

Practical 2a: Network Protocols

Objectives:

- Set up web-server2
- Using Wireshark
- Use Remote Desktop to connect to remote servers
- Using Netstat, FTP, Telnet, SSH, SCP and SFTP
- Ping and default Firewall settings
- Using PuTTY on Windows to connect to SSH Server
- Using SCP and FTP client software on Windows

Exercise 1. Setting up web-server2 virtual machine

A web-server2a virtual machine has been set up to use as a target in the exercises.

1. Download the web-server2a virtual machine from the same download links given when you downloaded Kali Linux.
1. Copy web-server2a.7z to your EHD folder.
2. Right-click on the web-server2a.7z file and choose 7-Zip, Extract files. Extract the files to your EHD folder.
3. Power on web-server2.
4. Login as user root and password centos. Type “ip addr” to find its IP address.

(Optional) Find out how to configure a static IP address for the web-server2 (CentOS).

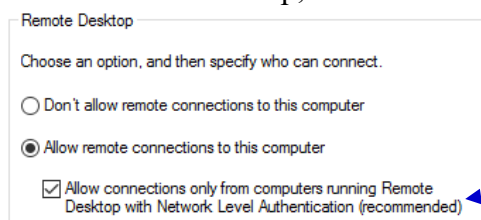
Exercise 2. Using Remote Desktop to connect to a remote system

Description :

You will enable Remote Desktop services on the Win10 virtual machine so that any other system is able to do a remote connection to it.

In Win10 VM:

1. Login as user admin.
2. Right-click on the Windows icon in the lower left corner and select System.
3. Click on “Advanced system settings”.
4. Click on the Remote tab.
5. Under Remote Desktop, select “Allow remote connections to this computer”.



Note : If your HostPC (your laptop or desktop) is unable to do a Remote Desktop connection with an encryption error, you may need to uncheck this box to allow your HostPC to connect.

6. Click on Select Users. View who is currently allowed to connect to the Win10 through Remote Desktop. Click Cancel.
7. Click OK.

8. In a Command Prompt, run “netstat -an” to see the ports that are opened. You should see that Port 3389, which is the default port number for Remote Desktop, is opened.
9. In the Cortana search textbox, type “firewall advanced” and run Windows Firewall with Advanced Security.
10. Click on Inbound Rules.
11. Enable the “Remote Desktop – User Mode (TCP-in)” rule for Public profile.

| | | | | |
|---------------------------------------|----------------|-----------------|-----|-------|
| ✓ Remote Desktop - User Mode (TCP-In) | Remote Desktop | Public | Yes | Allow |
| ✓ Remote Desktop - User Mode (TCP-In) | Remote Desktop | Domain, Private | Yes | Allow |

12. Run Wireshark and start capturing packets.

In Host PC (this refers to your laptop or desktop) :

13. In the Cortana search textbox, type “remote” and run Remote Desktop Connection.
14. For Computer, type in the IP address of your Win10 VM.
15. For username, click “More Choices” or “Show Options”. For username, use “192.168.10.67\admin”, changing the IP to your Win10-VM-IP.
16. Login to your Win10 VM as admin and password “1qwer\$#@!”
17. You may be asked about the certificate of the Win10 VM as it is not from a trusted Certificate Authority. Click Yes to accept it.
18. You now have remote access to the Desktop of your Win10 VM. You can run commands and applications just as if you are at the Win10 VM.
19. To exit Remote Desktop, click the cross icon in the top bar to close the connection.

In Win10 VM:

20. Stop the Wireshark capture.
21. Do a search to find the packet containing the password “1qwer\$#@!”. You should not be successful, as Remote Desktop Connection encrypts the network traffic.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--------------------------------------|
| 94 | 16.497622 | 172.16.10.1 | 172.16.10.172 | TLSv1.2 | 91 | Application Data |
| 95 | 16.497645 | 172.16.10.172 | 172.16.10.1 | TCP | 54 | 3389 → 52010 [ACK] Seq=2065 Ack=2000 |
| 96 | 16.497750 | 172.16.10.172 | 172.16.10.1 | TLSv1.2 | 94 | Application Data |
| 97 | 16.497923 | 172.16.10.1 | 172.16.10.172 | TLSv1.2 | 95 | Application Data |

> Frame 96: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{8198983...}

> Ethernet II, Src: VMware_0e:5f:d6 (00:0c:29:0e:5f:d6), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)

> Internet Protocol Version 4, Src: 172.16.10.172, Dst: 172.16.10.1

> Transmission Control Protocol, Src Port: 3389, Dst Port: 52010, Seq: 2065, Ack: 2000, Len: 40

▼ Transport Layer Security

> TLSv1.2 Record Layer: Application Data Protocol: tpkt

← The packets in the Remote Desktop connection are encrypted

Note : Remote Desktop should only be enabled when necessary.

