Lab8: Data Hiding

Pre-Requisite Knowledge and Skills

1. Understand basic knowledge of Computer network.
2. Be able to use Linux.
3. Be able to run Application in Linux.

Learning Objective:

1. Understand Data Transfer Application.
2. Understand vulnerabilities in data communication.
3. Understand sniffing attack in data communication.
4. Explain countermeasures of sniffing attack in data communication.

Recommended Running Environment and Software:

1. Raspberry Pi with accessories
2. Wireshark
3. Multi-port switch or Wireless router

Instructional Material:

1. 2 Raspberry Pi
2. Instructions of this activity

Video Demonstration:

1. to be developed

Lab Assessment:

1. Exercises
2. Quiz

Lab Instructions

This lab requires two (2) Raspberry Pi, running Raspbian or Linux OS with Ethernet port or Wi-Fi adapter. You may need multi-port switch with Ethernet port or Wireless router with Wi-Fi adapter. Raspberry Pi requires Monitor, SD card, SD card reader, USB keyboard and mouse. Raspberry Pi is diskless computer and OS should be installed in SD card. You can use any size of SD card but 16GB or higher is recommended.

Download Raspbian OS IMG first from the link below.
https://www.raspberrypi.org/downloads/raspbian/

Now, SD card should be formatted and copy the IMG to SD card using SD card formatter. Simple insert the SD card to the reader and plug the reader into the PC. Then, open formatter application and format SD card as shown in Figure 1. Click the “Format” button and then, select “yes” to execute format command.

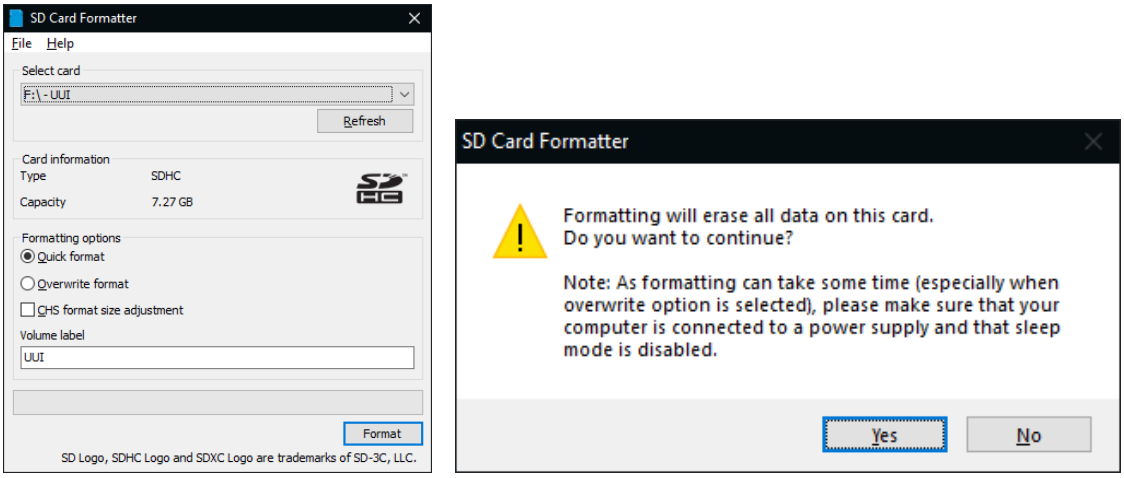


Figure 1. SD Card Formatter

Now, we need to copy OS IMG to SD card using application called “balenaEtcher”. Figure 2 shows the UI of application. First, select the IMG file, generally its extension is .iso, .zip, or .img. Select the IMG file and choose the SD card. Then, click “Flash” to upload the OS into SD card.

