

NAME : Shrishti Vishwakarma

CLASS : BVOC (First year) Sem 2

TITLE : Make a .Pcap file wgere you captures credentials using wireshark

INSTRUCTOR : Shubham sir

TABLE OF CONTENT

- 1.Introduction
2. Objectives
3. Tools Used
4. Result and screenshots
4. Conclusion

INTRODUCTION

This project demonstrates capturing credentials using Wireshark, a powerful network protocol analyzer. By monitoring network traffic, it is possible to intercept sensitive information, such as passwords and usernames, when transmitted over unencrypted protocols.

OBJECTIVE

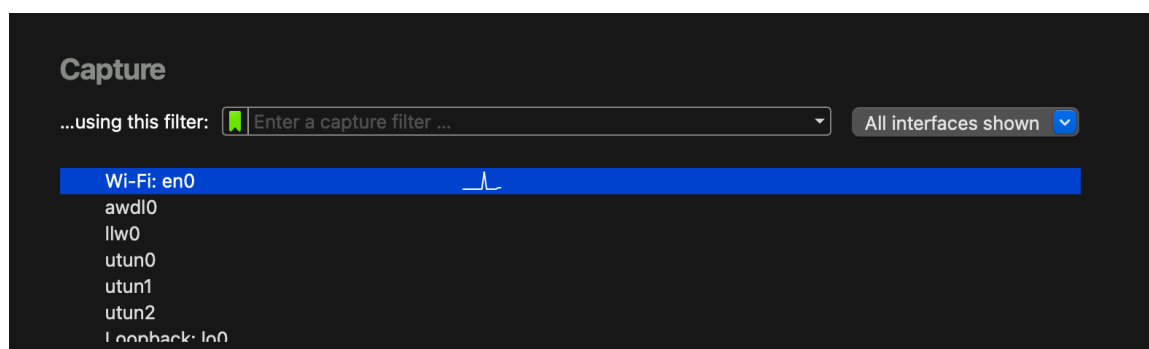
1. To understand how credentials can be intercepted over the network
2. To learn the importance of using secure communication protocols