In Win10 VM to disable Remote Desktop:

22. In System, click on “Advanced system settings”. Click the Remote tab.
23. Select “Don’t allow connections to this computer”. Click OK.

Exercise 3. Using Wireshark

Description:

Wireshark is a network traffic analyzer.

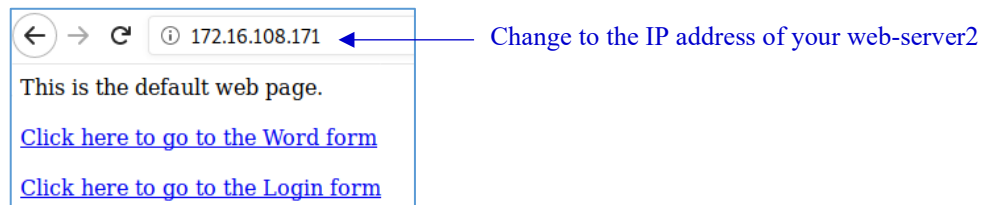
In Kali

1. Run Wireshark from Kali icon -> 09 Sniffing and Spoofing -> wireshark. Or you can just type “sudo wireshark” in a terminal.
2. If asked for a password, enter “kali”.
3. Go to the Capture menu and select Start to start capturing packets.
4. Generate some network traffic by pinging the web-server2 VM.

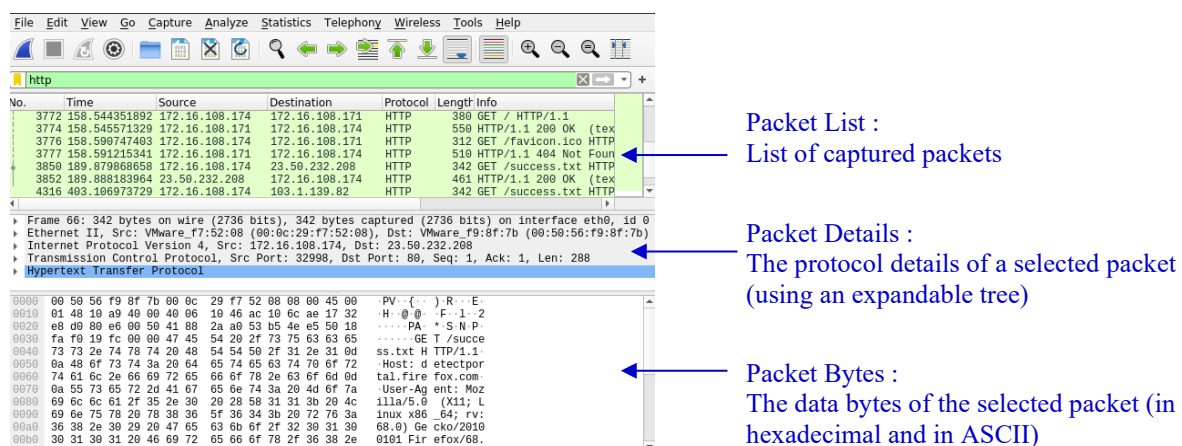
ping 172.16.108.171 ← Change to the IP address of your web-server2

Press Control-C to stop the ping.

5. Start the web browser and browse to the web-server2 IP address.

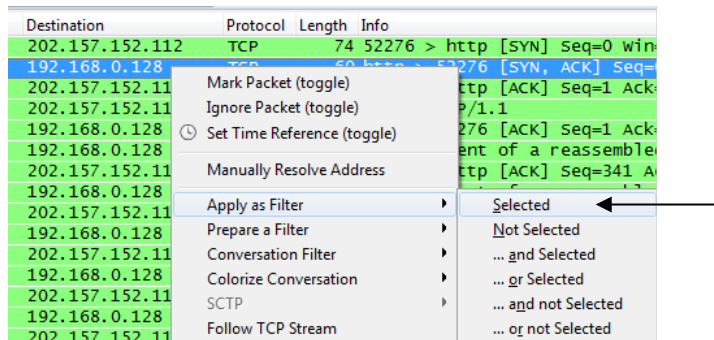


6. In the web browser, click the link to go to the Word form. Enter a word (eg rainbow) and click Submit.
7. In Wireshark, go to the Capture menu and select Stop to stop capturing packets.

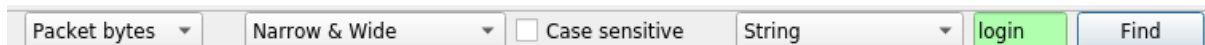


8. To view only the packets involved in the ping command, type “icmp” in the Filter textbox and press Enter. View the packets captured.
9. To view only the packets involved in the http command, type “http” in the Filter textbox and press Enter. View the packets captured.
10. To view only packets that are sent or received by your Kali VM, type “ip.addr==172.16.108.174” in the Filter box, changing the IP address to your Kali IP.