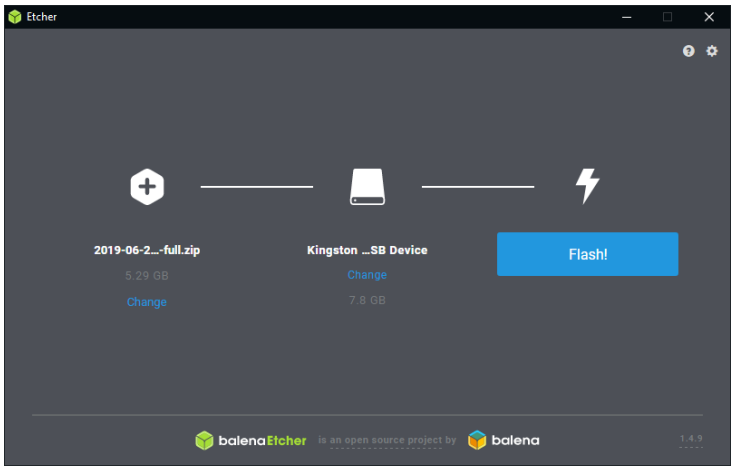


Figure 2. Copying IMG file to SD card

Insert SD card to the Raspberry Pi and it is ready to start. In order to run Raspberry Pi, one monitor and USB keyboard and mouse for each Raspberry Pi is recommended. However, you can switch them between two Raspberry Pi if you need.

Once Raspbian is running at the first time, it will ask to set the password for the user. Default login user should be set as “pi”. But you can create new user. Remember the user login ID and password. We need them for the rest of activities. Once log in the system, you will need to set up the network connection. Raspbian is based on Debian Linux OS and setting up network is similar to the Linux system. If you are familiar with Linux system, now set up the network. If not, please

watch and follow the Demo video. If Wireless router is used, you need to select correct Wi-Fi and IP address will be assigned automatically. If not, you will need to assign IP address and Subnet mask properly. Use following IP address and Subnet mask for both Raspberry Pi.

R-Pi 1: IP address: 192.168.10.5 Subnet mask: 255.255.255.0
R-Pi 2: IP address: 192.168.10.10 Subnet mask: 255.255.255.0

Raspbian may ask for the update if you are connected to Internet. If you want, you can update, but it is not necessary. If you choose to update, wait until it finishes the update and restart the system.

We will use two File Transfer Application, SSH (Secure Shell) and Telnet. SSH should be pre-installed while Telnet is not. Use following command to install Telnet.

<sudo apt-get install telnet> → client application
<sudo apt-get install telnetd> → server application

When you run above commands, you should see like Figure 3.

```
root@raspberrypi:/home/pi# apt-get install telnet
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libboost-system1.62.0 libboost-thread1.62.0 libreoffice-gtk2
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  telnet
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 60.7 kB of archives.
After this operation, 131 kB of additional disk space will be used.
Get:1 http://mirror.us.leaseweb.net/raspbian/raspbian buster/main armhf telnet armhf 0.17-41.2 [60.7 kB]
Fetched 60.7 kB in 1s (51.8 kB/s)
Selecting previously unselected package telnet.
(Reading database ... 135272 files and directories currently installed.)
Preparing to unpack .../telnet_0.17-41.2_armhf.deb ...
Unpacking telnet (0.17-41.2) ...
Setting up telnet (0.17-41.2) ...
update-alternatives: using /usr/bin/telnet.netkit to provide /usr/bin/telnet (telnet) in auto mode
Processing triggers for man-db (2.8.5-2) ...
pi@raspberrypi:~ $ sudo apt-get install telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  openbsd-inetd tcpd update-inetd
The following NEW packages will be installed:
  openbsd-inetd tcpd telnetd update-inetd
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 124 kB of archives.
After this operation, 334 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://raspbian.mirror.constant.com/raspbian buster/main armhf update-inet
d all 4.49 [27.8 kB]
Get:2 http://mirrors.syringanetworks.net/raspbian/raspbian buster/main armhf tcp
d armhf 7.6.q-28 [21.5 kB]
Get:3 http://mirrors.syringanetworks.net/raspbian/raspbian buster/main armhf ope
nbsd-inetd armhf 0.20160825-4 [34.3 kB]
Get:4 http://raspbian.mirror.constant.com/raspbian buster/main armhf telnetd arm
hf 0.17-41.2 [40.3 kB]
Fetched 124 kB in 2s (67.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package update-inetd.
```

Figure 3. Telnet installation

Install Telnet on both Raspberry Pi for the convenience. We will use one of powerful sniffing tool, called Wireshark. You need to install this application on only one Raspberry Pi, but you can install it on both. Use following command to install this application.

