

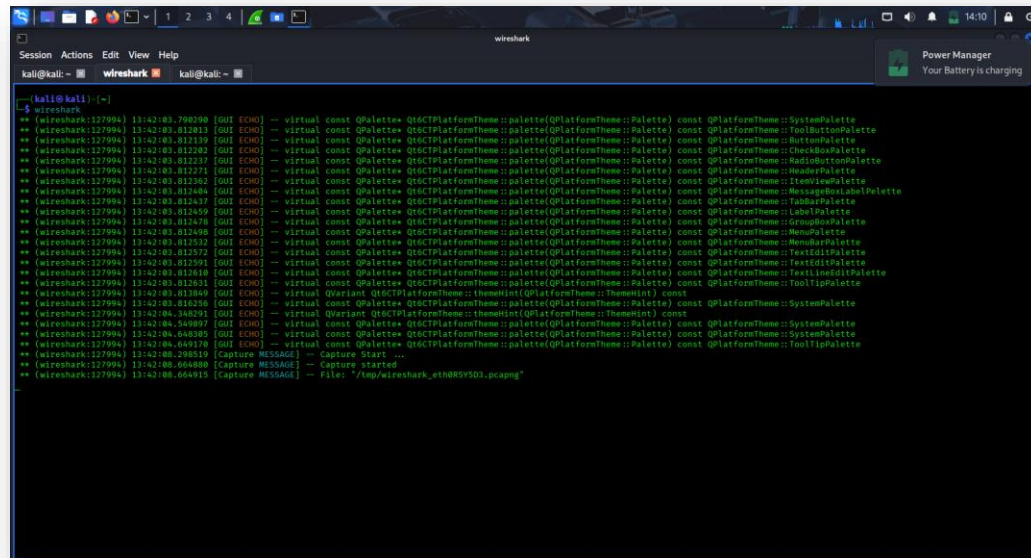
ARP Spoofing & FTP Credential Sniffing

-
REPORT

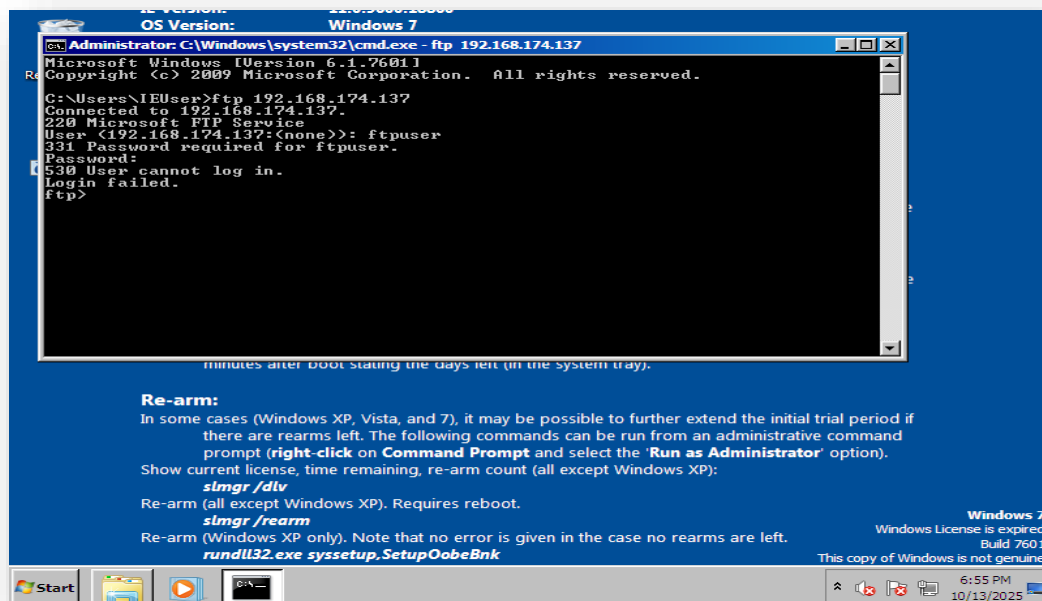
Prepared by: Ahmed Moataz Abdelmonem Elrefaey

