CYBER SECURITY INTERNSHIP

Task-5

Capture and Analyze Network Traffic Using Wireshark

Information

Name: K. Vamsi

Institution: Kalasalingam Academy of Research and Education

Internship Role: Cybersecurity Intern

Submission Date: 11/08/2025

1. Introduction

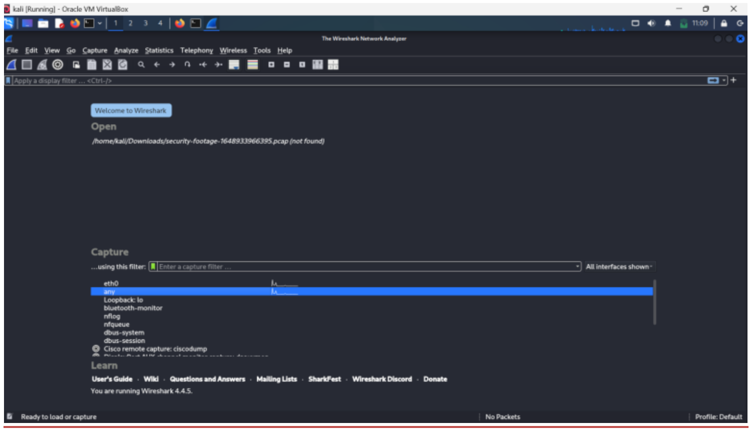
The purpose of this report is to Capture and Analyze Network Traffic Using Wireshark. Wireshark is open-source network protocol analyzer which is used to analyze the network packets, troubleshoot network issues and perform security auditing.

2. Tools and Environment

Tools	*Description*
Wireshark	*To Capture the network traffic.*
Kali Linux - Terminal	*Linux command line utility for pinging, connecting the ports like ftp, telnet etc...*

3. Methodology

WIRESHARK



kali [Running] - Oracle VM VirtualBox

The Wireshark Network Analyzer

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Open

/home/kali/Downloads/security-footage-1648933966395.pcap (not found)

Capture

...using this filter: Enter a capture filter ...

All interfaces shown

```
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
```

Learn

You are running Wireshark 4.4.5.

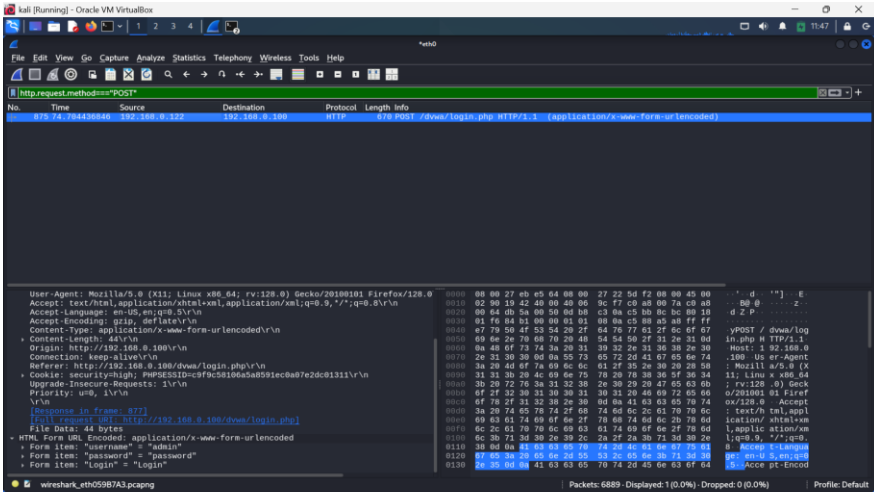
Ready to load or capture | No Packets | Profile: Default

11:09
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

Fig (1): Wireshark

.

