

Lab 6. TCP

Lab Objective:

Learn how to recognize a TCP packet.

Lab Purpose:

TCP is the first part of the naming convention for the entire TCP/IP suite. It enables all connection-oriented services and protocols to run over networks such as Telnet, FTP, and some routing protocols, such as BGP.

Lab Tool:

Wireshark

Putty

Google

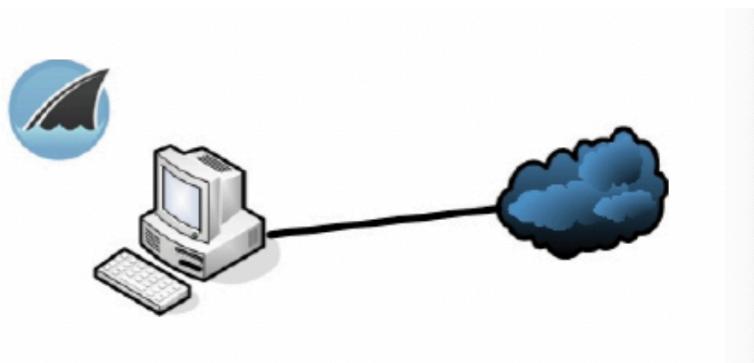
Lab Topology:

Run Wireshark.

Open Putty which is a Telnet/SSH client.

You can download Putty from <https://putty.org>.

It will make using Telnet much easier because most client software disables it by default.



Lab Walkthrough::

Task 1:

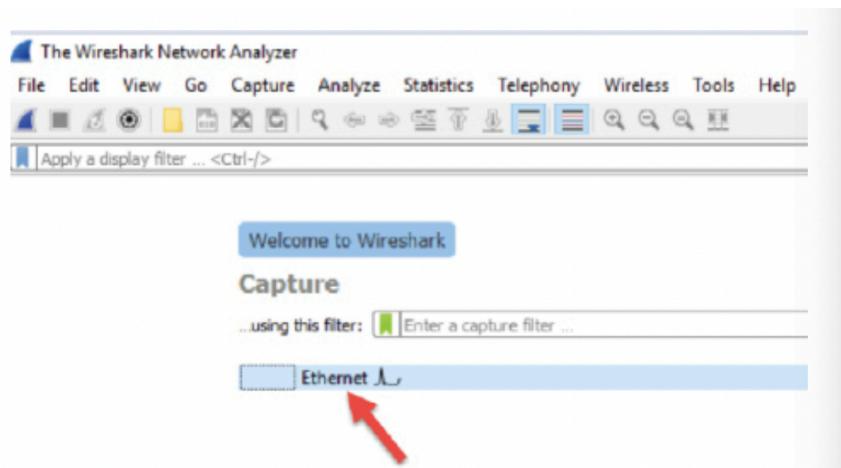
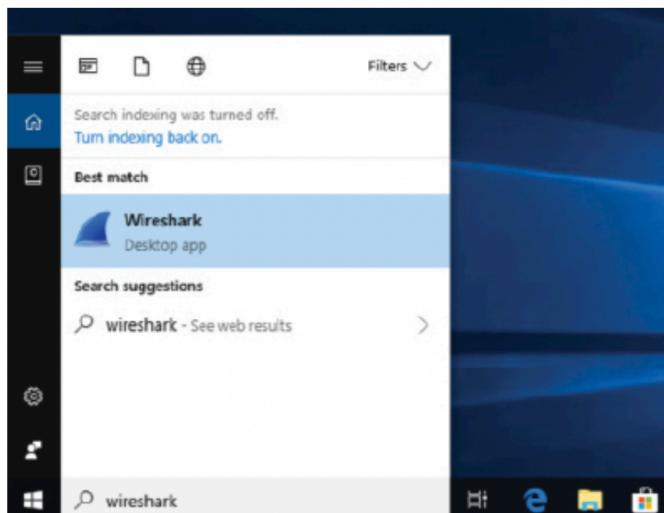
Install Putty onto your device.

Task 2:

You may find using Telnet to access other devices on your network a bit tricky, so I checked on Google for hosts that permit Telnet. I found <https://www.telnet.org/htm/places.htm> and tried some of the suggestions there. The list may change, so your first attempt may fail.

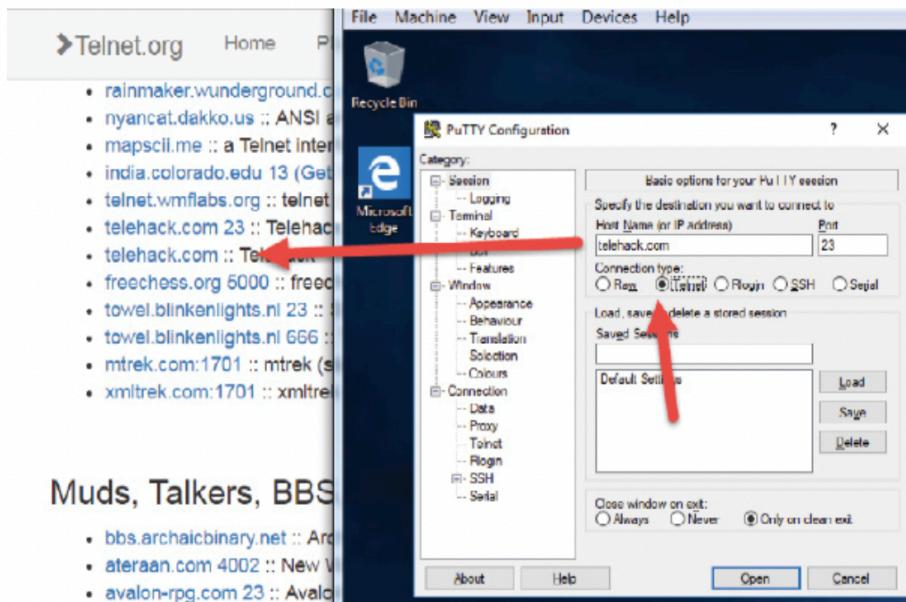
Task 3:

Boot Wireshark on your PC and check the correct interface is the one being monitored. Click on the interface name to open the capture window.



