1. (25%) Install and run Wireshark. Browse http://fuxi.cs.txstate.edu/~download/tools/, and use Wireshark to capture the first http request packet to this website and the following http response packet. Then show the information below.

Request Packet Screenshot

Graphical user interface, text, application, email

Description automatically generated

Request Packet

URL Shown

Response Packet Screenshot

Graphical user interface, text, application, email

Description automatically generated

Response Packet

(b) What are the source and destination in the MAC header of the request?

Graphical user interface, text, application, email

Description automatically generated

MAC Header

Destination MAC = 2c:7e:81:92:27:50

Source MAC = d8:3b:bf:fa:e1:6e

(c) What are the source and destination in the IP header of the request?

Graphical user interface, text, application, email

Description automatically generated

IP Header

Source Address = 192.168.1.65

Destination Address = 147.26.156.12

Graphical user interface, text, application, email

Description automatically generated(d) What are the source and destination in the TCP header of the request?

Source Port = 62569

TCP Header

Destination Port = 80

Graphical user interface, text, application, email

Description automatically generated(e) What is the HTTP payload in the request (if any)?

HTTP Packet Selected

Request Selected

HTTP Selecteddd

No Data Below HTTP == No HTTP Payload

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

Graphical user interface, text, application, email

Description automatically generated

Response Selected

HTTP Selecteddd

HTML Code in HTTP Payload for website

2. (15%) 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?

Destination IP is 147.25.156.12

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

<http://fuxi.cs.txstate.edu/~download/tools/>

<http://fuxi.cs.txstate.edu/icons/blank.gif>

<http://fuxi.cs.txstate.edu/icons/back.gif>

<http://fuxi.cs.txstate.edu/icons/folder.gif>

<http://fuxi.cs.txstate.edu/icons/compressed.gif>

<http://fuxi.cs.txstate.edu/~download/tools/Kali.vbox/>

<http://fuxi.cs.txstate.edu/icons/back.gif>

<http://fuxi.cs.txstate.edu/icons/text.gif>

<http://fuxi.cs.txstate.edu/icons/unknown.gif>

<http://fuxi.cs.txstate.edu/icons/blank.gif>

<http://fuxi.cs.txstate.edu/icons/script.gif>

http://fedoraproject.org/static/hotspot.txt

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

Graphical user interface, text, application, email

Description automatically generated

Readme File on how to install contained in text.

3. (15%) Install Zenmap. Identify the IP address of your own computer.

IP = 192.168.1.65

(a) Run Zenmap to scan your computer with "Quick scan". Show the screen shot of the output of NMap.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated(b) Run Zenmap to scan your computer with "Intense scan". Show the screen shot of the output of NMap.

(c) Compare the results of "Quick scan" and "Intense scan", and list the ports found in "Intense scan" but not "Quick scan".

Both show 4 ports being open, however 996 closed tcp ports were hidden on the intense scan vs 96 closed on the quick scan

4. (25%) 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.

Confidentiality. Mary can remove John’s permission to Read from Homework.

(b) Paul crashes Linda's system.

Availability. Linda may employ a backup system using different software.

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

Integrity. Carol may prevent the check from being revised completely after creation.

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

Integrity. Roger may employ system to have secondary security on all credit purchases.

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

Integrity. Prevention and detection through firewall may protect from attacks.

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

Confidentiality. Julie may encrypt access to her computer past the IP address.