Packet Sniffing and Credential Capture in a Controlled Lab Environment

1. Student Details

Name: Shubham Shah

Submission Date: 15/07/2025

2. Objective

To perform packet sniffing in a lab environment using appropriate tools and techniques in order to capture plaintext usernames and passwords transmitted over the network.

3. Tools & Technologies Used

- Operating System: Kali Linux / Windows
- Sniffing Tool: Wireshark
- Virtualization: VMware
- Network Type: Bridged
- Target Machine: Windows 10

4. Lab Setup

- One Attacker Machine (Kali Linux)
- One Victim Machine (Windows 10)
- Wireshark installed on attacker machine
- Same network interface used

5. Methodology

5.1. For Certifiedhacker.com

1. Enabled packet sniffing using Wireshark on interface eth0.
2. Started capturing traffic while victim accessed certifiedhacker.com whiles the victim connect with FTP using CMD and given port is 21.
3. Applied filters tcp.port == 21 on wireshark.
4. Identified IP Address and Port Number which containing form data.
5. Extracted credentials from the raw data or packet details.

5.2. For testphp.vulnweb.com

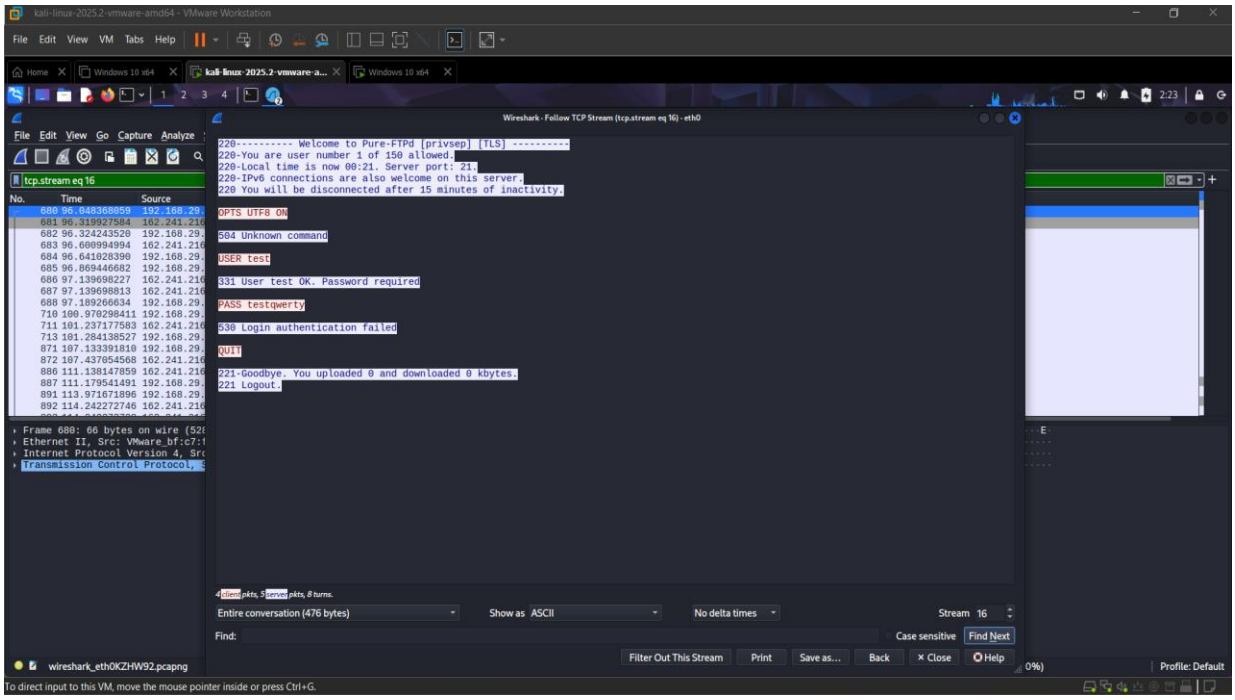
1. Enabled packet sniffing using Wireshark on interface eth0.
2. Started capturing traffic while victim accessed testphp.vulnweb.com.
3. Applied filters http on wireshark.
4. Identified HTTP POST which containing form data.
5. Extracted credentials from the raw data or packet details.

