**Practical 1a : Network Protocols**

**Objectives:** Set up Kali and web-server2

Using Wireshark

Using Netstat, FTP, Telnet, SSH, SCP and SFTP

Set up Windows VM

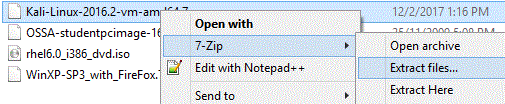
**Exercise Setting up your Kali Linux**

In this exercise, you will set up a Kali Linux virtual machine.

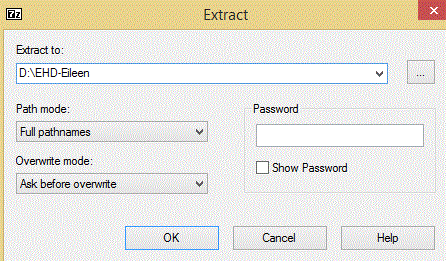
1. Login to the lab desktops.
2. Create a folder D:\EHD-yourname (eg D:\EHD-johntan). You can keep your EHD files in this folder.
3. Go to C:\BaseImages. Right-click on the kali-linux-2022.1-vmware-amd64.7z file and choose 7-Zip, Extract files.

You can also download the 2.5GB Kali Linux VMware machine from the following URL. (you will need to login with your SP iChat account) Or download the latest version from [www.kali.org](http://www.kali.org) using BitTorrent which would be faster.

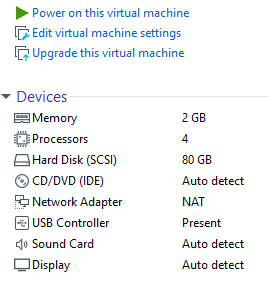
<https://ichatspedu-my.sharepoint.com/:f:/g/personal/eileen_yeo_ichat_sp_edu_sg/EtTRt10iic5MtZDOlnX6sMUBsuraEm2l7dPwPLDwtwLpyg>



1. Change the folder to where you want to keep your EHD virtual machines (see following diagram).



1. Click OK. The Kali virtual machine will be extracted.
2. When the extract is complete, go to your EHD folder. Open the Kali Linux VM using VMware Workstation.



Network Adapter is “NAT”

USB Controller is Present

1. Check that you have a USB Controller listed under Devices for your Win10 virtual machine (see image above).
2. If you do not have a USB Controller, do the following steps to add it :
3. Under Commands, click on Edit virtual machine settings.
4. Under Hardware, click the Add button at the bottom.
5. Select USB Controller and click Next. Click Finish. Click OK.

Adding a USB controller means you can access USB devices in your image.

1. Check that the Network Adapter is set to “NAT” or Network Address Translation (see image above).
2. If the Network Adapter is not set to “NAT”, do the following steps to add it :
   1. Under Commands, click on Edit virtual machine settings.
   2. Under Hardware, select Network Adapter.
   3. In the right-hand pane, select the radio button NAT. Click OK.

NAT networking means the virtual machine is in a private network on the Host PC.

1. Power on the Kali virtual machine. Select “I copied it” when asked,
2. When the boot menu appears, choose the default first item "Kali GNU Linux" and press Enter.
3. Login with username “kali” and password “kali”.
4. Right-click anywhere on the Kali desktop and choose Open Terminal.

You are now logged in as a normal user “kali”, who has limited access. In order to do admin tasks like installing new software, you need to use the sudo command.

1. As user kali, try to run “fdisk -l” to list out partition tables. You will not be successful as this command requires root permission.
2. Use the sudo command to run the “fdisk -l” command. Enter kali’s password when asked.

sudo fdisk -l

1. This time, the partitions will be listed.

**Exercise Using Kali Linux**

**Description :**

We will now explore more commands and settings on Kali.

