Lab #4

Class: CECS 303 – Networks and Network Security
Instructor: Chris Samayoa
Due Date: March 7, 2022 by 9pm PST

Objective: Understand the basics of using a packet sniffing/capture tool and examine a packet capture from both unencrypted and encrypted network traffic.

Legend:

- *Server*: refers to the two Ubuntu Server VMs that were created in Lab 1
  - *Apache Server*: refers to the server VM with Apache installed on it
- *Workstation*: refers to the Ubuntu Desktop VM that was created in Lab 2

Links

- Download Wireshark: https://www.wireshark.org/download.html

Add iptables commands to allow protocols for labs

Add iptables commands to allow inbound traffic on both server VMs for the following protocols:

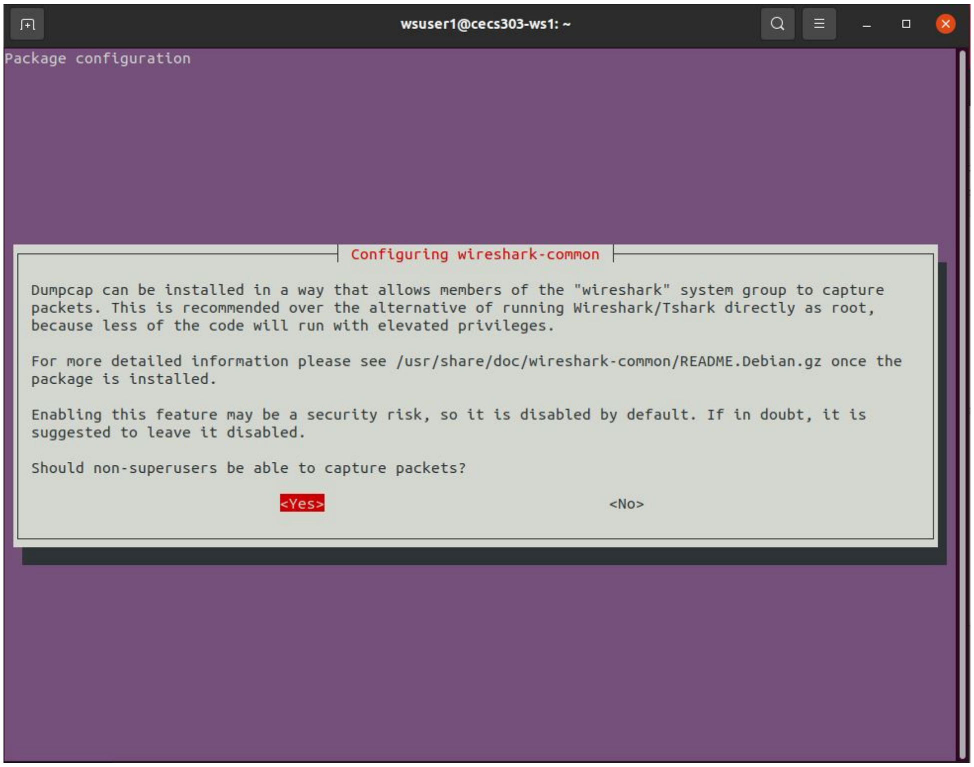
1. Telnet
2. SSH
3. Be sure to save your changes to the iptables on each machine ('sudo netfilter-persistent save')

Note: The Telnet Server service should already be running on both of your server VMs per Lab #2. If the Telnet Server service is not already installed, see lab #2 for installation instructions.

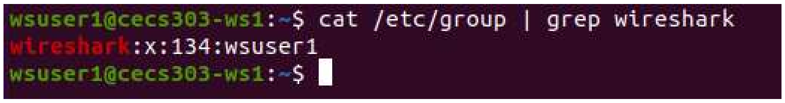
Install Wireshark

Since the virtual machines in this class were created with 'Bridged Adapters', you will not be able to directly analyze traffic from your host machine. Instead you will need to install Wireshark on the Ubuntu Workstation VM:

