E&ICT IIT KANPUR ETHICAL HACKING SUMMER TRAINING PROGRAM - MINI PROJECT REPORT

Capturing FTP and SMB Credentials using sniffing tools

Shameer Basha Shaik

Contents:

Introduction:

This project demonstrates a Man-in-the-Middle (MITM) attack to capture FTP and SMB credentials using Kali Linux between two Ubuntu 24.04 VMs (Server and Client) in VMware. The Server Ubuntu hosts FTP/SMB services, the Client Ubuntu generates traffic, and Kali intercepts the credentials in Bridged network mode, highlighting network security vulnerabilities.

Objective

To capture FTP and SMB credentials (victimuser:victimpass) by performing a Man-in-the-Middle (MITM) attack using **Kali Linux** between two **Ubuntu 24.04** VMs (Server Ubuntu and Client Ubuntu) in VMware, utilizing a Bridged network adapter.

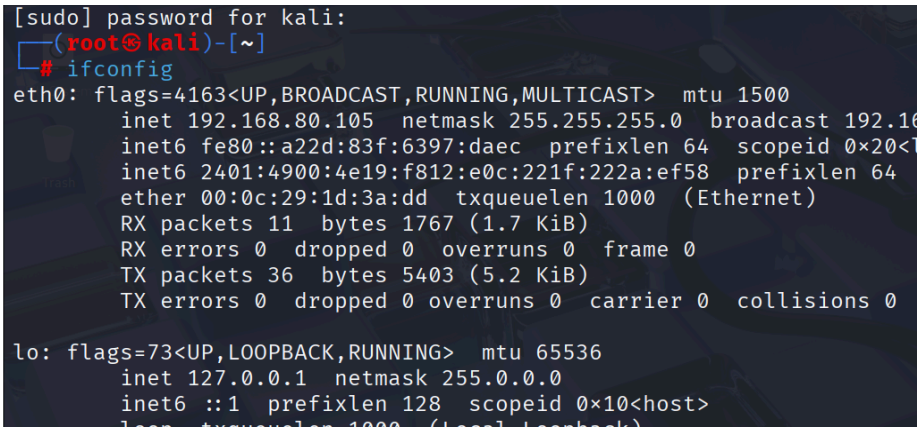
Tools and Environment

- **Hardware**: Laptop connected to a mobile hotspot.
- **Software**:
    - VMware Workstation.
    - Kali Linux (MITM).
    - Two Ubuntu 24.04 VMs:
        - Server Ubuntu (FTP/SMB server, IP: 192.168.80.19).
        - Client Ubuntu (FTP/SMB client, IP: 192.168.80.139).
- **Network**: Bridged mode (connected to mobile hotspot, gateway).
- **Tools**: Ettercap, arpspoof.

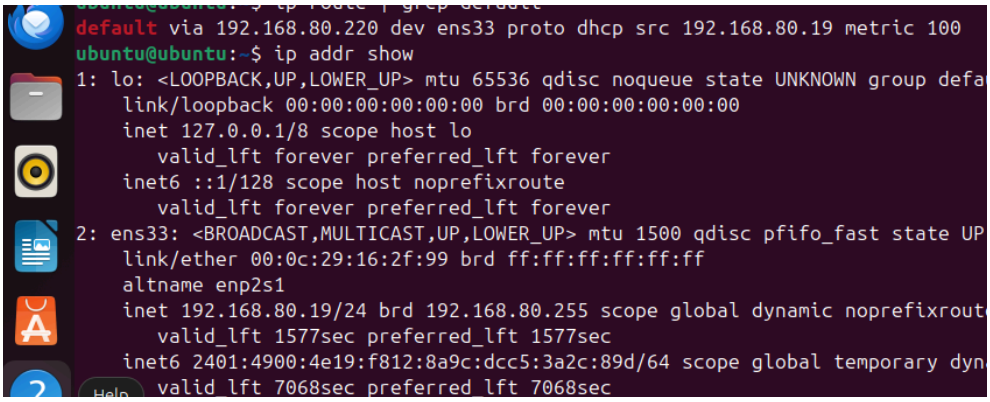
Procedure

Network Setup:

