Task 1 - Wireshark Walkthrough

AIM :

The task is to prove that the credentials entered in the admin panel of the webpage can be captured.

Tools:

Wireshark (Installed on the system) or tcpdump (Installed on the system), patience.

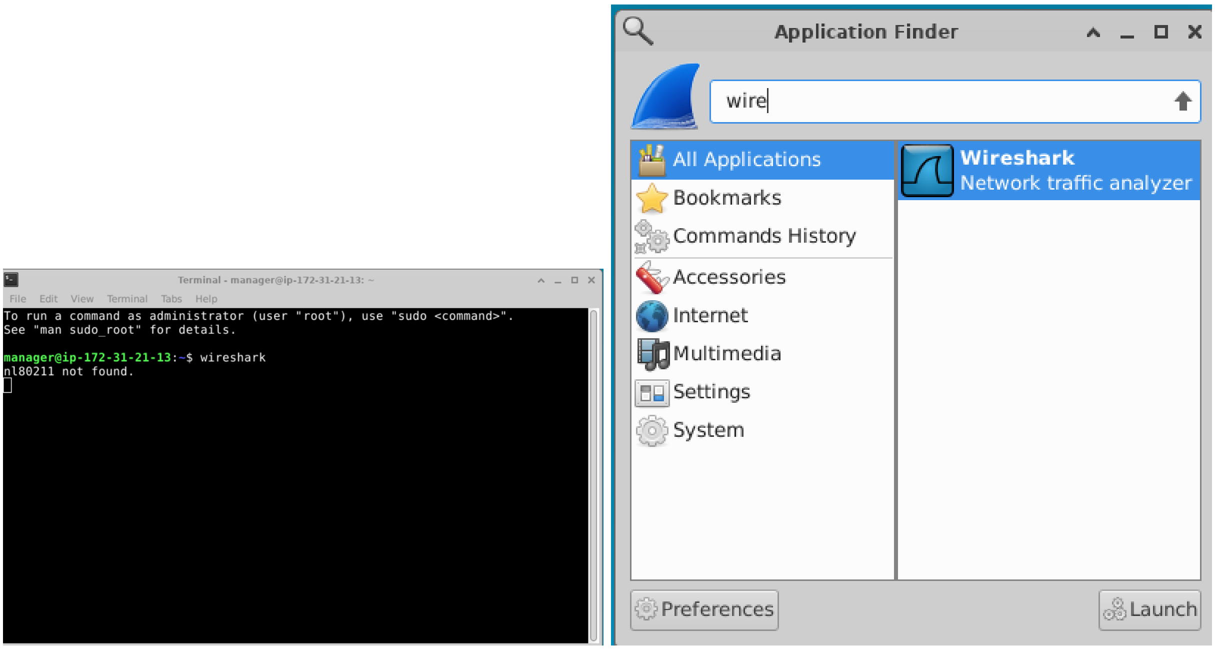
Wireshark Implementation

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

So when the communication happens between the client(your browser) and server (webpage), the Wireshark tool captures those network packets which can be analyzed. Here in our task, when user credentials are entered in the admin site these are captured by Wireshark and can be viewed by using appropriate filters. As the website is using http, the credentials are being sent over the network unencrypted, due to which once there are captured by the Wireshark the attacker can view the actual credentials in plain-text.