1. Install via command terminal
   a. Open a command terminal on your Ubuntu Desktop VM

   b. ‘sudo apt-get update’
   c. ‘sudo apt-get install wireshark’
      i. During installation, select ‘Yes’ when prompted with “Configuring wireshark-common”
      ii. 

```
Package configuration

                       ┤ Configuring wireshark-common ├

 Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture
 packets. This is recommended over the alternative of running Wireshark/Tshark directly as root,
 because less of the code will run with elevated privileges.

 For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.gz once the
 package is installed.

 Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is
 suggested to leave it disabled.

 Should non-superusers be able to capture packets?

                     <Yes>                                        <No>
```

2. Add your user account to the “wireshark” user group
   a. ‘sudo usermod -a -G wireshark <username>’ adds your username to the user group
   b. Verify that the change was successful by viewing the user group line for the “wireshark” group
      i. ‘cat /etc/group | grep wireshark’
      ii. 

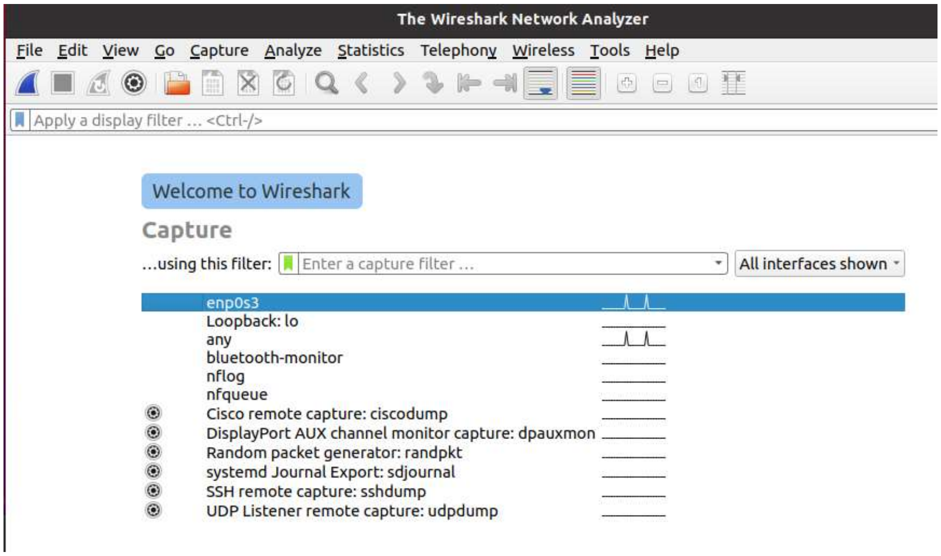
```
wsuser1@cecs303-ws1:~$ cat /etc/group | grep wireshark
wireshark:x:134:wsuser1
wsuser1@cecs303-ws1:~$ 
```

3. Restart the Ubuntu Workstation VM after modifying the group

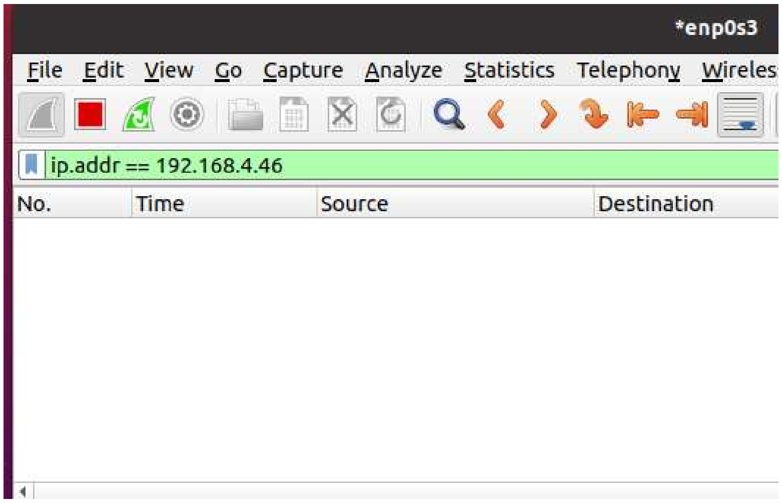
Capture Unencrypted Telnet Credentials

Telnet is a plain text network protocol. Because of this, credentials and other sensitive data can easily to “sniffed” using a packet capture.

