Lab 1

Objectives:

1. Install VM
2. Understand packet capture, filter them, inspect them using wireshark and pyshark
3. Understand CIA Triad

Task 1. Install and run Wireshark on ubuntu machine.

(a) Update apt: sudo apt update

(b) Upgrade apt: sudo apt upgrade

(c) Install wireshark: sudo apt install wireshark

(d) Enable root privileges: When Wireshark installs on your system, you will be prompted by a window, as Wireshark requires superuser/root privileges to operate, this option asks to enable or disable permissions for all every user on the system. Press the “Yes” button to allow other users, or press the “No” button to restrict other users from using Wireshark.

(e) Reconfigure permission settings:

sudo dpkg-reconfigure wireshark-common

Select Yes

sudo usermod -a -G wireshark <username>

reboot

(f) Launch wireshark

Task 2. Use Wireshark to capture the first http request packet to this website and the following http response packet. Then show the information below.

(a) Use "http" as filter in wireshark and show the screenshot of the http request packet when browsing the website.

(b) What are the source and destination in the MAC header of the request?
source: (08:00:27:93:ef:b4) Destination: (52:54:00:12:35:02)

(c) What are the source and destination in the IP header of the request?
Source: 10.0.2.25 Destination: 35.223.170.84

(d) What are the source and destination in the TCP header of the request?
source port: 56334 destination Port: 80

(e) What is the HTTP payload in the request (if any)?
88 bytes

(f) What is the HTTP payload in the response (if any)?
148 bytes

Task 3. Use Wireshark to open the attached "hw1.q2.pcapng" that includes the sniffed traffic when a user tried to browse a website and download a text file.

(a) What is the IP address of the website?

source: 192.168.0.86 destination: 147.26.156.12

(b) What are the web URLs the user successfully browsed in order?

(c) What is the content of the text file (not just text, but a text file, and only one text file) from the website?

Task 4: Install pyshark and related dependencies

(a) sudo apt install tshark

(b) pip install pyshark

If pip is not recognized<< sudo apt install python3-pip

(c) Open Python terminal and run following commands

```
>>> import pyshark
>>> capture = pyshark.LiveCapture(interface='eno0')
>>>capture.sniff(timeout=5)
>>>for pkt in capture:
...         print(pkt)
...
>>>
```

Task 5: For each scenario, choose ONLY ONE BEST out of confidentiality, integrity and availability, and describe a defensive measure to either prevent or detect the security violation.

(a) John copies Mary's homework.

(b) Paul crashes Linda's system.

(c) Carol changes the amount of Angelo's check from $100 to $1000.

(d) Gina forges Roger's signature on a deed.

(e) Rhonda deletes all web services from university's web servers.

(f) Henry spoofs Julie's IP address to gain access to her computer.

What to Submit:

Upload a single pdf file containing the screenshot, answer to each question on Canvas. The file should be named as Lab1-netid.pdf.

Rubric

Task	Points
Task 1	25
Task 2	25
Take 3	15
Task 4	10
Task 5	25

Reference Materials:

1. https://www.wireshark.org/download/docs/Wireshark%20User%27s%20Guide.pdf

This is an in-depth user manual for Wireshark from the company's website. Their website has other tutorials as well if you wish to know more.

2. Tutorial on how to install VB, and ubuntu