Name:	Student #:	Group:

CSP Lab #2: Secure Network Communication

Required Resources:

- Kali Linux
- Internet connection

Learning Objectives:

Part 1: Using Telnet and SSH in the Linux terminal
Part 2: Capturing and analysing traffic using Wireshark. (50%)
Part 3: Using Tcpdump, Linux tools options, and man pages (30%)
Part 4: Secure web browsing, more Wireshark filters, driftnet.

Instructions

You are required to submit a written report of how you accomplished the tasks in this laboratory. The report should consist of a series of screen shots and a written account of your observations. The report must be submitted to Blackboard within a week of completing the laboratory session. Standard CIT penalties for late submission will apply.

Part 1: Using Telnet, SSH, and FTP

Telnet and Secure Shell (SSH) are protocols used for remote administration. Both protocols allow a user to log into a system with a username and passwords and run commands on that system or access a service hosted there. File Transfer Protocol (FTP) allows a user to upload/download (pull/push) files to and from a server.

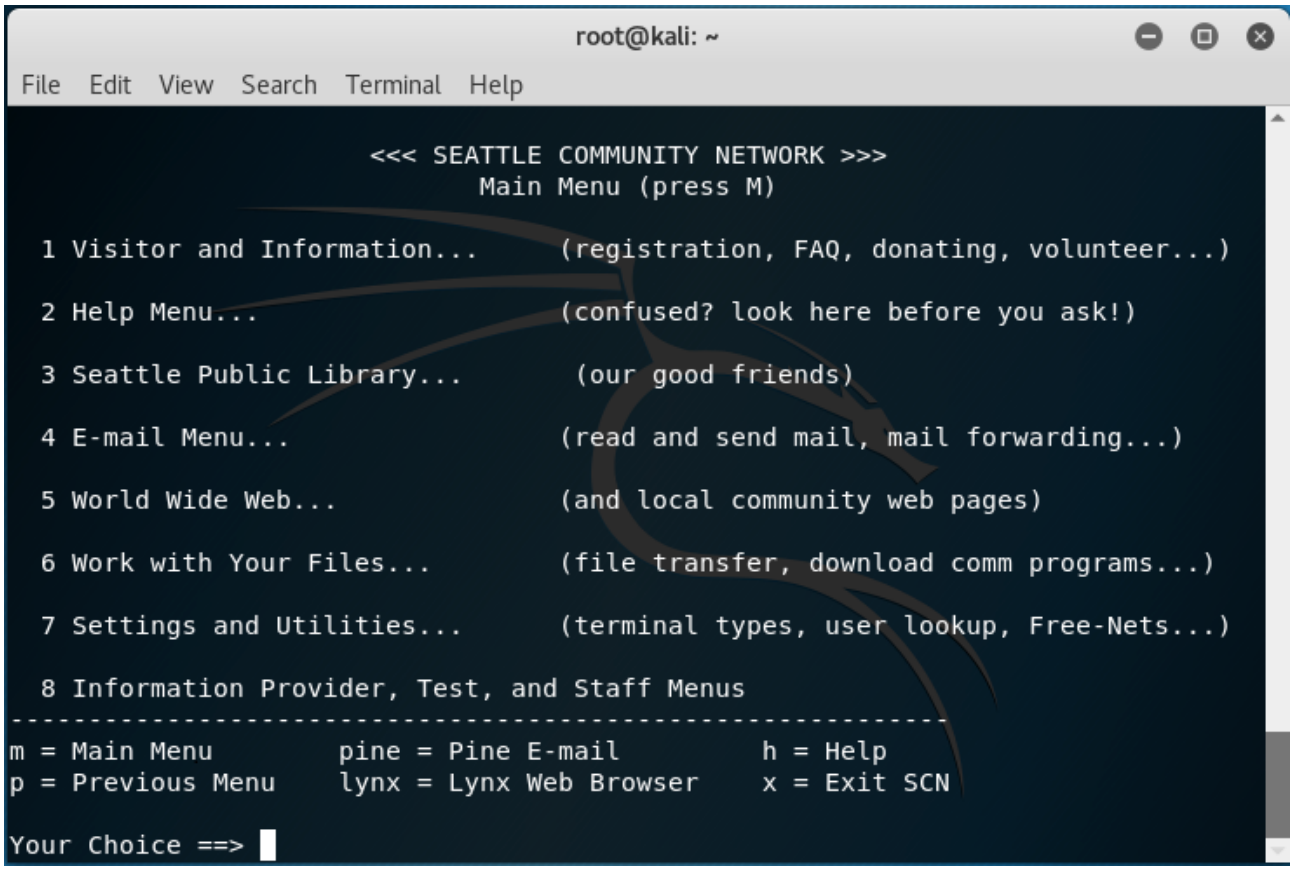
First, power on your Kali Linux machine/VM and log in (default credentials are “user: root, pass: toor”). Then open a terminal. The terminal application can usually be found under “Favorites” in the applications menu.