1. Be sure that at least one of your server VMs are running
2. Open Wireshark on Ubuntu workstation VM

    a. Search for wireshark under your Ubuntu Workstation applications OR
    b. Open a command terminal and run command “wireshark”
3. Double-click on your network facing adapter (enp0s3)
    a. 
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown

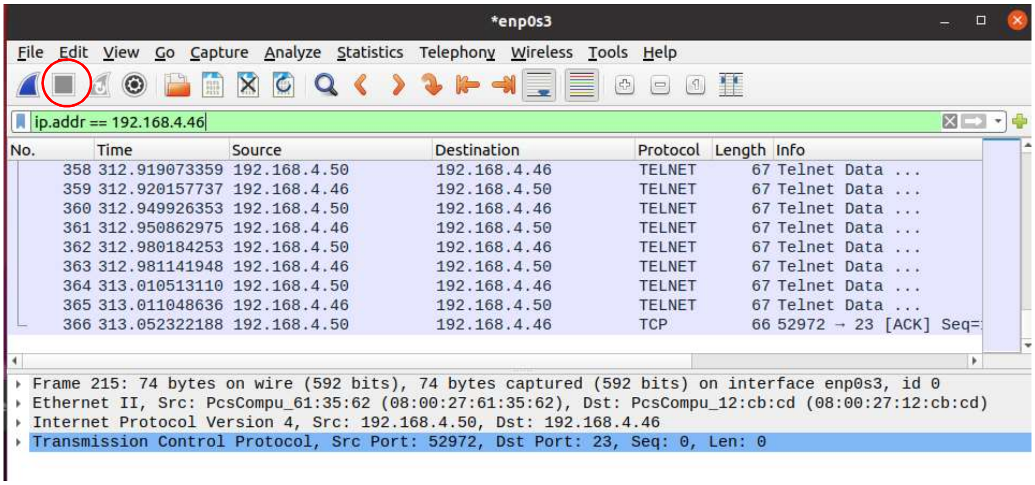
```
enp0s3
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

4. Apply filter to the server VM you will be connecting to
    a. Enter filter in filter bar: ‘ip.addr == <server ip adddress>’
        i. 
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireles
No. Time Source Destination

```
ip.addr == 192.168.4.46
```

    b. Leave Wireshark with filter running in the background
5. Telnet to one of your server VMs
    a. Open a command terminal from Ubuntu Workstation VM
    b. ‘telnet <server ip address>’ establishes a telnet session
        i. Enter your credentials
        ii. You should now have a remote terminal connection established to your server VM
6. Stop the Wireshark Packet capture

a. Click on stop button in upper menu bar

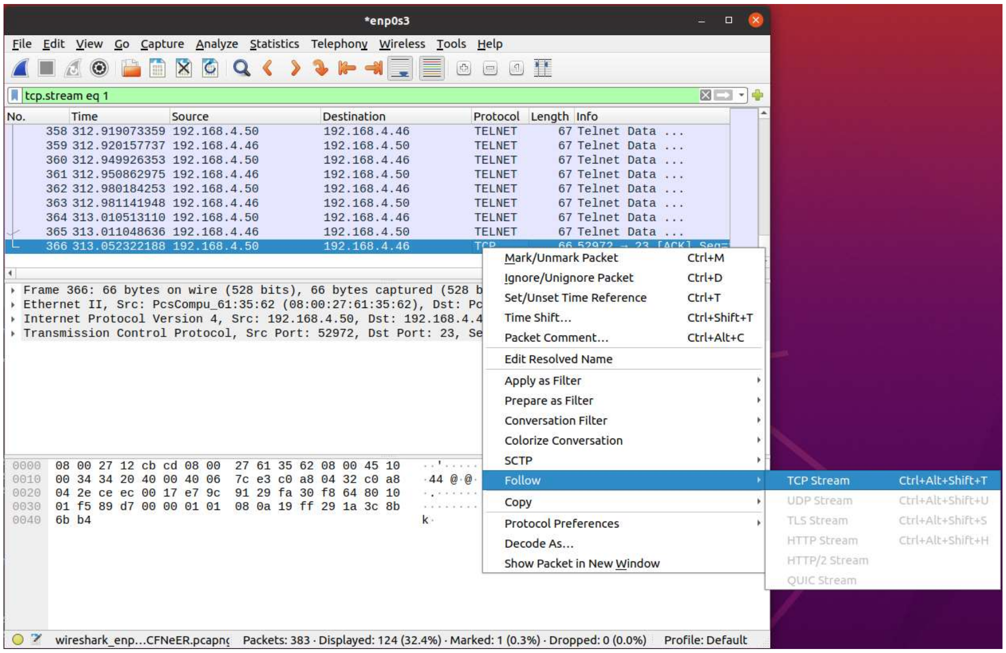
i. 
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.4.46

