SNIFFING USING WIRESHARK

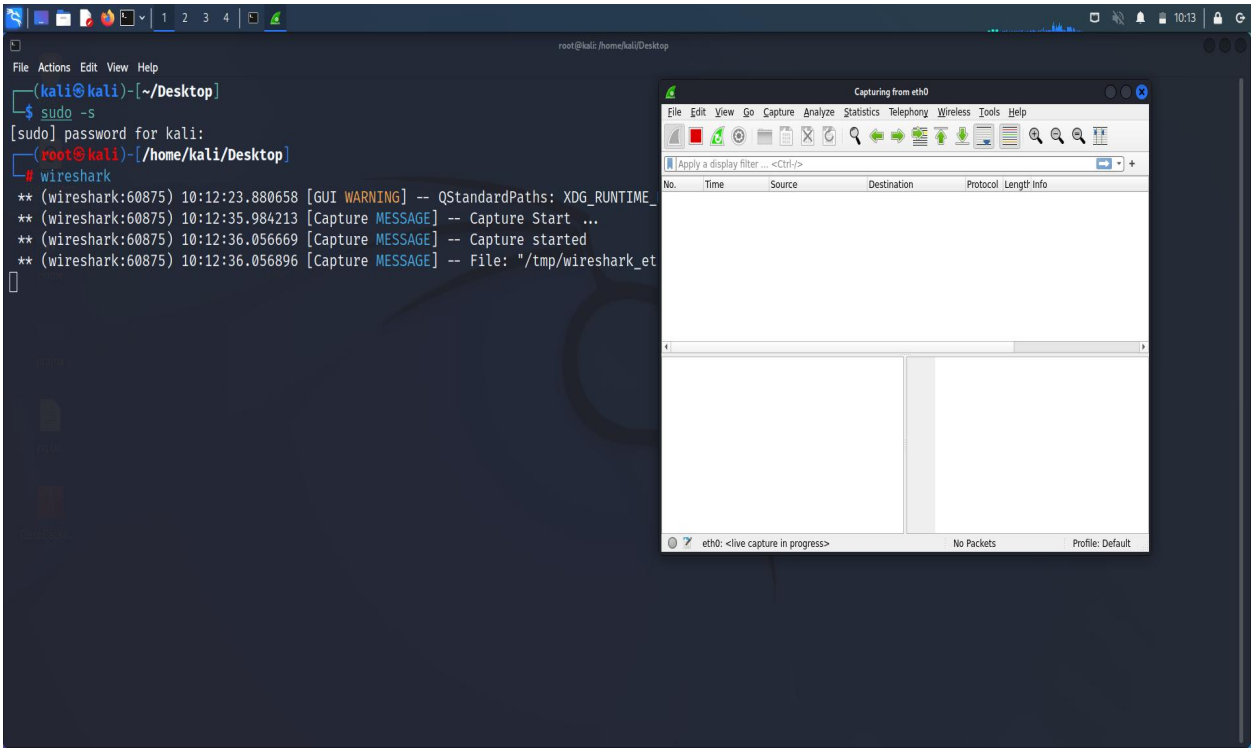
Wireshark is a free open source tool that analyzes network traffic in real-time for Windows, Mac, Unix, and Linux systems. It captures data packets passing through a network interface (such as Ethernet, LAN, or SDRs) and translates that data into valuable information for IT professionals and cybersecurity teams.

Wireshark is a type of packet sniffer (also known as a network protocol analyzer, protocol analyzer, and network analyzer). Packet sniffers intercept network traffic to understand the activity being processed and harvest useful insights.Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things.