Part 2: Sniff Traffic with Wireshark

- Launch Wireshark
wireshark



- Connect from FTP Client and Enter credentials
ftp 192.168.174.137



- Search for FTP packets
`tcp.port == 21`

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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 | 1321.9415573 | 192.168.174.134 | 192.168.174.137 | TCP | 60 | 49197 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0 |
| 5493 | 1321.9419074 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 5494 | 1321.9420045 | 192.168.174.137 | 192.168.174.134 | TCP | 81 | [TCP Retransmission] 21 → 49197 [PSH, ACK] Seq=1 Ack=1 Win=64240 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=0 |
| 5550 | 1332.0989140 | 192.168.174.134 | 192.168.174.137 | FTP | 68 | Request: USER ftpuser |
| 5551 | 1332.1003097 | 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 | 1332.1003809 | 192.168.174.132 | 192.168.174.137 | TCP | 90 | [TCP Retransmission] 21 → 49197 [PSH, ACK] Seq=28 Ack=15 Win=64226 Len=36 |
| 5554 | 1332.3064459 | 192.168.174.134 | 192.168.174.137 | TCP | 60 | 49197 → 21 [ACK] Seq=15 Ack=64 Win=8129 Len=0 |
| 5552 | 1332.3120574 | 192.168.174.137 | 192.168.174.134 | FTP | 68 | Request: PASS ftpuser |
| 5563 | 1336.3747251 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 5564 | 1336.3747493 | 192.168.174.132 | 192.168.174.137 | ICMP | 107 | Redirect (Redirect for host) |
| 5565 | 1336.3747801 | 192.168.174.137 | 192.168.174.134 | TCP | 70 | [TCP Retransmission] 21 → 49197 [PSH, ACK] Seq=64 Ack=30 Win=64211 Len=25 |
| 5568 | 1336.0970073 | 192.168.174.134 | 192.168.174.137 | TCP | 60 | 49197 → 21 [ACK] Seq=30 Ack=69 Win=8184 Len=0 |
| 6498 | 1463.0106297 | 192.168.174.137 | 192.168.174.134 | TCP | 60 | 21 → 49197 [RST, ACK] Seq=89 Ack=30 Win=0 Len=0 |
| 6499 | 1463.0172281 | 192.168.174.132 | 192.168.174.137 | ICMP | 82 | Redirect (Redirect for host) |
| 6500 | 1463.0172582 | 192.168.174.137 | 192.168.174.134 | TCP | 54 | 21 → 49197 [RST, ACK] Seq=89 Ack=30 Win=0 Len=0 |

wireshark_eth0FH52D3.pcapng

Packets: 10785 - Displayed: 49 (0.5%) - Selected: 4 (0.0%) - Profile: Default

ftp

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

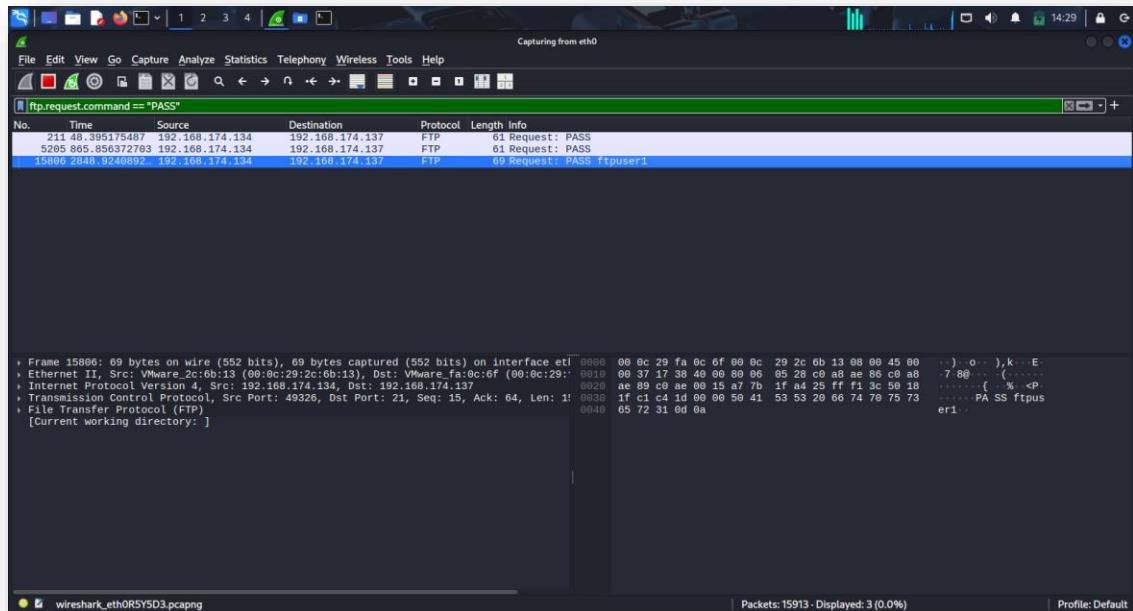
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|-----------------|-----------------|----------|--------|--|
| 157 | 38.233648404 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 236 | 50.694391065 | 192.168.174.134 | 192.168.174.137 | FTP | 67 | Request: USER hacker |
| 237 | 50.694675833 | 192.168.174.137 | 192.168.174.134 | FTP | 89 | Response: 331 Password required for hacker. |
| 245 | 56.487529100 | 192.168.174.134 | 192.168.174.137 | FTP | 68 | Request: PASS hacker1 |
| 246 | 56.488222591 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 5113 | 1248.7624203 | 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 | 1258.8231003 | 192.168.174.137 | 192.168.174.134 | FTP | 90 | Response: 331 Password required for arpuser. |
| 5229 | 1264.1266413 | 192.168.174.134 | 192.168.174.137 | FTP | 69 | Request: PASS arpuser1 |
| 5230 | 1264.1435253 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 5493 | 1321.9419974 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 5550 | 1332.0989446 | 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: 530 User cannot log in. |