11. To view packets that are sent or received by a subnet, type
“ip.addr==172.16.108.0/24” in the Filter box, changing the subnet to your VM subnet.
12. You can also apply the filter by right-clicking on the data in column, and choose Apply as Filter, Selected. (see following diagram)



13. Clear the Filter box and press Enter.
14. To search for packets containing the string “login”, go to Edit menu and choose Find Packet. Change the Display Filter to “String” and type “login” in the search textbox. Change “Packet list” to “Packet bytes” so that Wireshark will search for the string in the packet bytes pane. (see following diagram)



15. Click Find. The first packet found will be selected. You can click Find again to search for the next packet containing the string (if any).
16. Another way to search for strings is to type the following in the Filter textbox
frame contains login

17. Type the following in the Filter box to view only the 3 packets in the TCP 3-way handshake

`tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.initial_rtt)`
(rtt stands for round trip time)

Export Objects

Wireshark can reassemble data like images and export them out as files.

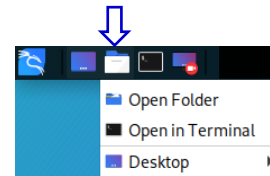
18. Go to File menu and select Export Objects. Choose HTTP.
19. You will see the two pictures that appeared in the Word form. (Note : If the pictures are not listed in Wireshark, it could be because your web browser has loaded the webpage before, and the pictures are already in the web browser cache. Clear the web browser history, start the Wireshark capture and load the webpage again.)

| Packet | Hostname | Content Type | Size | Filename |
|--------|--------------------------|--------------|-------------|-------------|
| 6 | 172.16.108.171 | text/html | 166 bytes | / |
| 9 | 172.16.108.171 | text/html | 209 bytes | favicon.ico |
| 12 | 172.16.108.171 | text/html | 235 bytes | word |
| 20 | 172.16.108.171 | text/html | 189 bytes | word |
| 23 | 172.16.108.171 | image/jpeg | 8,734 bytes | car.jpg |
| 72 | 172.16.108.171 | image/png | 97 kB | train.png |
| 78 | detectportal.firefox.com | text/plain | 8 bytes | success.txt |

The two pictures from the Word form

20. Select one of the pictures and click Save. Save the file to a directory on Kali (eg. You can save to /home/kali)

21. In Kali, click on the Explorer icon in the top left corner.



22. Browse to the directory where the picture was saved to. You can double-click the picture file to open it.

Follow TCP Stream

Wireshark can reassemble a stream of packets that belongs to a single TCP connection into an easier-to-read format.

23. In Wireshark, enter the following in the Filter textbox to view the packet that contains the Word form you posted to the web-server2. When web forms are submitted, they normally use the HTTP POST method.

