University of Dhaka
Department of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS)
Mid Term Examination
CSE 802: Information Security Fundamentals

Total Mark: 30 **Total Time: 1 Hour 30 Minutes**

Answer any Three (3) Questions

1. (a) Discuss different types of Handshake splitting mechanisms. Discuss how is split-handshake attack mounted? 4+2=6

   (b) Discuss the mechanism to mount Shrew DoS attack. 4

2. (a) Discuss how SPF email authentication protocol is used to ensure email security. 4

   (b) Discuss how DNS hijacking differs from DNS cache poisoning. 3

   (c) With an example discuss the advantages of using chroot jail. 3

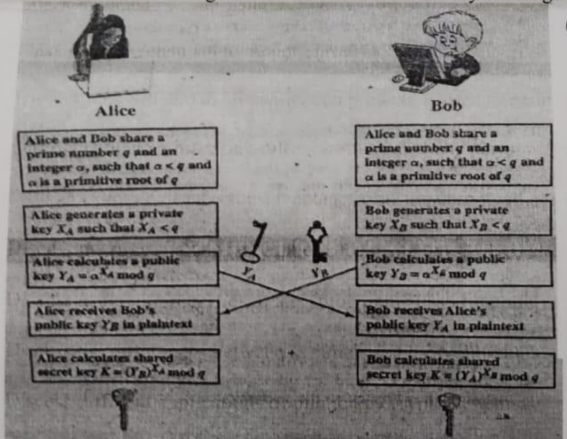
3. (a) Discuss the pros and cons of Cipher Block Chaining (CBC) along with its working procedure. 4

   (b) Discuss different properties of a cryptographic hash function. 3

   (c) Discuss the differences between symmetric and asymmetric key encryption. 3

4. (a) Discuss different applications of public key crypto systems. 2

   (b) Consider the following scenario of Diffie-Hellman key exchange scheme. 5



Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q

Alice generates a private key X_A such that $X_A < q$

Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$

Alice receives Bob's public key Y_B in plaintext

Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$

Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q

Bob generates a private key X_B such that $X_B < q$

Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$

Bob receives Alice's public key Y_A in plaintext

Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

Figure 1 The Diffie-Hellman Key Exchange

(a) Show the detailed calculation of K for Alice and Bob.
(b) Discuss why it is not possible to compromise private keys in this scheme.

   (c) Suppose A received a certificate from CA X_1 signed by the private key of X_1. Similarly, B received a certificate from CA X_2 signed by the private key of X_2. Now suppose A has access to B's certificate and wants to verify the public key of B. Describe how this can be achieved. 3

University of Dhaka
Professional Master's in Information and Cyber Security
Mid-Term Examination, 13th October 2023
Course 804: Network Security

Full Marks: 15 Time: 1.5 Hours

Answer any 3 (three) of the following questions

1 You are the network administrator for a mid-sized financial institution. One Monday morning, you notice that the organization's online banking portal is extremely slow and, at times, completely unresponsive. After initial investigations, you strongly suspect that the institution is a target of a Denial of Service (DoS) attack.

a) Describe the immediate steps you would take to confirm that it is indeed a DoS attack and not just a temporary network issue. 2

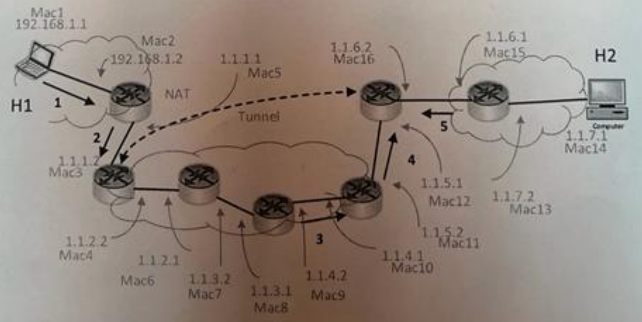
b) Once confirmed, outline the countermeasures you would implement to mitigate the impact of the DoS attack. 2

c) Explain how you would communicate this incident to both the management team and the affected customers. 1

2 a) What is Vulnerability and Threats? Explain briefly with appropriate examples. 3

b) A large organization has an API in DMZ which doesn't require any authentication. Please outline the threats and vulnerability from the scenario and justify your answer? 2

3 In the following network, H1 sent an HTTP request to the webserver (H2). The IP and MAC addresses of the hosts/routers on each interface is shown in Figure. Write down the packet headers (only Source IP, Destination IP, Mac address) as they flow through the links marked as 1-5. Consider the presence of NAT routers and the IP-IP tunnel.



a) Write down the packet headers (only Source IP, Destination IP, Mac address) as they flow through the links marked as 1-5. [Consider the presence of NAT routers and the IP-IP tunnel. However, the tunnel has not been set up by the endpoints yet] 2+ 1+ 2

b) Will there be any change in the answer found in previous question if the webserver supports only TLS 1.2 connection?

c) When the webserver changes to secure (TLS 1.2) connection, the client observed a decleased performance. Give possible causes for that.

4 MedTech Corp is a leader in the field of healthcare technology, particularly in producing IoT (Internet of Things) devices for remote patient monitoring. The company has developed a range of IoT products, such as wearable heart monitors and insulin delivery systems, that send patient data in real-time to healthcare providers.

MedTech Corp recently decided to implement Transport Layer Security (TLS) to secure the data being transferred between their IoT devices and healthcare provider servers. However, the initial implementation has led to some challenges. Several healthcare providers have reported latency issues in data transmission and raised concerns about the compatibility of older devices.

Further complicating the issue, a cybersecurity firm contacted MedTech Corp with evidence that a specific version of TLS implemented in their devices had a known vulnerability that had been exploited in other contexts.

Answer the following questions based on the above-mentioned scenario.

a) What could possible threats and vulnerabilities which led the company to go for TLS implementation? 2

b) How could the latency issues be related to the TLS implementation? 1

c) What challenges have arisen concerning the compatibility of older IoT devices with the new TLS implementation? 2