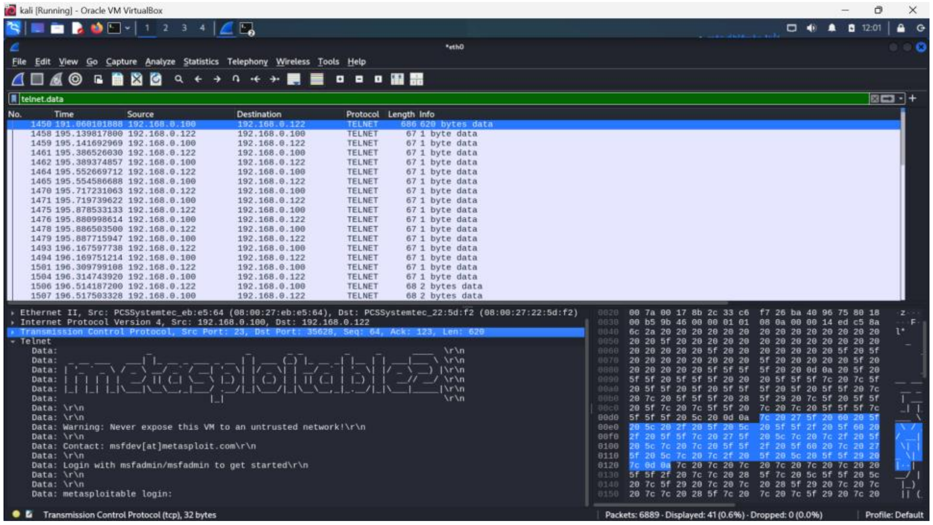
- Open Wireshark it displays all interfaces which is available like eth0, any etc..
- Select eth0 and start capturing the traffic to analyze after minute stope the Wireshark and analyze.
- Apply the filter to find the protocol.



```
http.request.method==="POST"

No.   Time          Source         Destination    Protocol  Length Info
  875 74.704436846  192.168.0.122  192.168.0.100  HTTP         670 POST /dvwa/login.php HTTP/1.1  (application/x-www-form-urlencoded)

    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 44\r\n
    Origin: http://192.168.0.100\r\n
    Connection: keep-alive\r\n
    Referer: http://192.168.0.100/dvwa/login.php\r\n
  › Cookie: security=high; PHPSESSID=c9f9c58106a5a8591ec0a07e2dc01311\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 877]
    [Full request URI: http://192.168.0.100/dvwa/login.php]
    File Data: 44 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "username" = "admin"
  › Form item: "password" = "password"
  › Form item: "Login" = "Login"

0000  08 00 27 eb e5 64 08 00  27 22 5d f2 08 00 45 00   ··'··d·· '"]···E·
0010  02 90 19 42 40 00 40 06  9c f7 c0 a8 00 7a c0 a8   ···B@·@· ·····z··
0020  00 64 db 5a 00 50 0d b8  c3 0a c5 bb 8c bc 80 18   ·d·Z·P·· ········
0030  01 f6 84 b1 00 00 01 01  08 0a c5 88 a5 a8 ff ff   ········ ········
0040  e7 79 50 4f 53 54 20 2f  64 76 77 61 2f 6c 6f 67   ·yPOST / dvwa/log
0050  69 6e 2e 70 68 70 20 48  54 54 50 2f 31 2e 31 0d   in.php H TTP/1.1·
0060  0a 48 6f 73 74 3a 20 31  39 32 2e 31 36 38 2e 30   ·Host: 1 92.168.0
0070  2e 31 30 30 0d 0a 55 73  65 72 2d 41 67 65 6e 74   .100··Us er-Agent
0080  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 58   : Mozill a/5.0 (X
0090  31 31 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   11; Linu x x86_64
00a0  3b 20 72 76 3a 31 32 38  2e 30 29 20 47 65 63 6b   ; rv:128 .0) Geck
00b0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
00c0  6f 78 2f 31 32 38 2e 30  0d 0a 41 63 63 65 70 74   ox/128.0 ··Accept
00d0  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 61 70 70 6c   : text/h tml,appl
00e0  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/ xhtml+xm
00f0  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 6d   l,applic ation/xm
0100  6c 3b 71 3d 30 2e 39 2c  2a 2f 2a 3b 71 3d 30 2e   l;q=0.9, */*;q=0.
0110  38 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   8··Accep t-Langua
0120  67 65 3a 20 65 6e 2d 55  53 2c 65 6e 3b 71 3d 30   ge: en-U S,en;q=0
0130  2e 35 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .5··Acce pt-Encod

wireshark_eth059B7A3.pcapng    Packets: 6889 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig (2): http protocol

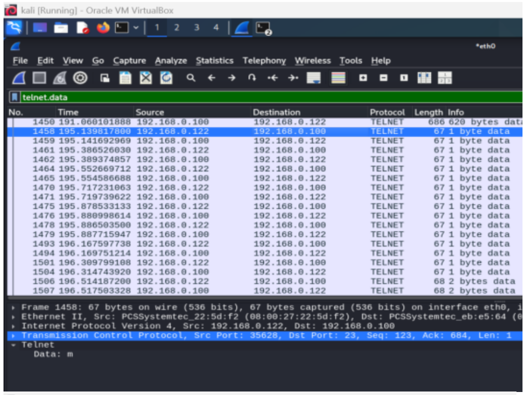
- We get source and destination IP address. Source IP is user's IP address and destination IP is the request sent by user.
- Apply the Filter http.request.method==”POST” to find the what the user is posted here username and password in the URL: http://192.168.0.100/dvwa/login.php
- To find the user cookies apply the filter http.cookie to get session id of the user using these cookies we can login user account if the website is vulnerable.



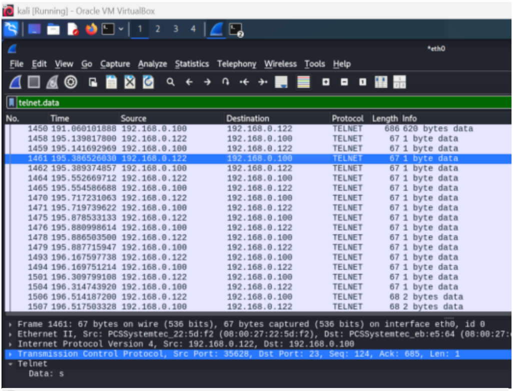
```
telnet.data