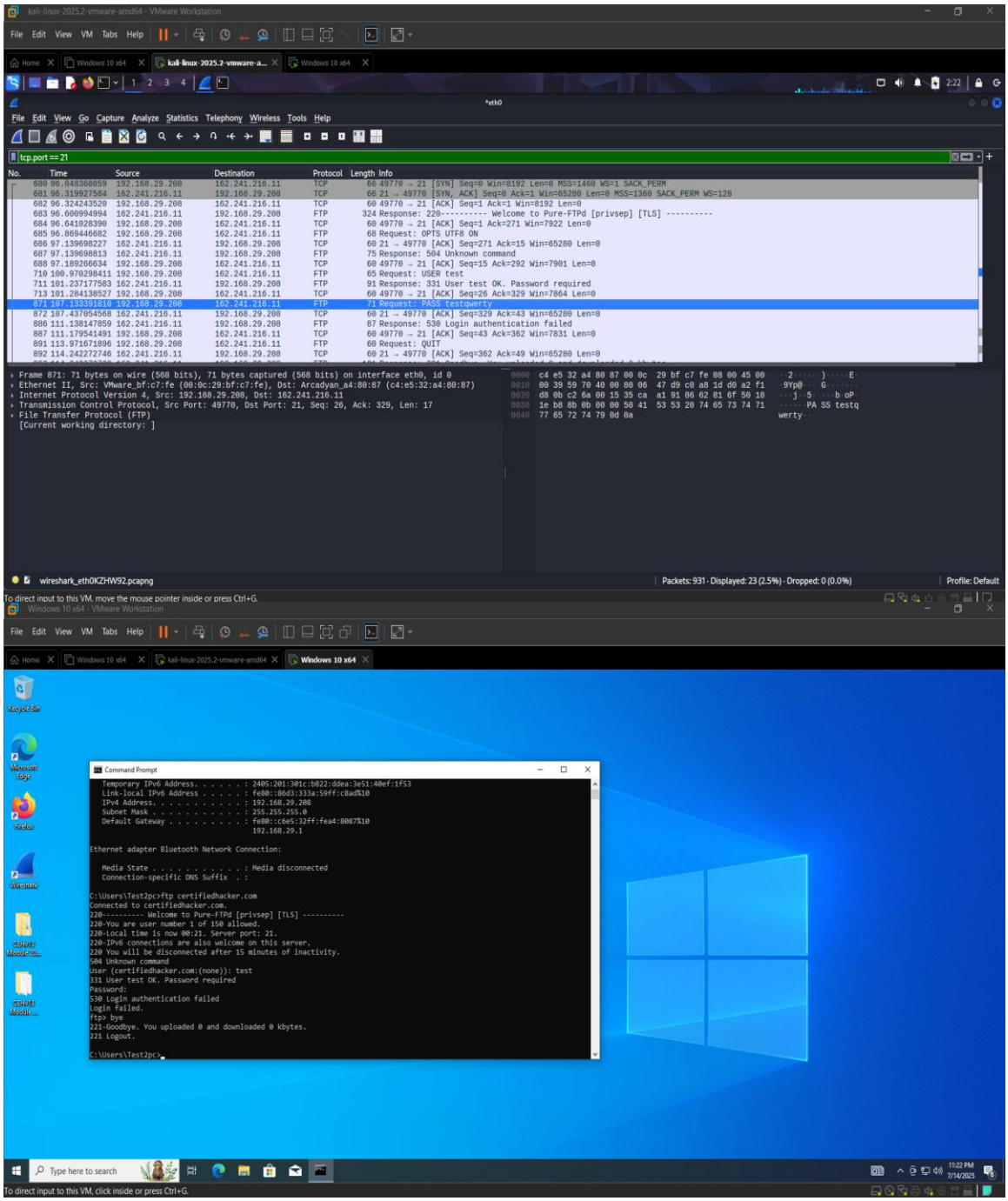
6. Observations

6.1. For Certifiedhacker.com

- Captured IP Address and Port Number.
- Username: test
- Password: testqwerty
- Protocol: FTP