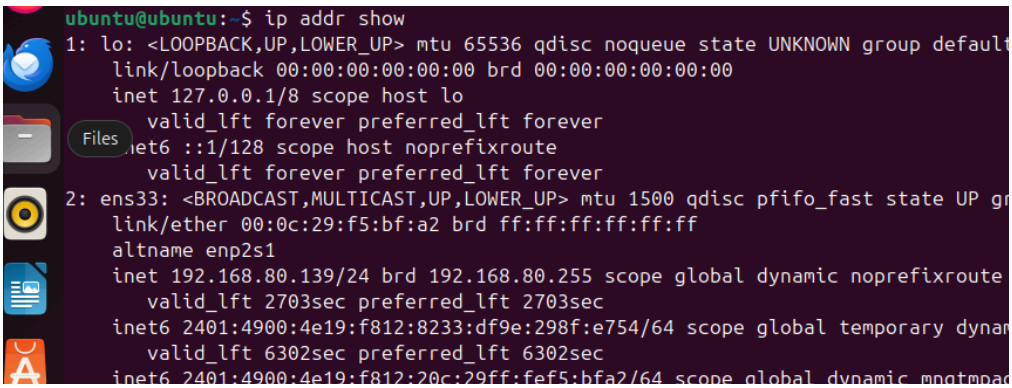
- Both VMs were configured in Bridged mode to join the local network (192.168.80.x).
- IPs:
    - Server Ubuntu: 192.168.80.19
    - Client Ubuntu: 192.168.80.139
    - Kali linux : 192.168.80.105



Kali → attacker :192.168.80.105



Ubuntu → server : 192.168.80.19

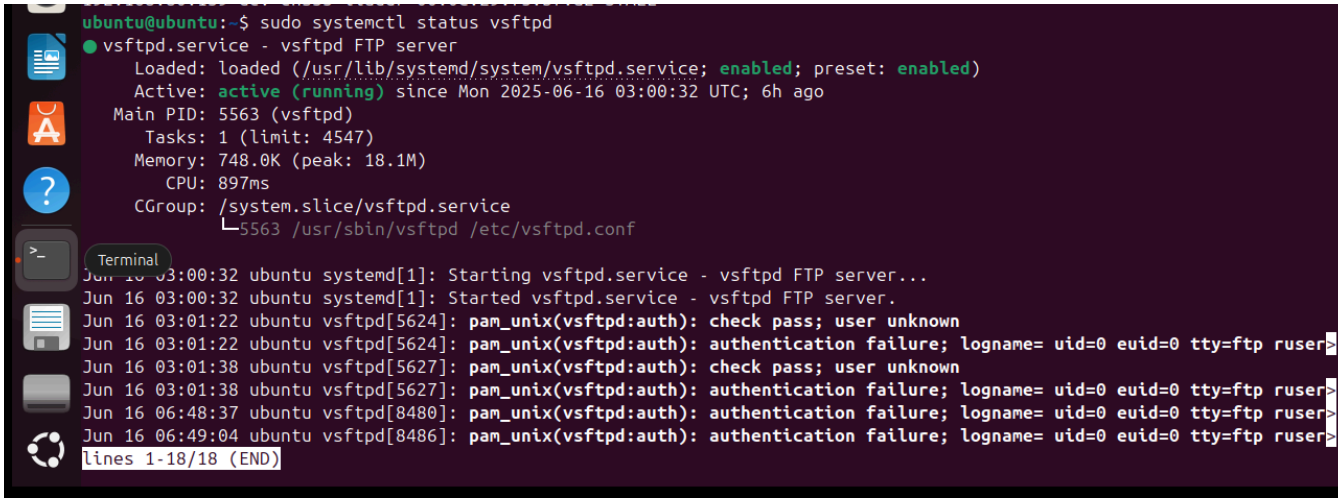


Ubuntu → Client : 192.168.80.139

Server Setup (Server Ubuntu)

FTP (vsftpd):

- Installed: sudo apt install vsftpd -y.
- Started: sudo systemctl start vsftpd.



SMB (Samba):

- Installed: sudo apt install samba -y.