TOOLS USED

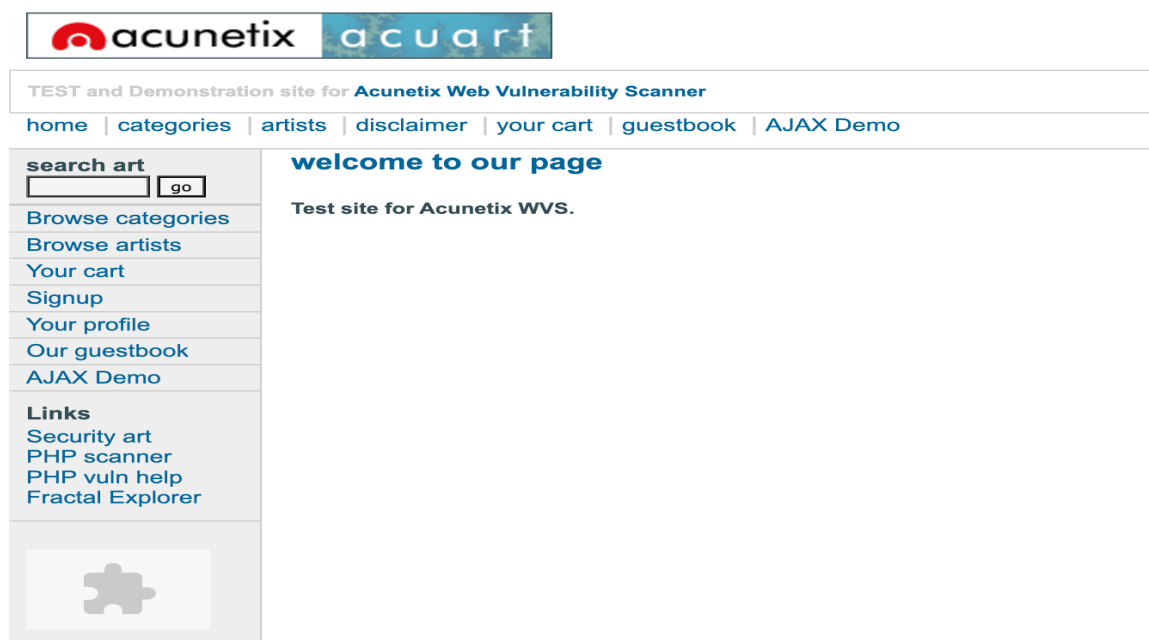
1. Wireshark
2. Vulnweb

RESULTS AND SCREENSHOTS

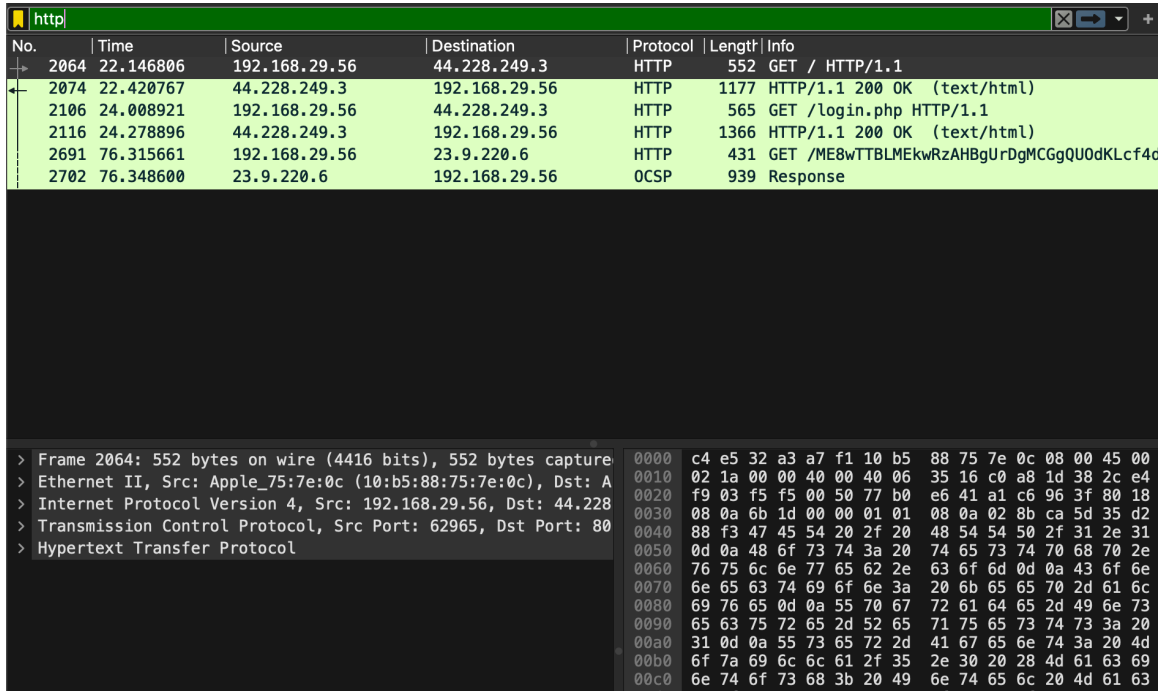
1. Open wireshark interface where the “eth()” network interface is selected for capturing packets, allowing us to capture network traffic.



2. Choose the website to generate traffic (vulnweb) to capture Http packets.



3. Then open your Wireshark and capture the HTTP packets.



No.	Time	Source	Destination	Protocol	Length	Info
2064	22.146806	192.168.29.56	44.228.249.3	HTTP	552	GET / HTTP/1.1
2074	22.420767	44.228.249.3	192.168.29.56	HTTP	1177	HTTP/1.1 200 OK (text/html)
2106	24.008921	192.168.29.56	44.228.249.3	HTTP	565	GET /login.php HTTP/1.1
2116	24.278896	44.228.249.3	192.168.29.56	HTTP	1366	HTTP/1.1 200 OK (text/html)
2691	76.315661	192.168.29.56	23.9.220.6	HTTP	431	GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU0dKLcf4c
2702	76.348600	23.9.220.6	192.168.29.56	OCSP	939	Response

Frame 2064: 552 bytes on wire (4416 bits), 552 bytes capture	
Ethernet II, Src: Apple_75:7e:0c (10:b5:88:75:7e:0c), Dst: A	0000 c4 e5 32 a3 a7 f1 10 b5 88 75 7e 0c 08 00 45 00
Internet Protocol Version 4, Src: 192.168.29.56, Dst: 44.228	0010 02 1a 00 00 40 00 40 06 35 16 c0 a8 1d 38 2c e4
Transmission Control Protocol, Src Port: 62965, Dst Port: 80	0020 f9 03 f5 f5 00 50 77 b0 e6 41 a1 c6 96 3f 80 18
Hypertext Transfer Protocol	0030 08 0a 6b 1d 00 00 01 01 08 0a 02 8b ca 5d 35 d2
	0040 88 f3 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31
	0050 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 2e
	0060 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f 6e
	0070 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c
	0080 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73
	0090 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20
	00a0 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d
	00b0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 4d 61 63 69
	00c0 6e 74 6f 73 68 3b 20 49 6e 74 65 6c 20 4d 61 63

CONCLUSION

The project highlights the vulnerabilities of unencrypted network communications and emphasizes the importance of using secure protocols to protect sensitive information from being intercepted.