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

24. Right-click on the HTTP POST packet and select Follow -> TCP Stream.

25. The packets that belong to this TCP connection will be reassembled to form the HTTP request and HTTP response.

```
POST /word/next.py HTTP/1.1
Host: 172.16.108.171
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.108.171/word/
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Connection: keep-alive
Upgrade-Insecure-Requests: 1

word=rainbowHTTP/1.1 200 OK
Date: Thu, 06 Feb 2020 01:36:00 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
Content-Length: 11
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

← The red part is the HTTP request sent by the web browser. Note that the word submitted is in cleartext as HTTP is not encrypted.

← The blue part is the HTTP response sent by the web server.

Thank you

Name Resolution

Instead of seeing IP addresses, Wireshark can try to resolve the IP addresses to hostnames.

26. In Wireshark, start capturing packets. You do not need to save the previous capture.

27. In the web browser, browse to a website, eg www.sp.edu.sg

28. After the webpage has loaded, stop the Wireshark capture.

29. In Wireshark, go to Edit menu and choose Preferences.

30. Select Name Resolution. Check the box "Resolve network (IP) addresses".

31. Wireshark will display the hostnames. (see following diagram)

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------------|----------------------------|----------|--------|---------------------|
| 664 | 7.043616933 | da4oz2t8ub3br.cloudf... | 172.16.108.174 | TCP | 60 | 443 → 55320 [ACK] |
| 665 | 7.045615891 | 172.16.108.174 | da4oz2t8ub3br.cloudfron... | TLSv1.2 | 167 | Application Data |
| 666 | 7.046111990 | da4oz2t8ub3br.cloudf... | 172.16.108.174 | TCP | 60 | 443 → 55320 [ACK] |
| 667 | 7.046841331 | www.google.com.sg | 172.16.108.174 | TCP | 60 | 80 → 34968 [SYN, A] |
| 668 | 7.046861000 | 172.16.108.174 | www.google.com.sg | TCP | 54 | 34968 → 80 [ACK] S |
| 669 | 7.046865592 | www.google.com.sg | 172.16.108.174 | TCP | 60 | 80 → 34966 [SYN, A] |
| 670 | 7.046869350 | 172.16.108.174 | www.google.com.sg | TCP | 54 | 34966 → 80 [ACK] S |
| 671 | 7.046891857 | standard.t-0001.t-ms... | 172.16.108.174 | TLSv1.2 | 92 | Application Data |

Public IP addresses are resolved to their hostnames.

32. Go to Edit menu -> Preferences -> Name Resolution and uncheck the box "Resolve network (IP) addresses".

Task 1

Download capture.zip from Brightspace or from the Dropbox link under the folder “Files-For-Topic1-NetworkProtocol”. Extract the two files capture01.pcap and capture02.pcap. Use Wireshark to open capture01.pcap. This file contains the packets captured when a user submitted a form at <http://192.168.6.53/word/index.jsp>.

- When did the user submit the form?
- What is the IP address of the user?
- What is the MAC address of the user?
- What word did this user enter?
- Identify the three packets that make up the 3-way handshake. Record the packet numbers below:

| | Packet number |
|----------------|---------------|
| SYN packet | |
| SYN/ACK packet | |
| ACK packet | |

(Answers can be found on Brightspace)

Task 2

Use Wireshark to open capture02.pcap extracted from capture.zip on Brightspace. Analyse the contents and try to figure out what is the user doing.

Suggested solution:

In Wireshark, you can see Packet 8 is a HTTP GET request to www.amazon.com, and the URL contains the string “Harry Potter Chamber Secrets Book”. So the user is requesting for the Amazon web page for the book Harry Potter and the Chamber of Secrets.

Most of the rest of the packets probably contain the HTTP response from Amazon, returning the web page. Right-click on any of these packets and choose Follow -> TCP Stream.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|---------------------------|--------------|----------------------------------|
| 8 | 1.766234 | 192.168.10.140 | 192.168.10.1 | HTTP | 1022 | GET http://www.amazon.com/H |
| 11 | 1.905478 | 192.168.10.1 | 192.168.10.140 | TCP | 60 | 8080 → 1316 [ACK] Seq=1 Ack |
| 20 | 2.616027 | 192.168.10.1 | 192.168.10.1 | Mark/Unmark Packet | Ctrl+M | 1445 8080 → 1316 [PSH, ACK] Seq= |
| 21 | 2.616648 | 192.168.10.1 | 192.168.10.1 | Ignore/Unignore Packet | Ctrl+D | 1514 8080 → 1316 [ACK] Seq=1392 |
| 22 | 2.616675 | 192.168.10.1 | 192.168.10.1 | Set/Unset Time Reference | Ctrl+T | 54 1316 → 8080 [ACK] Seq=969 A |
| 23 | 2.616729 | 192.168.10.1 | 192.168.10.1 | Time Shift... | Ctrl+Shift+T | 1514 8080 → 1316 [ACK] Seq=2852 |
| 24 | 2.616737 | 192.168.10.1 | 192.168.10.1 | Packet Comment... | Ctrl+Alt+C | 886 8080 → 1316 [PSH, ACK] Seq= |
| 25 | 2.616755 | 192.168.10.1 | 192.168.10.1 | Edit Resolved Name | | 54 1316 → 8080 [ACK] Seq=969 A |
| 26 | 2.616792 | 192.168.10.1 | 192.168.10.1 | Apply as Filter | > | 554 8080 → 1316 [PSH, ACK] Seq= |
| 27 | 2.617968 | 192.168.10.1 | 192.168.10.1 | Prepare as Filter | > | 1514 8080 → 1316 [ACK] Seq=5644 |
| 28 | 2.617987 | 192.168.10.1 | 192.168.10.1 | Conversation Filter | > | 54 1316 → 8080 [ACK] Seq=969 A |
| 29 | 2.618025 | 192.168.10.1 | 192.168.10.1 | Colorize Conversation | > | 1514 8080 → 1316 [ACK] Seq=7104 |
| 30 | 2.618032 | 192.168.10.1 | 192.168.10.1 | SCTP | > | 879 8080 → 1316 [PSH, ACK] Seq= |
| 31 | 2.618050 | 192.168.10.1 | 192.168.10.1 | Follow | > | 54 1316 → 8080 [ACK] Seq=969 A |
| 32 | 2.618100 | 192.168.10.1 | 192.168.10.1 | Copy | > | 554 8080 → 1316 [PSH, ACK] Seq= |
| 33 | 2.618146 | 192.168.10.1 | 192.168.10.1 | Protocol Preferences | > | 1514 8080 → 1316 [ACK] Seq=9889 |
| 34 | 2.618161 | 192.168.10.1 | 192.168.10.1 | Decode As... | > | |
| 35 | 2.618196 | 192.168.10.1 | 192.168.10.1 | Show Packet in New Window | > | |

In this example, right-click on Packet 11 and choose Follow -> TCP Stream

The packets will be reassembled to form the HTTP request and the HTTP response.