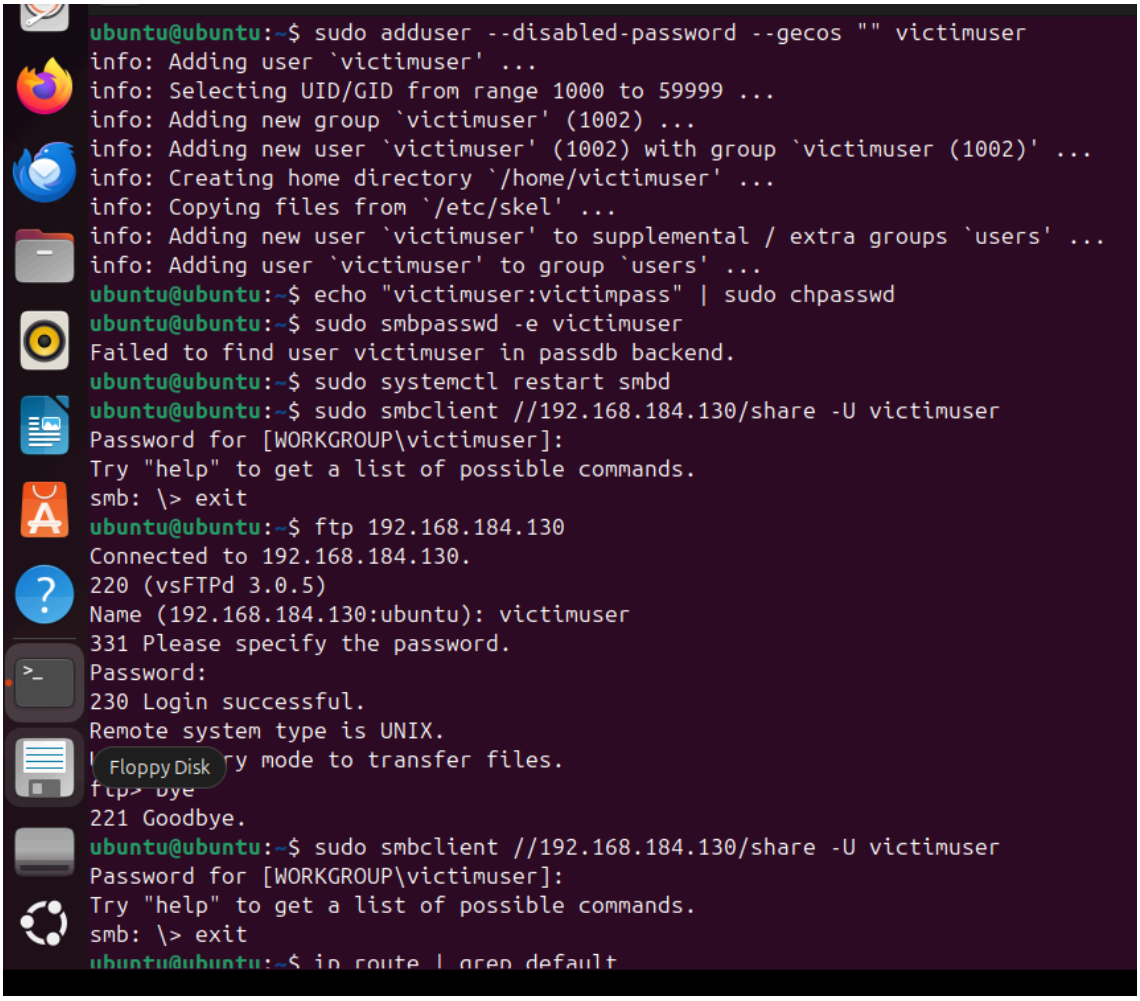
Created share directory:

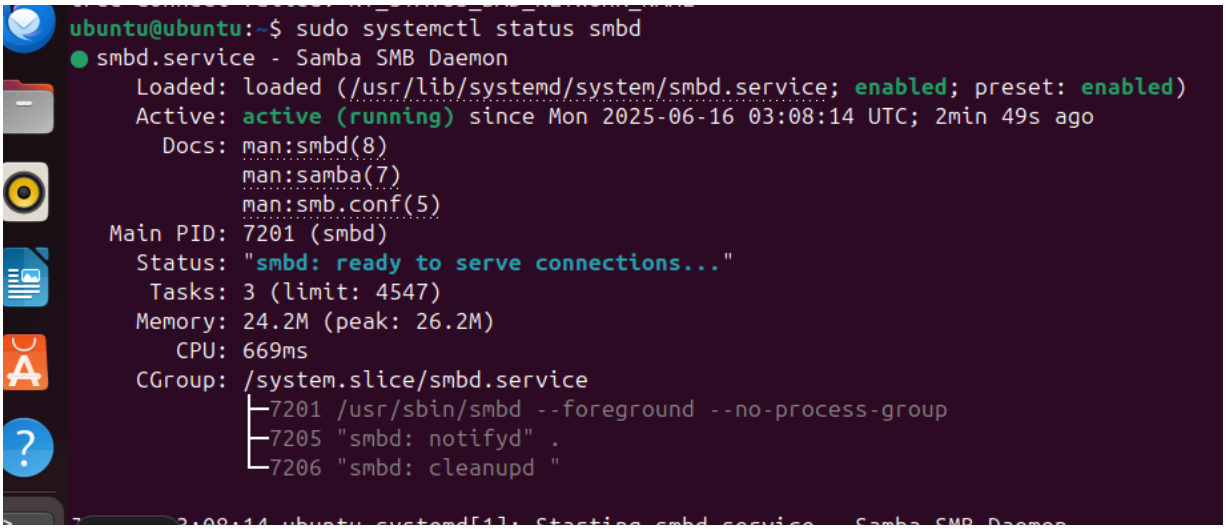
- sudo mkdir -p /srv/samba/share
- sudo chmod -R 777 /srv/samba/share

Added user:

- sudo adduser --disabled-password victimuser
- echo "victimuser:victimpass" | sudo chpasswd
- sudo smbpasswd -a victimuser.
- Started: sudo systemctl start smbd.

```
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package smbd
ubuntu@ubuntu:~$ sudo apt install samba -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  attr ibverbs-providers libattr1 libcephfs2 libibverbs1 librados2 librdma
  python3-gpg python3-ldb python3-markdown python3-samba python3-talloc py
  samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
Suggested packages:
  python3-trio python3-aioquic python3-h2 python3-httpx python3-httpcore p
  ldb-tools ntp | chrony winbind heimdal-clients
The following NEW packages will be installed:
  attr libcephfs2 librados2 librdmacm1t64 liburing2 python3-dnspython pyth
  python3-samba python3-talloc python3-tdb samba samba-ad-provision samba-
```