<sudo apt-get install wireshark>

Once the installation is completed, Wireshark can be open by typing “sudo wireshark” in the Terminal.

Now Raspberry Pi’s are ready to start this activity.

Scenario: Raspberry Pi 1 is a server and running Wireshark to monitor the network traffic. The other Raspberry Pi is a client for remote connection to the server using SSH and Telnet. Using this lab setup, we will perform one of “Man in the Middle attack”, Eavesdropping, as shown in Figure 4.

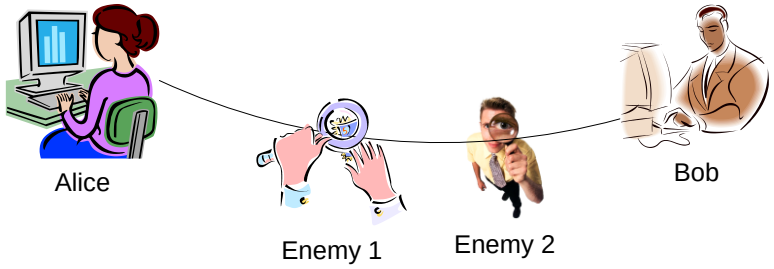
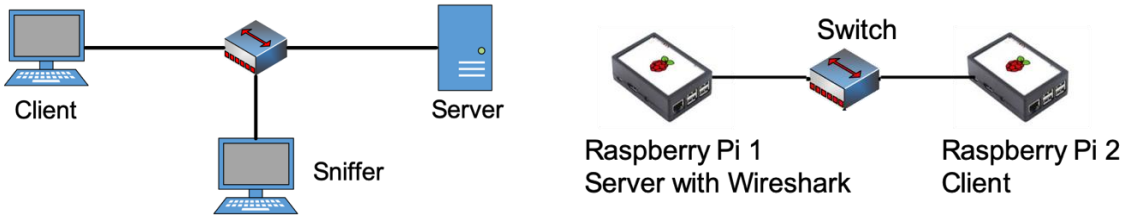


Figure 4. Eavesdropping – Man in the Middle attack

Figure 5 shows the real environment and our lab setup to emulate it.



(a) Real environment (b) Setup with Raspberry Pi

Figure 5. Lab setups

Step 1: Find the IP address of ***Server***. Type “ifconfig” in the Terminal to find the IP address. You will see something like in Figure 6.

```
its170@its170-virtual-machine:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:4d:e9:41
          inet addr:192.168.136.130  Bcast:192.168.136.255  Mask:255.255.255.0
          inet6 addr: fe80::38c4:8801:a3a0:e0fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1969 errors:0 dropped:0 overruns:0 frame:0
          TX packets:913 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2551554 (2.5 MB)  TX bytes:66946 (66.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:216 errors:0 dropped:0 overruns:0 frame:0
          TX packets:216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16539 (16.5 KB)  TX bytes:16539 (16.5 KB)

its170@its170-virtual-machine:~$
```

Figure 6. Result of ifconfig command in Raspbian

Step 2: No start the *Wireshark* at the ***Server*** by typing "sudo wireshark" in the Terminal and you will see it as in Figure 7. Select current Interface and Start capture. If you are not sure how to use it, please watch Demo video for the further instructions.