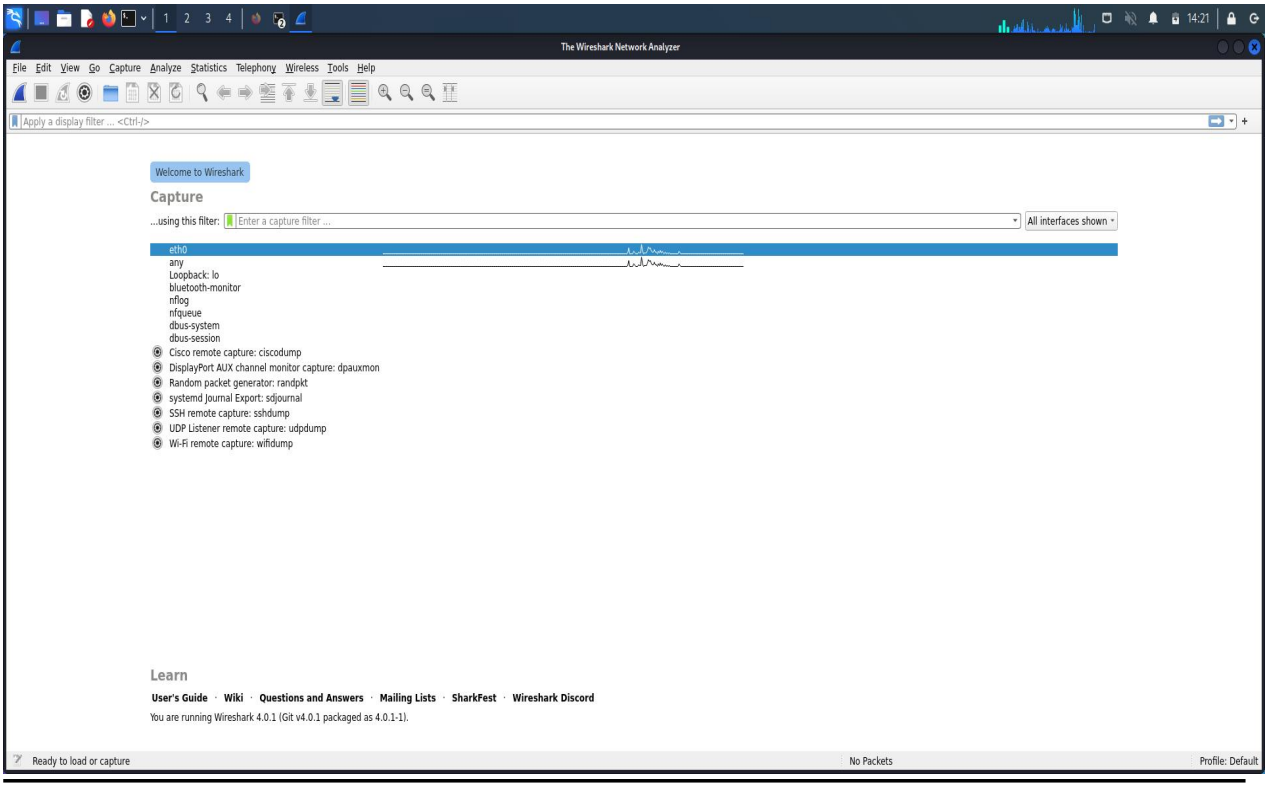
METHODS:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

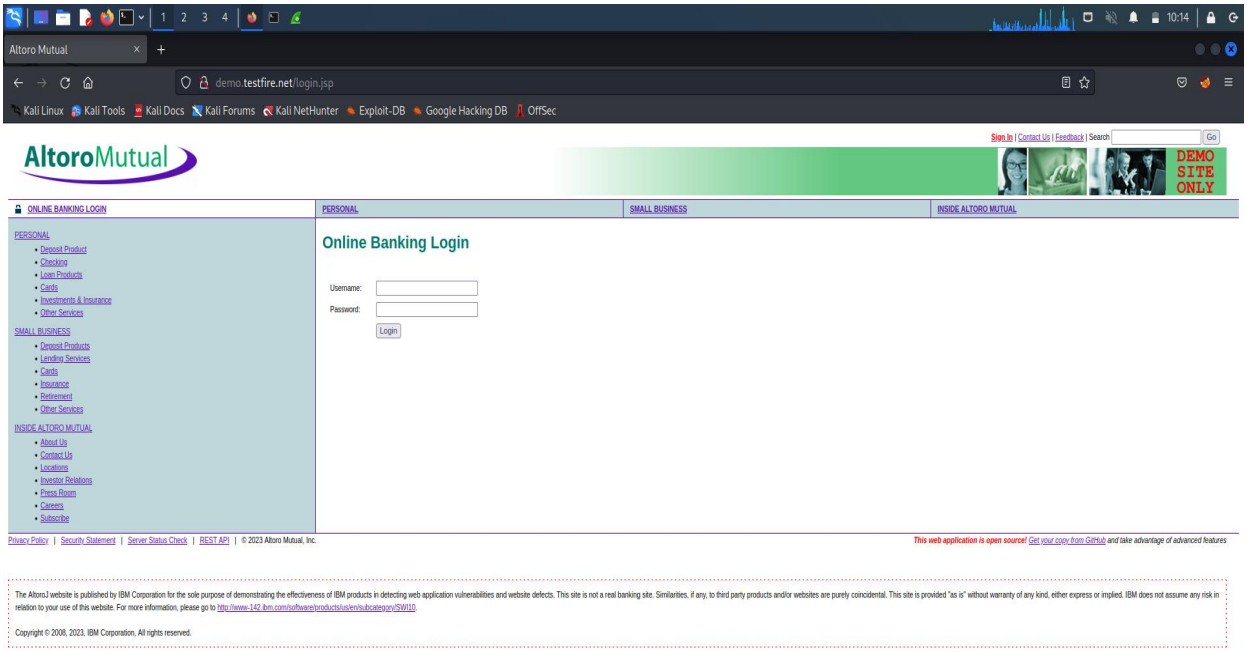
Step 1: Login to kali as root user and type Wireshark.