```
GET http://www.amazon.com/Harry-Potter-Chamber-Secrets-Book/dp/0439964872/
refer=1_12psbooks&ie=UTF8&qid=1334648841&sr=1-2 HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-
shockwave-flash, application/xml+xml, application/x-ms-xbap, application/x-ms-
application, */*
Referer: http://www.amazon.com/s/ref=nb_sb_noss?url=search-
alias%3Dstripbooks&field-keywords=harry-potter
Accept-Language: en-us
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C)
Host: www.amazon.com
Cookie: session-id=20827872011; session-id=175-7244074-0099246; ubid-
main=180-3239628-2414639; session-
token=MPD8d5Vbp4QcWbb4rkW42LD5U8dtWe9hF1SjJ6KrYGSnQfIAjV5j0NKRn6hr44NzqslVah
rV6andQqRyGa3J3S9QeUddXibQ8uZHK1zeprXvA8Ww2/q2mIT/
c/RV6NwCVXQFqQZ6jQcXEHWB4XXL7ygZw5Nnm9vOWStoS1T818281svenQke9v1MLBu78dI2G9S
N1sTFw1XQ/2n6DLJtQp4r88TcFU0mMD2kUodbThHybL6c90WwaphKk; csm-hit=50.89
HTTP/1.1 200 OK
```

This is the HTTP GET request, sent to www.amazon.com, requesting for the web page for the Harry Potter book

You can use the Export Objects feature to reassemble the web page that is displayed to the user.

In Kali, create a new directory to store the objects that will be exported from Wireshark

```
mkdir /home/kali/temp
```

In Wireshark, go to File -> Export Objects -> HTTP

Click Save All.

Browse to /home/kali/temp and click Open. The objects (images, html pages, etc) will be saved to the directory. Click Close.

In Kali, look for exported web pages in the directory.

```
ls /home/kali/temp/*.html*
```

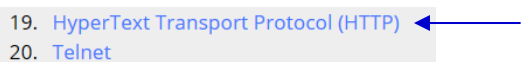
In the web browser, open the html file to see the reassembled web page that was returned to the user.

Task 3

The Wireshark Wiki contains many sample pcap files.

In Kali, browse to <https://wiki.wireshark.org/SampleCaptures>

Click on the link 19. Hypertext Transport Protocol.



19. [HyperText Transport Protocol \(HTTP\)](#)
20. [Telnet](#)

Download the http_with_jpegs cap file.

http_with_jpegs.cap.gz A simple capture containing a few JPEG pictures one can reassemble and save to a file.

You can use the gunzip command to unzip it.