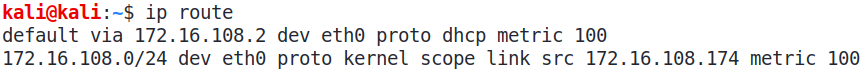
In Kali

1. To change the size of the VM screen, click on the Kali icon in the top left corner and choose Settings -> Display.
2. Choose your desired Screen Resolution. Click Apply.
3. To find out the Kali Linux version or the Kali Linux kernel version, run the following commands :

cat /etc/os-release

uname -a

1. In a terminal, type “ip addr” to view your IP address.
2. Type “ip route” to see the IP address of the gateway.



In this example, the gateway IP is 172.16.108.2

1. To see the DNS Server :

cat /etc/resolv.conf

1. To see a list of all the packages installed on your Kali Linux :

dpkg --list

You can use PageUp and PageDown keys to scroll through the list of installed packages. Press q to quit.

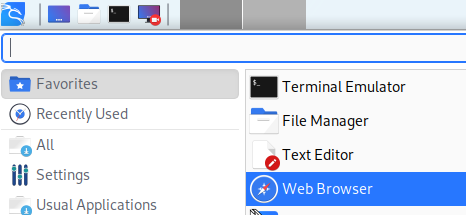
1. You can also use the apt command to view the list of all the packages installed on your Kali Linux :

apt list --installed

1. You can add the grep command for a quicker way to check if a certain package is already installed. For example, to see if the wireshark package is installed :

dpkg --list | grep wireshark

1. The web browser in Kali is Firefox and you can start it by clicking the Kali icon in the top left corner and selecting Favorites, Web Browser.

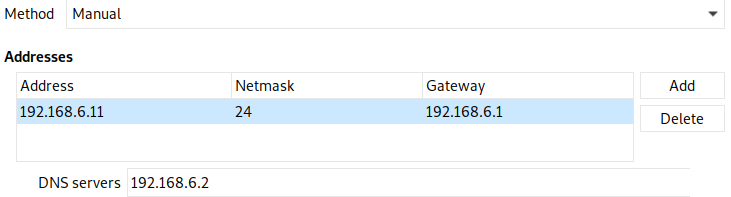


**Exercise Configuring network settings in Kali Linux**

In Kali Linux, Network Manager can be used to manage the network connections. The network interface device eth0, is connected to the Connection “Wired Connection 1”. By default it is using DHCP.

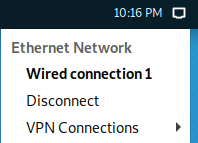
Configuring IP settings through the Network Manager GUI:

1. Click on the Kali icon in the top left corner and choose Settings -> Advanced Network Configuration. (or you can run the command nm-connection-editor)
2. Under Ethernet, double-click on Wired connection 1.
3. Click on the IPv4 settings tab.
4. You can select Automatic (DHCP) or Manual. If you pick Manual, you are setting a static IP address, and need to specify the Address, Netmask and Gateway.
5. If you are setting a static IP, under DNS, you can specify the DNS Server.



An example of setting a static IP address

1. To make any changes take effect, click on the Network icon in the top right corner and choose Disconnect.



1. Click on the Network icon and choose Wired connection 1 to activate it again.
2. You can also use the nmcli command (Network Manager Command Line Interface) to deactivate and activate the “Wired connection 1” for the changes to take effect.

nmcli connection down "Wired connection 1"

nmcli connection up "Wired connection 1"

Configuring IP Settings through the Network Manager configuration file

1. You can also make changes to the IP settings by modifying the config files. To configure “Wired connection 1”, edit the file “/etc/NetworkManager/system-connections/Wired connection 1” (remember sudo may be required) and change the section for ipv4 to the following static IP address

[ipv4]

method=manual

Change this to the gateway.

address1=172.16.108.191/24,172.16.108.2

Change this to the IP address and subnet mask you want to set.

1. Run the following command to get Network Manager to reload the changes you made to the config file.

sudo nmcli connection reload "Wired connection 1"

1. Down and up the “Wired connection 1”.

sudo nmcli connection down "Wired connection 1"

sudo nmcli connection up "Wired connection 1"

1. Use “ip addr” to view the new IP address.
2. To reset back “Wired connection 1” to use DHCP, edit the file “/etc/NetworkManager/system-connections/Wired connection 1” and change the section for ipv4 back to “auto” and remove the address and dns lines.