Telnet

A Telnet client is available by default on Kali Linux. The server you’ll be connecting to is designed to be a community hub for Seattle, USA. This server doesn’t let you run commands, but instead offers a menu driven application that supplies information for the local community. The following command launches the Telnet application and connects to port 23 on the server “scn.org”.
In the terminal type:

```
telnet scn.org
```

Use the username “visitor” to log in.
Follow the directions on-screen to reach the main menu and from there use “x” to exit.



SSH

Like Telnet, Kali has an SSH client available by default. For the SSH connection we’ll use a public SSH server. The following command will launch the SSH client, and connect to port 22 on the

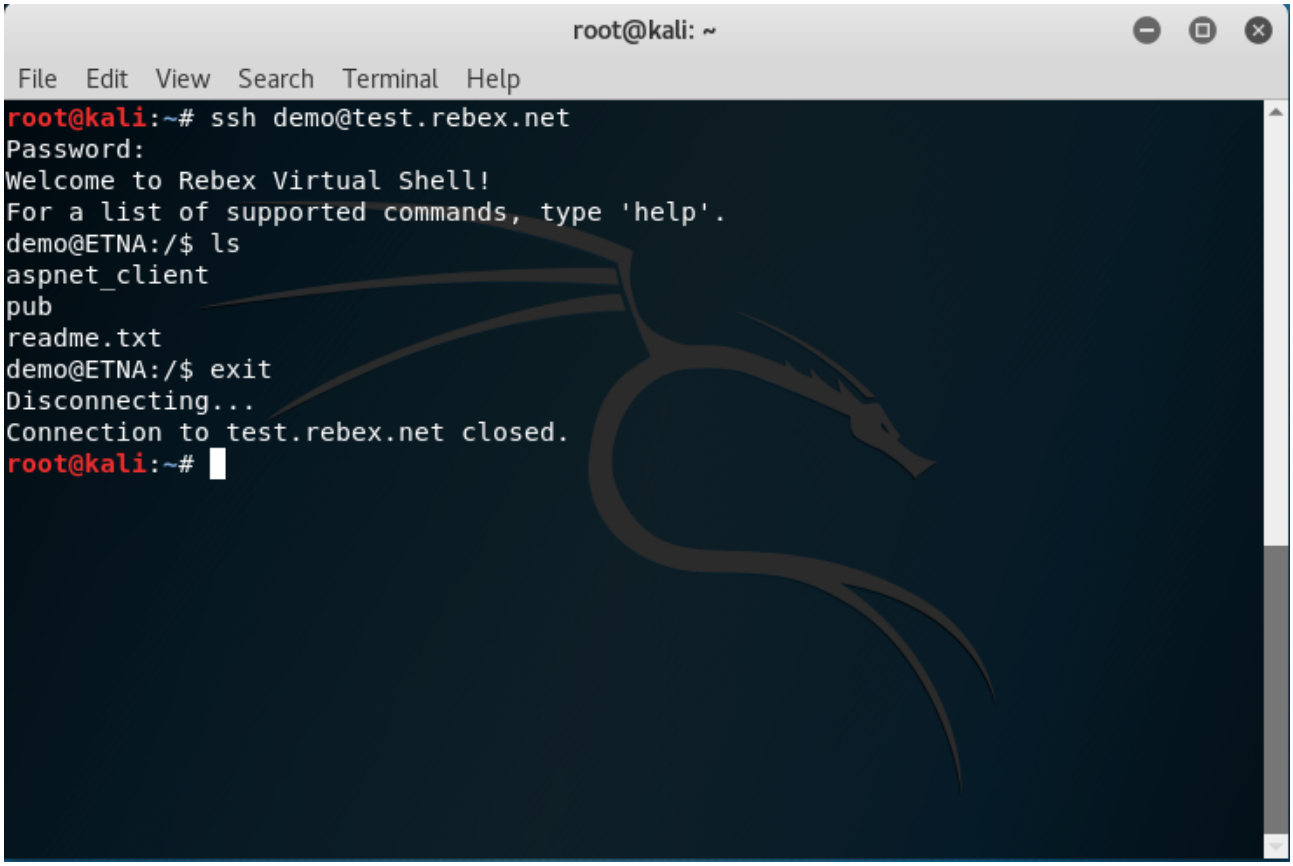
“test.rebex.net” server. The “demo@” pre-apended to the server name specifies the user we wish to log in as.