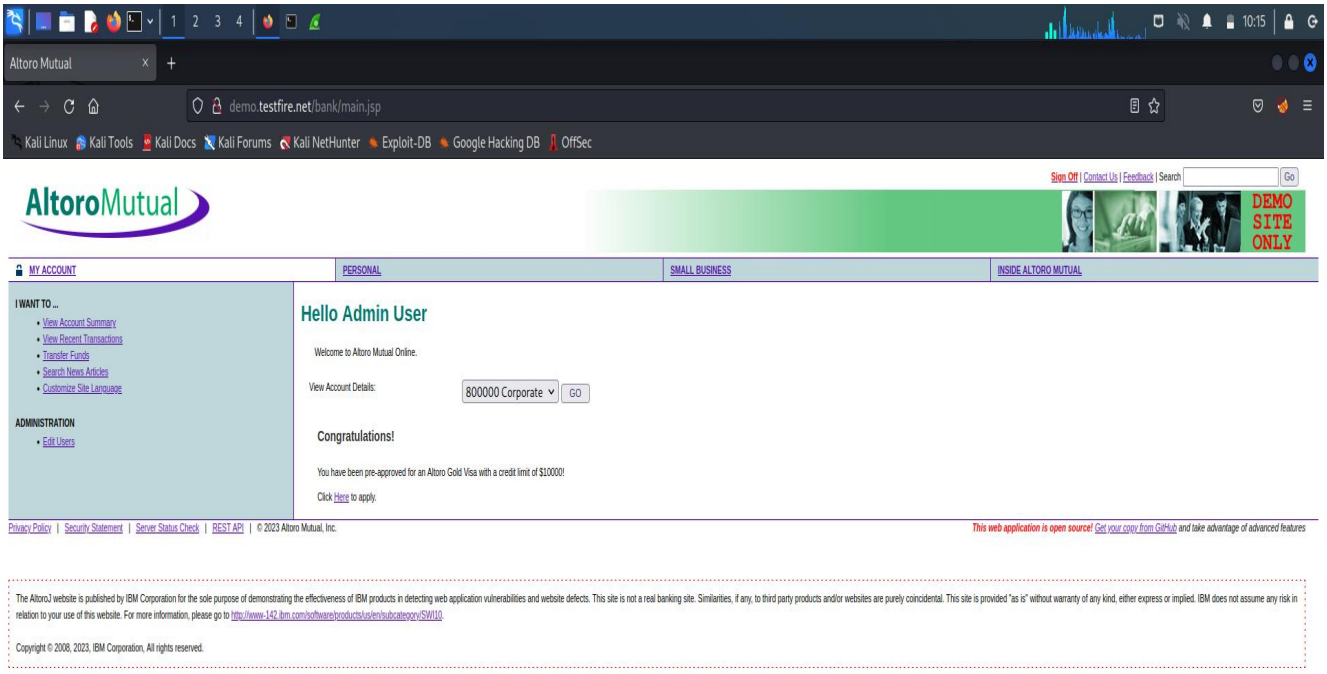
Step 2: Wireshark Network Analyzer will be opened and double click on **eth0**(1st option).



