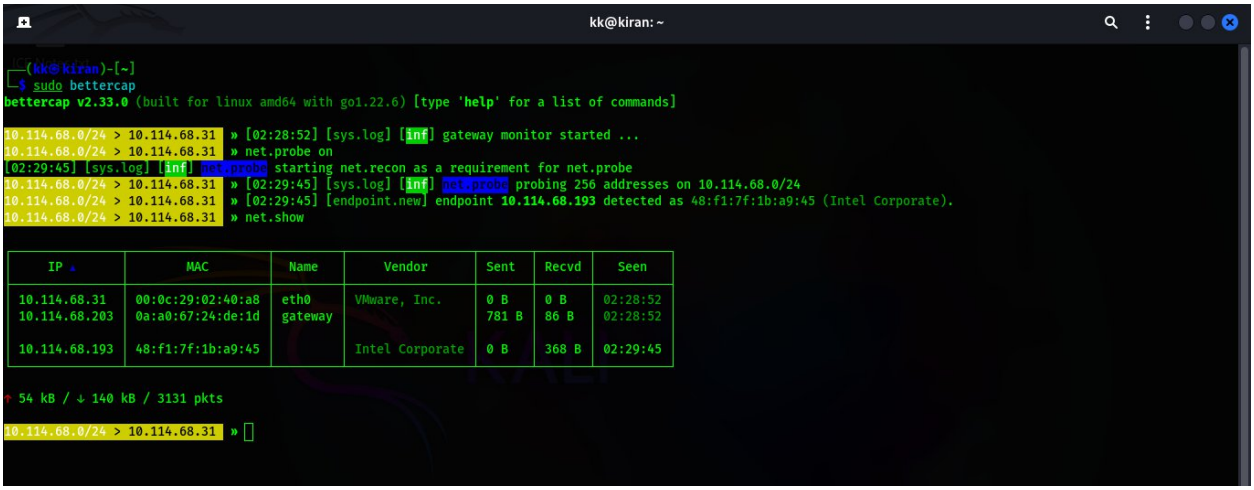
**BetterCap -**



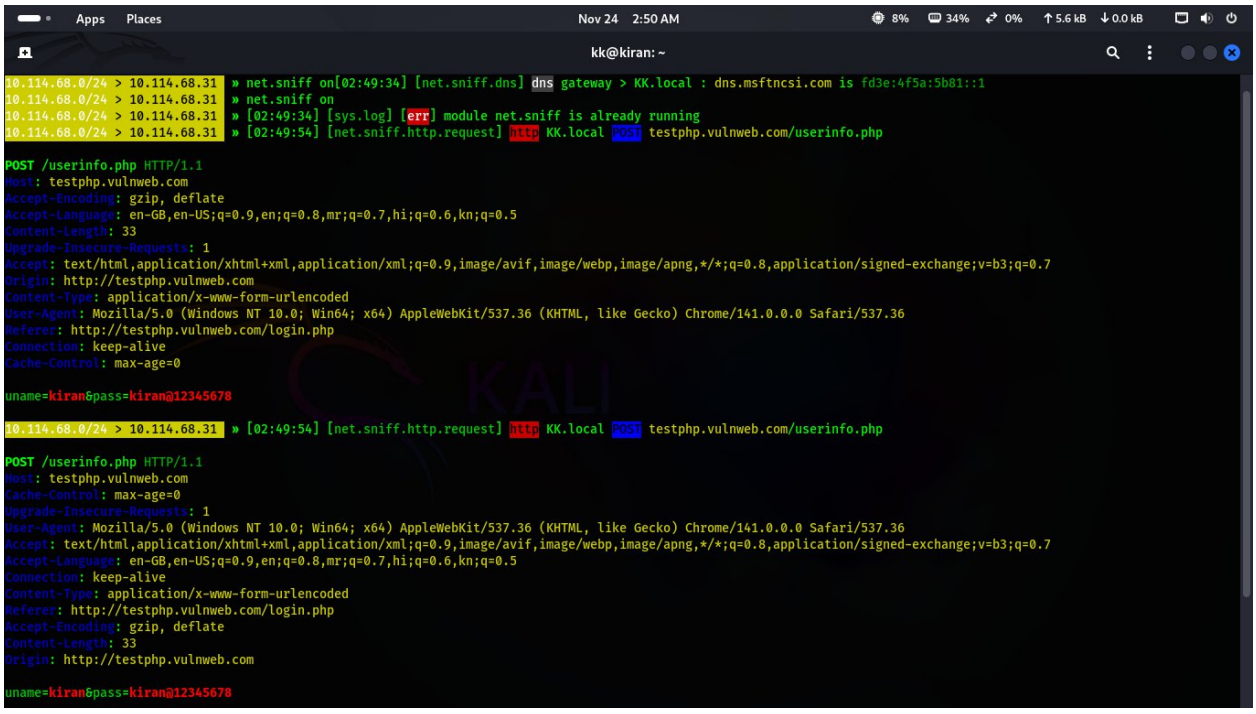

**Net.Probe ON -**



## Show Device on network -




## Sniffing Satrt & Capture Username & Pass -



**Results & Findings**

- Successfully hijacked traffic between victim and router
- Demonstrated traffic interception using Ettercap & Bettercap
- Verified credential leakage from unencrypted protocols
- Observed vulnerable traffic patterns (HTTP, plaintext login pages)
- Showed how attackers can manipulate ARP tables with minimal effort

**Security Impact**

If used maliciously, these attacks can lead to:

- Password theft
- Session hijacking
- Fake website redirection (DNS spoofing)
- Data manipulation
- Malware injection

**This demonstrates that MITM attacks are powerful and dangerous on insecure LAN networks.**

**Conclusion**

This home-lab experiment successfully demonstrated how ARP spoofing enables attackers to intercept and manipulate network traffic. The test reinforces the importance of network security measures and encrypted communication. Understanding these techniques is essential for defending real-world environments.