[ipv4]

method=auto

1. Reload, down and up “Wired connection 1”.

Configuring IP Settings through command line “ip addr”

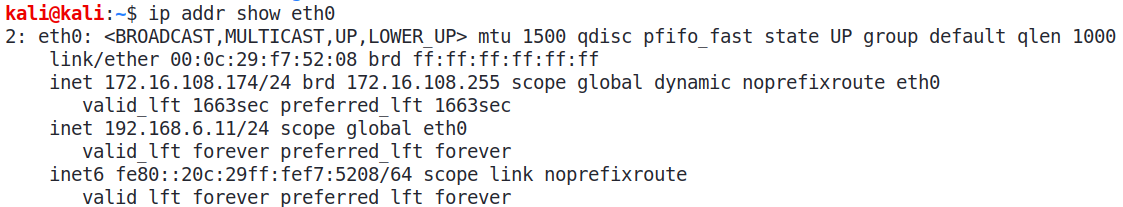
1. You can also make changes to the IP settings at the command line. Changes made using “ip addr” at the command line will be lost upon the next restart.

To add a new IP address for eth0 at the command line:

sudo ip addr add 192.168.6.11/24 dev eth0

Change this to the IP address and subnet mask you want to set.

1. Run “ip addr show eth0” to view the newly added IP address to the network interface eth0.



Original IP address for eth0

New IP address added for eth0

1. To delete the newly added IP address (change to the IP address and subnet mask that you added earlier):

sudo ip addr del 192.168.6.11/24 dev eth0

1. To reset back any changes, you can use the nmcli command to deactivate and activate the “Wired connection 1”.

nmcli connection down "Wired connection 1"

nmcli connection up "Wired connection 1"

**Exercise 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 OneDrive link:

<https://ichatspedu-my.sharepoint.com/:f:/g/personal/eileen_yeo_ichat_sp_edu_sg/EtTRt10iic5MtZDOlnX6sMUBsuraEm2l7dPwPLDwtwLpyg>

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.

**Exercise 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.

Change to the IP address of your web-server2

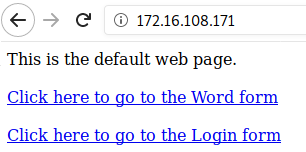
ping 172.16.108.171

ip ro

Press Control-C to stop the ping.

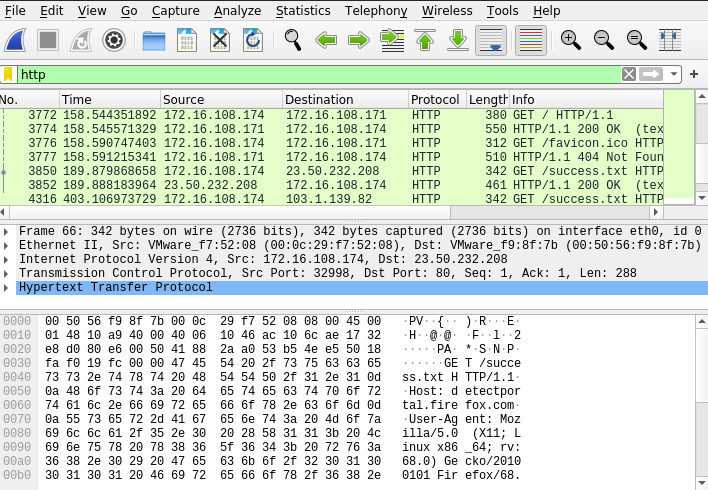
Mine : 192.168.126.128

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



Change to the IP address of your web-server2

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



Packet List :

List of captured packets

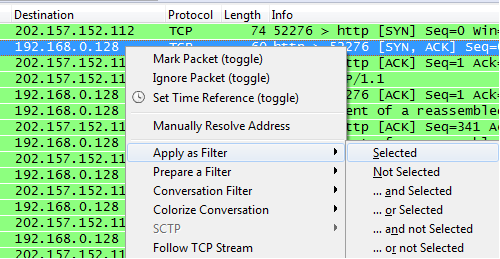
Packet Details :

The protocol details of a selected packet (using an expandable tree)

Packet Bytes :

The data bytes of the selected packet (in hexadecimal and in ASCII)

1. To view only the packets involved in the ping command, type “icmp” in the Filter textbox and press Enter. View the packets captured.
2. To view only the packets involved in the http command, type “http” in the Filter textbox and press Enter. View the packets captured.
3. 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.
4. 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.
5. You can also apply the filter by right-clicking on the data in column, and choose Apply as Filter, Selected. (see following diagram)