Task 4:

Open the Putty utility and enter the URL you wish to telnet to. I found that telehack.com worked well. You need to change from the default SSH to Telnet.



Task 5:

Your telnet session should work. Below is the window I was taken to for the Telehack website.

The screenshot shows a PuTTY terminal window titled "PuTTY (inactive)". The session has connected to "TELEHACK port 49". The output text includes the current time ("It is 5:49 pm on Sunday, September 9, 2018 in Mountain View, California, USA."), the number of local users ("There are 30 local users."), and network hosts ("There are 26637 hosts on the network."). It also provides command help ("Type HELP for a detailed command list.") and account creation instructions ("Type NEWUSER to create an account."). A message at the bottom reads "May the command line live forever." A large list of available commands follows, starting with 2048 and ending with zrun.

```
Connected to TELEHACK port 49

It is 5:49 pm on Sunday, September 9, 2018 in Mountain View, California, USA.
There are 30 local users. There are 26637 hosts on the network.

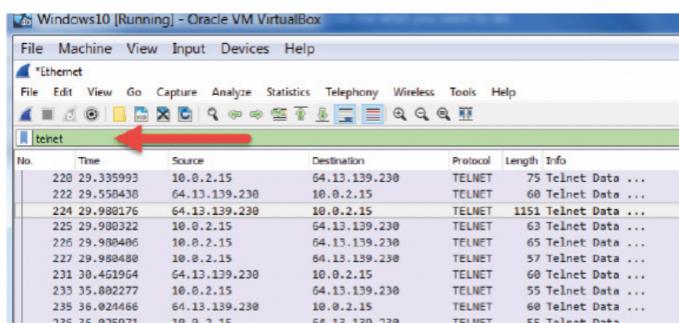
Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
 2048      ?          a2          ac          advent      basic
 bf        c8          cal         calc        ching       clear
 clock     cowsay      date        echo        eliza       factor
 figlet    finger      fnord      geoip       help        hosts
 ipaddr   joke        login      mac        md5        morse
 newuser  notes       octopus   phoon      pig        ping
 primes   privacy     qr         rain       rand       rfc
 rig      roll        rot13     sleep     starwars   traceroute
 units   uptime      usenet    users     uumap      uupath
 uuplot  weather     when      zc        zork      zrun
```

Task 6:

Go to Wireshark and in the filter box, type 'telnet' so you can see only the relevant traffic.



Task 7:

If you click on one of the packets, you can drill down to more detail. Please note that it says "TCP" which is what Telnet uses. Compare the fields to the image of the TCP packet below. See how many of the fields you can view.

You can see the source port is 23, which of course is Telnet. The bottom frame shows the actual text sent, which is in clear text, demonstrating the fact that there is no encryption involved.

Task 8:

You can use the below image as a reference to check the TCP fields

Task 9:

Lastly, note that Telnet does not encrypt the contents of the session, so you can easily see in the data stream what is being sent. This would include any passwords. You will find the actual data sent on the wire in the bottom windows of Wireshark.

```
PuTTY (inactive)

Connected to TELEHACK port 49

It is 5:49 pm on Sunday, September 9, 2018 in Mountain View, California, USA.
There are 30 local users. There are 26637 hosts on the network.

Type HELP for a detailed command list.
Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
 2048    ?      a2      ac      advent    basic
 bf      c8      cal     calc     ching     clear
 clock   cowsay   date    echo     eliza     factor
 figlet  finger   fnord   geoip    help     hosts
 ipaddr  joke     login   mac     md5     morse
 newuser notes   octopus phoon    pig     ping
 primes  privacy  qr     rain     rand     rfc
 rig     roll    rot13   sleep   starwars traceroute
 units   uptime  usenet  users   uumap   uupath
 uuplot  weather  when   xc     zork    zrun
```

02 0f 00 17 c2 9e 4a 07 2c 05 2e 3b 79 e3 50 18 ff ff e2 61 00 00 ff fb 01 ff fd 18 ff fd 1f 0d 0a 43 6f 6e 6e 65 63 74 65 64 20 74 6f 20 54 45 4c 45 48 41 43 4b 20 70 6f 72 74 20 34 39 0d 0a ff fe 20 ff fa 18 01 ff f0 ff fe 27 0d 0a 49 74 20 69 73 20 35 3a 34 39 20 70 6d 20 6f 6e 20 53 75 6e 64 61 79 2c 20 53 65 70 74 65 6d 62 65 72 20 39 2c 20 32 30 31 38 20 69 6e 20 4d 6f 75 6e 74 61 69 6e 20 56 69 65 77 2c 20 43 61 6c 69 66 6f 72 6e 69 61 2c 20 55 53 41 2e 0d 0a 54 68 65 72 65 20 61 72 65 20 33 30 20 6c 6f 63 61 6c 20 75 73 65 72 73 2e 20 54 68 65 72 65 20 61 72 65 20 32 36 36 33 37 20 68 6f 73 74 73 20 6f 6e 20J...,.jyP.a..... .Connect ed to TE LEHACK p ort 49..'..It is 5:49 pm on S unday, S eptember 9, 2018 in Moun tain Vie w, Calif ornia, U SA..The re are 3 0 local users. T here are 26637 h osts on
---	---