**ITCS 461 Computer & Communication Security Date : ­­­\_\_\_\_26/03/2023\_\_\_\_\_\_\_**

**ID: 6388014 Name: Waris Damkham Section :** \_\_\_\_\_\_\_2\_\_\_ **\_\_\_\_\_\_**

Save this answer sheet as “ **Lab6\_618xxx.docx**” (Removing all figures will help reduce the file size).

Submit this file to the lab folder in e-learning website according to your session.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab 7 : Network Analysis**

Follow Lab7 document (Lab7.pdf) and answer these questions:

**Part I: Preparation**

No question in this part.

**Part II: Wireshark Basics**

**Question 1:**

1. How many ICMP packets?
2. If one **“ping”** command consists of 1 request packet and 1 reply packet.

Then, how many **“ping”** commands has been called?

**Select one pair of ICMP packets, and inspect each packet in the detail panel.**

1. Find **“Time to live”** (TTL) value inside Internet Protocol 4.

What is TTL value for request packet? and reply packet?

1. What is ICMP Type number for request packet? and for reply packet?

Are they the same number? (Y/N)

1. Click on “Data” in ICMP protocol, it will highlight the byte values in raw content panel. How long is the ICMP data in request packet?

and how long in the reply?

1. Compare the raw data (in raw content panel) of both request and reply packet.

Are they the same? (Y/N)

**Question 2:**

1. What does Address Resolution Protocol do?
2. What is the value of “Hardware type” in packet No. 7? ( )
3. What is the value of “Protocol type” in packet No. 7? ( )
4. Using both packet No. 7 – 8, we can learn the MAC addresses of both sender and receiver.

IP address: 10.1.1.1 MAC address:

IP address: 10.1.1.4 MAC address:

**Part III: Network Analysis: TCP Port Scan**

**Question 3:**

1. Can you find what IP address is the target? (hint: public IP is likely to be a server)
2. What is IP address of the attacker?
3. What are the ports that being scanned? (hint: known ports are low numbers)

**Question 4:** Within packet No. 9-29:

1. What ports are following these TCP handshake? (It also means that the ports are opened for connection.)
2. Pick one of the opening port from above question, check if the number is following this diagram.   
   Port = , sequence number (x) = , sequence number (y) =
3. Do the acknowledgement numbers according to diagram above? (Y/N)

**Question 5:** Within packet No. 32 - 47:

1. What ports are in this scanning pattern?
2. What ports are opened? (hint: port that responds with SYN-ACK)

**Part IV:** **Network Analysis: Web**

**Question 6:** Filter the packets with “dns”

1. What is the domain name that used in DNS query?
2. What is the IP address response? (only IPv4 address)
3. Does DNS operate on-top of TCP? (Y/N)
4. What port is used by DNS?

**Question 7:**

1. What is the URL of the login page?
2. What is version of PHP the server is running?
3. What is the final username and password that got the attacker to login?

(hint: it returns “HTTP/1.1 200 OK”)

**Part V: Network Analysis: HTTPS**

**Question 8:**

1. There are 2 certificates sent in this packet. Can you find what are their subject and

issuer? (answer only field “id-at-common”)

* + certificiate 1:

subject =

issuer =

* + certificiate 2:

subject =

issuer =

1. What is version of Secure Sockets Layer used in this traffic?
2. After SSL Handshake, the data should be encrypted. In packet labeled “Application Data”, is the data still human-readable? (Y/N)