1. Clear the Filter box and press Enter.
2. 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)



1. 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).
2. Another way to search for strings is to type the following in the Filter textbox

frame contains login

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

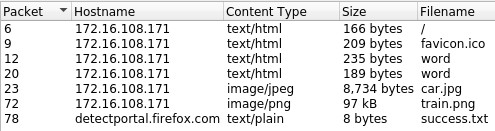
tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.initial\_rtt)

(rtt stands for round trip time)

Export Objects

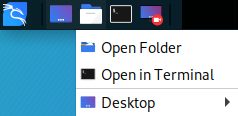
Wireshark can reassemble data like images and export them out as files.

1. Go to File menu and select Export Objects. Choose HTTP.
2. 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 and load the webpage again.)



The two pictures from the Word form

1. Select one of the pictures and click Save. Save the file to a directory on Kali (eg. You can save to /home/kali)
2. In Kali, click on the Explorer icon in the top left corner.



1. 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.

1. 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"

1. Right-click on the HTTP POST packet and select Follow -> TCP Stream.
2. The packets that belong to this TCP connection will be reassembled to form the HTTP request and HTTP response.



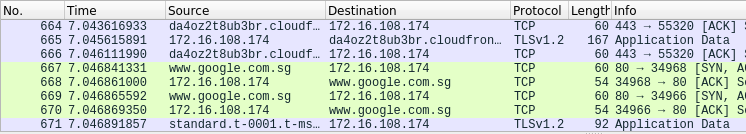
The blue part is the HTTP response sent by the web server.

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.

Name Resolution

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

1. In Wireshark, start capturing packets. You do not need to save the previous capture.
2. In the web browser, browse to a website, eg www.sp.edu.sg
3. After the webpage has loaded, stop the Wireshark capture.
4. In Wireshark, go to Edit menu and choose Preferences.
5. Select Name Resolution. Check the box “Resolve network (IP) addresses”.
6. Wireshark will display the hostnames. (see following diagram)



Public IP addresses are resolved to their hostnames

1. 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 OneDrive 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.

1. When did the user submit the form? Thu, 12 Apr 2012 11:06 am
2. What is the IP address of the user? 192.168.10.88
3. What is the MAC address of the user? 40:61:86:8b:59:e4 x
4. What word did this user enter? dinosaur
5. Identify the three packets that make up the 3-way handshake. Record the packet numbers below:

|  |  |
| --- | --- |
|  | Packet number |
| SYN packet | **9** |
| SYN/ACK packet | **10** |
| ACK packet | **14 x 11** |

(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.

Graphical user interface, text, website

Description automatically generated

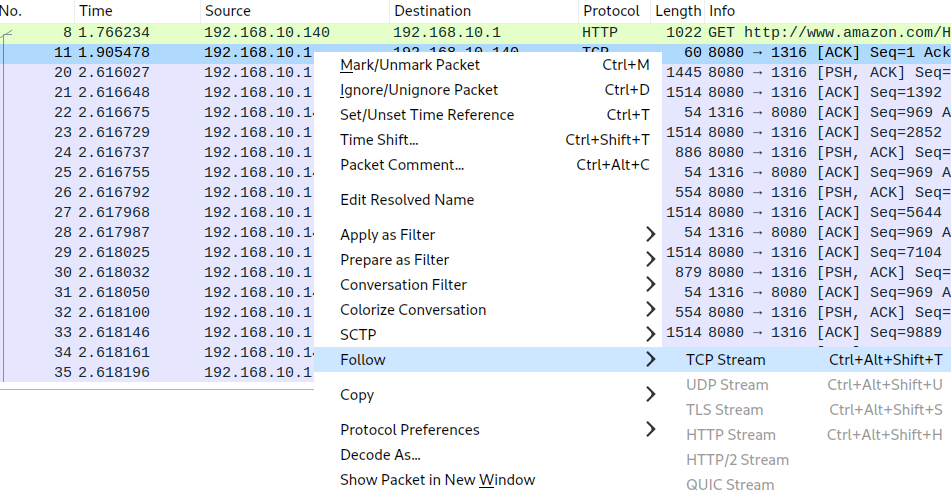
**He searched for Harry potter and the Chamber of secrets (book 2) on amazon.**

**He then added Harry potter and the Chamber of secrets (book 2) to his amazon cart.**

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.