Procedure

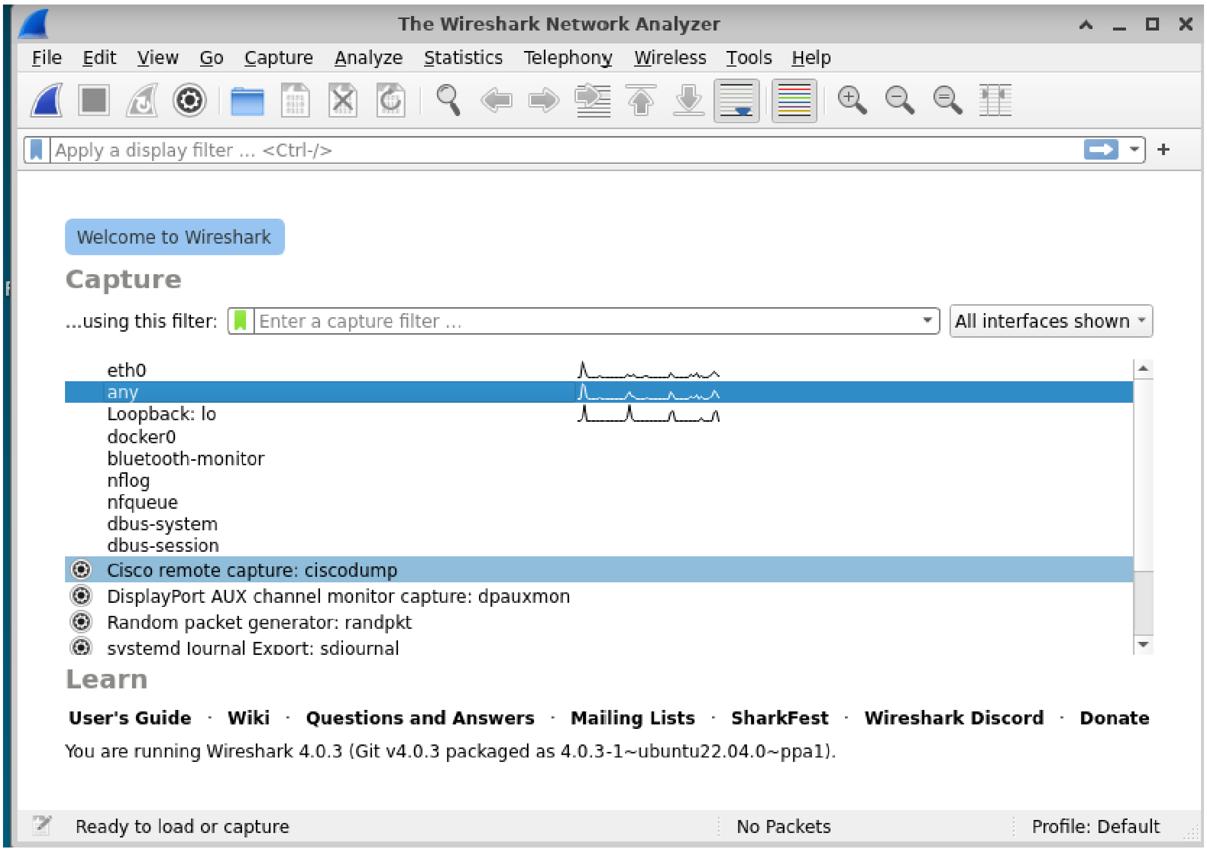
Step0: Open Wireshark, this can be done using the terminal, or the application finder. Both methods are shown below