File Transfer Protocol (FTP): Protocol

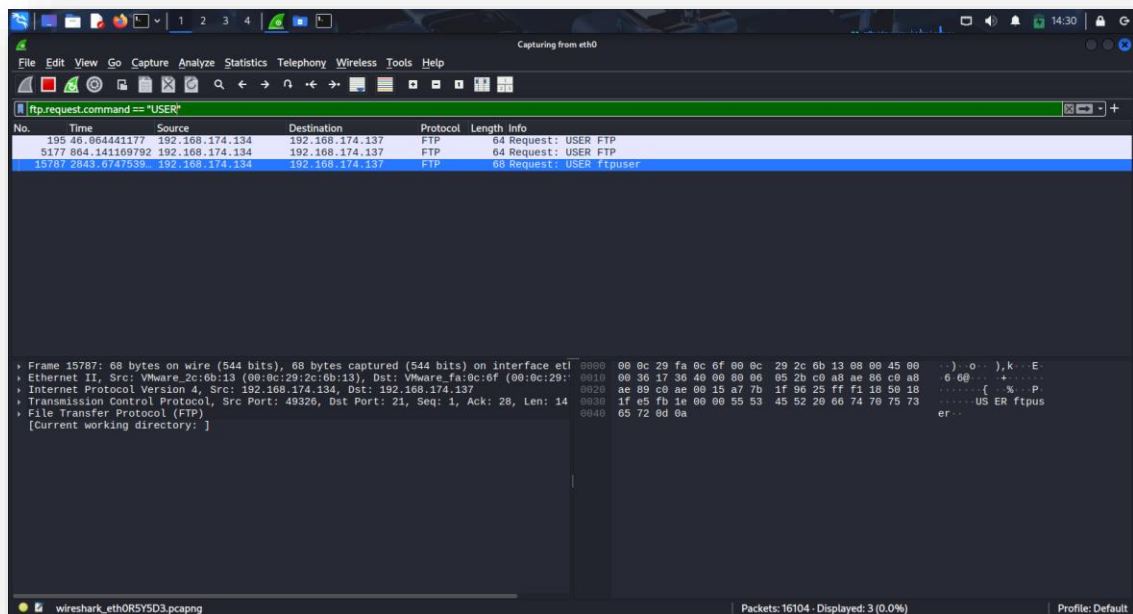
Packets: 11017 - Displayed: 15 (0.1%) - Selected: 5 (0.0%) - Profile: Default