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.



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

This is the HTTP response sent by www.amazon.com. Scroll down to see the contents of the returned web page.

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.



Download the http\_with\_jpegs cap 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 Identifying Open Ports in Linux - netstat (STOP HERE)**

**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 Connecting to the FTP Server**

FTP Server

(web-server2)

Client

Kali Linux

**Description:**

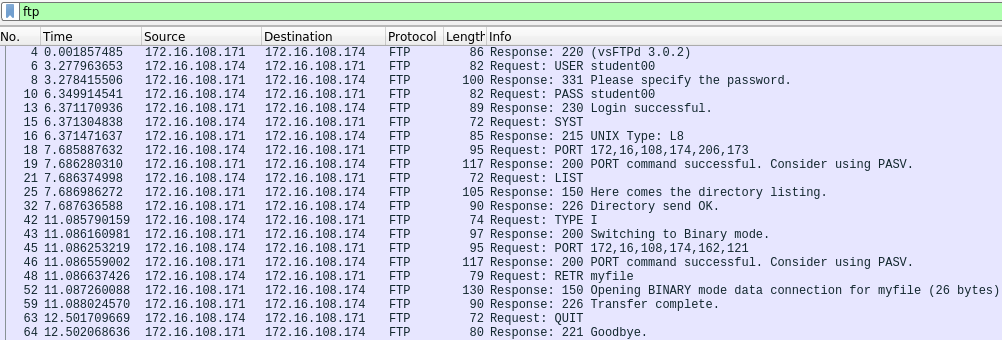
FTP (File Transfer Protocol) is used to upload or download files over the network. It has two types of TCP connections : control connection for the login, and data connection for the file upload/download. However, it is not a secured protocol (data is sent across the network in cleartext).

In Kali

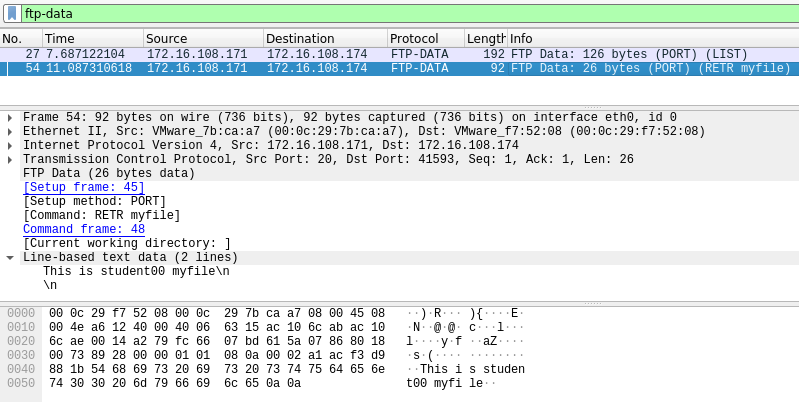
1. Run Wireshark and start capturing packets.
2. In a terminal, type “ftp *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
3. For User, enter “student00”.
4. For Password, enter “student00”. (you will not be able to see any characters appearing on screen as you type the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

You should see the file myfile listed.

1. To download myfile, type “get myfile”.
2. Type “bye” or “exit” to end the FTP connection.
3. Type “ls” to see the listing of the files in the current directory. You should see the myfile.
4. Type “cat myfile” to view the contents of the file.
5. Stop the Wireshark capture.
6. 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.
7. Type “ftp” in the Filter textbox. You will be able to see the username and password and the name of the downloaded file.



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

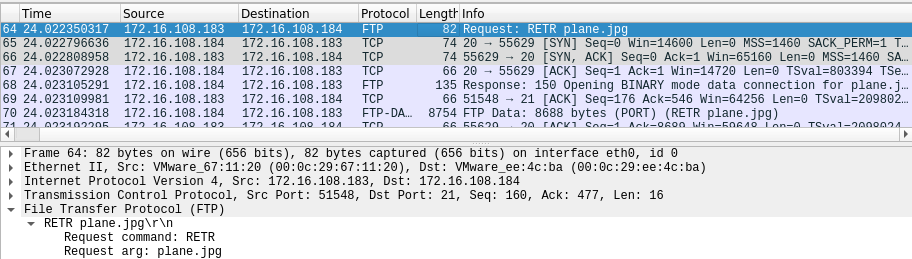


1. Clear the Filter. Right-click on any FTP packet and choose Follow -> TCP Stream. The FTP transaction will be displayed.