Note: If you are prompted to remember the remote host simply type “yes”.

```
ssh demo@test.rebex.net
```

Once connected you will be asked for a password. Use the password “password” to log in.

The server offers a limited number of commands which may be used. Type “ls” to list the directory contents. Type “exit” to disconnect.



Services such as the one seen with the Telnet connection can be offered over SSH (See the final section for links to public Telnet & SSH services). One important difference between Telnet and SSH is that traffic sent over Telnet is **unencrypted** while traffic send over SSH is encrypted. Furthermore, SSH clients and servers can be validated using certificates, making it very difficult for an attacked to impersonate a particular server.

Part 2: Capturing and analysing traffic using Wireshark (50%)

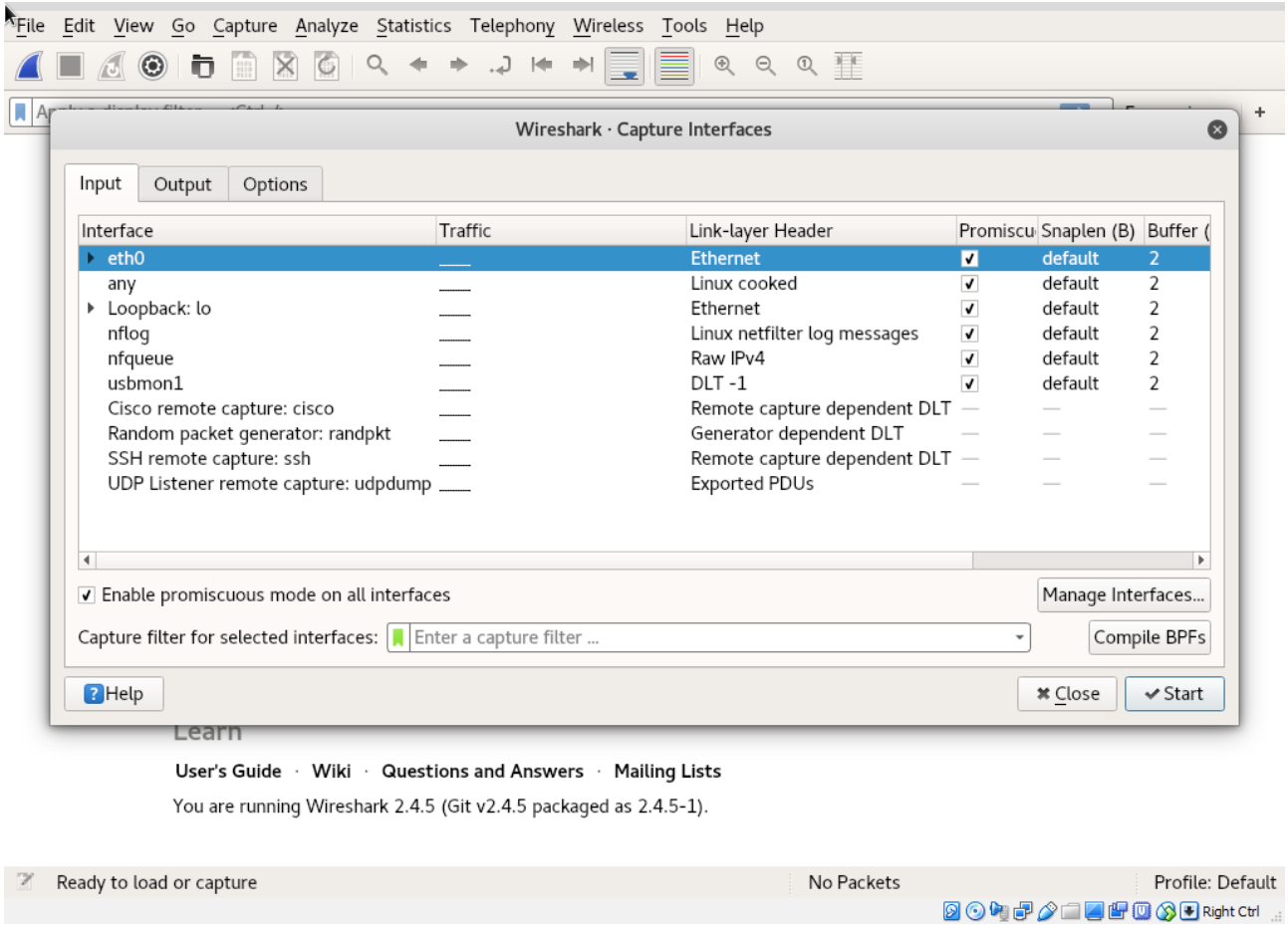
Wireshark is a tool used to capture and analyse network traffic. Using this tool, you will be able to see the difference between Telnet and SSH. This tool can be found under the “Sniffing & Spoofing” section of Kali’s applications menu.

Selecting an Interface

Before capturing traffic, you will have to specify the network interface you wish Wireshark to

capture traffic for.

To select an interface and start the traffic capture, navigate to “capture → options” on the main toolbar.



