

TCP/UDP Ports and services in Linux

To see the list of well known ports and services supported by linux, type the command:

```
#less /etc/services
```

Question 1: (2 points): What protocol and port number does DNS (Domain Name System)?

How to Access your Email (POP3) using Telnet

The Internet protocol associated with email accounts is POP, or Post Office Protocol. POP is usually accessed on port 110 of your Internet provider's POP server. Now what you have to do is to start a telnet session type the following at the prompt.

```
#telnet 10.0.4.1 110
```

Now let's go through the following sample telnet session. You will get to know the commands and their usage as we progress. After you have connected to the POP server, a message similar to the below will appear. Let's continue from there.

```
+OK POP3 tauren [cpop 19.0].
```

USER username

Use your login name instead **username**.

```
+OK please send PASS command
```

PASS mypassword

Use your email password.

```
+OK 2 messages ready for manages in /usr/spool/mail/manages
```

Note: Unlike most times when you enter your password, this time you will see it as you enter it. Please make sure that no one is staring at your screen over your shoulders.

2. Write down the POP3 Commands needed.(1 point each)

a. Log in a POP3 server 10.0.4.1 using the student account.

LIST This will display the total number of messages and size again as well as a list with each file number, a space and its size.

b. List the number of messages in the server

RETR msg# - Displays the message number msg#, including headers. Display the second message, but do not write it down.

DELE msg# - Deletes the message number msg#. This is how you delete a message. Note the message will only be deleted once you quit the POP session.

c. Delete the 2nd email.

NOOP - The POP3 server does nothing. It just reply with a positive response. This is useful to determine if the connection with the server is still up.

RSET - This resets (unmarks) any messages previously marked for deletion in this session so that the QUIT command will not delete them.

d. Reset any messages previously marked for deletion.

STAT - This displays the number of messages and total size of the messages, in Octets.

TOP msg# n - Displays the first n lines of the message number msg#. Unlike the **retr** command, this will not scroll the message to the end. This is useful if you want to read the whole message.

LAST msg# n - Same as top but displays the last n lines of message number msg#.

QUIT - ends your session. Simply closing the telnet session may hang your mailbox.

e. Quit the POP3 Session.

How to Access a web page using Telnet

Hyper text transfer protocol (http) is a stateless protocol accessible in port 80. To access a web server without using a web browser, enter the following command and issue GET commands to acquire the web pages. (Note: GET command is case sensitive and requires two new lines before it can execute.)

HTTP Request methods:

GET - This gets a page/resource from a web server.

POST or PUT- More advanced request method

The GET request method also allows you to access pages that accepts parameters from forms by encoding the form parameters in the URL.

The following example allows you to search using Google from telnet.

```
#telnet www.google.com 80
```

```
GET /search?q=joseph+hermocilla
```

Copy the result of the telnet session and save it in a file **google.html**. Open this file in your web browser. What is your observation?

3. TODO (2 points): Access the following page in peak-two:

```
http://10.0.4.1/~cjsb/index.html
```

write the commands needed and write the result.

4. TODO (2 points) Using iptraf/ethereal, what port and protocol does the ping command use?

5. TODO (3 points) Knowing that HTTP is a stateless protocol, how does a web server support user sessions or stateful transactions? (3 possible answers) (I am not asking for a programming language but how does a server keep track of its users connected and anonymous users browsing? Hint: s_____, c_____, u_____)

Using tcpdump

Tcpdump is a console based packet sniffer. It will capture packets based on a filter provided. Note: if you add more than one filter be sure to add "and / or" between the two filters. If you plan to use a complex filter, you can group expressions by the use of () parentheses but make sure to enclose your whole expression by single quotes '.

src host x.x.x.x – Source IP Address, src port x -Source Port

dst host x.x.x.x – Destination IP Address, dst port x – Destination Port

To know any other option, you could try to run "man tcpdump"

Note: while using tcpdump, you might need root access so run it.