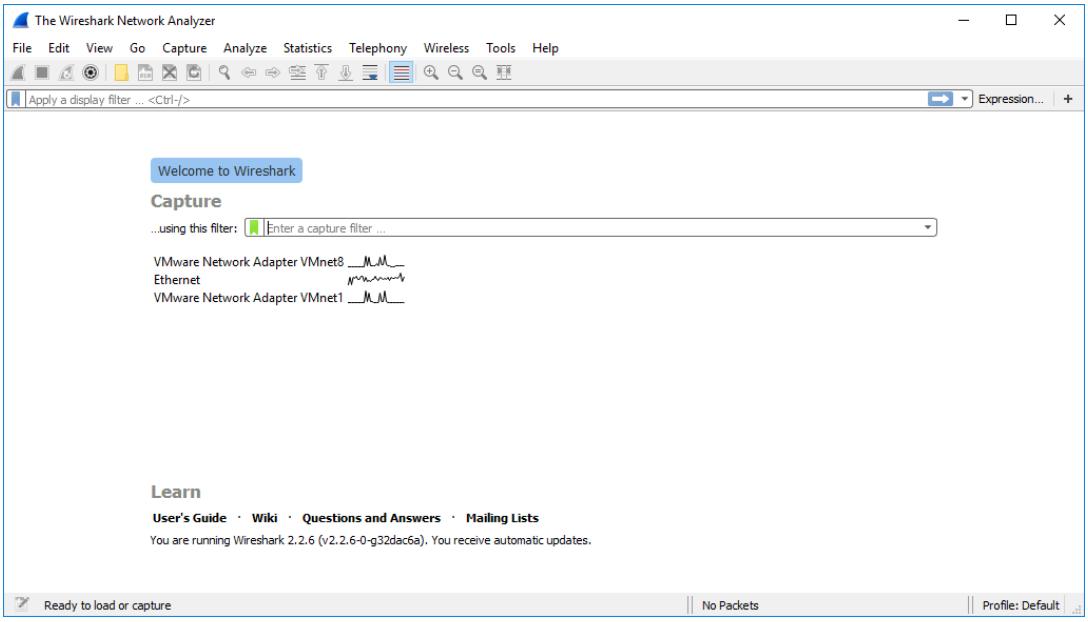


Figure 7. Running Wireshark at the Server

Step 3: Once Wireshark is running at **Server**, we will create remote Telnet connection from the client machine. At Client (Raspberrry Pi 2), typing "telnet <*Server IP address*>" in the Terminal to create the connection. For example if IP address of server is 192.168.10.5, you will need to typing "telnet 192.168.10.5". Then, it will ask for credential such as user ID and password. Enter your user ID and password to create remote connection to the server.

Step4: Now, stop Wireshark capturing at the server. Then, we will look into the captured packet. Use following filtering command to extract the Telnet related packet only. "ip.dst == *Server IP address* && telent". For example, if your server IP address is 192.168.10.5, then your filtering command will be "ip.dst == 192.168.10.5 && telent".

Step 5: Once the filtering is applied, you will need to observe the bottom of the Wireshark as circled in Figure 8. Now observe circled area for each TCP packet and check if login ID and password can be found.