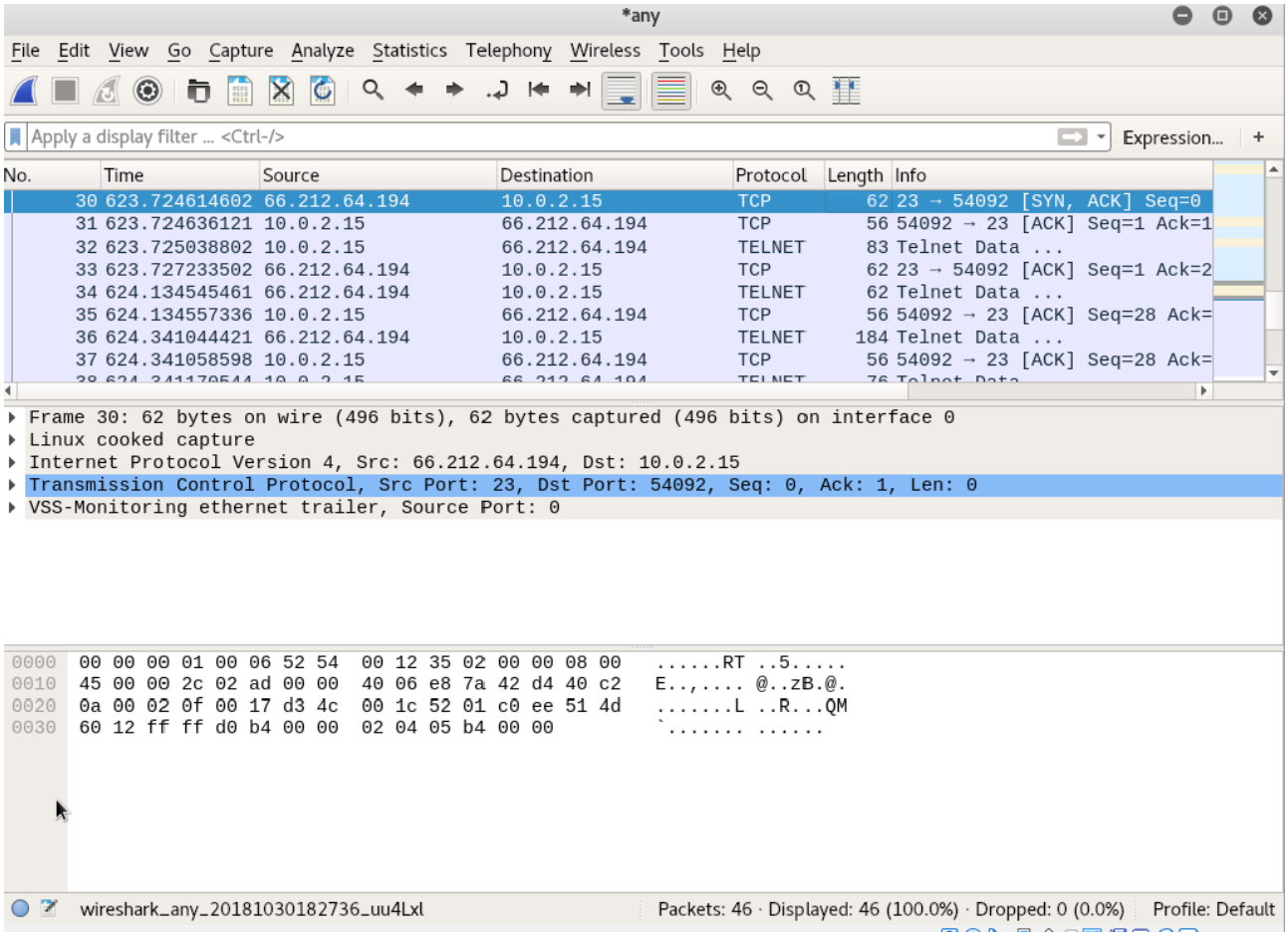
To simplify things for this lab you will capture traffic on all interfaces. To do this, just select “any” as the interface and click “Start” to continue. Wireshark is now capturing traffic.

Capturing Telnet and SSH Traffic

With Wireshark capturing traffic, repeat the steps in part 1. Once the steps have been completed, navigate to “capture → stop” in the main toolbar. Clicking on stop will stop the current packet capture. The packets Wireshark has captured will contain packets from both the Telnet and SSH connection.

