

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 Lab6 document (Lab6.pdf) and answer these questions:

Part I: Preparation

No question in this part.

Part II: Wireshark Basics

Question 1:

- 1) How many ICMP packets? 6
- 2) If one “**ping**” command consists of 1 request packet and 1 reply packet.
Then, how many “**ping**” commands has been called? 3
Select one pair of ICMP packets, and inspect each packet in the detail panel.
- 3) Find “**Time to live**” (TTL) value inside Internet Protocol 4.
What is TTL value for request packet? 64 and reply packet? 48
- 4) What is ICMP Type number for request packet? 8 and for reply packet? 0
Are they the same number? No (Y/N)
- 5) 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? 48
and how long in the reply? 48
- 6) Compare the raw data (in raw content panel) of both request and reply packet.
Are they the same? Yes (Y/N)

Question 2:

- 1) What does Address Resolution Protocol do? protocol used in computer networking to map a network address (such as an IP address) to a physical address (such as a MAC address) for communication between devices on the same network
- 2) What is the value of “Hardware type” in packet No. 7? Ethernet(1)
- 3) What is the value of “Protocol type” in packet No. 7? IPv4(0x0800)
- 4) Using both packet No. 7 – 8, we can learn the MAC addresses of both sender and receiver.
Sender IP address: 10.1.1.1 MAC address: 52:54:00:12:35:00
Target IP address: 10.1.1.4 MAC address: 08:00:27:e3:ed:4c
Sender IP address: 10.1.1.4 MAC address: 08:00:27:e3:ed:4c
Target IP address: 10.1.1.1 MAC address: 00:00:00:00:00:00

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) 45.77.47.63
- 2) What is IP address of the attacker? 10.1.1.4
- 3) What are the ports that being scanned? (hint: known ports are low numbers) 25,80,22,8080,21,443

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.) 80,25,22,443
- 2) Pick one of the opening port from above question, check if the number is following this diagram.
Port = 80 , sequence number (x) = 0 , sequence number (y) = 0
- 3) Do the acknowledgement numbers according to diagram above? Y (Y/N)

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.1.1.4	45.77.47.63	TCP	60	25	42158	25 → 42158 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
2	0.000000	45.77.47.63	10.1.1.4	TCP	60	22	42646	22 → 42646 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	0.000000	10.1.1.4	45.77.47.63	TCP	74	42158	25	42158 → 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1713411283 TSecr=0 WS=128
4	0.000000	10.1.1.4	45.77.47.63	TCP	74	42646	22	42646 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1713411283 TSecr=0 WS=128
5	0.000000	10.1.1.4	45.77.47.63	TCP	54	42158	25	42158 → 25 [ACK] Seq=1 Ack=1 Win=29200 Len=0
6	0.000000	10.1.1.4	45.77.47.63	TCP	54	42158	25	42158 → 25 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.000000	10.1.1.4	45.77.47.63	TCP	54	42646	22	42646 → 22 [ACK] Seq=1 Ack=1 Win=29200 Len=0
8	0.000000	10.1.1.4	45.77.47.63	TCP	54	42646	22	42646 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Question 5: Within packet No. 32 - 47:

- 1) What ports are in this scanning pattern? 80
- 2) What ports are opened? (hint: port that responds with SYN-ACK) 80

Part IV: Network Analysis: Web

Question 6: Filter the packets with “dns”

- 1) What is the domain name that used in DNS query? muict.securitylab.ninja
- 2) What is the IP address response? (only IPv4 address) 45.77.47.63
- 3) Does DNS operate on-top of TCP? N (Y/N)
- 4) What port is used by DNS? 53

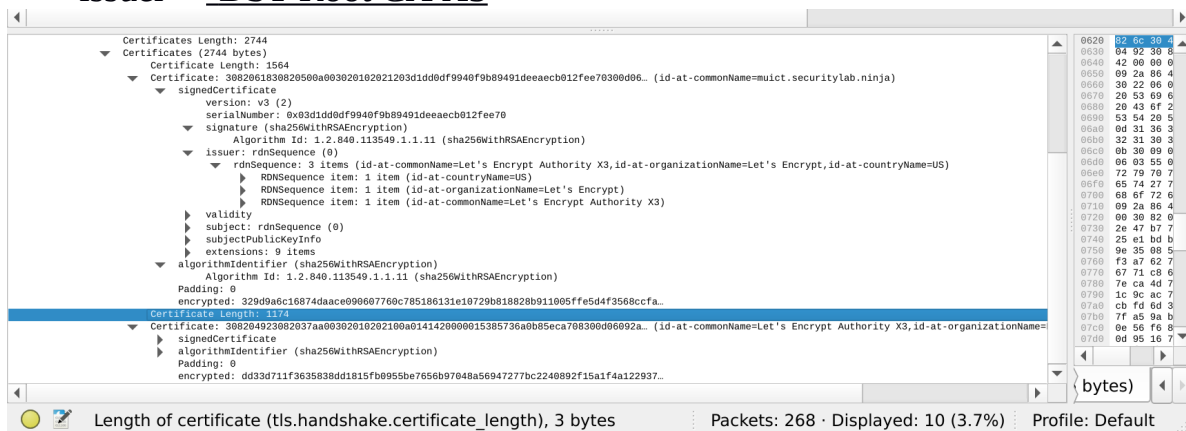
Question 7:

- 1) What is the URL of the login page?
http://muict.securitylab.ninja/netsec/admin/main.php
- 2) What is version of PHP the server is running? Nginx/1.11.10
- 3) What is the final username and password that got the attacker to login?
(hint: it returns “HTTP/1.1 200 OK”) admin : P@ssw0rd1!

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”)
 - certificate 1:
subject = muict.securitylab.ninja
issuer = Let's Encrypt Authority X3
 - certificate 2:
subject = Let's Encrypt Authority X3
issuer = DST Root CA X3



- 2) What is version of Secure Sockets Layer used in this traffic? TLSv1.2
- 3) After SSL Handshake, the data should be encrypted. In packet labeled “Application Data”, is the data still human-readable? N (Y/N)