No.   Time           Source         Destination    Protocol  Length Info
 1450 191.060101888  192.168.0.100  192.168.0.122  TELNET       686 620 bytes data
 1458 195.139817800  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1459 195.141692969  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1461 195.386526030  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1462 195.389374857  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1464 195.552669712  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1465 195.554586688  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1470 195.717231063  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1471 195.719739622  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1475 195.878533133  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1476 195.880998614  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1478 195.886503500  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1479 195.887715947  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1493 196.167597738  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1494 196.169751214  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1501 196.309799108  192.168.0.122  192.168.0.100  TELNET        67 1 byte data
 1504 196.314743920  192.168.0.100  192.168.0.122  TELNET        67 1 byte data
 1506 196.514187200  192.168.0.122  192.168.0.100  TELNET        68 2 bytes data
 1507 196.517503328  192.168.0.100  192.168.0.122  TELNET        68 2 bytes data

› Ethernet II, Src: PCSSystemtec_eb:e5:64 (08:00:27:eb:e5:64), Dst: PCSSystemtec_22:5d:f2 (08:00:27:22:5d:f2)
› Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.122
› Transmission Control Protocol, Src Port: 23, Dst Port: 35628, Seq: 64, Ack: 123, Len: 620
⌄ Telnet
    Data:                                                          \r\n
    Data:                                                          \r\n
    Data:                                                          |\r\n
    Data:                                                          \r\n
    Data:                                                          |\r\n
    Data:                                                          \r\n
    Data: \r\n
    Data: \r\n
    Data: Warning: Never expose this VM to an untrusted network!\r\n
    Data: \r\n
    Data: Contact: msfdev[at]metasploit.com\r\n
    Data: \r\n
    Data: Login with msfadmin/msfadmin to get started\r\n
    Data: \r\n
    Data: \r\n
    Data: metasploitable login:

0020  00 7a 00 17 8b 2c 33 c6  f7 26 ba 40 96 75 80 18
0030  00 b5 9b 46 00 00 01 01  08 0a 00 00 14 ed c5 8a
0040  6c 2a 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0050  20 20 5f 20 20 20 20 20  20 20 20 20 20 20 20 20
0060  20 20 20 20 20 5f 20 20  20 20 20 20 20 5f 20 5f
0070  20 20 20 20 20 20 20 20  5f 20 20 20 20 20 5f 20
0080  20 20 20 20 20 5f 5f 5f  5f 20 20 0d 0a 20 5f 20
0090  5f 5f 20 5f 5f 5f 20 20  20 5f 5f 5f 7c 20 7c 5f
00a0  20 5f 5f 20 5f 20 5f 5f  5f 20 5f 20 5f 5f 20 7c
00b0  20 7c 20 5f 5f 5f 20 28  5f 29 20 7c 5f 20 5f 5f
00c0  20 5f 7c 20 7c 5f 5f 20  7c 20 7c 20 5f 5f 5f 7c
00d0  5f 5f 5f 20 5c 20 0d 0a  7c 20 27 5f 20 60 20 5f
00e0  20 5c 20 2f 20 5f 20 5c  20 5f 5f 2f 20 5f 60 20
00f0  2f 20 5f 5f 7c 20 27 5f  20 5c 7c 20 7c 2f 20 5f
0100  20 5c 7c 20 7c 20 5f 5f  2f 20 5f 60 20 7c 20 27
0110  5f 20 5c 7c 20 7c 2f 20  5f 20 5c 20 5f 5f 29 20
0120  7c 0d 0a 7c 20 7c 20 7c  20 7c 20 7c 20 7c 20 20
0130  5f 5f 2f 20 7c 7c 20 28  5f 7c 20 5c 5f 5f 20 5c
0140  20 7c 5f 29 20 7c 20 7c  20 28 5f 29 20 7c 20 7c
0150  20 7c 7c 20 28 5f 7c 20  7c 20 7c 5f 29 20 7c 20

Transmission Control Protocol (tcp), 32 bytes    Packets: 6889 · Displayed: 41 (0.6%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig (3): Telnet protocol

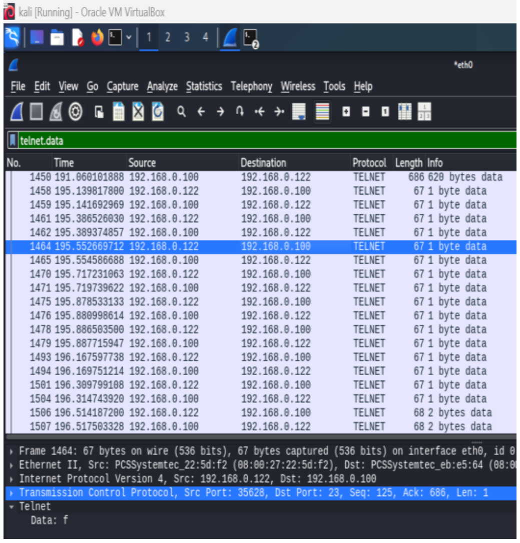
- Apply the filter for telnet.data for telnet protocol. So here the Wireshark show's the requests which is related to telnet.
- No observe the each request carefully we get data. Observe the picture data carefully.


kali [Running] - Oracle VM VirtualBox
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

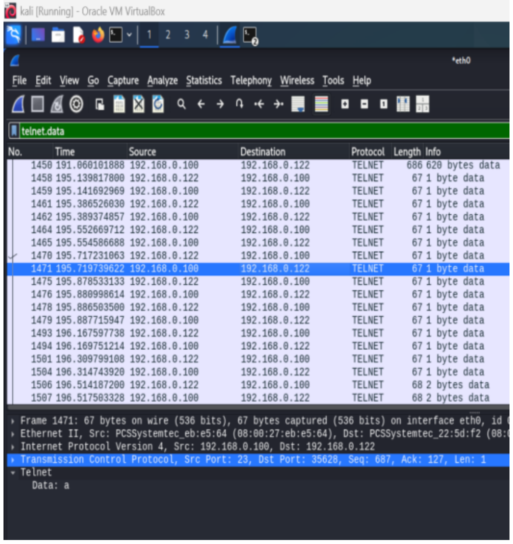
```
telnet.data
No.    Time          Source          Destination     Protocol Length Info
  1450 191.060101888 192.168.0.100   192.168.0.122   TELNET    686 620 bytes dat
  1458 195.139817800 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1459 195.141692969 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1461 195.386526030 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1462 195.389374857 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1464 195.552669712 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1465 195.554586688 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1470 195.717231063 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1471 195.719739622 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1475 195.878533133 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1476 195.880998614 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1478 195.886503500 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1479 195.887715947 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1493 196.167597738 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1494 196.169751214 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1501 196.309799108 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1504 196.314743920 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1506 196.514187200 192.168.0.122   192.168.0.100   TELNET     68 2 bytes data
  1507 196.517503328 192.168.0.100   192.168.0.122   TELNET     68 2 bytes data

› Frame 1458: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, i
› Ethernet II, Src: PCSSystemtec_22:5d:f2 (08:00:27:22:5d:f2), Dst: PCSSystemtec_eb:e5:64 (0
› Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.100
› Transmission Control Protocol, Src Port: 35628, Dst Port: 23, Seq: 123, Ack: 684, Len: 1
▾ Telnet
    Data: m
```


kali [Running] - Oracle VM VirtualBox
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