Part 3: Analyze FTP Credentials

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



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

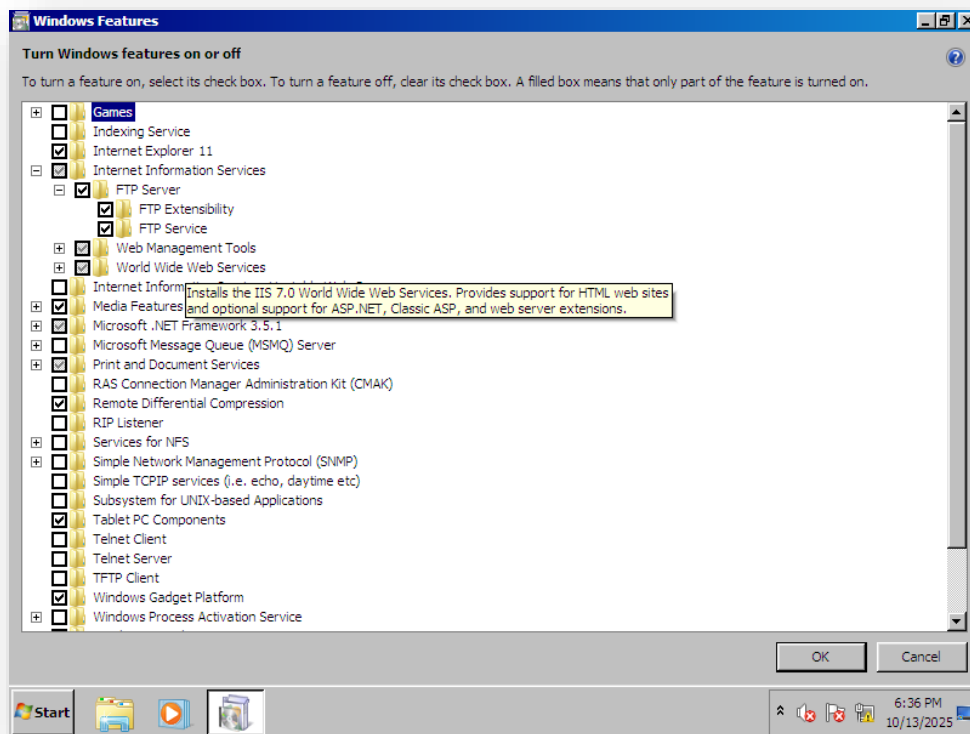


Short Explanation

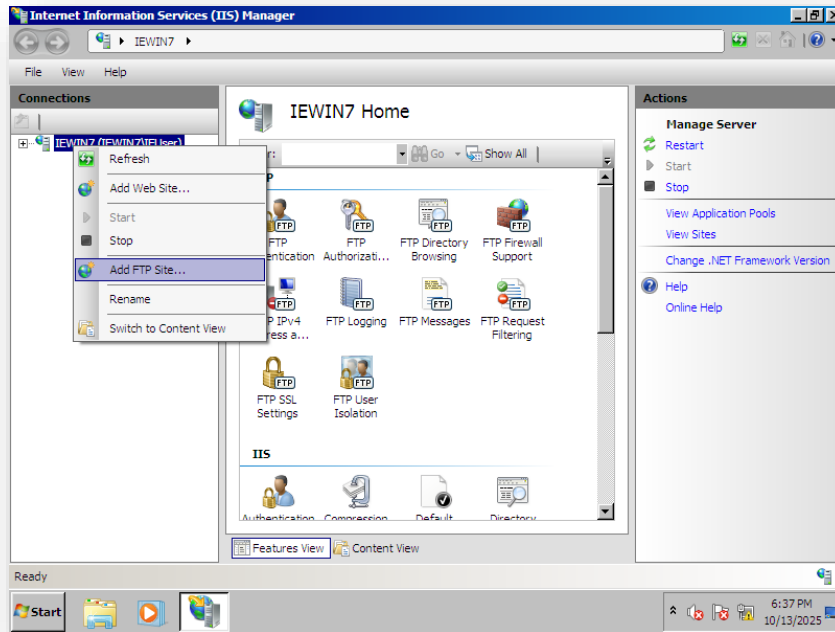
ARP spoofing was successfully executed to poison the ARP tables of both FTP client and server, creating a Man-in-the-Middle position. This allowed interception of all unencrypted FTP traffic between the victims. Wireshark captured cleartext FTP credentials (USER and PASS commands).

Bonus

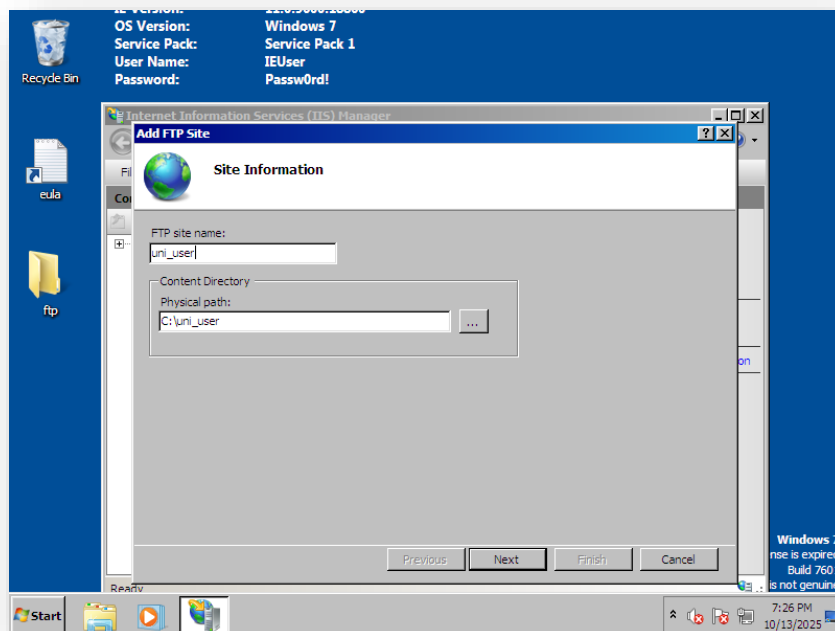
- Create a new user on the FTP server (VM1) with a unique username and password.
 - ❖ Enable IIS and FTP Server from “turn windows features on or off” # **I did these steps before Part 1 but without creating user with password**