```
No.  Time          Source          Destination     Protocol Length Info
 358 312.919073359 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 359 312.920157737 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 360 312.949926353 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 361 312.950862975 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 362 312.980184253 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 363 312.981141948 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 364 313.010513110 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 365 313.011048636 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 366 313.052322188 192.168.4.50    192.168.4.46    TCP         66 52972 → 23 [ACK] Seq=
```

```
Frame 215: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_61:35:62 (08:00:27:61:35:62), Dst: PcsCompu_12:cb:cd (08:00:27:12:cb:cd)
Internet Protocol Version 4, Src: 192.168.4.50, Dst: 192.168.4.46
Transmission Control Protocol, Src Port: 52972, Dst Port: 23, Seq: 0, Len: 0
```

7. View the TCP Stream for the connection to your server VM (in the example below, the server VM IP address is 192.168.4.46)
    a. Rick click on any packet number that shows the destination IP of the server VM you established a telnet connection with
        i. Select Follow -> TCP Stream

ii. 
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream

tcp.stream eq 1

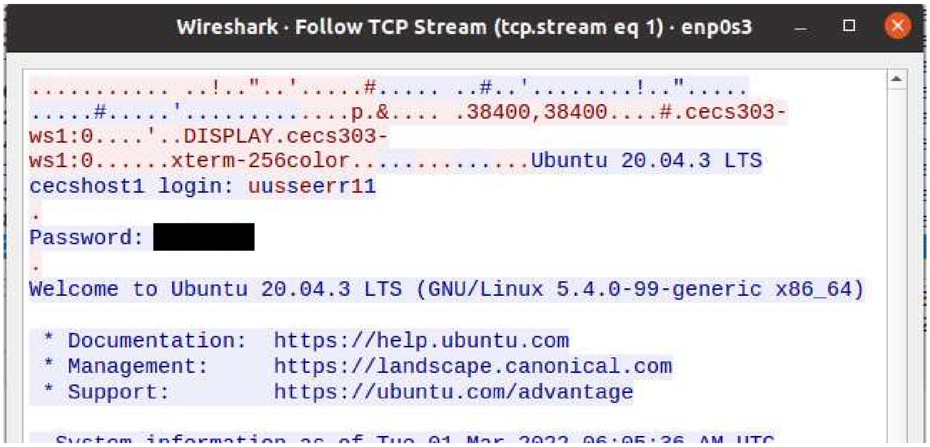
```
No.  Time          Source          Destination     Protocol Length Info
 358 312.919073359 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 359 312.920157737 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 360 312.949926353 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 361 312.950862975 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 362 312.980184253 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 363 312.981141948 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 364 313.010513110 192.168.4.50    192.168.4.46    TELNET      67 Telnet Data ...
 365 313.011048636 192.168.4.46    192.168.4.50    TELNET      67 Telnet Data ...
 366 313.052322188 192.168.4.50    192.168.4.46    TCP         66 52972 → 23 [ACK] Seq=
```

```
Frame 366: 66 bytes on wire (528 bits), 66 bytes captured (528 b
Ethernet II, Src: PcsCompu_61:35:62 (08:00:27:61:35:62), Dst: Pc
Internet Protocol Version 4, Src: 192.168.4.50, Dst: 192.168.4.4
Transmission Control Protocol, Src Port: 52972, Dst Port: 23, Se
```