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

manager@ip-172-31-21-13:~$ wireshark
nl80211 not found.
```

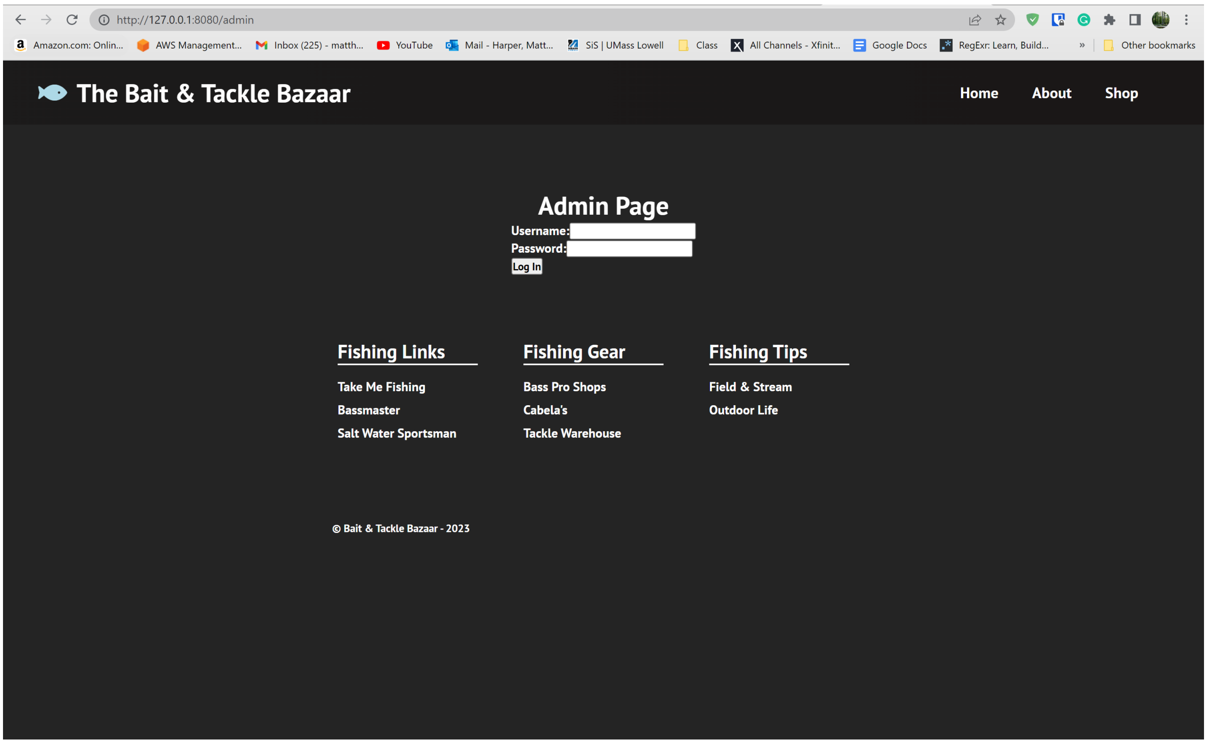
Step1: Select the network interface you want to listen on. Once selected, click on *Capture* and Wireshark will start sniffing network packets. We can select **eth0** or to be safe **any** as shown below by double clicking the interface.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (Git v4.0.3 packaged as 4.0.3-1~ubuntu22.04.0~ppa1).

Ready to load or capture | No Packets | Profile: Default

Step2: In your browser, add "/admin" at the end of the current url to open the admin site, where you can see placeholders for the credentials.

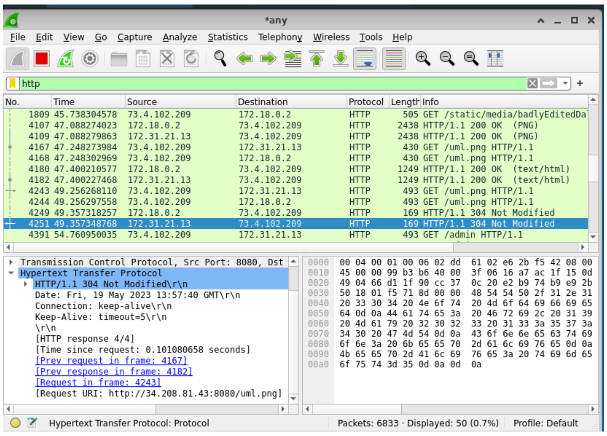

http://127.0.0.1:8080/admin
Amazon.com: Onlin... AWS Management... Inbox (225) - matth... YouTube Mail - Harper, Matt... SIS | UMass Lowell Class All Channels - Xfinit... Google Docs RegExr: Learn, Build... Other bookmarks
The Bait & Tackle Bazaar
Home About Shop
Admin Page
Username:
Password:
Log In
Fishing Links
Take Me Fishing
Bassmaster
Salt Water Sportsman
Fishing Gear
Bass Pro Shops
Cabela's
Tackle Warehouse
Fishing Tips
Field & Stream
Outdoor Life
© Bait & Tackle Bazaar - 2023

Step3: Wireshark in the background will be capturing the data packets, now enter the login credentials in the admin page.

Step4: Stop the capturing process in the Wireshark. As Wireshark captures every data packet it is obvious the output is overwhelming.

Step5: To find the necessary data (credentials in our case) from that heap, Wireshark filters need to be used.

Step6: There are several different filters that can be used to eliminate unnecessary data from the generated output. A few easy examples of those filters are, using protocol name (http, telnet, ssh), using source ip (ip.src == X.X.X.X) and destination ip (ip.dst == X.X.X.X) to name a few. Below we show captures of HTTP and Telnet traffic.


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

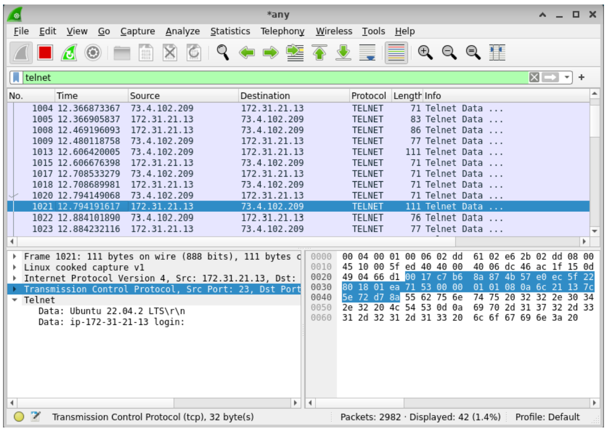
http