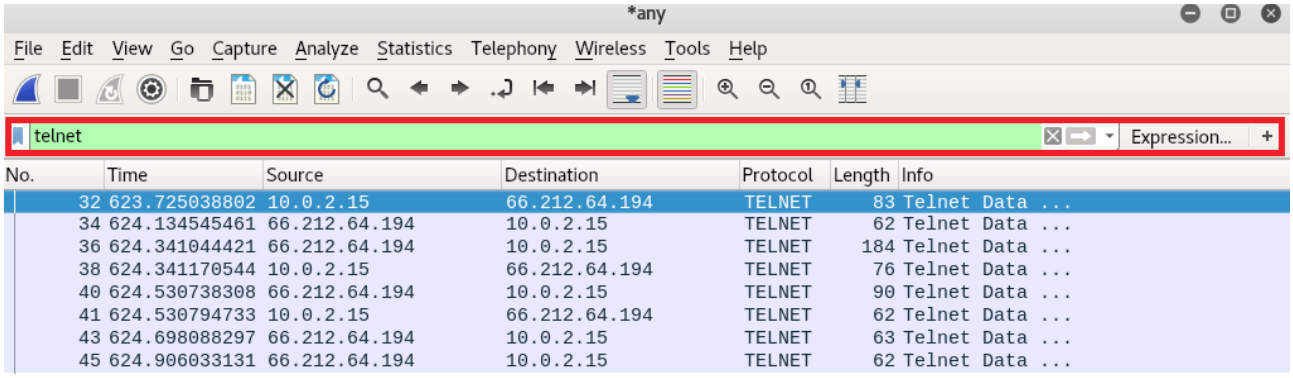
Viewing the Captured Traffic

The Wireshark window is divided into 3 rows, or panels. The topmost panel contains one-line synopsis of captured packets. The type of information seen here is source, destination, protocol, length, and a short snippet of information. The contents of this panel can be scrolled through and clicked on. Once a packet in this panel has been clicked and selected, the middle panel will display detailed information on each protocol included in the packet. The bottom panel will display the packet in hexadecimal and show the ASCII representation where possible.

