Telnet Lab Exercise

Raymond Ng: JQG999
IS 3033-CY1 – Summer 2022
July 6, 2022

1. **Determine the server IP address**

```
ubuntu@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:14:00:03
          inet addr:172.20.0.3  Bcast:172.20.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6609 (6.6 KB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Typed in `ifconfig` to view IP address of the server.

`Innet addr:` `172.20.0.3`

2. **Telnet to telnet server and display a file on the server**

```
ubuntu@server:~$ cat filetoview.txt
# Filename: filetoview.txt
#
# Description: This is a pre-created file for each student (telnet-server) container

# This file is modified when container is created
# The string below will be replaced with a keyed hash
My string is: 55a786db544f66870f9351b227f45824
```

To left is a screenshot of the contents inside `filetoview.txt`.

3. **View plaintext passwords**

```
14:14:17.172303 IP telnetlab.client.student.some_network.42552 > server.telnet: Flags [.], ack 131,
win 229, options [nop,nop,TS val 157948524 ecr 1004952296], length 0
        0x0000:  4510 0034 e2a7 4000 4006 ffde ac14 0002  E..4..@.@.......
        0x0010:  ac14 0003 a638 0017 aeec a677 08be 004b  .....8.....w...K
        0x0020:  8010 00e5 5854 0000 0101 080a 096a 1a6c  ....XT.......j.l
        0x0030:  3be6 5ae8                                ;.Z.
14:14:17.173144 IP server.telnet > telnetlab.client.student.some_network.42552: Flags [P.], seq 131:
145, ack 133, win 227, options [nop,nop,TS val 1004952297 ecr 157948524], length 14
        0x0000:  4510 0042 b867 4000 4006 2a11 ac14 0003  E..B.g@.@.*.....
        0x0010:  ac14 0002 0017 a638 08be 004b aeec a677  .......8...K...w
        0x0020:  8018 00e3 5862 0000 0101 080a 3be6 5ae9  ....Xb......;.Z.
        0x0030:  096a 1a6c 7365 7276 6572 206c 6f67 696e  .j.lserver.login
        0x0040:  3a20                                     :.
14:14:17.173178 IP telnetlab.client.student.some_network.42552 > server.telnet: Flags [.], ack 145,
win 229, options [nop,nop,TS val 157948525 ecr 1004952297], length 0
        0x0000:  4510 0034 e2a8 4000 4006 ffdd ac14 0002  E..4..@.@.......
        0x0010:  ac14 0003 a638 0017 aeec a677 08be 0059  .....8.....w...Y
        0x0020:  8010 00e5 5854 0000 0101 080a 096a 1a6d  ....XT.......j.m
        0x0030:  3be6 5ae9                                ;.Z.
```

After executing `sudo tcpdump -I eth0 -X tcp` on the server window and beginning a telnet session on the client computer, I noticed that anything I entered in the client computer would change the output depicting in the server window, depicting the TCP network traffic. Noticeably, when I entered the server login and password, after letter I typed I notice the letter depicting in every other packet with "`ack`".

4. **Use SSH to protect communications with the server**

```
14:30:48.030853 IP telnetlab.client.student.some_network.49390 > server.ssh: Flags [.], ack 3982, wi
n 290, options [nop,nop,TS val 158939364 ecr 1005943136], length 0
        0x0000:  4510 0034 1170 4000 4006 d116 ac14 0002  E..4.p@.@.......
        0x0010:  ac14 0003 c0ee 0016 d07a e723 678e 89d6  .........z.#g...
        0x0020:  8010 0122 5854 0000 0101 080a 0979 38e4  ...."XT.......y8.
        0x0030:  3bf5 7960                                ;.y`
14:30:48.030876 IP server.ssh > telnetlab.client.student.some_network.49390: Flags [P.], seq 3982:40
18, ack 3018, win 291, options [nop,nop,TS val 1005943136 ecr 158939364], length 36
        0x0000:  4510 0058 b065 4000 4006 31fd ac14 0003  E..X.e@.@.1.....
        0x0010:  ac14 0002 0016 c0ee 678e 89d6 d07a e723  ........g....z.#
        0x0020:  8018 0123 5878 0000 0101 080a 3bf5 7960  ...#Xx......;.y`
        0x0030:  0979 38e4 3638 97fd a2fd 82eb 508f 3e34  .y8.68......P.>4
        0x0040:  7ac1 1bfa ac92 eae4 fb0a e8a7 5372 3db4  z...........Sr=.
        0x0050:  4817 e759 2800 451f                      H..Y(.E.
14:30:48.033321 IP server.ssh > telnetlab.client.student.some_network.49390: Flags [P.], seq 4582:46
58, ack 3018, win 291, options [nop,nop,TS val 1005943139 ecr 158939365], length 76
        0x0000:  4510 0080 b06f 4000 4006 31cb ac14 0003  E....o@.@.1.....
        0x0010:  ac14 0002 0016 c0ee 678e 8c2e d07a e723  ........g....z.#
        0x0020:  8018 0123 58a0 0000 0101 080a 3bf5 7963  ...#X.......;.yc
        0x0030:  0979 38e5 cf32 e01e c7d3 47fd 198b be08  .y8..2....G.....
        0x0040:  d2b0 9b80 65dc 11bd 0c6d eb7d 2c1d e0f4  ....e....m.},....
        0x0050:  6d70 1470 5a0b 2169 9ea0 c372 3770 3f58  mp.pZ.!i...r7p?X
        0x0060:  3637 7363 3da6 5dd6 33cc cc6a 4deb 0434  67sc=.].3..jM..4
        0x0070:  c768 8056 bdad b122 57b0 c181 cf1b 6a15  .h.V...."W.....j.
14:30:48.033348 IP telnetlab.client.student.some_network.49390 > server.ssh: Flags [.], ack 4658, wi
```

I noticed that there was a difference in the `tcpdump` output via server window from when I used `telnet` versus Secure Shell (`ssh`). When using `telnet` I can see the data in plain text, but not in `ssh`. This is likely because `ssh` encrypts the data, probably making it the safer and more favorable option to use versus `telnet`.