```
No.   Time          Source         Destination    Protocol Length Info
 1809 45.738304578  73.4.102.209   172.18.0.2     HTTP     505 GET /static/media/badlyEditedDa
 4107 47.088274023  172.18.0.2     73.4.102.209   HTTP     2438 HTTP/1.1 200 OK  (PNG)
 4109 47.088279863  172.31.21.13   73.4.102.209   HTTP     2438 HTTP/1.1 200 OK  (PNG)
 4167 47.248273984  73.4.102.209   172.31.21.13   HTTP     430 GET /uml.png HTTP/1.1
 4168 47.248302969  73.4.102.209   172.18.0.2     HTTP     430 GET /uml.png HTTP/1.1
 4180 47.400210577  172.18.0.2     73.4.102.209   HTTP     1249 HTTP/1.1 200 OK  (text/html)
 4182 47.400227468  172.31.21.13   73.4.102.209   HTTP     1249 HTTP/1.1 200 OK  (text/html)
 4243 49.256268110  73.4.102.209   172.31.21.13   HTTP     493 GET /uml.png HTTP/1.1
 4244 49.256297558  73.4.102.209   172.18.0.2     HTTP     493 GET /uml.png HTTP/1.1
 4249 49.357318257  172.18.0.2     73.4.102.209   HTTP     169 HTTP/1.1 304 Not Modified
 4251 49.357348768  172.31.21.13   73.4.102.209   HTTP     169 HTTP/1.1 304 Not Modified
 4391 54.760950035  73.4.102.209   172.31.21.13   HTTP     493 GET /admin HTTP/1.1
```

```
▸ Transmission Control Protocol, Src Port: 8080, Dst
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 19 May 2023 13:57:40 GMT\r\n
    Connection: keep-alive\r\n
    Keep-Alive: timeout=5\r\n
    \r\n
    [HTTP response 4/4]
    [Time since request: 0.101080658 seconds]
    [Prev request in frame: 4167]
    [Prev response in frame: 4182]
    [Request in frame: 4243]
    [Request URI: http://34.208.81.43:8080/uml.png]
```

```
0000  00 04 00 01 00 06 02 dd  61 02 e6 2b f5 42 08 00
0010  45 00 00 99 b3 b6 40 00  3f 06 16 a7 ac 1f 15 0d
0020  49 04 66 d1 1f 90 cc 37  0c 20 e2 b9 74 b9 e9 2b
0030  50 18 01 f5 71 8d 00 00  48 54 54 50 2f 31 2e 31
0040  20 33 30 34 20 4e 6f 74  20 4d 6f 64 69 66 69 65
0050  64 0d 0a 44 61 74 65 3a  20 46 72 69 2c 20 31 39
0060  20 4d 61 79 20 32 30 32  33 20 31 33 3a 35 37 3a
0070  34 30 20 47 4d 54 0d 0a  43 6f 6e 6e 65 63 74 69
0080  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a
0090  4b 65 65 70 2d 41 6c 69  76 65 3a 20 74 69 6d 65
00a0  6f 75 74 3d 35 0d 0a 0d  0a
```

Hypertext Transfer Protocol: Protocol | Packets: 6833 · Displayed: 50 (0.7%) | Profile: Default


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

