ITCS 461 Computer & Communication Security Date : 22/3/2022

ID: 6288102 Name: Krissanapong Palakham Section : 1

Lab 6 : 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 <u>one pair</u> 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? N (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? Y (Y/N)

Question 2:

1) What does Address Resolution Protocol do? map MAC addresses to IP addresses
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.
   IP address: 10.1.1.1 MAC address: 52:54:00:12:35:00
   IP address: 10.1.1.4 MAC address: 08:00:27:e3:ed:4c

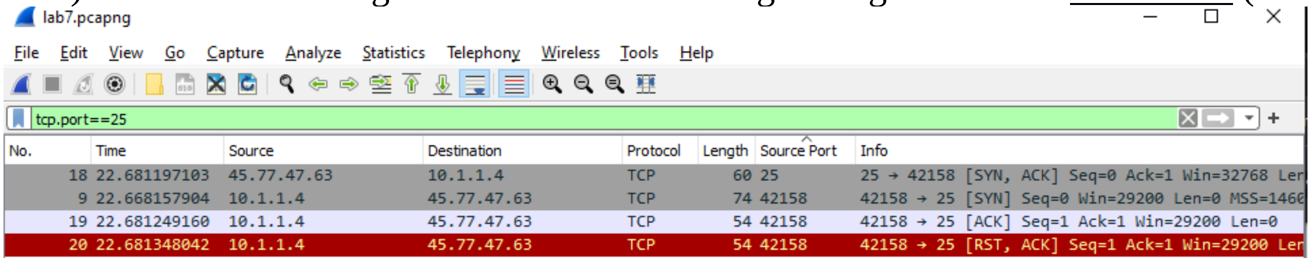
Part III: Network Analysis: TCP Port Scan

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.) ______25, 80, 22, 443____________________
2) Pick one of the opening port from above question, check if the number is following this diagram.
   Port = _____25__________ , sequence number (x) = _____0______ , sequence number (y) = _____0__________
3) Do the acknowledgement numbers according to diagram above? ____Y____ (Y/N)



tcp.port==25

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
18	22.681197103	45.77.47.63	10.1.1.4	TCP	60	25	25 → 42158 [SYN, ACK] Seq=0 Ack=1 Win=32768 Ler
9	22.668157904	10.1.1.4	45.77.47.63	TCP	74	42158	42158 → 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
19	22.681249160	10.1.1.4	45.77.47.63	TCP	54	42158	42158 → 25 [ACK] Seq=1 Ack=1 Win=29200 Len=0
20	22.681348042	10.1.1.4	45.77.47.63	TCP	54	42158	42158 → 25 [RST, ACK] Seq=1 Ack=1 Win=29200 Ler

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__________

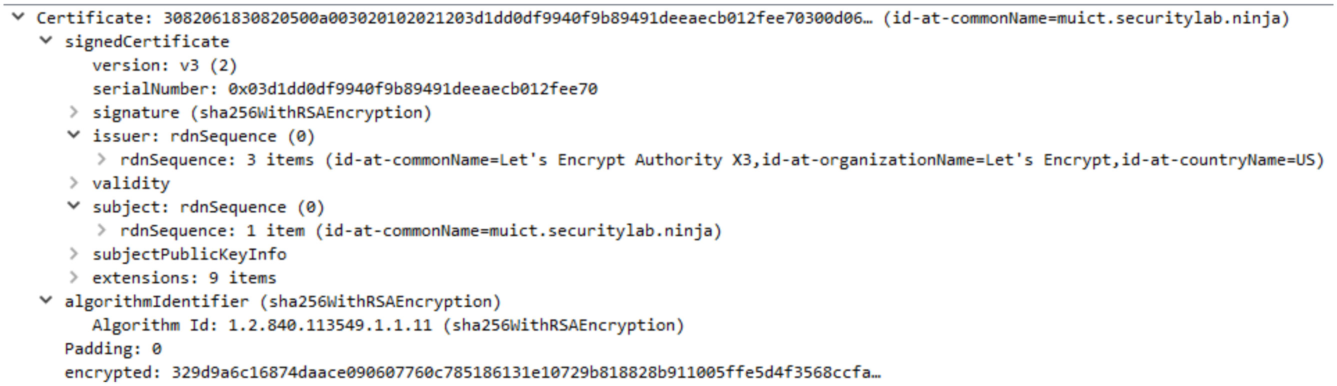
Question 7:

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

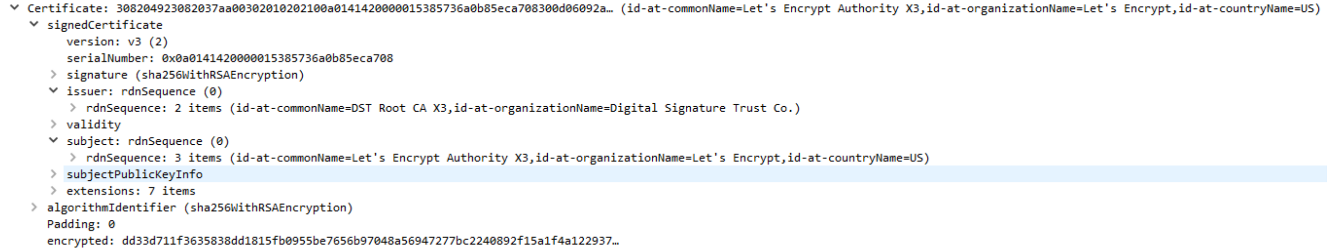
Question 8:

1) There are 2 certificates sent in this packet. Can you find what are their <u>subject</u> and <u>issuer</u>? (answer only field "id-at-common")
   - certificiate 1:
     subject = muict.securitylab.ninja
     issuer = Let's Encrypt Authority X3



```
⌄ Certificate: 3082061830820500a003020102021203d1dd0df9940f9b89491deeaecb012fee70300d06… (id-at-commonName=muict.securitylab.ninja)
  ⌄ signedCertificate
      version: v3 (2)
      serialNumber: 0x03d1dd0df9940f9b89491deeaecb012fee70
    › signature (sha256WithRSAEncryption)
    ⌄ issuer: rdnSequence (0)
      › rdnSequence: 3 items (id-at-commonName=Let's Encrypt Authority X3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)
    › validity
    ⌄ subject: rdnSequence (0)
      › rdnSequence: 1 item (id-at-commonName=muict.securitylab.ninja)
    › subjectPublicKeyInfo
    › extensions: 9 items
  ⌄ algorithmIdentifier (sha256WithRSAEncryption)
      Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    Padding: 0
    encrypted: 329d9a6c16874daace090607760c785186131e10729b818828b911005ffe5d4f3568ccfa…
```

   - certificiate 2:
     subject = Let's Encrypt Authority X3
     issuer = DST Root CA X3



```
⌄ Certificate: 308204923082037aa00302010202100a0141420000015385736a0b85eca708300d06092a… (id-at-commonName=Let's Encrypt Authority X3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)
  ⌄ signedCertificate
      version: v3 (2)
      serialNumber: 0x0a0141420000015385736a0b85eca708
    › signature (sha256WithRSAEncryption)
    ⌄ issuer: rdnSequence (0)
      › rdnSequence: 2 items (id-at-commonName=DST Root CA X3,id-at-organizationName=Digital Signature Trust Co.)
    › validity
    ⌄ subject: rdnSequence (0)
      › rdnSequence: 3 items (id-at-commonName=Let's Encrypt Authority X3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)
    › subjectPublicKeyInfo
    › extensions: 7 items
  › algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
    encrypted: dd33d711f3635838dd1815fb0955be7656b97048a56947277bc2240892f15a1f4a122937…
```

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)