```
gunzip http_with_jpegs.cap.gz
```

Use Wireshark to open the cap file. Use the features of Wireshark to find the JPEG pictures.

Exercise 4. Identifying Open Ports in Linux - netstat

Description :

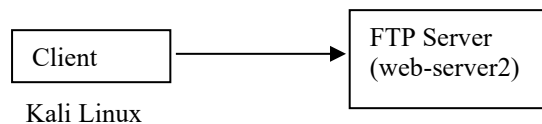
Netstat can be used to list opened ports on your system. You have used the Netstat command

on Windows before. The options for listing opened ports on a Linux system are slightly different.

In web-server2

1. Run “netstat -tuna” to see the currently opened ports. The options -tuna will display all TCP and UDP connections in numeric format.
2. To see the processes that are responsible for opening the ports, run “netstat -tunap”.

Exercise 5. Connecting to the FTP Server



Description:

a (File Transfer Protocol) is used to upload or download files over the network. It has two types of TCP connections : control connection for the login, and data connection for the file upload/download. However, it is not a secured protocol (data is sent across the network in cleartext).

In Kali

3. Run Wireshark and start capturing packets.
4. In a terminal, type “ftp *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
5. For User, enter “student00”.
6. For Password, enter “student00”. (you will not be able to see any characters appearing on screen as you type the password)
7. Type “help” to see a list of available commands for FTP.
8. Type “dir” or “ls” to get a listing of the current directory on the FTP server.

You should see the file `myfile` listed.

9. To download myfile, type “get myfile”.
10. Type “bye” or “exit” to end the FTP connection.
11. Type “ls” to see the listing of the files in the current directory. You should see the myfile.
12. Type “cat myfile” to view the contents of the file.
13. Stop the Wireshark capture.
14. In Wireshark, find the packets that make up the 3-way handshake. There should be at least two sets of 3-way handshakes : one for the FTP control connection, and one (or more) for the FTP data connection.
15. Type “ftp” in the Filter textbox. You will be able to see the username and password and the name of the downloaded file.

AY232

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------|----------------|----------|--------|---|
| 4 | 0.001857485 | 172.16.108.171 | 172.16.108.174 | FTP | 86 | Response: 220 (vsFTpd 3.0.2) |
| 6 | 3.277963653 | 172.16.108.174 | 172.16.108.171 | FTP | 82 | Request: USER student00 |
| 8 | 3.278415506 | 172.16.108.171 | 172.16.108.174 | FTP | 100 | Response: 331 Please specify the password. |
| 10 | 6.349914541 | 172.16.108.174 | 172.16.108.171 | FTP | 82 | Request: PASS student00 |
| 13 | 6.371170936 | 172.16.108.171 | 172.16.108.174 | FTP | 89 | Response: 230 Login successful. |
| 15 | 6.371304838 | 172.16.108.174 | 172.16.108.171 | FTP | 72 | Request: SYST |
| 16 | 6.371471637 | 172.16.108.171 | 172.16.108.174 | FTP | 85 | Response: 215 UNIX Type: L8 |
| 18 | 7.685887632 | 172.16.108.174 | 172.16.108.171 | FTP | 95 | Request: PORT 172,16,108,174,206,173 |
| 19 | 7.686280310 | 172.16.108.171 | 172.16.108.174 | FTP | 117 | Response: 200 PORT command successful. Consider using PASV. |
| 21 | 7.686374998 | 172.16.108.174 | 172.16.108.171 | FTP | 72 | Request: LIST |
| 25 | 7.686986272 | 172.16.108.171 | 172.16.108.174 | FTP | 105 | Response: 150 Here comes the directory listing. |
| 32 | 7.687636588 | 172.16.108.171 | 172.16.108.174 | FTP | 90 | Response: 226 Directory send OK. |
| 42 | 11.085790159 | 172.16.108.174 | 172.16.108.171 | FTP | 74 | Request: TYPE I |

16. Type “ftp-data” in the Filter textbox to see the packet that contains the downloaded file.

The screenshot shows a Wireshark packet capture with the filter 'ftp-data' applied. The packet list shows two packets: packet 27 (FTP-DATA, 192 bytes) and packet 54 (FTP-DATA, 92 bytes). Packet 54 is selected, and its details are expanded. The details show the packet is an FTP Data packet (26 bytes) from 172.16.108.171 to 172.16.108.174. The packet bytes show the text 'This is student00 myfile\n'.

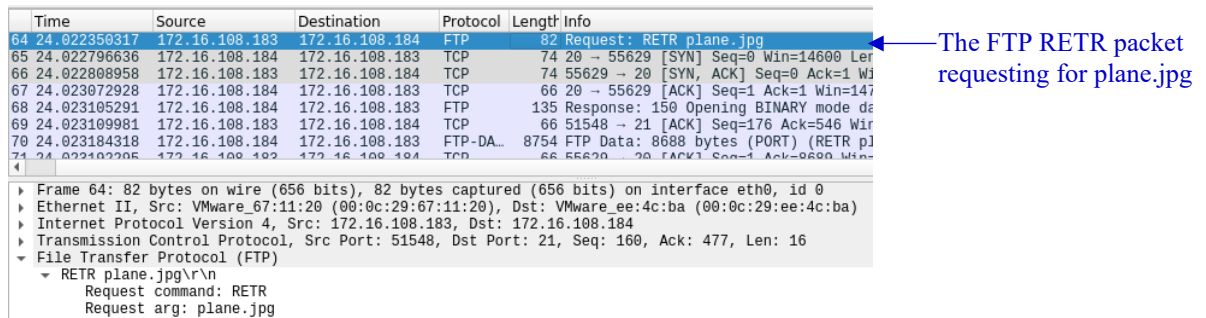
17. Clear the Filter. Right-click on any FTP packet and choose Follow -> TCP Stream. The FTP transaction will be displayed.

Anonymous FTP login

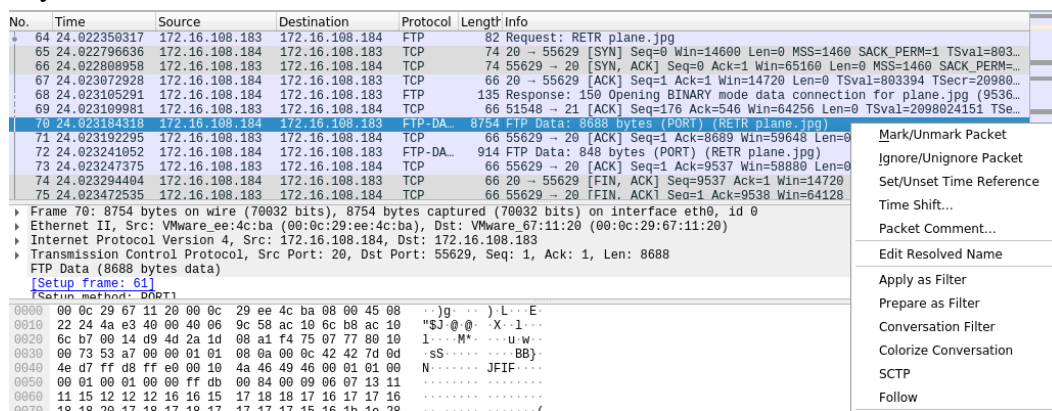