```
No.   Time          Source         Destination    Protocol Length Info
 1004 12.366873367  73.4.102.209   172.31.21.13   TELNET   71 Telnet Data ...
 1005 12.366905837  172.31.21.13   73.4.102.209   TELNET   83 Telnet Data ...
 1008 12.469196093  172.31.21.13   73.4.102.209   TELNET   86 Telnet Data ...
 1009 12.480118758  73.4.102.209   172.31.21.13   TELNET   77 Telnet Data ...
 1013 12.606420005  73.4.102.209   172.31.21.13   TELNET  111 Telnet Data ...
 1015 12.606676398  172.31.21.13   73.4.102.209   TELNET   71 Telnet Data ...
 1017 12.708533279  73.4.102.209   172.31.21.13   TELNET   71 Telnet Data ...
 1018 12.708689981  172.31.21.13   73.4.102.209   TELNET   71 Telnet Data ...
 1020 12.794149068  73.4.102.209   172.31.21.13   TELNET   71 Telnet Data ...
 1021 12.794191617  172.31.21.13   73.4.102.209   TELNET  111 Telnet Data ...
 1022 12.884101890  73.4.102.209   172.31.21.13   TELNET   76 Telnet Data ...
 1023 12.884232116  172.31.21.13   73.4.102.209   TELNET   77 Telnet Data ...
```

```
▸ Frame 1021: 111 bytes on wire (888 bits), 111 bytes c
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 172.31.21.13, Dst:
▸ Transmission Control Protocol, Src Port: 23, Dst Port
▾ Telnet
    Data: Ubuntu 22.04.2 LTS\r\n
    Data: ip-172-31-21-13 login:
```

```
0000  00 04 00 01 00 06 02 dd  61 02 e6 2b 02 dd 08 00
0010  45 10 00 5f ed 40 40 00  40 06 dc 46 ac 1f 15 0d
0020  49 04 66 d1 00 17 c7 b6  8a 87 4b 57 e0 ec 5f 22
0030  80 18 01 ea 71 53 00 00  01 01 08 0a 6c 21 13 7c
0040  5e 72 d7 8a 55 62 75 6e  74 75 20 32 32 2e 30 34
0050  2e 32 20 4c 54 53 0d 0a  69 70 2d 31 37 32 2d 33
0060  31 2d 32 31 2d 31 33 20  6c 6f 67 69 6e 3a 20
```

Transmission Control Protocol (tcp), 32 byte(s) | Packets: 2982 · Displayed: 42 (1.4%) | Profile: Default

Step7: The filtered output will be relatively less complex. When a packet is selected, at the bottom, detailed information about the packet is given. Look for the packets which send login information and expand it to learn more about the data being sent out/received. Unencrypted user credentials are available in one of these packets.

This proves that, a http website transfers unencrypted data and if a attacker captures these packets plain text data is leaked.

You should search through telnet traffic for a username and password you can use.

tcpdump Implementation

Tcpdump is a network packet analyzer which mostly works like the wireshark but tcpdump is cli (command line interface) tool.

Similar to wireshark, even here we filter the collected packets using certain filters but these filter and the capturing process is done by CLI commands.

Procedure

Step1: Install tcpdump on your system. In terminal/command prompt enter installation commands

```
sudo apt-get update
sudo apt-get install tcpdump
```

Step2: Just like in wireshark, where we select which interface to work on, even in tcpdump interface needs to be mentioned before the process starts. to see the list of interfaces that are elibible to list use the command:

```
sudo tcpdump -D
```

Step3: Without using proper filters the output given by tcpdump will be closely impossible to understand. To avoid this the ideal way is to mention certain things like, port number, protocol, source ip, destination ip.

```
sudo tcpdump -i all -A port 8000
```

This command runs using sudo privilages. where: -i all says to listen on app interfaces, in place of all proper interface can be used to reduce complexity. -A Prints the packet contents as ASCII text. This allows you to see the HTTP payload data in a readable format. port 8000 role is to listen on 8000 port.