AASHNA KUNKOLIENKAR
190905304
lab 3 COMPUTER NETWORKS

Q 3.1.Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages. Also capture response messages and analyze them. During the lab session, also examine and analyze some HTTP headers.

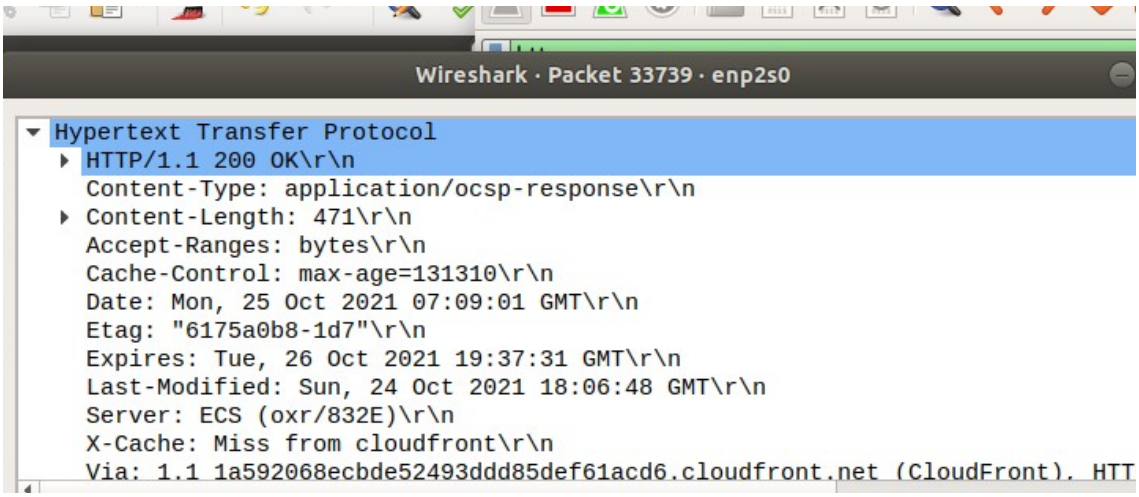
I first tried these filters:
dns
form contains manipal
tcp.port == 80 || udp.port == 80
http.accept
http.response
tcp.ack
tcp
http.content_length_header

I started wireshark and logged in to www.manipal.edu as well as a few other websites.

First, I captured all the packets. I notice various protocols such as ARP, SSDP, TCP, UDP, NBSS, HSRP, MDNS, etcetera.

Now, i used the filter “http”. The most common messages i found were
HTTP code 200 – OK
I went to youtube.com, which is restricted by the server, and got another message
HTTP code 204 No Content

I also analysed HTTP reponse headers where it gave me some details like the content length, Date, etc.

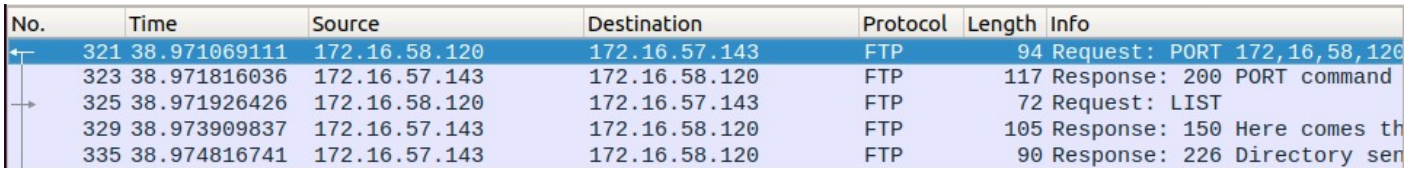


Q 3.2 Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

Source IP address is 172.16.58.120 and destination IP address is 172.16.57.143.

Control connection uses port number 21 (FTP) , data connection uses port 20 (TCP). Data connection gets opened and closed.... control connection is consistent.

In the info part of wireshark we can see “plain text” mentioned so it is obvious that the communication is done in plain text and is insecure.



No.	Time	Source	Destination	Protocol	Length	Info
321	38.971069111	172.16.58.120	172.16.57.143	FTP	94	Request: PORT 172,16,58,120
323	38.971816036	172.16.57.143	172.16.58.120	FTP	117	Response: 200 PORT command
325	38.971926426	172.16.58.120	172.16.57.143	FTP	72	Request: LIST
329	38.973909837	172.16.57.143	172.16.58.120	FTP	105	Response: 150 Here comes th
335	38.974816741	172.16.57.143	172.16.58.120	FTP	90	Response: 226 Directory sen

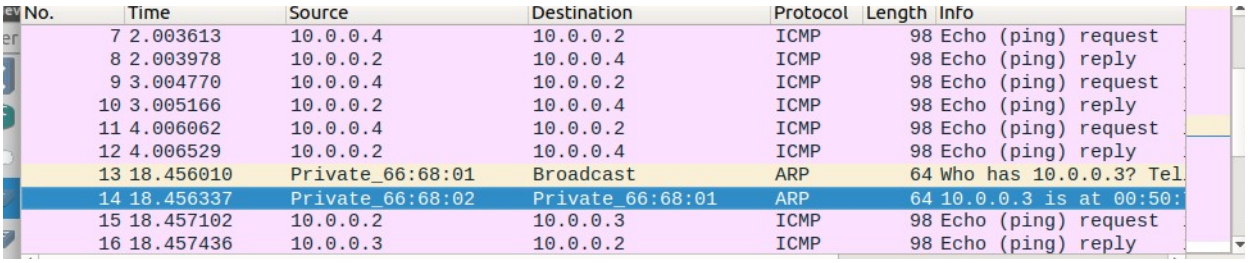
Question 4)

I connected 4 virtual Pcs to a Hub and assigned each of them different IP addresses.
PC1- 10.0.0.1/24
PC2-10.0.0.2/24
PC3-10.0.0.3/24
PC4-10.0.0.4/24

Then, i pinged PC4 from PC2 and messages started getting sent. (echo)
(by typing ping 10.0.0.4 in the terminal for PC2)

I then pinged PC3 from PC2. As we know, PC2 is already receiving messages from PC4.

This is why we see a change in protocol in wireshark from ICMP to ARP just twice (one for request one for response)



No.	Time	Source	Destination	Protocol	Length	Info
7	2.003613	10.0.0.4	10.0.0.2	ICMP	98	Echo (ping) request
8	2.003978	10.0.0.2	10.0.0.4	ICMP	98	Echo (ping) reply
9	3.004770	10.0.0.4	10.0.0.2	ICMP	98	Echo (ping) request
10	3.005166	10.0.0.2	10.0.0.4	ICMP	98	Echo (ping) reply
11	4.006062	10.0.0.4	10.0.0.2	ICMP	98	Echo (ping) request
12	4.006529	10.0.0.2	10.0.0.4	ICMP	98	Echo (ping) reply
13	18.456010	Private_66:68:01	Broadcast	ARP	64	Who has 10.0.0.3? Tel
14	18.456337	Private_66:68:02	Private_66:68:01	ARP	64	10.0.0.3 is at 00:50:
15	18.457102	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) request
16	18.457436	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) reply