Include screenshot(s) of:
- Packet capture showing credentials

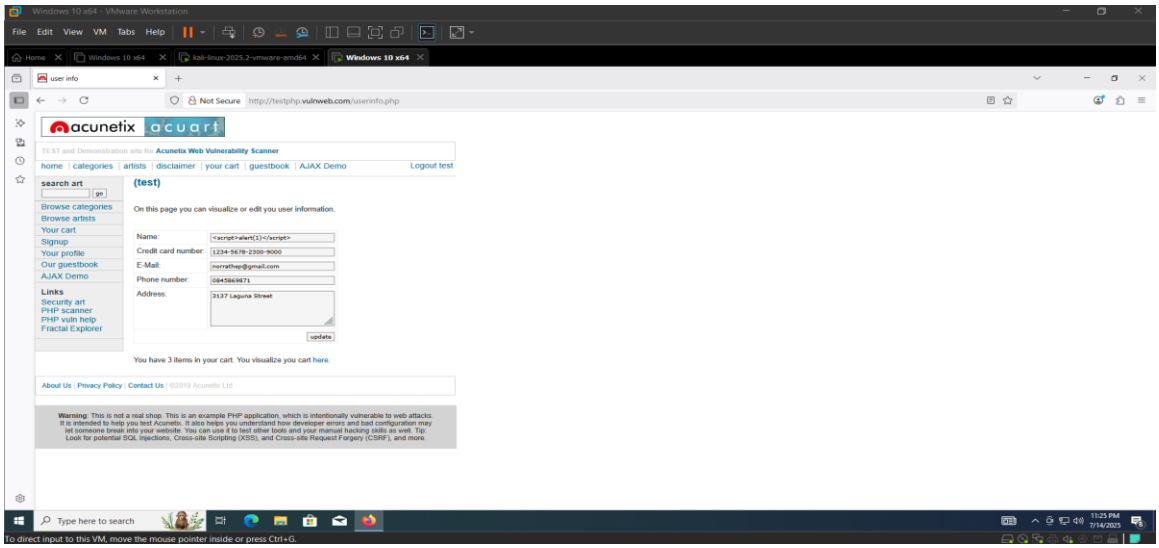


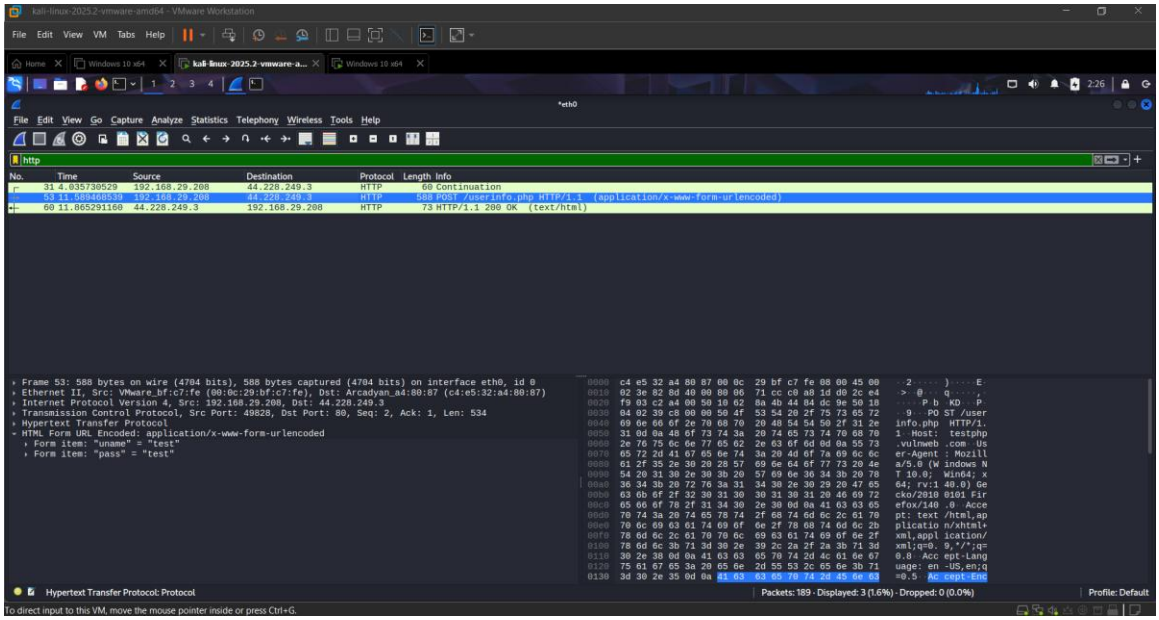

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2025.2-vmware-a...
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
680 96.048368059 192.168.29.208 162.241.216.11 TCP 66 49770 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM
681 96.319927584 162.241.216.11 192.168.29.208 TCP 66 21 → 49770 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1360 SACK_PERM WS=128
682 96.324243520 192.168.29.208 162.241.216.11 TCP 60 49770 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
683 96.600994904 162.241.216.11 192.168.29.208 FTP 324 Response: 220--------- Welcome to Pure-FTPd [privsep] [TLS] ----------
684 96.641028390 192.168.29.208 162.241.216.11 TCP 60 49770 → 21 [ACK] Seq=1 Ack=271 Win=7922 Len=0
685 96.869446682 192.168.29.208 162.241.216.11 FTP 68 Request: OPTS UTF8 ON
686 97.139698227 162.241.216.11 192.168.29.208 TCP 60 21 → 49770 [ACK] Seq=271 Ack=15 Win=65280 Len=0
687 97.139698813 162.241.216.11 192.168.29.208 FTP 75 Response: 504 Unknown command
688 97.189266634 192.168.29.208 162.241.216.11 TCP 60 49770 → 21 [ACK] Seq=15 Ack=292 Win=7901 Len=0
710 100.970290411 192.168.29.208 162.241.216.11 FTP 65 Request: USER test
711 101.237177583 162.241.216.11 192.168.29.208 FTP 91 Response: 331 User test OK. Password required
713 101.284138527 192.168.29.208 162.241.216.11 TCP 60 49770 → 21 [ACK] Seq=26 Ack=329 Win=7864 Len=0
871 107.133391810 192.168.29.208 162.241.216.11 FTP 71 Request: PASS testqwerty
872 107.437054568 162.241.216.11 192.168.29.208 TCP 60 21 → 49770 [ACK] Seq=329 Ack=43 Win=65280 Len=0
886 111.138147859 162.241.216.11 192.168.29.208 FTP 87 Response: 530 Login authentication failed
887 111.179541491 192.168.29.208 162.241.216.11 TCP 60 49770 → 21 [ACK] Seq=43 Ack=362 Win=7831 Len=0
891 113.971671896 192.168.29.208 162.241.216.11 FTP 60 Request: QUIT
892 114.242272746 162.241.216.11 192.168.29.208 TCP 60 21 → 49770 [ACK] Seq=362 Ack=49 Win=65280 Len=0
Frame 871: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface eth0, id 0
Ethernet II, Src: VMware_bf:c7:fe (00:0c:29:bf:c7:fe), Dst: Arcadyan_a4:80:87 (c4:e5:32:a4:80:87)
Internet Protocol Version 4, Src: 192.168.29.208, Dst: 162.241.216.11