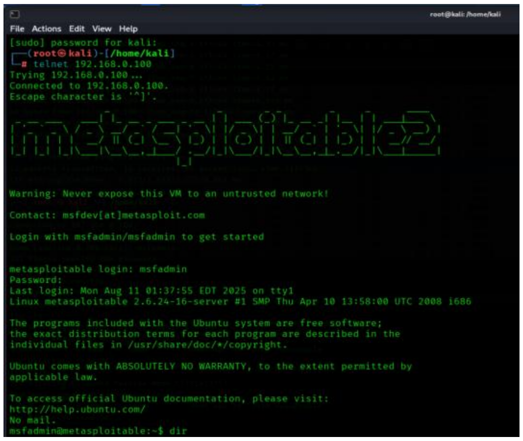
```
telnet.data
No.    Time          Source          Destination     Protocol Length Info
  1450 191.060101888 192.168.0.100   192.168.0.122   TELNET    686 620 bytes data
  1458 195.139817800 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1459 195.141692969 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1461 195.386526030 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1462 195.389374857 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1464 195.552669712 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1465 195.554586688 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1470 195.717231063 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1471 195.719739622 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1475 195.878533133 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1476 195.880998614 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1478 195.886503500 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1479 195.887715947 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1493 196.167597738 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1494 196.169751214 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1501 196.309799108 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1504 196.314743920 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1506 196.514187200 192.168.0.122   192.168.0.100   TELNET     68 2 bytes data
  1507 196.517503328 192.168.0.100   192.168.0.122   TELNET     68 2 bytes data

› Frame 1461: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_22:5d:f2 (08:00:27:22:5d:f2), Dst: PCSSystemtec_eb:e5:64 (08:00:27:
› Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.100
› Transmission Control Protocol, Src Port: 35628, Dst Port: 23, Seq: 124, Ack: 685, Len: 1
▾ Telnet
    Data: s
```


kali [Running] - Oracle VM VirtualBox
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet.data
No.    Time          Source          Destination     Protocol Length Info
  1450 191.060101888 192.168.0.100   192.168.0.122   TELNET    686 620 bytes data
  1458 195.139817800 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1459 195.141692969 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1461 195.386526030 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1462 195.389374857 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1464 195.552669712 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1465 195.554586688 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1470 195.717231063 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1471 195.719739622 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1475 195.878533133 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1476 195.880998614 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1478 195.886503500 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1479 195.887715947 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1493 196.167597738 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1494 196.169751214 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1501 196.309799108 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1504 196.314743920 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1506 196.514187200 192.168.0.122   192.168.0.100   TELNET     68 2 bytes data
  1507 196.517503328 192.168.0.100   192.168.0.122   TELNET     68 2 bytes data

› Frame 1464: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_22:5d:f2 (08:00:27:22:5d:f2), Dst: PCSSystemtec_eb:e5:64 (08:0
› Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.100
› Transmission Control Protocol, Src Port: 35628, Dst Port: 23, Seq: 125, Ack: 686, Len: 1
▾ Telnet
    Data: f
```


kali [Running] - Oracle VM VirtualBox
1 2 3 4
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
telnet.data
No.    Time          Source          Destination     Protocol Length Info
  1450 191.060101888 192.168.0.100   192.168.0.122   TELNET    686 620 bytes data
  1458 195.139817800 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1459 195.141692969 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1461 195.386526030 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1462 195.389374857 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1464 195.552669712 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1465 195.554586688 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1470 195.717231063 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1471 195.719739622 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1475 195.878533133 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1476 195.880998614 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1478 195.886503500 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1479 195.887715947 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1493 196.167597738 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1494 196.169751214 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1501 196.309799108 192.168.0.122   192.168.0.100   TELNET     67 1 byte data
  1504 196.314743920 192.168.0.100   192.168.0.122   TELNET     67 1 byte data
  1506 196.514187200 192.168.0.122   192.168.0.100   TELNET     68 2 bytes data
  1507 196.517503328 192.168.0.100   192.168.0.122   TELNET     68 2 bytes data

› Frame 1471: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface eth0, id 
› Ethernet II, Src: PCSSystemtec_eb:e5:64 (08:00:27:eb:e5:64), Dst: PCSSystemtec_22:5d:f2 (08:0
› Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.122
› Transmission Control Protocol, Src Port: 23, Dst Port: 35628, Seq: 687, Ack: 127, Len: 1
▾ Telnet
    Data: a
```