Many public FTP sites allow anonymous login. This allows anyone to connect to these public FTP servers without needing to authenticate, to view or download publicly available files.

18. Start a Wireshark capture.
19. In a terminal, type “ftp *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
20. For User, enter “anonymous”.
21. For Password, you can just press Enter.
22. Type “ls” to see the listing of the current directory. You should see a directory called “pub” (short for public). All files in the pub directory are accessible to anyone.
23. Type “cd pub” to change to that directory.
24. Type “ls” to see the listing of the pub directory. You should see two files “file1” and “plane.jpg”.
25. Type “get file1” to download it.
26. Type “get plane.jpg” to download it.
27. Type “bye” to close the connection.
28. Stop the Wireshark capture.

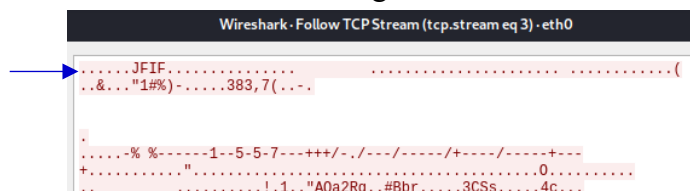
29. As FTP has no encryption, you can see what files have been transferred from the packet capture.
30. In Wireshark, look for the FTP packet sent by your Kali to request to get plane.jpg. You can use “FTP” in the filter to help your search.



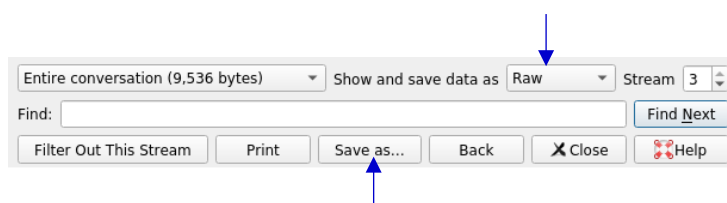
31. In Wireshark, look for the packet(s) containing the contents of plane.jpg. Right-click on any of them and choose Follow -> TCP Stream.



32. The Follow TCP Stream dialog box contains the file that was downloaded. Note that the file header contains the string “JFIF” which indicates it is a JPEG file.



33. To see what picture has been downloaded, change to “Show and save data as Raw” and click “Save as”. Save the file to a directory on your Kali, eg /home/kali.



34. In Kali, in the top left menu bar, click on the Folder icon and browse to where you have saved the picture. Double-click on the picture to view it.

Exercise 6. Using Telnet

Description:

Telnet is used to connect to a remote computer. However, it is not a secured protocol (data is sent across the network in cleartext).

In web-server2 VM:

1. Edit the file `/etc/xinetd.d/telnet`. Change the following line to enable telnet
`disable = no`
2. Start the xinetd service if it is not already running.
`systemctl start xinetd`
3. Use Netstat to check that the Telnet Port 23 is opened.
`netstat -tuna`
4. The firewall has to be adjusted to allow connections to the Telnet port 23. Edit the file `/etc/firewalld/zones/public.xml`. Add the following line among the other services.
`<service name="telnet"/>`
5. Restart the firewall.
`systemctl restart firewalld`

In Kali VM

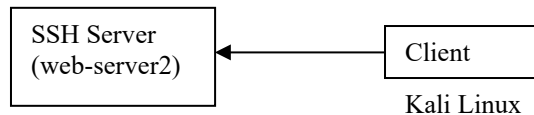
6. Start a Wireshark capture.
7. In a terminal, type `"telnet web-server2-IP"` where *web-server2-IP* is the IP Address of your web-server2.
8. Login using the student00 account (password is student00).
9. Type `"ls"`. You should be able to see a listing of the files on your web-server2. You can also run other commands on your web-server2.
10. Type `"exit"` to exit the Telnet session.
11. Stop the Wireshark capture.
12. In Wireshark, right-click on any of the TELNET packets and choose Follow -> TCP Stream.
13. As Telnet is unencrypted, you can see the password, commands and messages that are sent between the web-server2 and the client.

In web-server2 VM:

14. Edit the file `/etc/xinetd.d/telnet`. Change the following line to disable telnet
`disable = yes`
15. Restart the xinetd service so that the telnet service will not be running any more.
`systemctl restart xinetd`

You do not need to reset the firewall settings because we want the firewall to allow connections to Port 23 in Practical 1b when we do basic port scans.

Exercise 7. Using SSH, SFTP and SCP at command line



In Kali Linux

1. In a terminal, run “ssh student00@*web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
2. As this is the first time, you are connecting to the SSH Server from your Kali, you will see a message about the key fingerprint of the host. Type “yes” to continue connecting.
3. Type “student00” for the password. You will be logged in to the SSH service on your web-server2.
4. Type “ls” to view the student’s home directory.
5. Type “exit” to close the connection.

SFTP (Secure FTP) allows the transfer of files through a secured SSH channel.

In Kali Linux

6. Run Wireshark to start capturing packets
7. Run “sftp student00@ *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