```
0000  08 00 27 12 cb cd 08 00  27 61 35 62 08 00 45 10   ··'·····
0010  00 34 34 20 40 00 40 06  7c e3 c0 a8 04 32 c0 a8   ·44 @·@·
0020  04 2e ce ec 00 17 e7 9c  91 29 fa 30 f8 64 80 10   ·.······
0030  01 f5 89 d7 00 00 01 01  08 0a 19 ff 29 1a 3c 8b   ········
0040  6b b4                                              k·
```

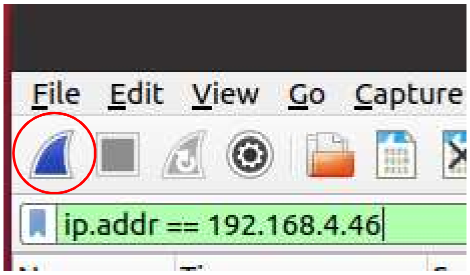
wireshark_enp...CFNeER.pcapng Packets: 383 · Displayed: 124 (32.4%) · Marked: 1 (0.3%) · Dropped: 0 (0.0%) Profile: Default

b. The details of the telnet connection will be visible in the TCP stream, including the credentials you entered

i. 

```
........... ..!.."..'.....#..... ..#..'........!..".....
.....#.....'.............p.&.... .38400,38400....#.cecs303-
ws1:0....'..DISPLAY.cecs303-
ws1:0......xterm-256color..............Ubuntu 20.04.3 LTS
cecshost1 login: uusseerr11
.
Password: [redacted]
.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-99-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 01 Mar 2022 06:05:36 AM UTC
```

1. *Screenshot the TCP Stream showing the credentials section (black out your password as shown above) for your submission*
2. Note that the characters of the username are shown twice (once in red and once in blue), this is because the server is echoing back the characters to the client as they are being entered
    a. Traffic from the client to the server is in red
    b. Traffic from the server to the client is in blue

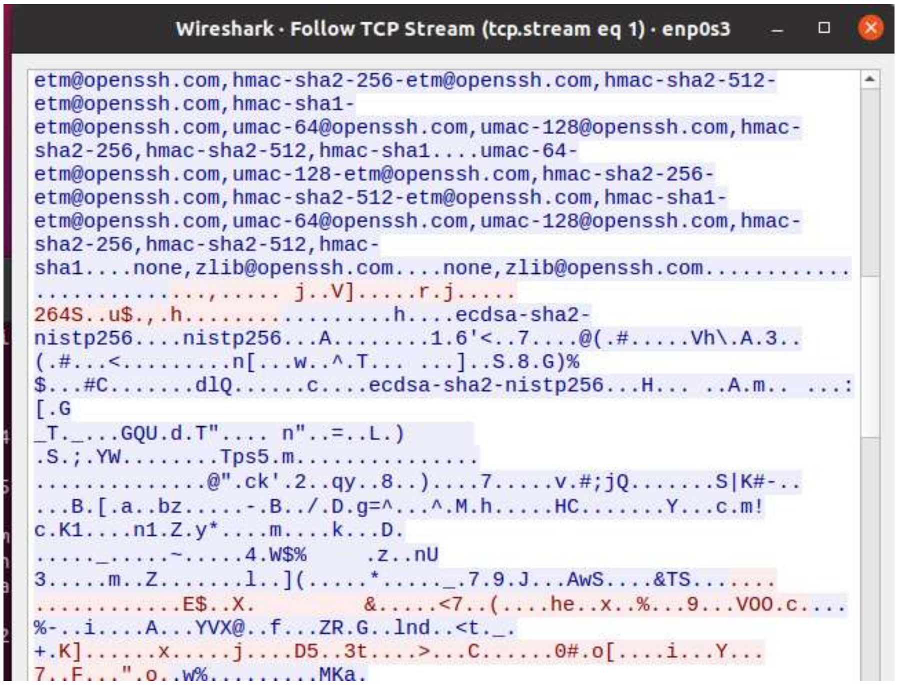