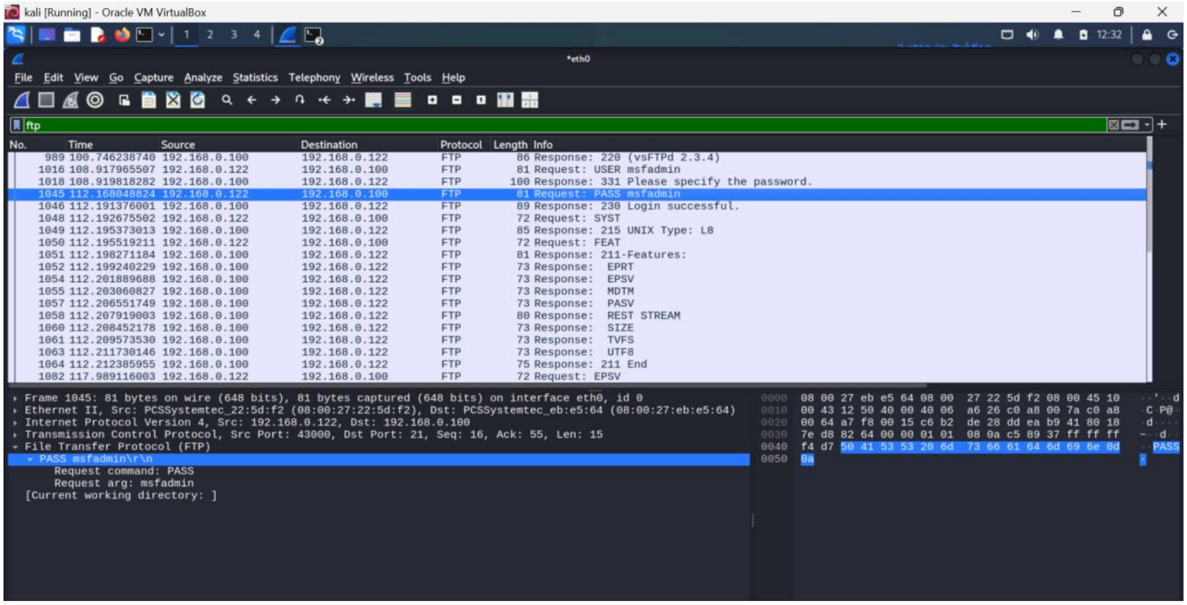
```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.0.100
Trying 192.168.0.100...
Connected to 192.168.0.100.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Aug 11 01:37:55 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ dir
```

telnet

- Observe the all request we get username: msfadmin, password: msfadmin.
- Got to kali terminal send request to 192.160.0.100 for accessing telnet services.

COMMAND:

telnet 192.168.0.100


kali [Running] - Oracle VM VirtualBox
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp