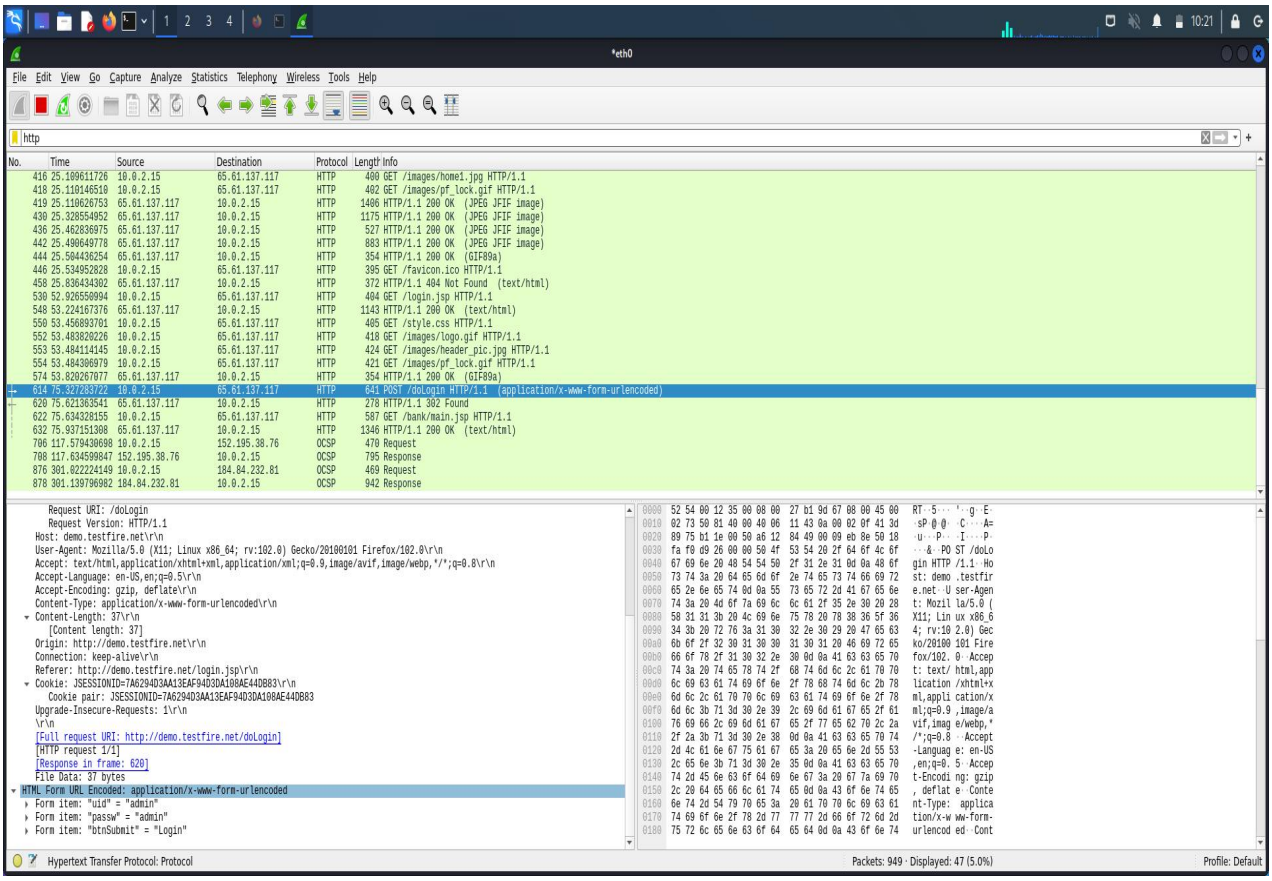
Step 3: Go to Firefox and search **testfire.net**



Username: **admin** Password: **admin**



Step 4: Go to wire shark and in search bar filter http -post. By clicking last option, you will get the password and username to crack it.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
416 25.109611726 10.0.2.15 65.61.137.117 HTTP 400 GET /images/home1.jpg HTTP/1.1
418 25.110146510 10.0.2.15 65.61.137.117 HTTP 402 GET /images/pf_lock.gif HTTP/1.1
419 25.110626753 65.61.137.117 10.0.2.15 HTTP 1406 HTTP/1.1 200 OK (JPEG JFIF image)
430 25.328554952 65.61.137.117 10.0.2.15 HTTP 1175 HTTP/1.1 200 OK (JPEG JFIF image)
436 25.462836975 65.61.137.117 10.0.2.15 HTTP 527 HTTP/1.1 200 OK (JPEG JFIF image)
442 25.490649778 65.61.137.117 10.0.2.15 HTTP 883 HTTP/1.1 200 OK (JPEG JFIF image)
444 25.504436254 65.61.137.117 10.0.2.15 HTTP 354 HTTP/1.1 200 OK (GIF89a)
446 25.534952828 10.0.2.15 65.61.137.117 HTTP 395 GET /favicon.ico HTTP/1.1
458 25.836434302 65.61.137.117 10.0.2.15 HTTP 372 HTTP/1.1 404 Not Found (text/html)
530 52.926560994 10.0.2.15 65.61.137.117 HTTP 404 GET /login.jsp HTTP/1.1
548 53.224167376 65.61.137.117 10.0.2.15 HTTP 1143 HTTP/1.1 200 OK (text/html)
550 53.456893701 10.0.2.15 65.61.137.117 HTTP 405 GET /style.css HTTP/1.1
552 53.483820226 10.0.2.15 65.61.137.117 HTTP 418 GET /images/logo.gif HTTP/1.1
553 53.484114145 10.0.2.15 65.61.137.117 HTTP 424 GET /images/header_pic.jpg HTTP/1.1
554 53.484306979 10.0.2.15 65.61.137.117 HTTP 421 GET /images/pf_lock.gif HTTP/1.1
574 53.820267077 65.61.137.117 10.0.2.15 HTTP 354 HTTP/1.1 200 OK (GIF89a)
614 75.327283722 10.0.2.15 65.61.137.117 HTTP 641 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
620 75.621363541 65.61.137.117 10.0.2.15 HTTP 278 HTTP/1.1 302 Found
622 75.634328155 10.0.2.15 65.61.137.117 HTTP 587 GET /bank/main.jsp HTTP/1.1
632 75.937151308 65.61.137.117 10.0.2.15 HTTP 1346 HTTP/1.1 200 OK (text/html)
706 117.579430698 10.0.2.15 152.195.38.76 OCSP 470 Request
708 117.634599847 152.195.38.76 10.0.2.15 OCSP 795 Response
876 301.022224149 10.0.2.15 184.84.232.81 OCSP 469 Request
878 301.139796982 184.84.232.81 10.0.2.15 OCSP 942 Response
Request URI: /doLogin
Request Version: HTTP/1.1
Host: demo.testfire.net\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 37\r\n
[Content length: 37]
Origin: http://demo.testfire.net\r\n