8. If you restart the packet capture in Wireshark and type in commands to the remotely connected server, you can repeat the above steps and see that all commands you enter via the telnet session are easily visible in a packet capture
    a. 

ip.addr == 192.168.4.46

9. Type ‘exit’ in the telnet session when you are done in order to close the connection

Capture an SSH Session

SSH is an encrypted network protocol, because of this it is not as easily monitored for credentials or other sensitive information.

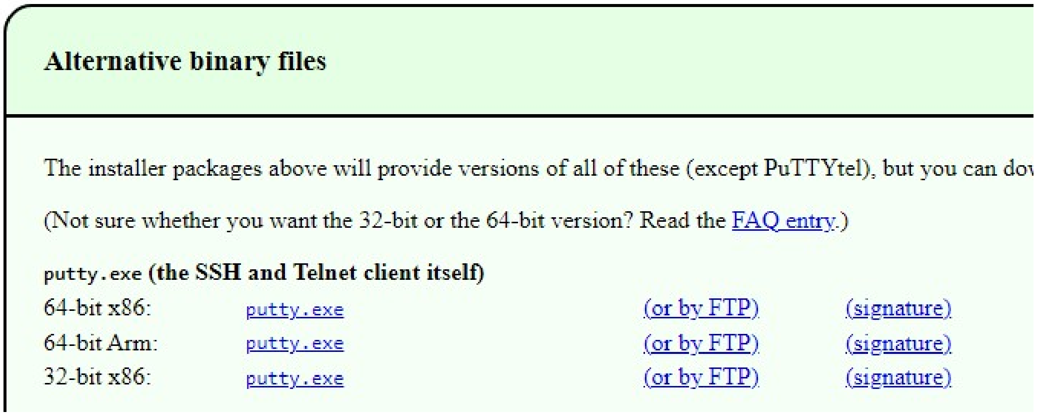
1. Start a new packet capture with the appropriate filter in place to monitor for traffic to the server VM you will be connecting to (same as before)
    a. Leave wireshark running in the background
2. SSH to your selected server VM
    a. Open a command terminal from Ubuntu Workstation VM
    b. 'ssh <username>@<server ip address>' establishes a telnet session
        i. e.g. ssh user1@192.168.4.46
        ii. Note that you need to specify the remote server's user in the ssh command. Otherwise, it will attempt to use your local user to connect (which will work if you created the same user on both machines).
3. Stop the Wireshark capture
4. Follow the TCP Stream for the connection as done previously
    a. You will note that first in the TCP stream, an encryption mechanism is negotiated
    b. Once the connection is established, all of the "sniffed" traffic is encrypted and illegible
        i. 