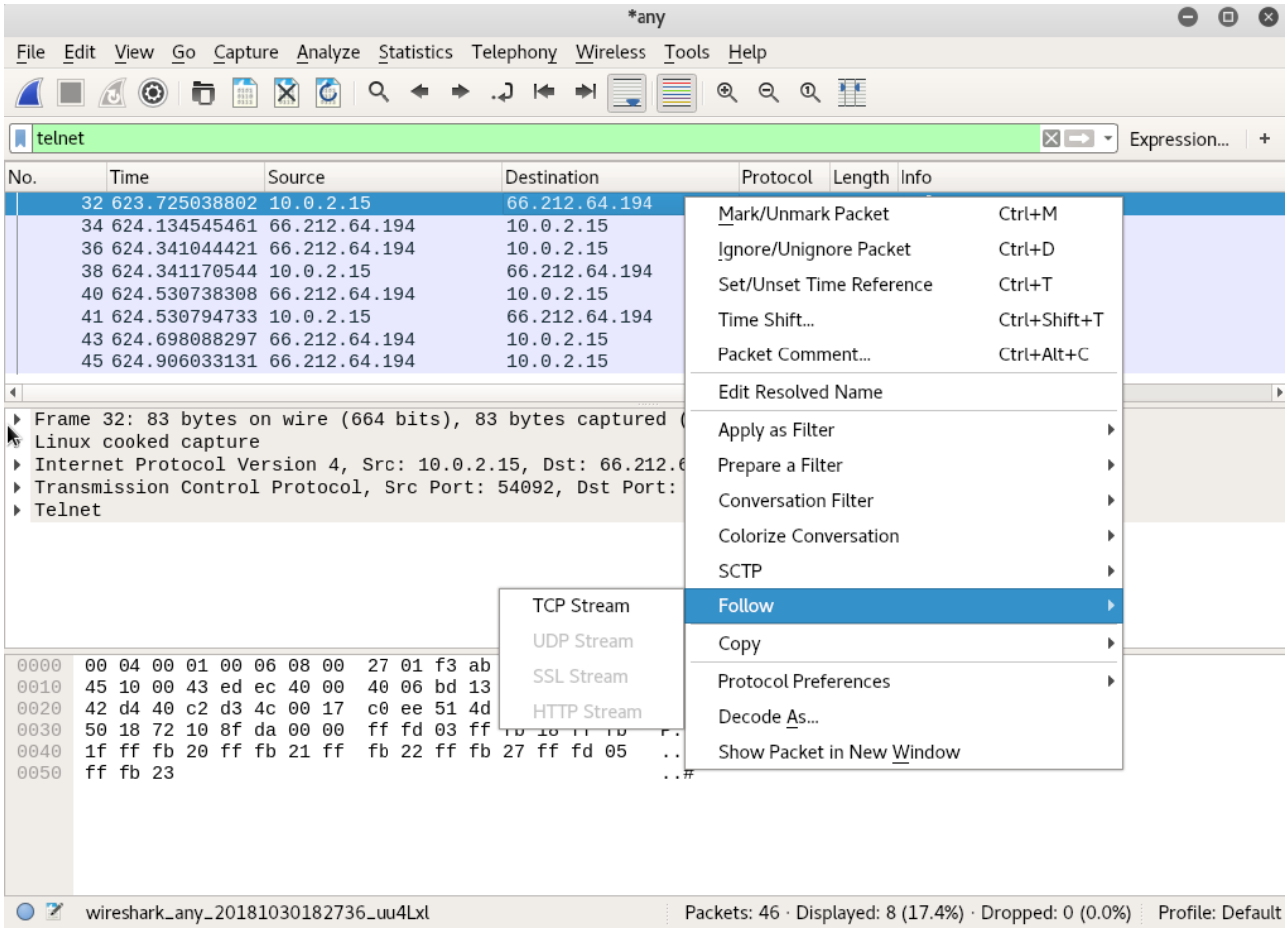


Filtering and Viewing Data

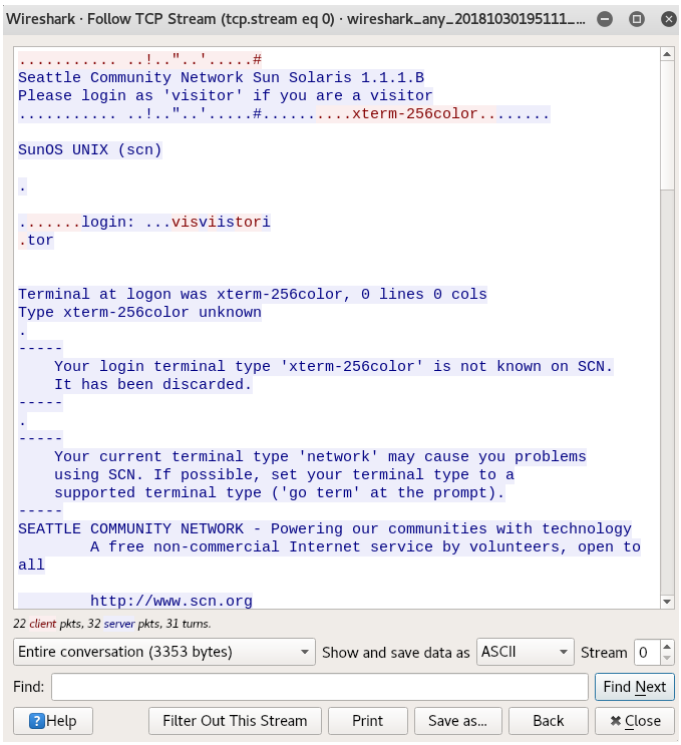
Wireshark allows filters to be used to help in analysing traffic. Filters can be typed into the bar just below the main toolbar. Typing in “telnet” will show traffic relevant to Telnet, and typing “ssh” will filter to only SSH traffic.



It’s also possible to filter to a specific conversation and view the data sent during that conversation. To do this, right click on one of the Telnet packets, navigate to “Follow”, and select “TCP Steam”.



Wireshark will display the data from the conversation in ASCII representation.



Perform the same action with the captured SSH traffic.

By clicking through the captured Telnet packets and observing the data displayed in the bottom panel, can you find the packet which contains the text from the scn.org application's main menu? Take a screenshot of this packet highlighted, and with the menu data showing in the bottom panel of Wireshark. Add this to your report.

