

EX NO: 03 WIRESHARK (Password Capturing)

AIM:

To analyze **network traffic packets** using **Wireshark** and identify suspicious or malicious network activities.

DESCRIPTION / THEORY:

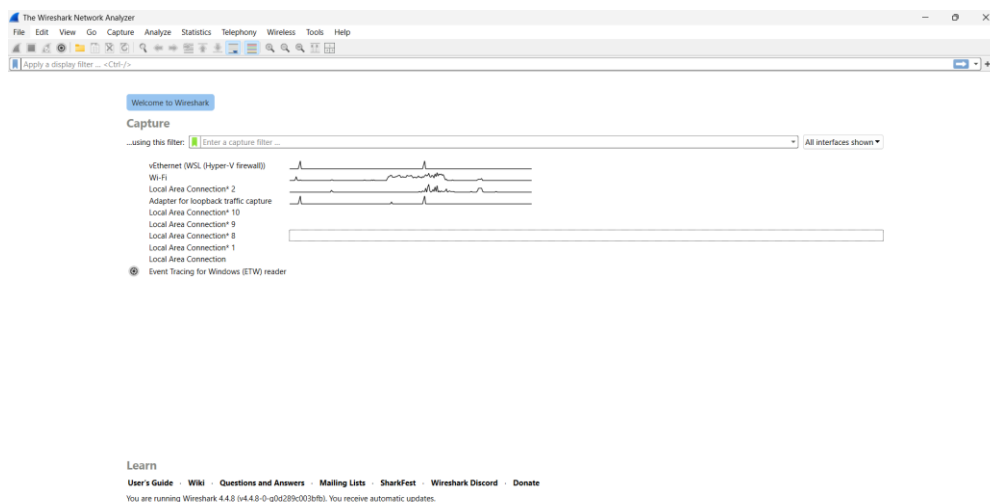
Wireshark is a free and open-source **network protocol analyzer** used for real-time network monitoring and analysis. It captures live network traffic and displays detailed information about each packet—such as source and destination IP addresses, protocols, ports, and payload data.

It supports hundreds of protocols like **TCP, UDP, HTTP, HTTPS, DNS, FTP, SMTP**, etc., and helps in:

- Diagnosing network issues
- Monitoring bandwidth and latency
- Detecting unauthorized access or malware communication
- Analyzing captured .pcap files for forensic evidence

Wireshark provides both graphical and filter-based views of packets, enabling investigators to isolate suspicious traffic patterns or anomalies in a network.

PROCEDURE:



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CloudNetwork_F9:e6:...	Broadcast	ARP	60	Who has 10.1.7.173? Tell 10.1.6.226
2	0.108299	fe80:a04a:f8ff:fe0... ff02::2		ICMPv6	70	Router Solicitation from a2:4a:f8:0c:44:b8
3	0.108299	8e:46:de:61:a4:b2	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.8.112
4	0.307935	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.3.3? Tell 10.1.0.1
5	0.307936	CloudNetwork_F9:e6:...	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.6.226
6	0.308228	da:f8:b0:40:91:66	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.8.110
7	0.308228	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.1.35? Tell 10.1.0.1
8	0.409707	fe80::c4f4:dfff:fee... ff02::2		ICMPv6	70	Router Solicitation from c6:f4:dc:e7:4d:c6
9	0.409707	8a:fc:e6:68:45:fa	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.6.169
10	0.512251	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.0.45? Tell 10.1.0.1
11	0.512251	:: ff02::1:ffa2:5de8		ICMPv6	86	Neighbor Solicitation for fe80::1003:4e5d:eca2:5de8
12	0.614393	fe80::1003:4e5d:eca... ff02::2		ICMPv6	62	Router Solicitation
13	0.614713	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa38fcd60
14	0.614713	10.1.0.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xa38fcd60
15	0.614713	1a:7e:6e:7a:01:e3	Broadcast	ARP	60	ARP Announcement for 10.1.0.236
16	0.717644	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.0.75? Tell 10.1.0.1
17	0.717644	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.14.161? Tell 10.1.0.1
18	0.717860	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.2.217? Tell 10.1.0.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{70238D93-1...}

> Ethernet II, Src: CloudNetwork_F9:e6:bf (d8:80:83:f9:e6:bf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff ff ff d8 80 83 f9 e6 bf 08 06 00 010.....

0010 00 00 06 04 00 01 d8 80 83 f9 e6 bf 0a 01 06 e20.....

0020 00 00 00 00 00 00 0a 01 07 ad 00 00 00 00 00 00K.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000.....