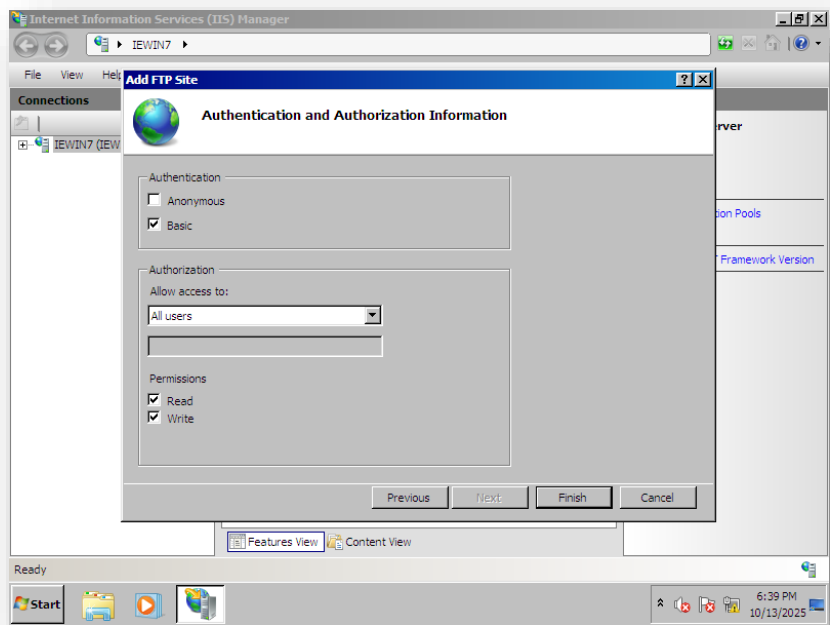
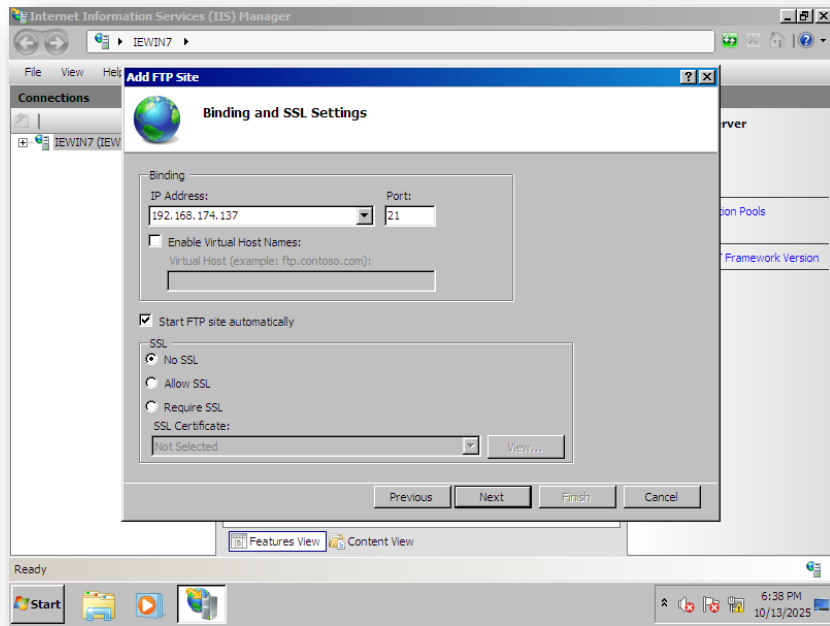
❖ Open IIS and right click on PC-User then **Add FTP site**