8. Type “student00” for the password. Type “ls” to view the student’s home directory. Note that there is a file called “myfile”.
9. Type “get myfile” to download this file to your Kali Linux.
10. Type “exit” to close the connection.
11. View the contents of the downloaded file “myfile”. (You can type “cat myfile” to view the file contents)
12. Stop Wireshark and inspect the captured packets. Are you able to see the username and password of student or the contents of myfile? You should not be able to do so as the transaction is through a secured channel.

SCP (Secure Copy) also allows copying of files through a secured SSH channel. SCP does not allow listing of remote files (eg using ls).

In Kali Linux

In this example, you will use SCP to copy /home/student00/myfile from the web-server2 to your current directory in Kali and name the copied file “myfile1”.

13. Run “scp student00@*web-server2-IP*:/home/student00/myfile myfile1”.
14. Type “student00” for the password.
15. View the contents of the copied file “myfile1”. (You can type “cat myfile1” to view the file contents)

Exercise 8. Ping and default Firewall settings

Description:

The ping command uses the ICMP protocol. If you are able to ping another computer, it means that computer is up. However, most firewalls have been configured to block the ping packet so that attackers can not tell which computer is up.

From your Host PC (this refers to your laptop or desktop)

1. In Command Prompt, are you able to ping your Win10 VM?

You can not ping your Win10 VM because the default Windows firewall is blocking ping requests.

In Win10 VM

2. In the Cortana search textbox, type “firewall”. Click on “Windows Firewall with Advanced Security”.
3. In the left hand pane, click on Inbound Rules.
4. Look for the rules “File and Printer Sharing (Echo Request - ICMPv4-In)”. Currently these rules are disabled, so ICMPv4 packets are being blocked.
5. Right-click on these rules and Enable them.

| | | | |
|---|--------------------------|-----------------|-----|
| ✓ File and Printer Sharing (Echo Request - ICMPv4-In) | File and Printer Sharing | Private, Public | Yes |
| ✓ File and Printer Sharing (Echo Request - ICMPv4-In) | File and Printer Sharing | Domain | Yes |

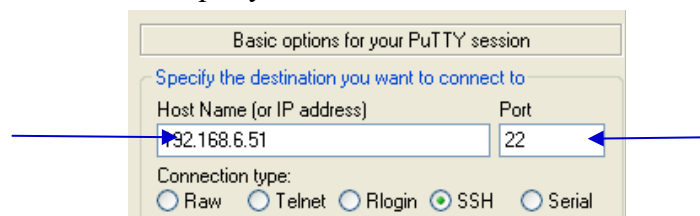
6. From your Host PC, try to ping your Win10 VM. You should be successful.

Exercise 9. Using PuTTY on Windows to connect to SSH Server

Putty can be used on Windows to connect to various servers, like SSH Server.

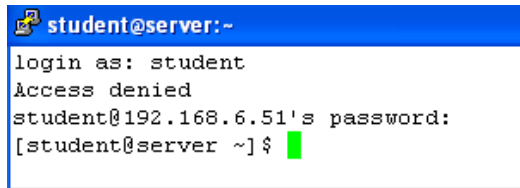
In Win10 VM

1. Browse to www.putty.org or Brightspace or the download link (under Topic 1) and download Putty.
2. Double-click on putty.exe to run it.



3. For the IP address, enter the web-server2 IP.
4. Check that Port is set to “22”. Click Open.

5. If you see a PuTTY Security Alert about the server's host key, click **Yes** to trust the SSH Server.



```
student@server:~  
login as: student  
Access denied  
student@192.168.6.51's password:  
[student@server ~]$
```

6. Login with username “student00” and password “student00”.
7. When you have logged in, type “pwd” and “ls” to view the student00’s home directory on the SSH Server.
8. Type “exit” to close the SSH connection.

Exercise 10. Using SCP and FTP client software on Windows

In Win10 VM

1. To do SCP from a Windows system, you can use WinSCP (or other similar software). Download the WinSCP installation file from the download link (under Topic 1), or you can download the latest version from <https://www.winscp.net>.
2. Install and explore WinSCP. Use WinSCP to connect to your web-server2 as user “student00” to do a Secure Copy of the file "myfile" from student00's home directory.
3. To do FTP from a Windows system, you can use Filezilla client (or other similar software). Download the Filezilla Client installation file from the download link (under Topic 1), or you can download the latest version from <https://filezilla-project.org>.
4. Install and explore Filezilla client. Use Filezilla to connect to your web-server2 as user “student00” to download the file "myfile" from student00's home directory.
5. Use Filezilla to connect to your web-server2a as the anonymous user with no password to download the file “file1” from the pub directory.

End of Practical