Connection: keep-alive\r\n
Referer: http://demo.testfire.net/login.jsp\r\n
Cookie: JSESSIONID=7A6294D3AA13EAF94D3DA108AE44DB83\r\n
Cookie pair: JSESSIONID=7A6294D3AA13EAF94D3DA108AE44DB83
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://demo.testfire.net/doLogin]
[HTTP request 1/1]
[Response in frame: 620]
File Data: 37 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "admin"
Form item: "passw" = "admin"
Form item: "btnSubmit" = "Login"
0000 52 54 00 12 35 00 08 00 27 b1 9d 67 08 00 45 00 RT··5··· '··g··E·
0010 02 73 50 81 40 00 40 06 11 43 0a 00 02 0f 41 3d ·sP·@·@· ·C····A=
0020 89 75 b1 1e 00 50 a6 12 84 49 00 09 eb 8e 50 18 ·u···P·· ·I····P·
0030 fa f0 d9 26 00 00 50 4f 53 54 20 2f 64 6f 4c 6f ···&··PO ST /doLo
0040 67 69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f gin HTTP /1.1··Ho
0050 73 74 3a 20 64 65 6d 6f 2e 74 65 73 74 66 69 72 st: demo .testfir
0060 65 2e 6e 65 74 0d 0a 55 73 65 72 2d 41 67 65 6e e.net··U ser-Agen
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0080 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 X11; Lin ux x86_6
0090 34 3b 20 72 76 3a 31 30 32 2e 30 29 20 47 65 63 4; rv:10 2.0) Gec
00a0 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 ko/20100 101 Fire
00b0 66 6f 78 2f 31 30 32 2e 30 0d 0a 41 63 63 65 70 fox/102. 0··Accep
00c0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/ html,app
00d0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+x
00e0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x
00f0 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 ml;q=0.9 ,image/a
0100 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a vif,imag e/webp,*
0110 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 /*;q=0.8 ··Accept
0120 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 -Languag e: en-US
0130 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 ,en;q=0. 5··Accep
0140 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
0150 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 74 65 , deflat e··Conte
0160 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 nt-Type: applica
0170 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d tion/x-w ww-form-
0180 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 urlencod ed··Cont
Hypertext Transfer Protocol: Protocol
Packets: 949 · Displayed: 47 (5.0%)
Profile: Default