EXPERIMENT--03

Aim:
To capture and analyse network packets using Wireshark and extract login credentials transmitted via insecure protocols.

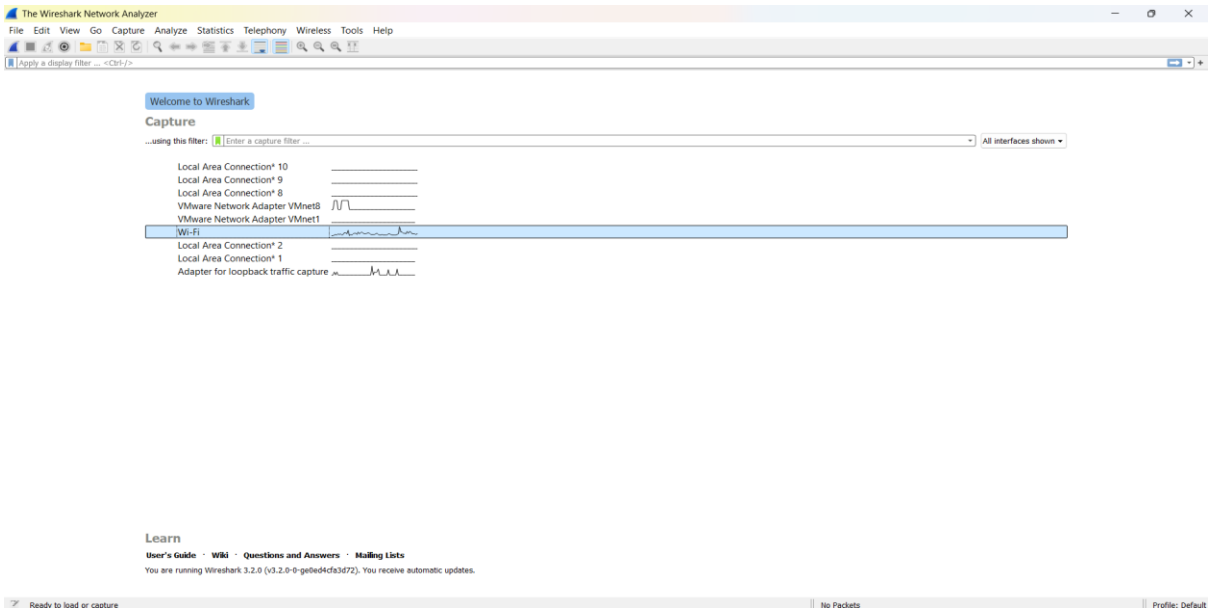
Tools Used:

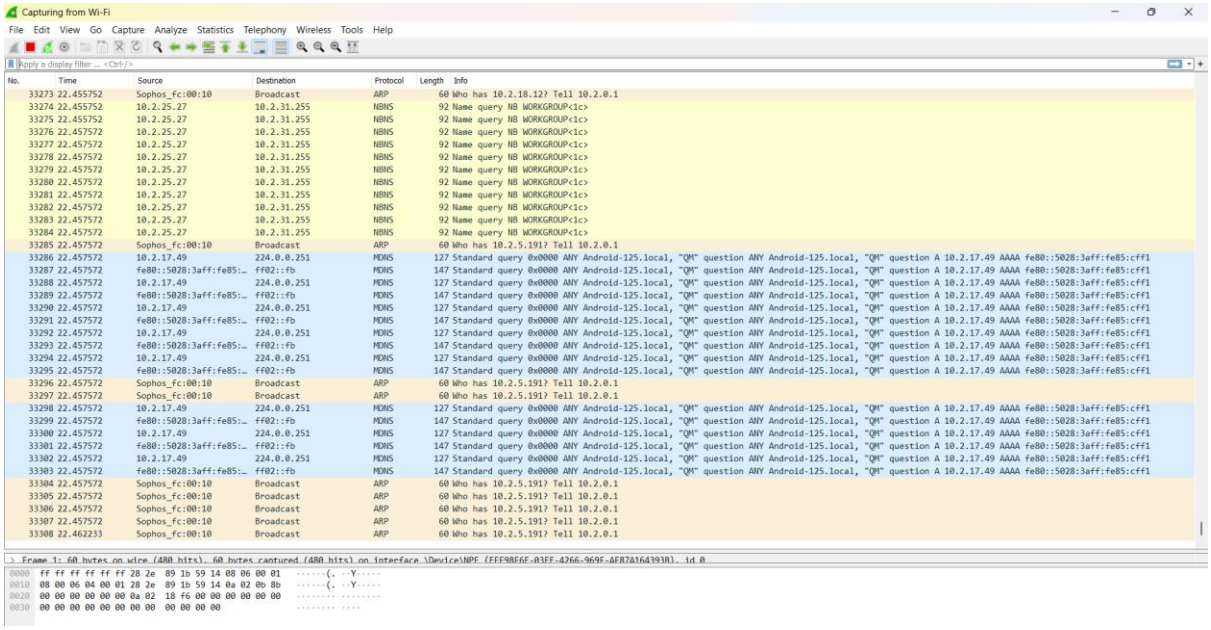
- Wireshark
- Windows/Linux system
- Web browser(**http://testphp.vulnweb.com/login.php**)