Anonymous FTP login

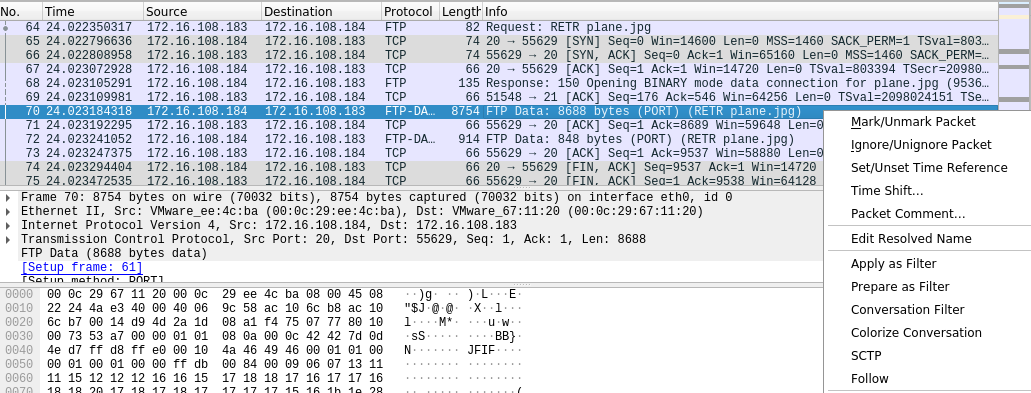
Many public FTP sites allow anonymous login. This allows anyone to connect to these public FTP servers without needing to authenticate, to view or download publicly available files.

1. Start a Wireshark capture.
2. In a terminal, type “ftp *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
3. For User, enter “anonymous”.
4. For Password, you can just press Enter.
5. 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.
6. Type “cd pub” to change to that directory.
7. Type “ls” to see the listing of the pub directory. You should see two files “file1” and “plane.jpg”.
8. Type “get file1” to download it.
9. Type “get plane.jpg” to download it.
10. Type “bye” to close the connection.
11. Stop the Wireshark capture.
12. As FTP has no encryption, you can see what files have been transferred from the packet capture.
13. 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.

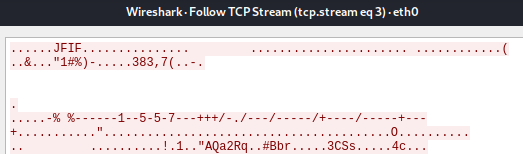


The FTP RETR packet requesting for plane.jpg

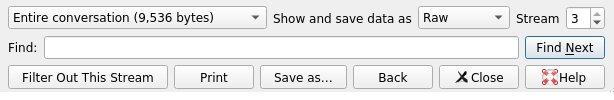
1. In Wireshark, look for the packet(s) containing the contents of plane.jpg. Right-click on any of them and choose Follow -> TCP Stream.



1. 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.



1. 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.



1. 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 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

1. Start the xinetd service if it is not already running.

systemctl start xinetd

1. 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"/>

1. Restart the firewall.

systemctl restart firewalld

1. Use Netstat to check that the Telnet Port 23 is opened.

netstat -tuna

In Kali VM

1. Start a Wireshark capture.
2. In a terminal, type “telnet *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
3. Login using the student00 account (password is student00).
4. 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.
5. Type “exit” to exit the Telnet session.
6. Stop the Wireshark capture.
7. In Wireshark, right-click on any of the TELNET packets and choose Follow -> TCP Stream.
8. 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:

1. Edit the file /etc/xinetd.d/telnet. Change the following line to disable telnet

disable = yes

**Exercise Using SSH, SFTP and SCP at command line**

SSH Server

(web-server2)

Client

Kali Linux

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

1. Run Wireshark to start capturing packets
2. Run “sftp student00@ *web-server2-IP*” where *web-server2-IP* is the IP Address of your web-server2.
3. Type “student00” for the password. Type “ls” to view the student’s home directory. Note that there is a file called “myfile”.
4. Type “get myfile” to download this file to your Kali Linux.
5. Type “exit” to close the connection.
6. View the contents of the downloaded file “myfile”. (You can type “cat myfile” to view the file contents)
7. 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”.