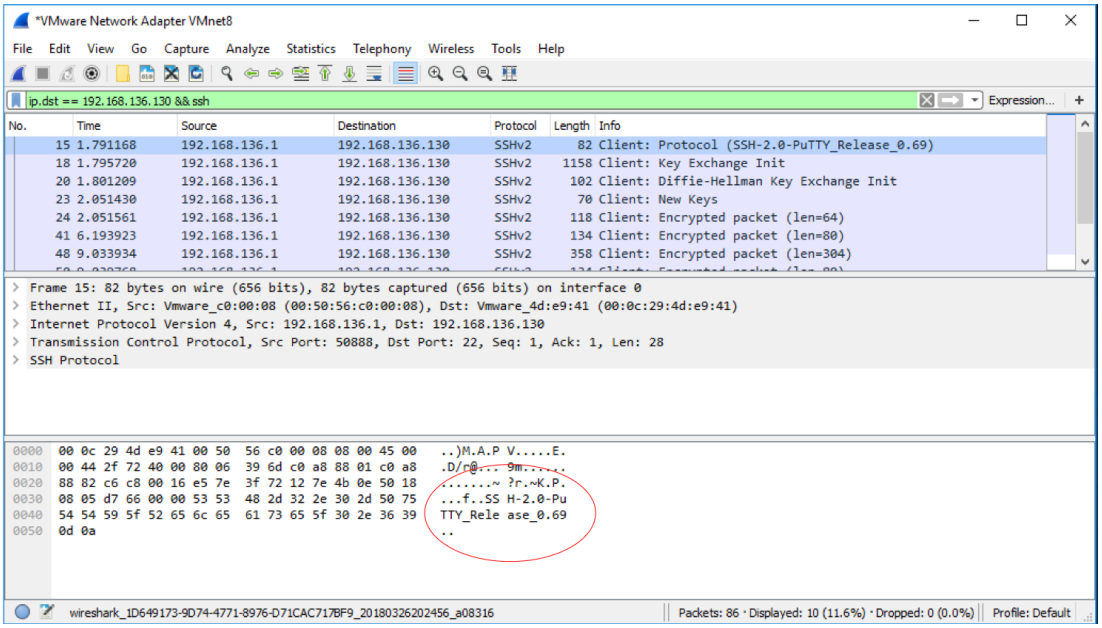


Figure 8. Result of filtering

Step 6: Disconnect Telnet session at the client machine by typing "quit". Now, we will observe SSH connection to see how it is different from Telnet. First, you will need to start new capture at the Wireshark before proceeding next steps.

Step 7: SSH service should be activated at the server now. Type "sudo service ssh start" at the Terminal. Next, we will open SSH session at the Client machine. Type "ssh -l <login ID> <IP address>" at the Terminal to create SSH session. If your login ID at the server is "pi" and server IP address is 192.168.10.5, then it will be "ssh -l pi 192.168.10.5". Then, go through the credential to access remote login to server.

Step 8: Now, stop Wireshark capturing at the server. Then, we will look into the captured packet. Similarly, use following filtering command to extract the SSH related packet only. "ip.dst == *Server IP address* && ssh". For example, if your server IP address is 192.168.10.5, then your filtering command will be "ip.dst == 192.168.10.5 && ssh".

Step 9: Once the filtering is applied, you will need to observe the bottom of the Wireshark as you did it at **Step 5**. Now observe circled area for each TCP packet and check if login ID and password can be found.

Discussion

- **Discuss the differences between Telnet and SSH based on your observation.**

  You can find login ID and password one letter by one letter when you observe the Telnet packets while may not be able to find them from SSH packets. The reason is that SSH uses encryption, but Telnet does not use it. When encryption is used, information can be hidden. Even though eavesdropping attack, one of Man in the Middle attacks, is presented, information can be securely delivered if encryption is used. However, Telnet

does not use encryption technique and plain text is delivered, which will let eavesdropping attacker obtain transferred data with clear text. Therefore, Telnet is not secure and SSH was developed for the replacement in order for the secure data transfer.

- **What other application uses encryption technique?**

  Encryption technique is using in many different applications. Full disk encryption encrypts the full disk in order to protect user data supported by Operating System (OS). Virtual Private Network (VPN) uses the encrypted connection between remote user and a server. The most famous application using encryption is Secure Web Browsing using HTTPS provided by TLS (Transport Layer Security). HTTP does use plain text while HTTPS uses encryption.

- **Discuss symmetric and asymmetric keys in Encryption technique.**

  Encryption technique requires key to provide the protection. There are two key types, symmetric and asymmetric. Symmetric key uses same key at both site while asymmetric uses different keys at each site. When encryption is used, key should be securely used. If key is exposed, anyone who has key can decrypt the information. Since symmetric key uses same key, it is weaker than asymmetric key and one of problems is key exchange. However, asymmetric key requires a lot of computation time, which produces a delay. Therefore, current application such as HTTPS uses both keys. Asymmetric key is used to exchange symmetric key.