❖ Create FTP site



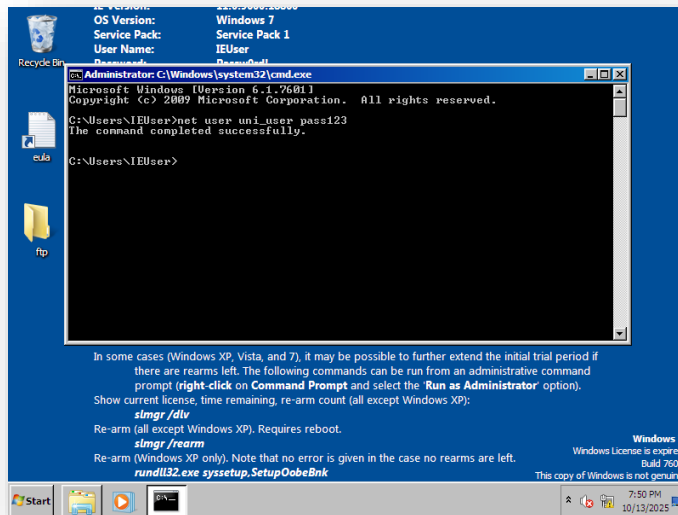
❖ Setup FTP site



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

- Create New User on FTP Server

`net user uni_user pass123 /add`



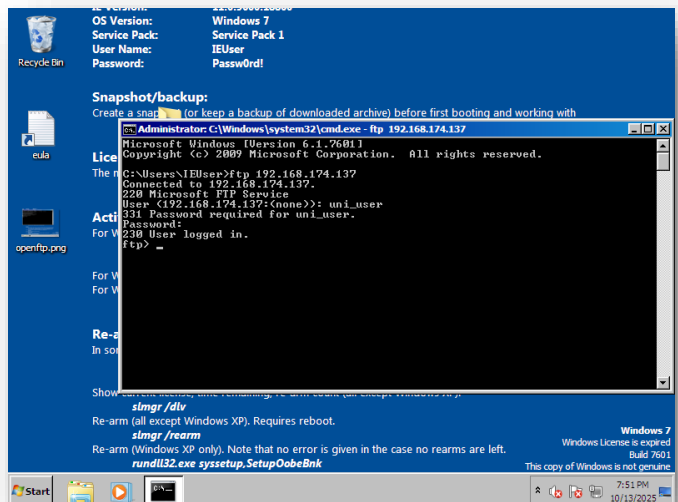
- Capture New User Traffic

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

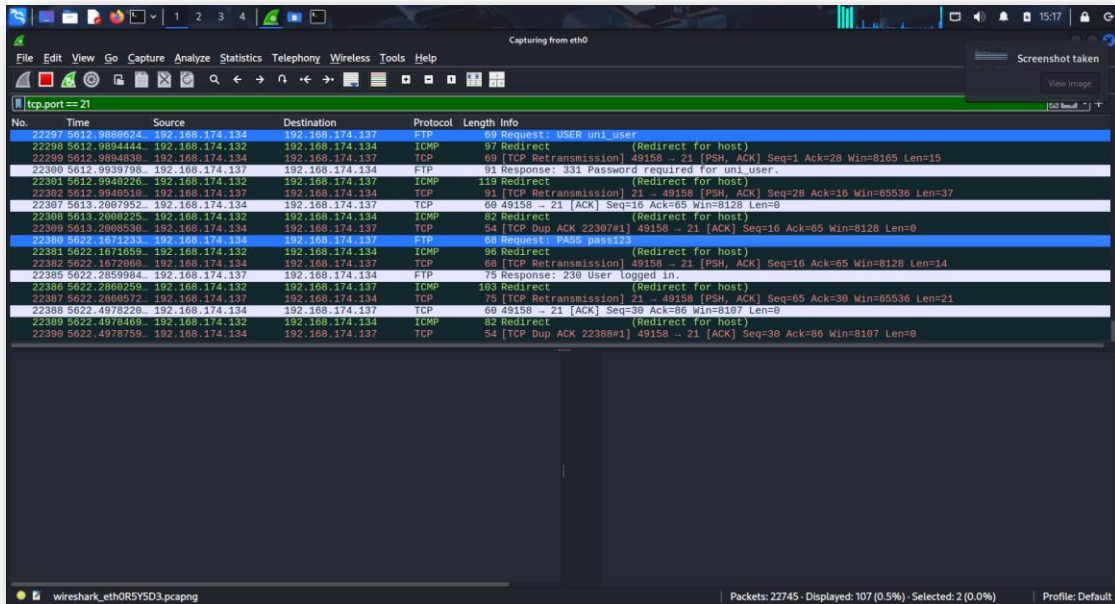
`ftp 192.168.174.137`

`User: uni_user`

`Pass: pass123`

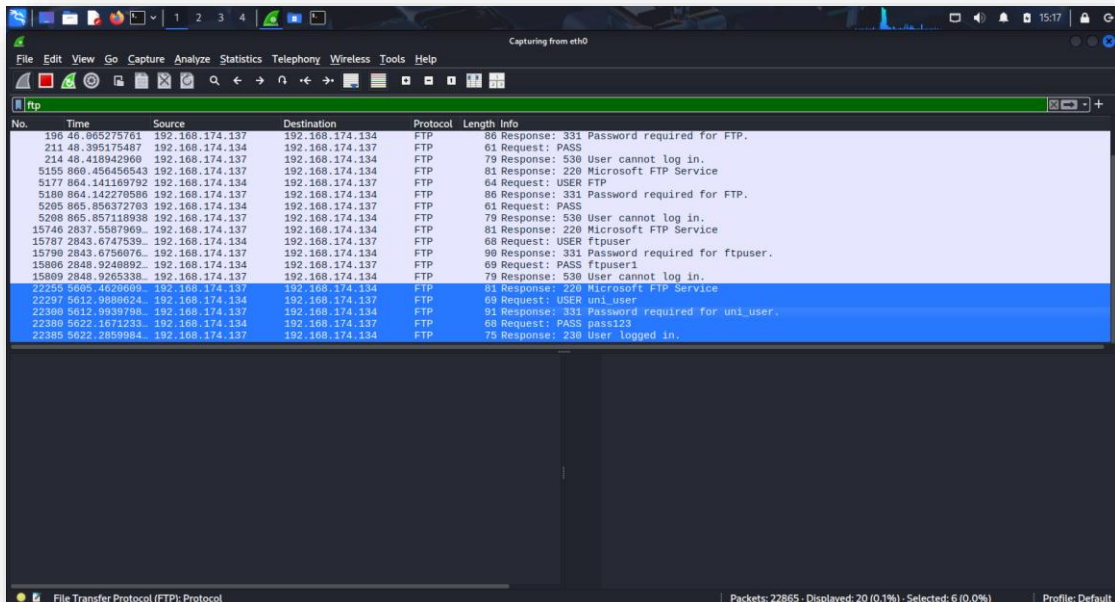


- Search for FTP packets
`tcp.port == 21`



| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|--------------|-----------------|-----------------|----------|--------|---|
| 22297 | 5612.9886924 | 192.168.174.134 | 192.168.174.137 | FTP | 69 | Request: USER uni_user |
| 22298 | 5612.9894444 | 192.168.174.132 | 192.168.174.134 | ICMP | 97 | Redirect (Redirect for host) |
| 22299 | 5612.9894830 | 192.168.174.134 | 192.168.174.137 | TCP | 69 | [TCP Retransmission] 49158 → 21 [PSH, ACK] Seq=1 Ack=28 Win=8165 Len=15 |
| 22300 | 5612.9939798 | 192.168.174.137 | 192.168.174.134 | FTP | 91 | Response: 331 Password required for uni_user. |
| 22301 | 5612.9949226 | 192.168.174.132 | 192.168.174.137 | ICMP | 119 | Redirect (Redirect for host) |
| 22302 | 5612.9948518 | 192.168.174.137 | 192.168.174.134 | TCP | 91 | [TCP Retransmission] 21 → 49158 [PSH, ACK] Seq=28 Ack=16 Win=65536 Len=37 |
