20PW14

20XC46 COMPUTER NETWORKS LAB

&

### 20XW46 COMPUTER NETWORKS AND TCP/IP LAB

### Wireshark Lab-Basic Filters and Password sniffing

**Capture the Wireshark logs and perform/analyse the following:**

1) Log into the FTP server. Using Wireshark logs, capture the FTP login, username and password.

Cmp prompt: ftp [ftp.gnu.org](ftp://ftp.gnu.org)

And login

Display filter: ftp

2) What is the filter command for listing all outgoing HTTP traffic?

Display filter: tcp dstport==80

3) How would you filter/restrict the traffic between your machine and one another machine ONLY in the network?

Capture filter: host *another\_ipaddress*

Display filter: ip.addr== *your\_ipaddress* and ip.addr==*another\_ipaddress*

4) Browse to any HTTP based website. Display only the HTTP and DNS traffic.

Display filter : http or dns

5) What filter would you use to filter out certain protocols? Say, you want to filter DNS, TCP and ICMP protocols.

Display filter : *protocol\_name*

6) Browse to any HTTP based website. What filter would you use to analyse HTTP GET and POST requests?

Display filter: http.request.method=="GET" or http.request.method=="POST"

7) What is the MAC address of your Host? Which layer of OSI provides this information? Name the protocol.

cmd : ipconfig/all

Mac address: 4C-72-B9-98-85-81

Host name: CSLAB3-02.

The data-link layer provides the mac address.

IEEE, PPP

8) What is the IP address of your Host? Which layer of OSI provides this information? Name the protocol.

Ip address: 10.1.67.211

The Network Layer provides the ip address.

IP, ARP

9) Why is Wireshark not displaying HTTPS messages?

HTTPS messages are encrypted and hence wireshark can not display them.

10) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

The time interval between the HTTP GET message and HTTP OK message was 17.104070s – 17.055122s = 0.048948s

11) What is the Internet address of the LinkedIn server ([www.linkedin.com](http://www.linkedin.com))?

13.107.42.14

12)Does Facebook server have an IPv6 address?

**2a03:2880:2130:cf05:face:b00c::25de**

13) Execute “ping <IP of any server in Internet>” command in your machine. Capture Wireshark logs. What are the protocols used in the implementation of PING command?

ping 10.1.66.212

14) Do a new capture on your interface, go to menu > statistics > protocol hierarchy. What is the ratio between IPv4 and IPv6 on your interface?

Ratio 44.1/2.2 = 20.04545454545…

15) What are the Layer4, Layer 3, Layer 2 protocols executing at Client and Server ends for HTTP and TLS?

Layer 2 : Ethernet

Protocol : PPP, SBTV ,SLIP

Layer 3 : TCP , UDP

Layer 4 : **TCP, UDP, DCCP, and SCTP**

16) Extract files from FTP using Wireshark

File -> Extract objects -> TFTP

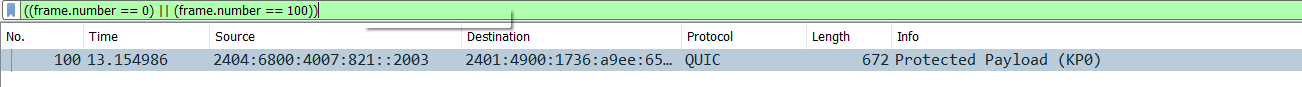
17) Capture files (images) from HTTP traffic

File -> Extract objects -> HTTP -> save images

18)Total number of packets and bytes

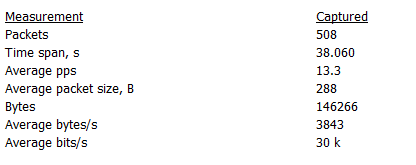
19) Time difference between first and last packet

(ip.addr == 192.168.148.11) && ((frame.number == 85) || (frame.number == 86))

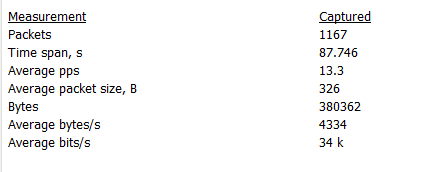


20) Total number of packets and bytes for TCP,UDP and ICMP traffic

TCP :



UDP :



**https://www.guru99.com/wireshark-passwords-sniffer.html**

http password

Sets a filter for any packet that has x.x.x.x as IP address

Ip.addr

Sets a conversation filter between two specific IP addresses

Ip.src=192.168.1.2 &&ip.dst==

Sets a filter to display all http and dns protocols

http

https

ssl

dns

tsl

Sets filters for any TCP packet with a specific source or destination port

Tcp.port==80

displays all TCP packets that contain a certain term

tcp contains GET

tcp contains /

. filters all HTTP GET and POST requests

http.request.method ==POST

filter out certain types of protocols

!(DNS or ARP)

Nightcap 192.182.2.2 7777

Password

Wireshark –packet-follow tcp stream

Can Wireshark capture passwords?

Can Wireshark capture passwords?

yes

Wireshark can capture not only passwords, but any kind of information passing through the network – usernames, email addresses, personal information, pictures, videos, anything. As long as we are in position to capture network traffic, Wireshark can sniff the passwords going through.

lain text network protocols

So how is it actually possible that Wireshark can capture passwords? That’s because some network protocols do not use encryption. Such protocols are called clear text (or plain text) protocols. And since clear text protocols do not encrypt the communication, all data are visible to the naked eye, including passwords. Anybody who is in position to see the communication (e.g. man in the middle) can ultimately see everything.

Following table lists some of the most popular clear text protocols still being used today and also some other protocols which allow clear text authentication:

Capture Insecure Connections (Net Cat)

Capture FTP Passwords

Extract files from FTP using Wireshark

Tcp.stream eq ipaddr

Capture HTTP Passwords

Capture files (images) from HTTP traffic

Filter png

Stop the capture

File –export-http images

https://www.guru99.com/wireshark-passwords-sniffer.html

http --password capture

ftp 65.2.95.61

kali linux 2019.2 vmware amd64

What is the Internet address and MAC of your Internet gateway?

No need to use Wireshark, even though you could. It is usually much easier just to use a couple of system commands to find that one out.

E.g. on Windows, run "ipconfig /all" on a command line to see the IP address of your gateway. Then ping that IP. Finally, run "arp -a" and find the gateway IP. Next to it you'll see the MAC address.

If you want to do it with Wireshark, ping the gateway and capture the ICMP packets. Look at the ethernet layer for the echo request destination MAC.