Transmission Control Protocol, Src Port: 49770, Dst Port: 21, Seq: 26, Ack: 329, Len: 17
File Transfer Protocol (FTP)
[Current working directory:]
0000 c4 e5 32 a4 80 87 00 0c 29 bf c7 fe 08 00 45 00
0010 00 39 59 70 40 00 80 06 47 d9 c0 a8 1d d0 a2 f1
0020 d8 0b c2 6a 00 15 35 ca a1 91 86 62 81 6f 50 18
0030 1e b8 8b 0b 00 00 50 41 53 53 20 74 65 73 74 71
0040 77 65 72 74 79 0d 0a
wireshark_eth0KZHW92.pcapng
Packets: 931 · Displayed: 23 (2.5%) · Dropped: 0 (0.0%)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2025.2-vmware-amd64
Recycle Bin
Microsoft Edge
Firefox
Wireshark
Command Prompt
Temporary IPv6 Address. . . . . : 2405:201:301c:b022:ddea:3e51:40ef:1f53
Link-local IPv6 Address . . . . . : fe80::86d3:333a:59ff:c8ad%10
IPv4 Address. . . . . : 192.168.29.208
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c6e5:32ff:fea4:8087%10
192.168.29.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Test2pc>ftp certifiedhacker.com
Connected to certifiedhacker.com.
220--------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 150 allowed.
220-Local time is now 00:21. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
504 Unknown command
User (certifiedhacker.com:(none)): test
331 User test OK. Password required
Password:
530 Login authentication failed
Login failed.
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
C:\Users\Test2pc>
Type here to search
11:22 PM
7/14/2025
To direct input to this VM, click inside or press Ctrl+G.

6.2. For testphp.vulnweb.com

- Captured POST request.
- Username: test
- Password: test
- Protocol: HTTP (no SSL/TLS)

Include screenshot(s) of:
- Packet capture showing credentials, Filtered POST data





7. Analysis

- Password was sent in plaintext because HTTP lacks encryption.
- Demonstrates the risk of using unencrypted communication.

8. Security Implications

- Such sniffing techniques can be used by attackers for credential harvesting.
- Importance of using HTTPS and secure login mechanisms.
- Recommendations:
  - Use SSL/TLS encryption.
  - Implement secure password storage.
  - Monitor network traffic for anomalies.

9. Conclusion

This assignment demonstrated the risks of transmitting credentials over unencrypted channels. Packet sniffing was successfully used to intercept login data, emphasizing the need for secure web communication practices.