| 22307 | 5613.2087952 | 192.168.174.134 | 192.168.174.137 | TCP | 60 | 49158 → 21 [ACK] Seq=16 Ack=65 Win=8128 Len=0 |
| 22308 | 5613.2088225 | 192.168.174.132 | 192.168.174.134 | ICMP | 82 | Redirect (Redirect for host) |
| 22309 | 5613.2088530 | 192.168.174.134 | 192.168.174.137 | TCP | 84 | [TCP Dup ACK 22307#1] 49158 → 21 [ACK] Seq=16 Ack=65 Win=8128 Len=0 |
| 22380 | 5622.1671233 | 192.168.174.134 | 192.168.174.137 | FTP | 68 | Request: PASS pass123 |
| 22381 | 5622.1671059 | 192.168.174.132 | 192.168.174.134 | ICMP | 90 | Redirect (Redirect for host) |
| 22382 | 5622.1672060 | 192.168.174.134 | 192.168.174.137 | TCP | 68 | [TCP Retransmission] 49158 → 21 [PSH, ACK] Seq=16 Ack=65 Win=8128 Len=14 |
| 22383 | 5622.2850904 | 192.168.174.137 | 192.168.174.134 | FTP | 19 | Response: 330 User logged in |
| 22386 | 5622.2860259 | 192.168.174.132 | 192.168.174.137 | ICMP | 103 | Redirect (Redirect for host) |
| 22387 | 5622.2860572 | 192.168.174.134 | 192.168.174.137 | TCP | 75 | [TCP Retransmission] 21 → 49158 [PSH, ACK] Seq=30 Ack=66 Win=65536 Len=21 |
| 22388 | 5622.4978226 | 192.168.174.134 | 192.168.174.137 | TCP | 60 | 49158 → 21 [ACK] Seq=30 Ack=66 Win=8107 Len=0 |
| 22389 | 5622.4978400 | 192.168.174.132 | 192.168.174.137 | ICMP | 124 | Redirect (Redirect for host) |
| 22390 | 5622.4978759 | 192.168.174.134 | 192.168.174.137 | TCP | 84 | [TCP Dup ACK 22388#1] 49158 → 21 [ACK] Seq=30 Ack=66 Win=8107 Len=0 |