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

**Exercise Setting up a Windows virtual machine**

Set up a Windows virtual machine that can be used as a target client in future exercises.

1. Go to C:\BaseImages and copy the Win10 folder to your D:\EHD folder.

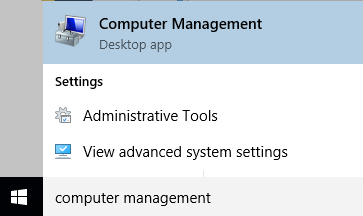
You can also download the Win10 virtual machine Win10.7z from the same OneDrive link:

1. Use VMware Workstation to open the Win10 virtual machine.
2. Check that the Network Adapter is set to “NAT”. Power on the Win10 virtual machine.
3. Login as user “admin” and password 1qwer$#@!
4. When the image has started up, you may want to install/update VMware Tools if it is not installed yet. Go to VM menu and choose Install VMware Tools or Update VMware Tools.

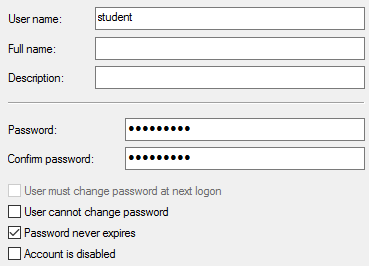
**Exercise Configure your Windows operating system**

Screen Resolution and User Accounts

1. To change the size of the VM screen, right-click on the background and choose “Display settings”. Click “Advanced display settings”.
2. Choose your desired Screen Resolution. Click Apply.
3. In the Cortana search textbox, search for “computer management”.
4. Click on Computer Management. (see following diagram)



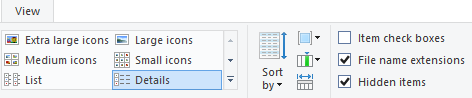
1. In Computer Management, expand Local Users and Groups.
2. Right-click on Users and choose New User.
3. Create a new user with username “student” and password “1qwer$#@!” (or you can set another password value).
4. Uncheck “User must change password at next logon”.
5. Check “Password never expires”. (Because this is for testing, we set the password to never expire. )



1. Click Create. Click Close.
2. Close the Computer Management window.

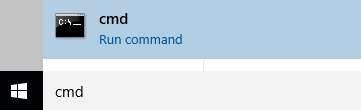
Do not hide extensions for known file types

1. In Windows Explorer, click on View menu.
2. Check the boxes for “File name extensions” and “Hidden items”.



IP address and Computer Name

1. In the Cortana search textbox, type “cmd” and select the cmd command (Command Prompt).



1. In the Command Prompt, type “ipconfig”. Take note of your IP address (under Local Area Connection).
2. If you want to change your computer name, do the following steps:
   1. In Windows Explorer, right-click on“This PC” and chooseProperties.
   2. Under Computer name, domain and workgroup settings, click “Change Settings”.
   3. Click on the Change button.
   4. Enter the new computer name. Click OK.
   5. You will be asked to restart your computer. Restart your VM for the new computer name to take effect.

**Exercise Install Wireshark for Windows**

In Win10 VM

1. Browse to www.wireshark.org or Brightspace or the OneDrive link (under Topic 1) and download and install Wireshark (64-bit version) with default options.

**Exercise 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

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



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

**Exercise Using PuTTY on Windows to connect to SSH Server**

**(STOP HERE)**

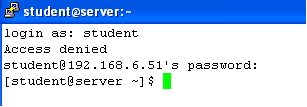
Putty can be used on Windows to connect to various servers, like SSH Server.

In Win10 VM

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



1. For the IP address, enter the web-server2 IP.
2. Check that Port is set to “22”. Click Open.
3. If you see a PuTTY Security Alert about the server’s host key, click **Yes** to trust the SSH Server.



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

*End of Practical*