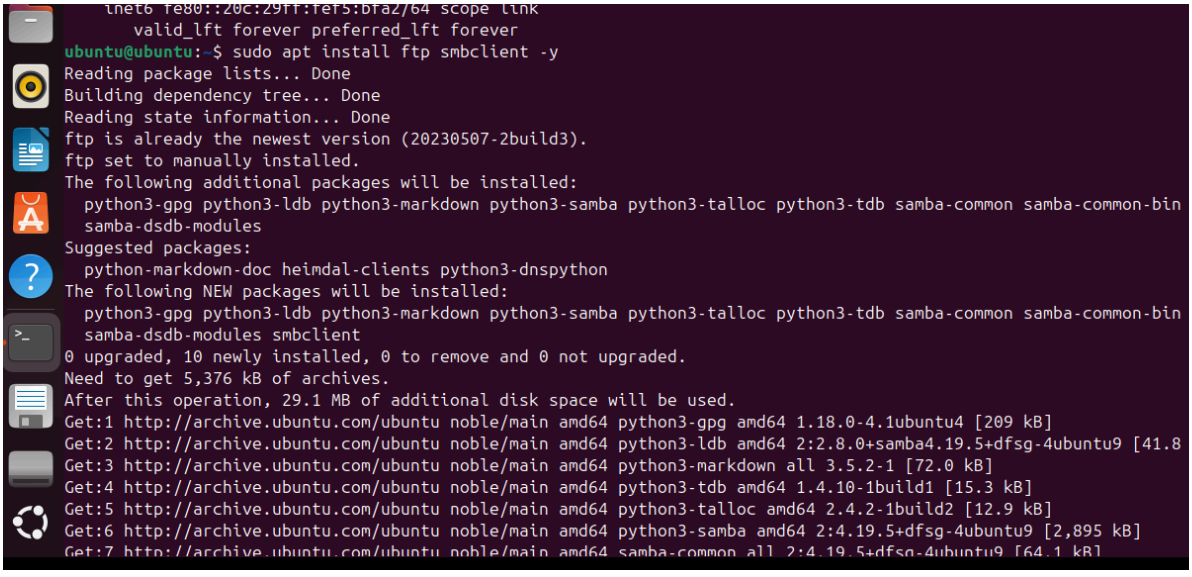




Client Setup (Client Ubuntu)

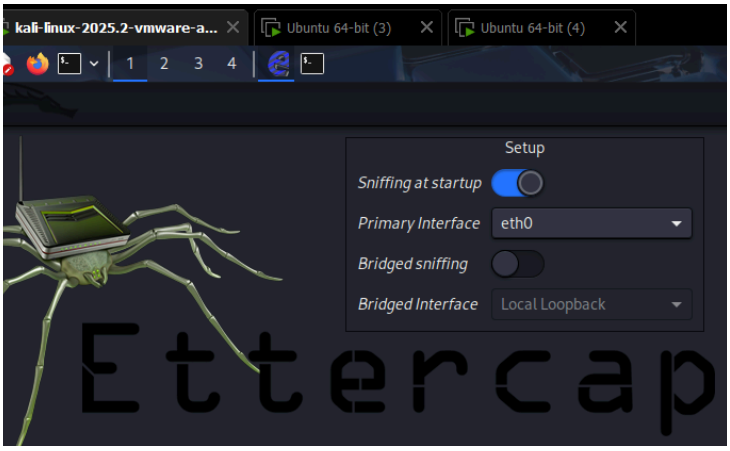
Installed FTP and SMB clients:

- sudo apt update
- sudo apt install ftp smbclient -y

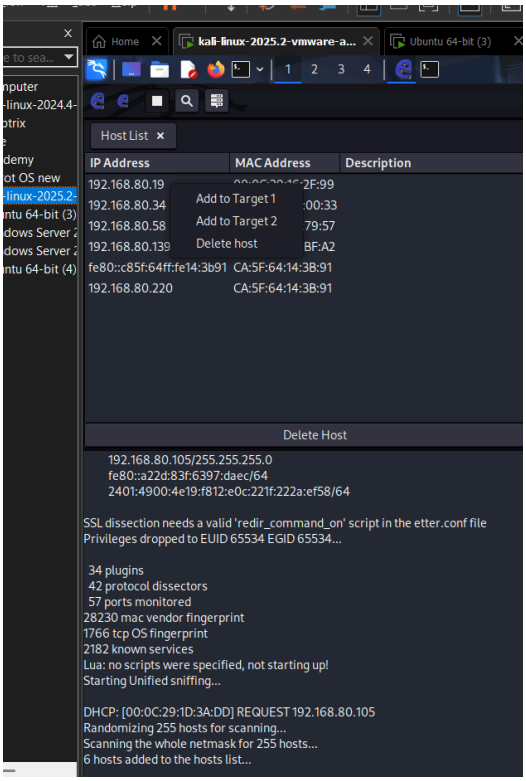


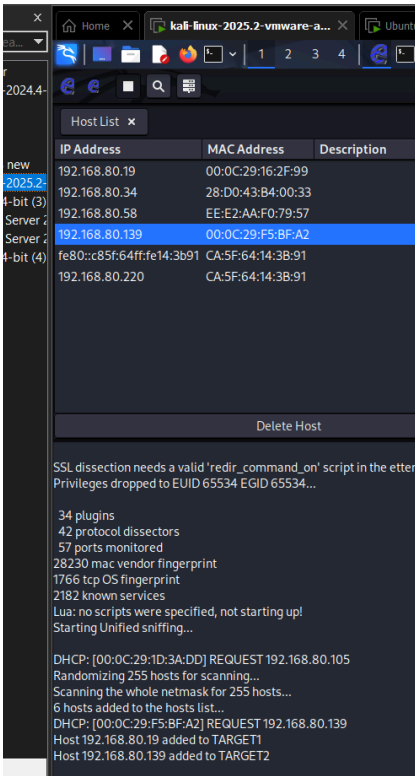
MITM Setup (Kali Linux)

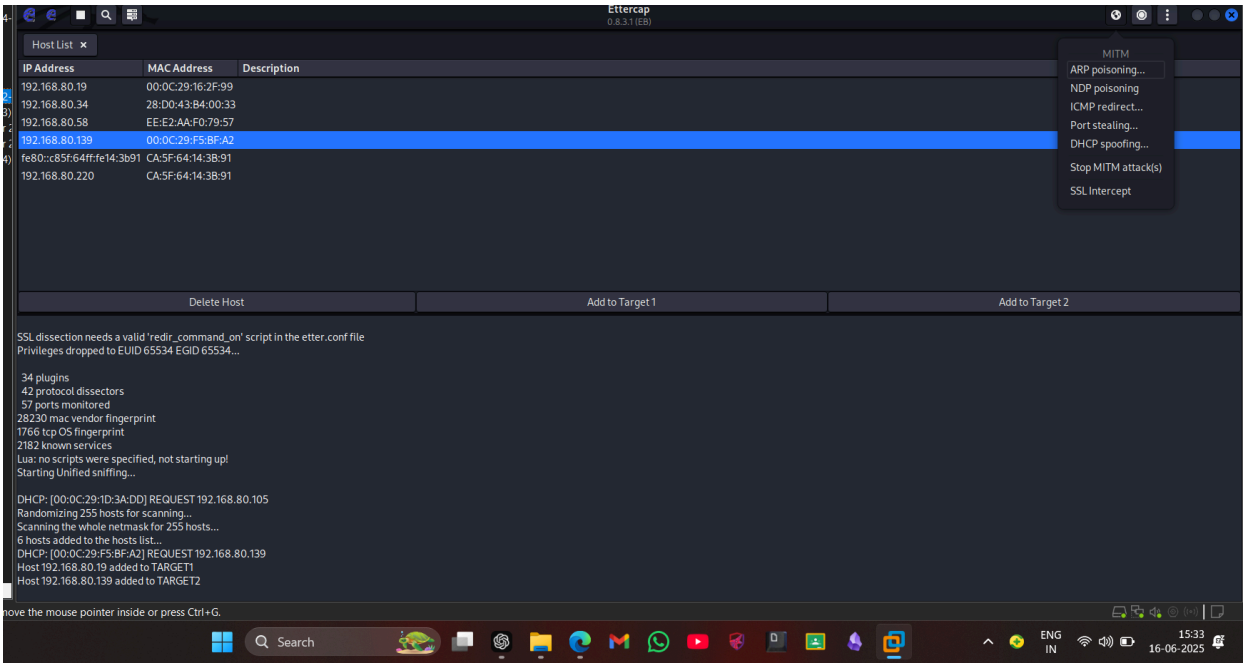
- Used Ettercap to spoof between Server Ubuntu and Client Ubuntu:



Opening ettercap GUI interface from tools and set eth0 interface

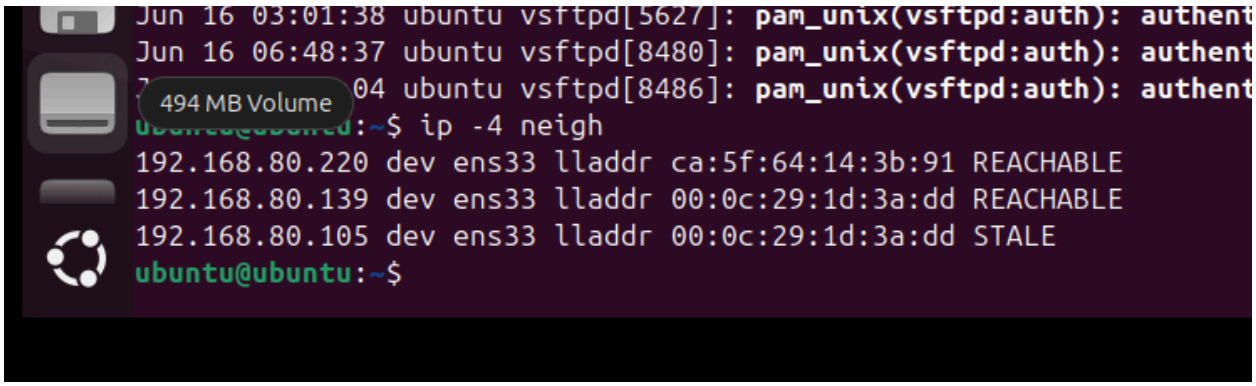






Verified ARP poisoning:

- On Server Ubuntu: ip -4 neigh (showed Kali's MAC for 192.168.1.129).



Traffic Generation

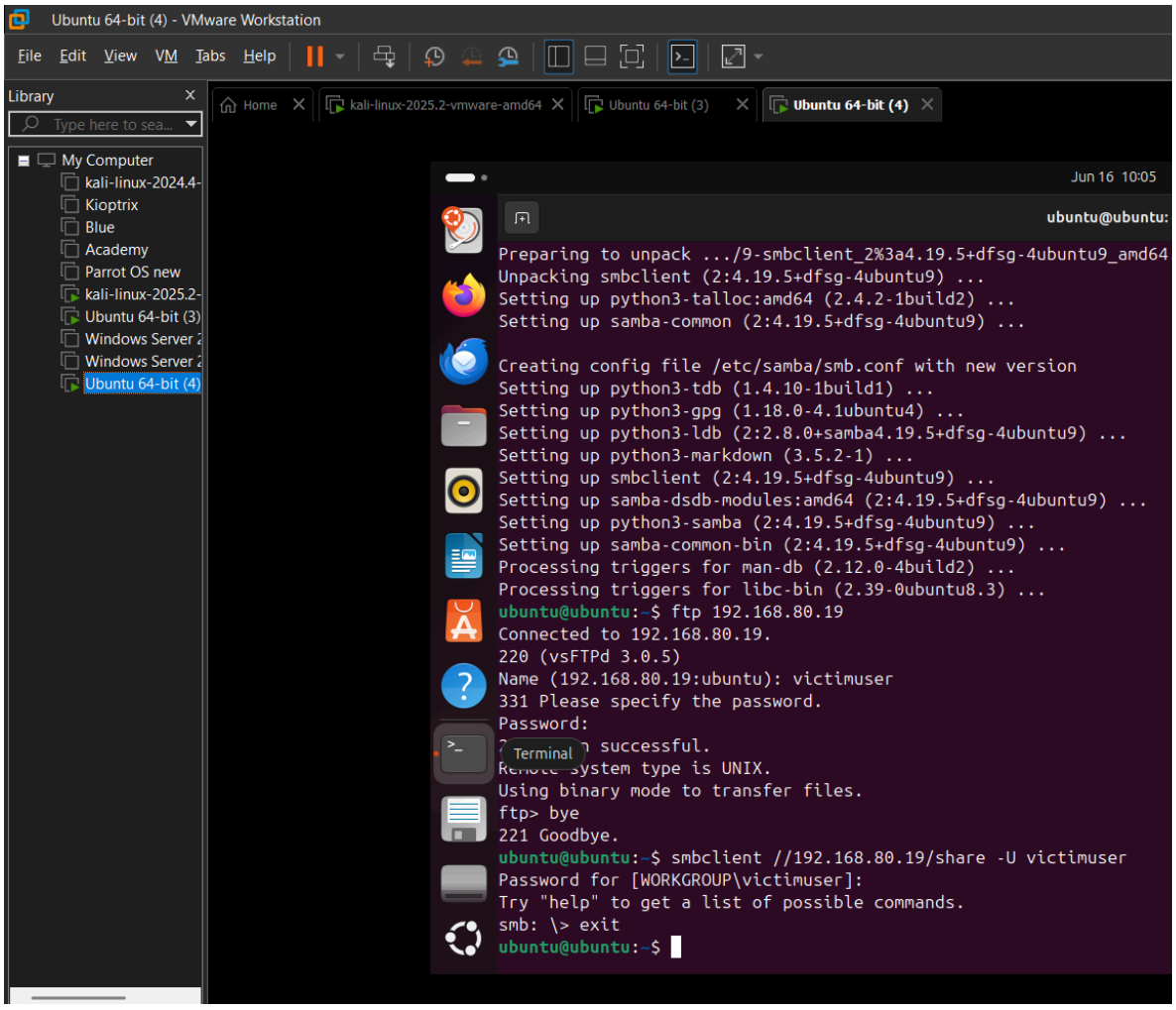
On Client Ubuntu:

- FTP:
  ftp 192.168.1.128

  # Username: victimuser, Password: victimpass, then bye

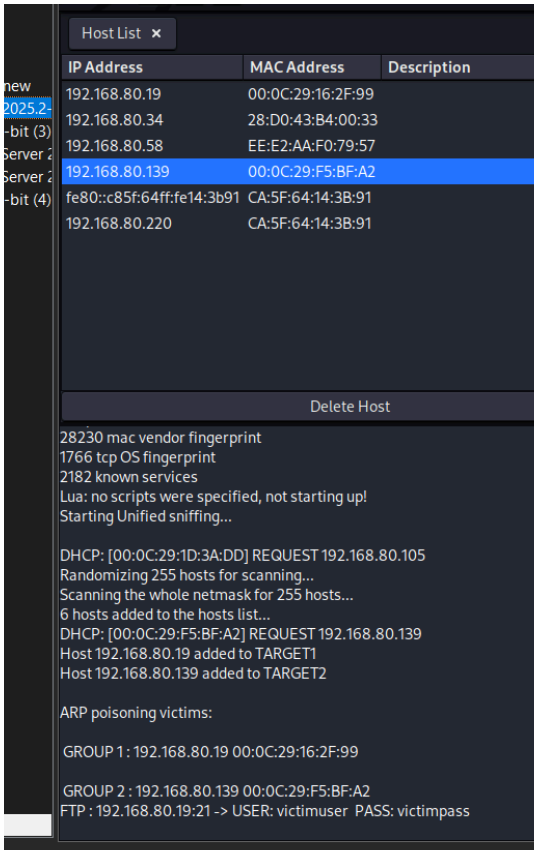
- SMB:
  smbclient //192.168.1.128/share -U victimuser

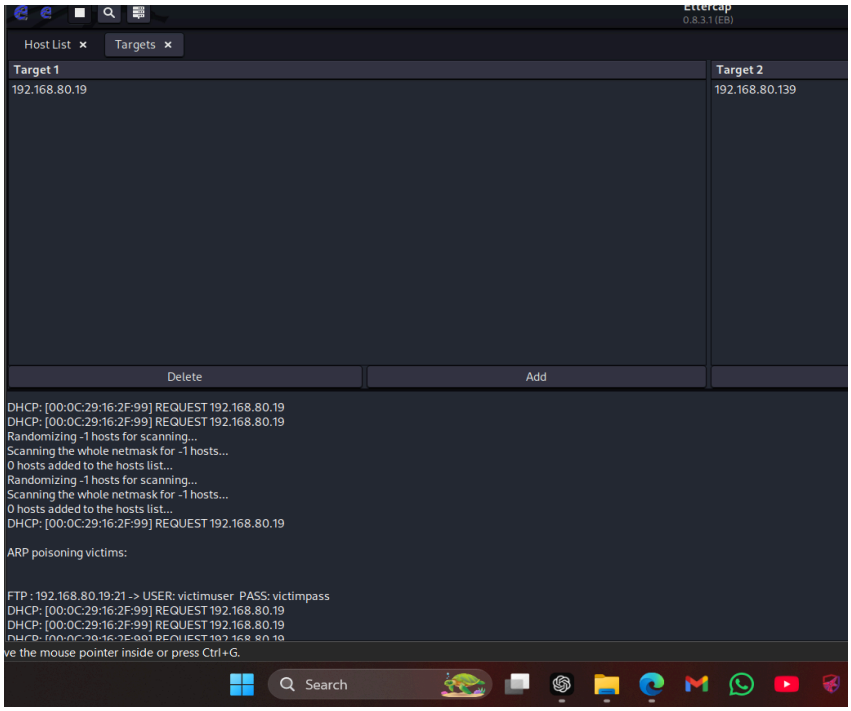
  # Password: victimpass, then exit



Credential Capture

- Ettercap on Kali captured the credentials:



