Man-In-The-Middle (MITM) Attack Report

# 1. Introduction

This report demonstrates the execution of a Man-In-The-Middle (MITM) attack using Ettercap and Wireshark on a virtualized Kali Linux environment. The objective was to capture HTTP login credentials transmitted over an unsecured network by performing ARP poisoning between a Windows host and the network gateway.

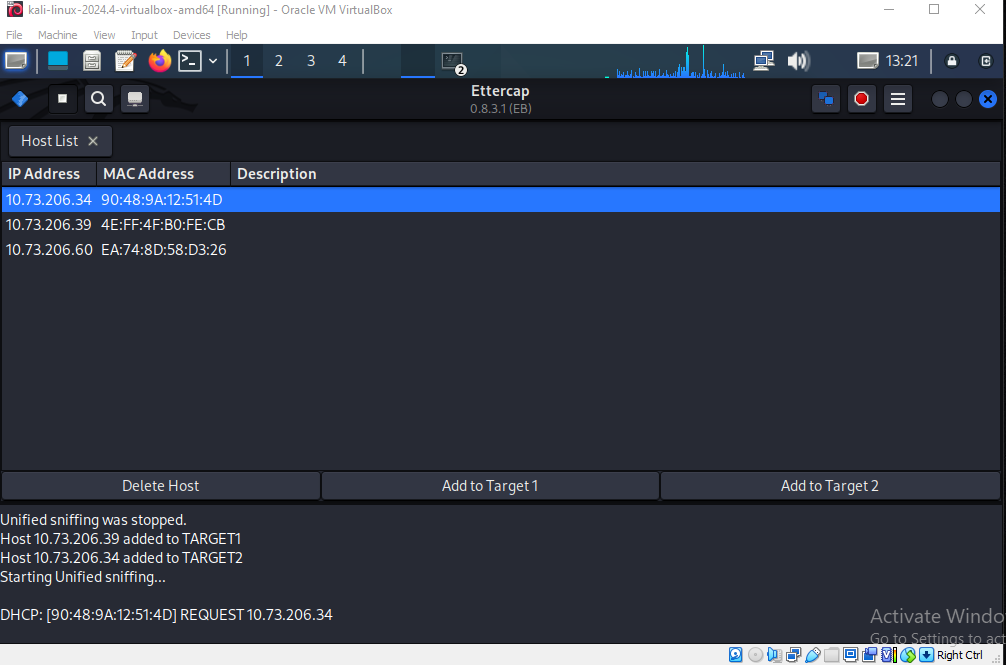
# 2. Tools Used

- Kali Linux 2024.4 (VirtualBox VM)  
- Ettercap (GUI Mode)  
- Wireshark  
- Windows Host Machine (Victim)  
- HTTP Test Website: http://testphp.vulnweb.com/login.php

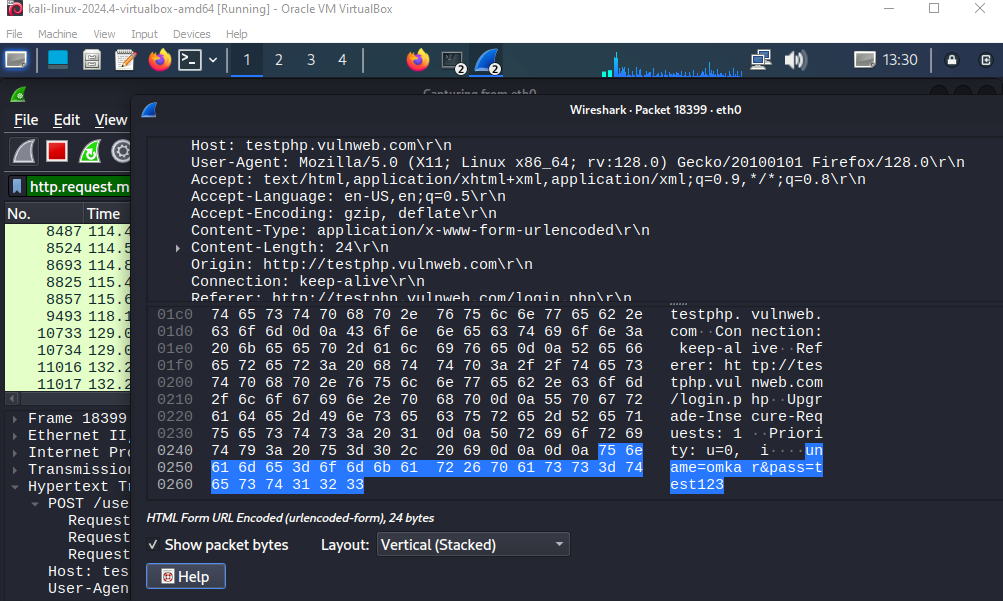
# 3. Methodology

1. Configured Kali Linux VM and connected it to the same network as the Windows host.  
2. Launched Ettercap in GUI mode and selected Unified Sniffing on the network interface (eth0).  
3. Scanned for hosts and identified the Windows host and router IPs.  
4. Assigned the victim IP to Target 1 and the router IP to Target 2.  
5. Enabled ARP poisoning with sniff remote connections enabled.  
6. Started packet capture using Wireshark on interface eth0 with an HTTP filter.  
7. Accessed the test site from the Windows host and submitted login credentials.  
8. Captured and analyzed the HTTP POST request containing username and password in Wireshark.

# 4. Screenshots



Ettercap running with ARP poisoning and Unified Sniffing enabled



Wireshark capturing HTTP POST request with captured credentials

# 5. Conclusion

The MITM attack using Ettercap and Wireshark was successful in capturing HTTP login credentials. This highlights the importance of using HTTPS for secure data transmission over networks, as HTTP is vulnerable to sniffing attacks like MITM.