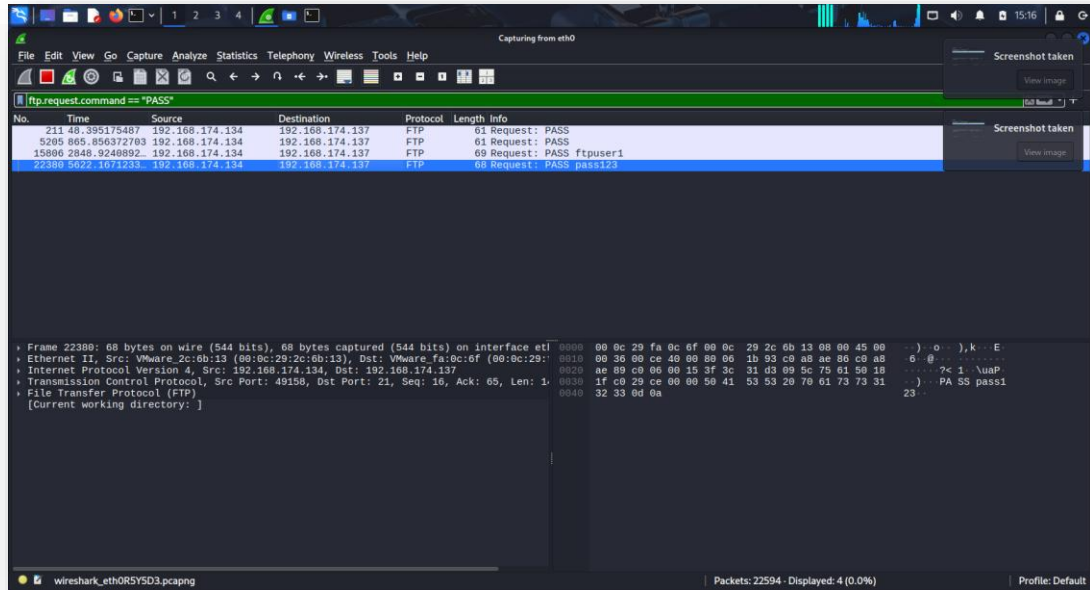
ftp



| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|---------------|-----------------|-----------------|----------|--------|---|
| 196 | 46.065275761 | 192.168.174.137 | 192.168.174.134 | FTP | 80 | Response: 331 Password required for FTP. |
| 211 | 48.395175487 | 192.168.174.134 | 192.168.174.137 | FTP | 61 | Request: PASS |
| 214 | 48.418942960 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 5155 | 860.456456543 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 5177 | 864.141189792 | 192.168.174.134 | 192.168.174.137 | FTP | 64 | Request: USER FTP |
| 5180 | 864.142279586 | 192.168.174.137 | 192.168.174.134 | FTP | 80 | Response: 331 Password required for FTP. |
| 5205 | 865.856372793 | 192.168.174.134 | 192.168.174.137 | FTP | 61 | Request: PASS |
| 5208 | 865.85718938 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 15746 | 2837.5587969 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 15787 | 2843.6747539 | 192.168.174.134 | 192.168.174.137 | FTP | 68 | Request: USER ftpuser |
| 15790 | 2843.6756976 | 192.168.174.137 | 192.168.174.134 | FTP | 80 | Response: 331 Password required for ftpuser. |
| 15806 | 2848.9248892 | 192.168.174.134 | 192.168.174.137 | FTP | 69 | Request: PASS ftpuser1 |
| 15809 | 2848.9265338 | 192.168.174.137 | 192.168.174.134 | FTP | 79 | Response: 530 User cannot log in. |
| 22255 | 5685.4629689 | 192.168.174.137 | 192.168.174.134 | FTP | 81 | Response: 220 Microsoft FTP Service |
| 22297 | 5612.9886924 | 192.168.174.134 | 192.168.174.137 | FTP | 69 | Request: USER uni_user |
| 22380 | 5612.9939798 | 192.168.174.137 | 192.168.174.134 | FTP | 91 | Response: 331 Password required for uni_user. |
| 22380 | 5622.1671233 | 192.168.174.134 | 192.168.174.137 | FTP | 68 | Request: PASS pass123 |
| 22385 | 5622.2859984 | 192.168.174.137 | 192.168.174.134 | FTP | 75 | Response: 330 User logged in. |

■ Locate Credentials in Wireshark

`ftp.request.command == "PASS"`



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