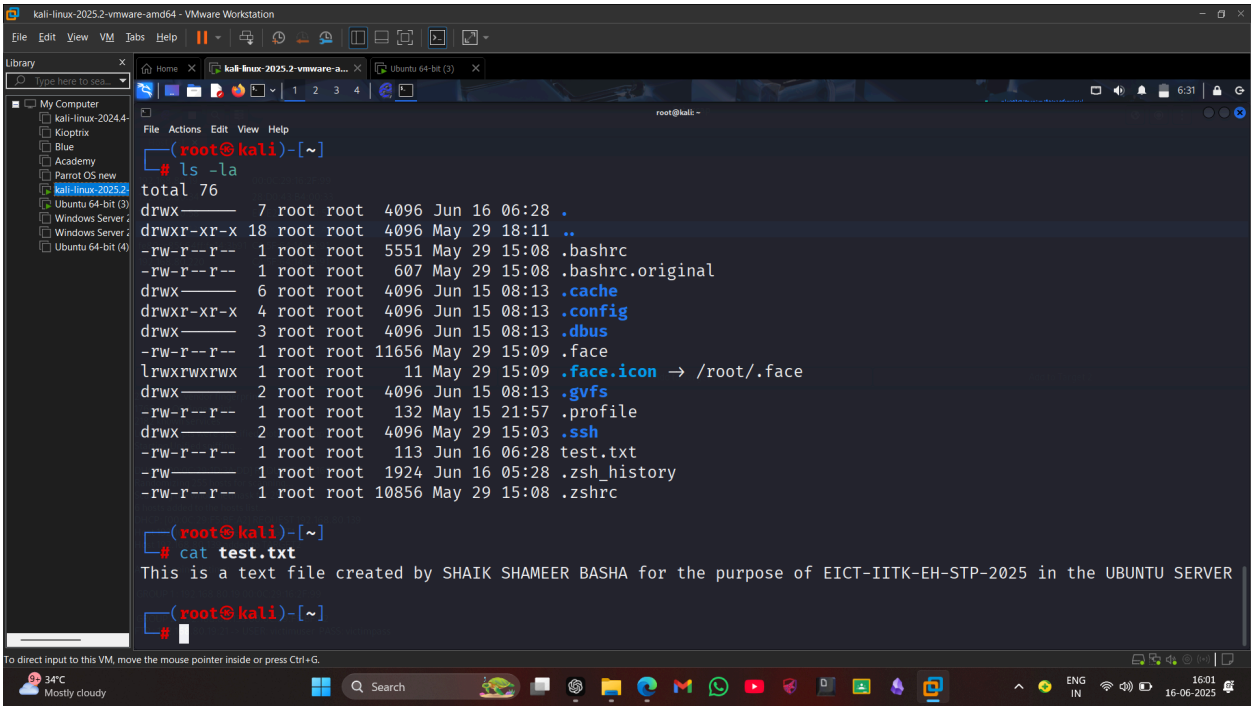


File Transfer

- dir → Displays the files in the directory
- get test.txt → downloads the file to the attacker kali

```
┌──(root㉿kali)-[~]
└─# smbclient //192.168.80.19/share -U victimuser
Password for [WORKGROUP\victimuser]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jun 16 06:27:22 2025
  ..                                  D        0  Mon Jun 16 06:27:22 2025
  test.txt                            N      113  Mon Jun 16 06:27:22 2025

                1980488 blocks of size 1024. 1477740 blocks available
smb: \> get test.txt
getting file \test.txt of size 113 as test.txt (8.5 KiloBytes/sec) (average 8.5 KiloBytes/sec)
smb: \> exit
```



Shell-gpt

- ARP Spoofing with arpspoof
    - sgpt "Generate commands to enable IP forwarding and perform ARP spoofing between 192.168.1.128 and 192.168.1.129 on interface eth0 using arpspoof on Kali Linux."
    - **Work Done**: Sets up MITM by enabling IP forwarding and ARP spoofing between Server Ubuntu and Client Ubuntu.
    - **Comparison to Manual**: Automates command generation, saving time over manually recalling and typing sysctl and arpspoof commands, reducing syntax errors.
- Ettercap for MITM and Credential Capture
    - sgpt "Provide a command to use Ettercap on Kali Linux to perform ARP poisoning between 192.168.1.128 and 192.168.1.129 on interface eth0 to capture FTP/SMB credentials."
    - **Work Done**: Performs ARP poisoning and captures credentials (victimuser:victimpass) from FTP/SMB traffic.
    - **Comparison to Manual**: Generates the exact Ettercap command, avoiding the need to remember complex options like -M arp:remote.
- Traffic Capture with tcpdump
    - sgpt "Generate a tcpdump command to capture FTP and SMB traffic on interface eth0 in ASCII format on Kali Linux."
    - **Work Done**: Captures FTP (port 21) and SMB (port 445) traffic to verify credentials.
    - **Comparison to Manual**: Simplifies filter syntax creation (tcp port 21 or tcp port 445), ensuring accurate traffic capture without manual trial-and-error.
- Access SMB Share to Retrieve File
    - sgpt "Provide commands to connect to an SMB share at 192.168.1.128/share using smbclient with username victimuser, list files, and download testfile.txt on Kali Linux."

- **Work Done**: Connects to the SMB share, lists files, and downloads testfile.txt.
- **Comparison to Manual**: Automates the sequence of smbclient commands, eliminating the need to manually type and recall dir, get, and exit steps.

Conclusion

The project successfully captured FTP and SMB credentials using an MITM attack. Bridged mode was critical for ensuring network traffic was interceptable, and using two separate VMs avoided loopback issues. This demonstrates the importance of network configuration in security testing.