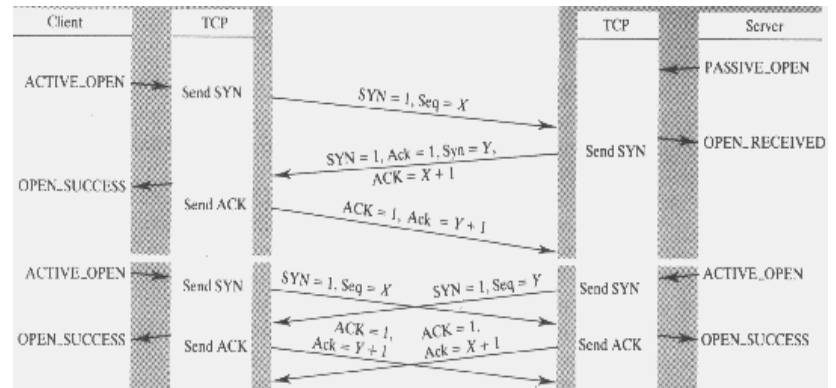
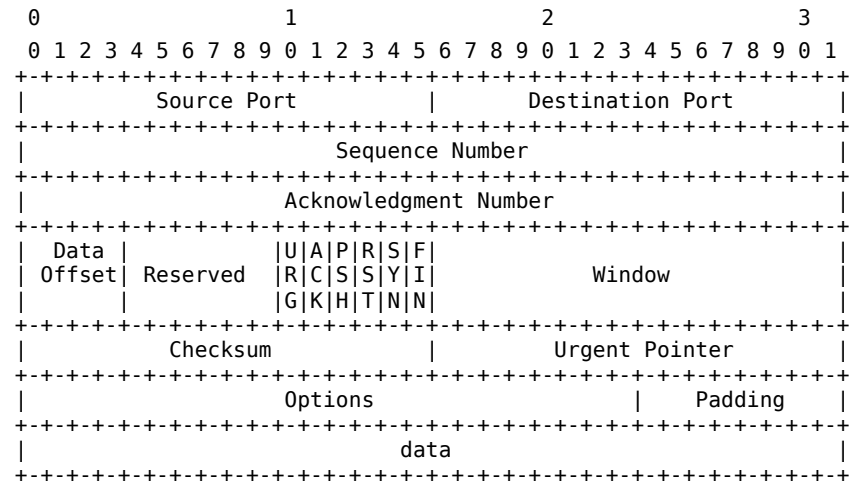
6. TODO(2 points): Using tcpdump what is the command to sniff all the traffic between the client and peaktwo only?

7. TODO(3 points): Get a copy of the tcpdump output of the three way handshake while the client is initiating a POP3 transaction. Write only the relevant information and also the tcpdump command used.

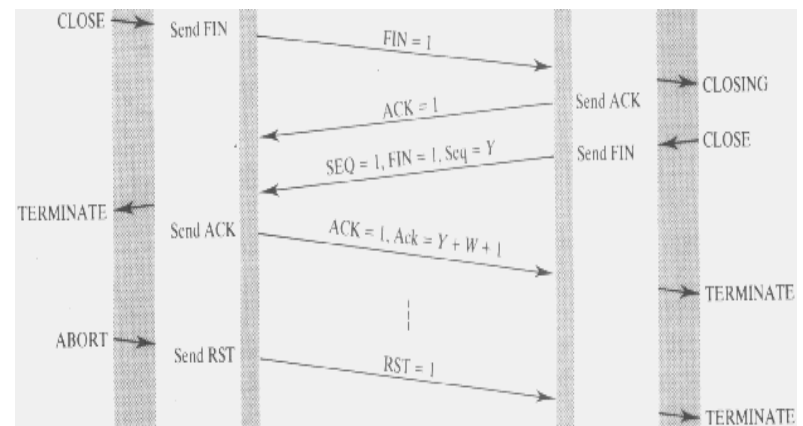
8. TODO(3 points): Get a copy of the tcpdump output of termination of the connection while the client is terminating the POP3 transaction. Write only relevant information and also the tcpdump command used.

9. TODO(5 points): Can you see the POP3 password inputted by the client? How can you prevent other users of your LAN or in the Internet from sniffing your packets containing sensitive data? (Example: passwords) (Hint: Refer to the OSI Layers)

TCP Header



Establishment



Termination