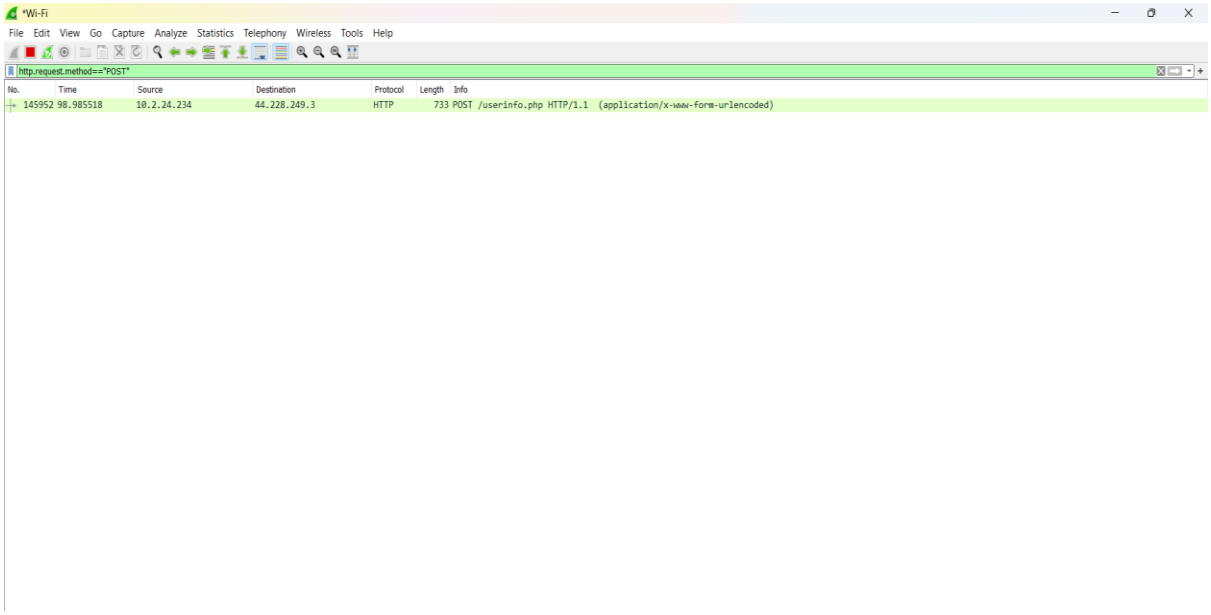
Procedure:

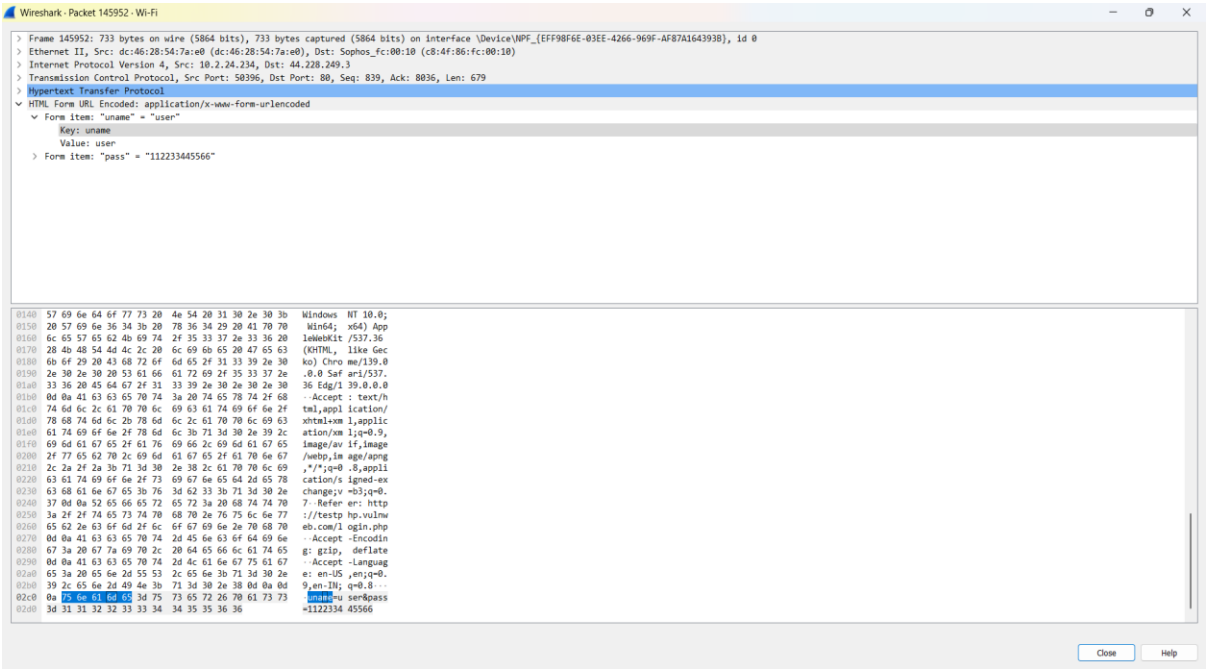
1. Open Wireshark and select the active network interface (e.g., Wi-Fi).
2. Start packet capturing to record live network traffic.
3. Open a website using HTTP protocol and log in with sample credentials.
4. Stop the capture after submitting the login form.
5. Apply the display filter http to view only HTTP packets.
6. Search for requests with GET and POST methods.
7. Expand the HTTP packet details to locate form data containing the captured username and password.

Outputs:




Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
33273 22.455752 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.18.12? Tell 10.2.0.1
33274 22.455752 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33275 22.455752 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33276 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33277 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33278 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33279 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33280 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33281 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33282 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33283 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33284 22.457572 10.2.25.27 10.2.31.255 NBNS 92 Name query NB WORKGROUP<1c>
33285 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33286 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33287 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33288 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33289 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33290 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33291 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33292 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33293 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33294 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33295 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33296 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33297 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33298 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33299 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33300 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33301 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33302 22.457572 10.2.17.49 224.0.0.251 MDNS 127 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33303 22.457572 fe80::5028:3aff:fe85:... ff02::fb MDNS 147 Standard query 0x0000 ANY Android-125.local, "QM" question ANY Android-125.local, "QM" question A 10.2.17.49 AAAA fe80::5028:3aff:fe85:cff1
33304 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33305 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33306 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33307 22.457572 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
33308 22.462233 Sophos_fc:00:10 Broadcast ARP 60 Who has 10.2.5.191? Tell 10.2.0.1
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{FFF98F6F-03FF-4766-969F-AF87A164393B}, id 0
0000 ff ff ff ff ff ff 28 2e 89 1b 59 14 08 06 00 01 ......(. ..Y.....
0010 08 00 06 04 00 01 28 2e 89 1b 59 14 0a 02 0b 8b ......(. ..Y.....
0020 00 00 00 00 00 00 0a 02 18 f6 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method=="POST"
No. Time Source Destination Protocol Length Info
145952 98.985518 10.2.24.234 44.228.249.3 HTTP 733 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)



Result:

Wireshark successfully captured network packets and revealed the transmitted login credentials from an insecure HTTP website.