ITCS 461 Computer & Communication Security   Date : _____

ID:___640315___ Name:___สิทธิกร เฉลิมกิตติชัย___   Section : __01_____ _____

_____

Lab 7 : Network Analysis

Follow Lab 7 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? ___6___
2) If one **"ping"** command consists of 1 request packet and 1 reply packet.
   Then, how many **"ping"** commands has been called? ___8___
   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 bytes___
   and how long in the reply? ___48 bytes___
6) Compare the raw data (in raw content panel) of both request and reply packet.
   Are they the same? ___N___ (Y/N)

Question 2:
1) What does Address Resolution Protocol do? _____
   _____ ปอมตัว แล้วเรียกชื่อ protocol _____
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: ___RealtekU_12:35:00___
   (52:54:00:12:35:00) _____
   IP address: 10.1.1.4   MAC address: ___PcsCompu_e3:ed:4c___
   (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)
   <u>45.77.47.63</u>
2) What is IP address of the attacker? <u>10.1.1.4</u>
3) What are the ports that being scanned? (hint: known ports are low numbers)
   <u>21</u>

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.) <u>443</u>
2) Pick one of the opening port from above question, check if the number is following this diagram.
   Port = <u>443</u> , sequence number (x) = <u>0</u> , sequence number (y) = <u>1</u>

3) Do the acknowledgement numbers according to diagram above? <u>Y</u> (Y/N)

Question 5: Within packet No. 32 - 47:
1) What ports are in this scanning pattern? <u>80</u>
2) What ports are opened? (hint: port that responds with SYN-ACK)
   <u>44054</u>

Part IV: Network Analysis: Web

Question 6: Filter the packets with "dns"
1) What is the domain name that used in DNS query?
   <u>Muict.securitylab.ninja</u>
2) What is the IP address response? (only IPv4 address) <u>10.1.1.4</u>
3) Does DNS operate on-top of TCP? <u>N</u> (Y/N)
4) What port is used by DNS? <u>192.168.1.1</u>

Question 7:
1) What is the URL of the login page? <u>[Full request URI: http://muict.securitylab.ninja/netsec/admin/main.php]</u>
2) What is version of PHP the server is running? <u>7.1.2</u>
3) What is the final username and password that got the attacker to login?
   (hint: it returns "HTTP/1.1 200 OK") _____
   Username = admin
   Password = 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 = <u>muict.securitylab.ninja</u>
     issuer = <u>Let's Encrypt Autherity X3</u>

   - certificiate 2: <u>Let's Encrypt Autherity X3</u>
     subject = <u>Let's Encrypt Autherity X3</u>
     issuer = <u>DST Root CA X3</u>

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