Searching through the SSH traffic, can you find the packet which contained the directory content data? Add details of your answer to your report.

What is the main security issue you observe with the Telnet traffic? Add details (including screenshots) of this to your report.

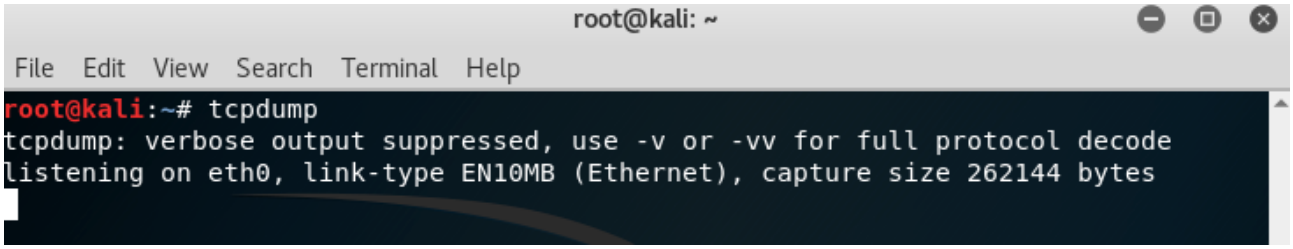
Part 3: Using Tcpdump (30%)

Another useful tool for capturing traffic is Tcpdump. This tool works in the terminal, and unlike Wireshark, doesn't require any desktop environment. This is useful in situations where you may have connected to a remote server using SSH and want to capture traffic.

Running Tcpdump
Open a terminal window and use the following command to launch Tcpdump:

```
tcpdump
```

Tcpdump will launch and capture on interface "eth0" by default.



Flags, or options, can be passed to Tcpdump to allow things such as the interface to be specified. The available options can be seen by using "--help" after the tcpdump command like so:

```
tcpdump --help
```

A manual page is also available for Tcpdump, which can be access using the following command:

```
man tcpdump
```

Type "q" to quit.

Using the information from the help text and the man page, it can be seen that the "-i" option is used to specify the interface Tcpdump should capture on. The following command will tell Tcpdump to capture on the localhost interface:

```
tcpdump -i lo
```

Adding “icmp” to the end of the command will have Tcpdump filter for ICMP (ping) traffic.
Use Tcpdump to capture on the localhost interface, filter for pings, and print packets in ASCII representation (*Hint: this option can be found using the Tcpdump man page*). Add this command to your report and include an explanation of each option used.

In another terminal window, use the following command to send a ping:

```
ping -c 1 127.0.0.1
```

Using the output from Tcpdump, identify the payload (data) of the ping that you sent. Include a screenshot of this in your report.

Use Wireshark to capture the ping and take a screenshot of the ICMP payload.

Part 4: (Challenge) Secure Web Browsing (20%)

Using Wireshark, capture traffic between Kali and the following sites:
http://www.1112.net/lastpage.
https://www.warnerbros.com/

In part 2, the "telnet" filter was used to filter traffic in Wireshark. What filters could be used to distinguish between the connections to the two websites?
What difference can you observe between the two connections? Can you view the data from the web pages in Wireshark?

Kali has a tool called "driftnet" installed. Using http://www.cit.ie demonstrate how this tool can be used. Does this tool work for every website? If not, why not?

Document your answers to the above questions in your report. Use screenshots to support your answers.

Additional Resources:

Small collection of PCAP files, including packet captures from Malware:
https://www.netresec.com/?page=PcapFiles

More PCAP files:
https://wiki.wireshark.org/SampleCaptures

Watch Star Wars over Telnet (Yes, really)
towel.blinkenlights.nl

Other places to telnet
https://www.telnet.org/htm/places.htm
https://www.jumpjet.info/Offbeat-Internet/Public/TelNet/url.htm