```
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256,hmac-sha2-512,hmac-sha1....umac-64-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256,hmac-sha2-512,hmac-
sha1....none,zlib@openssh.com....none,zlib@openssh.com...........
...............,..... j..V].....r.j.....
264S..u$.,.h.....................h....ecdsa-sha2-
nistp256....nistp256...A.........1.6'<..7....@(.#.....Vh\.A.3..
(.#...<.........n[...w..^.T... ...]..S.8.G)%
$...#C.......dlQ......c....ecdsa-sha2-nistp256...H... ..A.m.. ...:
[.G
_T._...GQU.d.T".... n"..=..L.)
.S.;.YW........Tps5.m...............
..............@".ck'.2..qy..8..)....7.....v.#;jQ.......S|K#-..
...B.[.a..bz.....-.B../.D.g=^...^.M.h.....HC.......Y...c.m!
c.K1....n1.Z.y*....m....k...D.
....._.....~.....4.W$%     .z..nU
3.....m..Z.......l..](.....*....._.7.9.J...AwS....&TS.......
............E$..X.          &.....<7..(....he..x..%...9...VOO.c....
%-..i....A...YVX@..f...ZR.G..lnd..<t._.
+.K]......x.....j....D5..3t....>...C......0#.o[....i...Y...
7..F...".o..w%.........MKa.
```

            1. *Screenshot a sample of this encrypted TCP stream for your submission*
5. Type 'exit' in the ssh session when you are done in order to close the connection

Optional: Install and use SSH client to connect from your host machine to your VM servers

You may have noticed that the VirtualBox VM windows are often inconvenient to use (especially for the servers). If you configured your VMs using bridged adapters, you can remotely connect to your server VMs using a simple SSH client such as Putty.exe; this will allow you to scroll up and down in a terminal window and scale the terminal window size. NOTE: If you're using a Mac or Linux machine as your host, then you do not need a separate client. You can natively ssh to your server VMs from a command terminal.

1. Download putty.exe: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
    a. I typically just download the executable and run it as a stand-alone application
    b. 

       Alternative binary files

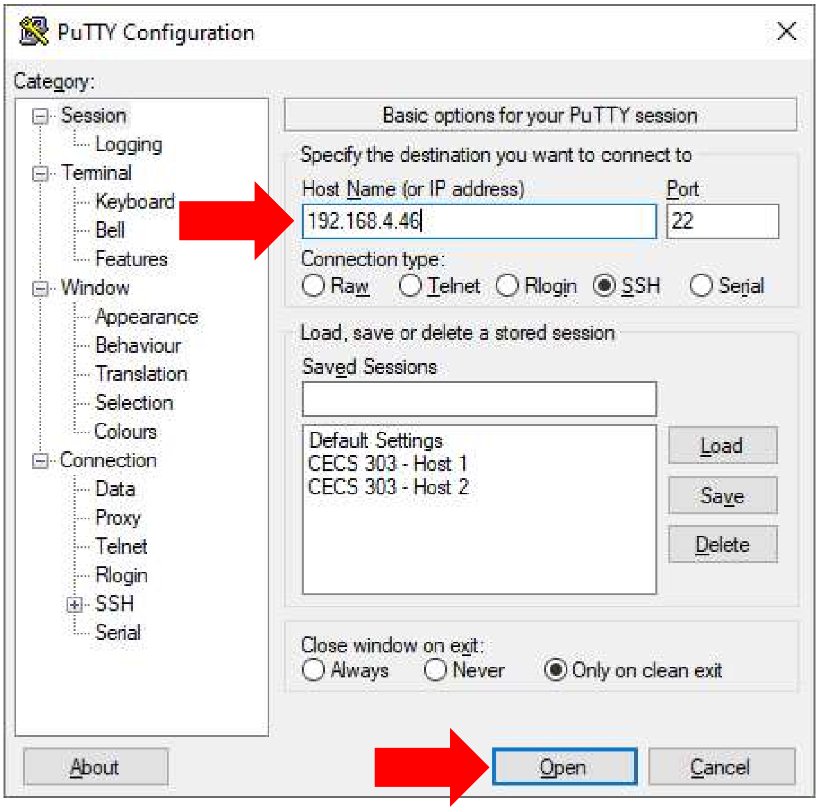
       The installer packages above will provide versions of all of these (except PuTTYtel), but you can do

       (Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

       `putty.exe` **(the SSH and Telnet client itself)**

64-bit x86:	putty.exe	(or by FTP)	(signature)
64-bit Arm:	putty.exe	(or by FTP)	(signature)
32-bit x86:	putty.exe	(or by FTP)	(signature)
2. Once putty.exe is downloaded, double-click the file to open a new session
3. Enter the IP address of your server VM in the "Host Name (or IP Address)" section and select "Open"
    a. After you enter your credentials, you will be remotely connected
    b. You can also save the session if you would like, but remember that your server IP addresses will change depending on what LAN you are connected to

c.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.4.46

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
CECS 303 - Host 1
CECS 303 - Host 2

Close window on exit: ○ Always ○ Never ● Only on clean exit

Deliverables (submit via BeachBoard)

1. Run the 'sudo iptables –L' command on one of your server VMs and take a screenshot of the output to show the allowed inbound telnet and ssh configuration.
    a. I suggest connecting using Putty.exe (or your host machine's other ssh client) to make the iptables easier to screenshot
2. Although the encrypted ssh connection makes it so that an attacker cannot easily capture credentials and other sensitive data within the session, what type of information can the attacker still collect by monitoring the traffic using a tool such as Wireshark?
3. Compile the three screenshots requested throughout the document in a single .doc, .docx, or .pdf file along with the answer to question #2 and submit via BeachBoard.

Note: Command "shutdown now" will cleanly shut down virtual machines when you are done working with them