Wi-Fi: <live capture in progress> Packets: 422 Profile: Default

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
18	0.717860	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.2.217? Tell 10.1.0.1
19	0.717860	LittonTechno_78:45:...	Broadcast	ARP	60	Who has 10.1.7.49? Tell 10.1.8.56
20	0.717860	32:2f:e7:3d:f2:2f	Broadcast	ARP	60	Gratuitous ARP for 10.1.0.179 (Reply)
21	0.819391	CloudNetwork_F9:e6:...	Broadcast	ARP	60	Who has 10.1.6.226? (ARP Probe)
22	0.819391	6a:f2:99:63:4b:b7	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.9.58
23	0.820364	fe80::8f41:f46b:8f1... ff02::1		ICMPv6	86	Neighbor Advertisement fe80::8f41:f46b:8f1:cedc (ovr) is at d8:80:83:f9:e6:bf
24	0.820364	fe80::c0e8:a7ff:fe0... ff02::2		ICMPv6	70	Router Solicitation from c2:e8:a7:03:52:d2
25	0.921946	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.1.110? Tell 10.1.0.1
26	0.921946	16:d1:a6:d8:4f:5a	Broadcast	ARP	60	Gratuitous ARP for 10.1.10.101 (Reply)
27	1.002454	10.1.5.119	104.208.16.92	TCP	55	58424 -> 443 [ACK] Seq=1 Win=255 Len=1
28	1.024463	16:d1:a6:d8:4f:5a	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.10.101
29	1.034789	10.1.5.119	104.208.16.92	TCP	55	58423 -> 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
30	1.126587	de:47:55:a7:3f:e8	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.3.52
31	1.126587	1a:cd:bb:d6:0d:16	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.1.63
32	1.259841	104.208.16.92	10.1.5.119	TCP	66	443 -> 58424 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
33	1.299486	104.208.16.92	10.1.5.119	TCP	66	443 -> 58423 [ACK] Seq=1 Ack=2 Win=16381 Len=0 SLE=1 SRE=2
34	1.332665	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.1.35? Tell 10.1.0.1
35	1.536701	Sophos_fc:00:0f	Broadcast	ARP	60	Who has 10.1.7.191? Tell 10.1.0.1

> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{70238D93-1...}

> Ethernet II, Src: Sophos_fc:00:0f (c8:4f:86:fc:00:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff ff ff c8 4f 86 fc 00 0f 08 06 00 010.....


0010 08 00 06 04 00 01 c8 4f 86 fc 00 0f 0a 01 06 e20.....

0020 00 00 00 00 00 00 0a 01 00 4b 00 00 00 00 00 00K.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 000.....

Hypertext Transfer Protocol: Protocol Packets: 2833 - Dropped: 0 (0.0%) Profile: Default

OUTPUT:



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)


[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :



You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
755	29.145182	10.1.5.119	23.44.5.227	HTTP	165	GET /connecttest.txt HTTP/1.1
761	29.217865	23.44.5.227	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
1357	55.398462	10.1.5.119	23.44.5.227	HTTP	178	GET /ncsl.txt HTTP/1.1
1360	55.449431	23.44.5.227	10.1.5.119	HTTP	233	HTTP/1.1 200 OK (text/plain)
1454	59.426971	10.1.5.119	23.200.218.161	HTTP	165	GET /connecttest.txt HTTP/1.1
1457	59.486979	23.200.218.161	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)
2479	89.577053	10.1.5.119	23.211.60.150	HTTP	165	GET /connecttest.txt HTTP/1.1
2484	89.620369	23.211.60.150	10.1.5.119	HTTP	241	HTTP/1.1 200 OK (text/plain)

> Frame 755: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{7023...}		0000	c8 4f 86 fc 00 0f f8 54	f6 50 6a f1 08 00 45 00	..O...T..Pj...E..
> Ethernet II, Src: AzureWaveTec_50:6a:f1 (f8:54:f6:50:6a:f1), Dst: Sophos_fc:00:0f (c8:4f:86:fc:00:0f)		0010	00 97 1d 80 40 00 80 06	b0 5a 0a 01 05 77 17 2c	...@...Z...w,
> Internet Protocol Version 4, Src: 10.1.5.119, Dst: 23.44.5.227		0020	05 e3 e4 3d 00 50 cc da	38 b8 a4 7d b2 87 50 18	...aP...8...P..
> Transmission Control Protocol, Src Port: 58429, Dst Port: 80, Seq: 1, Ack: 1, Len: 111		0030	00 ff 81 7f 00 00 47 45	54 20 2f 63 6f 6e 6e 65GET /conne
> Hypertext Transfer Protocol		0040	63 74 74 65 73 74 2e 74	78 74 20 48 54 54 50 2f	cttest.txt HTTP/
		0050	31 2e 31 0d 0a 43 6f 6e	6e 65 63 74 69 6f 6e 3a	1.1: Connection:
		0060	20 43 6c 6f 73 65 0d 0a	55 73 65 72 2d 41 67 65	Close: User-Age
		0070	6e 74 3a 20 4d 69 63 72	6f 73 6f 66 74 20 4e 43	nt: Microsoft NC
		0080	53 49 0d 0a 48 6f 73 74	3a 20 77 77 77 2e 6d 73	51: Host: www.ms
		0090	66 74 63 6f 6e 6e 65 63	74 74 65 73 74 2e 63 6f	ftconnec ttest.co
		00a0	6d 0d 0a 0d 0a		m....

RESULT:

The **Wireshark tool** was successfully used to capture and analyze network traffic. The experiment identified various network protocols, packet structures, and potential suspicious activities, demonstrating effective packet-level network monitoring.