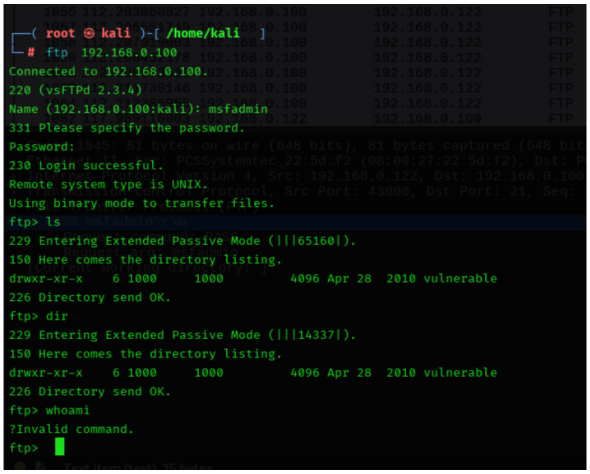
```
No.   Time           Source          Destination     Protocol Length Info
  989 100.746238740 192.168.0.100   192.168.0.122   FTP        86 Response: 220 (vsFTPd 2.3.4)
 1016 108.917965507 192.168.0.122   192.168.0.100   FTP        81 Request: USER msfadmin
 1018 108.919818282 192.168.0.100   192.168.0.122   FTP       100 Response: 331 Please specify the password.
 1045 112.168048824 192.168.0.122   192.168.0.100   FTP        81 Request: PASS msfadmin
 1046 112.191376001 192.168.0.100   192.168.0.122   FTP        89 Response: 230 Login successful.
 1048 112.192675502 192.168.0.122   192.168.0.100   FTP        72 Request: SYST
 1049 112.195373013 192.168.0.100   192.168.0.122   FTP        85 Response: 215 UNIX Type: L8
 1050 112.195519211 192.168.0.122   192.168.0.100   FTP        72 Request: FEAT
 1051 112.198271184 192.168.0.100   192.168.0.122   FTP        81 Response: 211-Features:
 1052 112.199240229 192.168.0.100   192.168.0.122   FTP        73 Response:  EPRT
 1054 112.201889688 192.168.0.100   192.168.0.122   FTP        73 Response:  EPSV
 1055 112.203060827 192.168.0.100   192.168.0.122   FTP        73 Response:  MDTM
 1057 112.206551749 192.168.0.100   192.168.0.122   FTP        73 Response:  PASV
 1058 112.207919003 192.168.0.100   192.168.0.122   FTP        80 Response:  REST STREAM
 1060 112.208452178 192.168.0.100   192.168.0.122   FTP        73 Response:  SIZE
 1061 112.209573530 192.168.0.100   192.168.0.122   FTP        73 Response:  TVFS
 1063 112.211730146 192.168.0.100   192.168.0.122   FTP        73 Response:  UTF8
 1064 112.212385955 192.168.0.100   192.168.0.122   FTP        75 Response: 211 End
 1082 117.989116003 192.168.0.122   192.168.0.100   FTP        72 Request: EPSV
```

```
› Frame 1045: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_22:5d:f2 (08:00:27:22:5d:f2), Dst: PCSSystemtec_eb:e5:64 (08:00:27:eb:e5:64)
› Internet Protocol Version 4, Src: 192.168.0.122, Dst: 192.168.0.100
› Transmission Control Protocol, Src Port: 43000, Dst Port: 21, Seq: 16, Ack: 55, Len: 15
⌄ File Transfer Protocol (FTP)
  ⌄ PASS msfadmin\r\n
      Request command: PASS
      Request arg: msfadmin
  [Current working directory: ]
```

```
0000  08 00 27 eb e5 64 08 00  27 22 5d f2 08 00 45 10   ··'··d
0010  00 43 12 50 40 00 40 06  a6 26 c0 a8 00 7a c0 a8   ·C·P@·
0020  00 64 a7 f8 00 15 c6 b2  de 28 dd ea b9 41 80 18   ·d····
0030  7e d8 82 64 00 00 01 01  08 0a c5 89 37 ff ff ff   ~··d··
0040  f4 d7 50 41 53 53 20 6d  73 66 61 64 6d 69 6e 0d   ··PASS
0050  0a                                                 ·
```

Filter: ftp

- Apply the filter for ftp for FTP protocol. So here the Wireshark shows the requests which is related to FTP.
- FTP is file transferring protocol the services on port 21.
- The actual file data in FTP may be sent over another port so if you also want to capture the file transfer data packets, you'd need.



```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.0.100
Connected to 192.168.0.100.
220 (vsFTPd 2.3.4)
Name (192.168.0.100:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65160|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> dir
229 Entering Extended Passive Mode (|||14337|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> whoami
?Invalid command.
ftp> 
```

ftp services

COMMAND

```
ftp 192.168.0.100
```

- Connect to ftp enter username and password which u find In the Wireshark and access the services.

Conclusion

Wireshark is a powerful open-source network protocol analyzer that turns bytes on the wire into network traffic you can analyze. Its simple-to-use interface provides an overview of your capture traffic in the list pane and specific information about each packet in the details pane.

You have seen how to examine network packets in granular detail, refine your view using Wireshark's display filters, and summarize network traffic with statistical analysis tools. These skills allow you to use Wireshark in the real world for following TCP streams to uncover conversations, extracting files, and identifying cyber attacks