University of Dhaka

Department of Computer Science and Engineering

Professional Masters in Computer and Information Security

CSE 802: Information Security Fundamentals

Total Mark: 15

Total Time: 25 m

Answer any Four (4) of the following questions

1. Why should you use the chroot jail?

2. Draw the block diagram of the operations of the public key crypto system.

3. Write on the Electronic Code Book (ECB) with its shortcomings.

4. Write on the advantages and disadvantages of DNS cache.

5. Discuss how a TCP SYN flooding is launched. Also write on the consequences of TCN SYN flooding with IP spoofing.

desired NIST CSF tier.

University of Dhaka

Department of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program, Jan 2024
CSE 808 – Information Infrastructure Protection
Class Test – 1, Date: February 24, 2024

Marks: 15 Time: 30 Minutes

Question – 1:

ABC Corporation, a leading technology company, has recently experienced a series of cyberattacks that resulted in unauthorized access to sensitive customer data. The company's leadership is concerned about the potential impact on customer trust and the overall business reputation. In response, they have decided to implement the NIST Cybersecurity Framework (CSF) to enhance their cybersecurity posture.

A) What is the primary objective of the NIST Cybersecurity Framework, and why is it important for organizations? 2

B) As the newly appointed cybersecurity manager at ABC Corporation, you are tasked with overseeing the implementation of the NIST CSF. Describe how you would approach the situation? Comment on the process of choosing desired NIST CSF tier. 5

Question – 2: 1

Which of the following principles is the foundation of the CIA triad in cybersecurity?

A) Consistency, Integrity, Availability
B) Confidentiality, Integrity, Availability
C) Continuous Integration and Automation
D) Cryptographic Identification Algorithm

Question – 3: 1

Which of the following attacks is not a threat to integrity?

A) Unauthorized modification attacks
B) Impersonation attacks
C) Man-In-The-Middle (MITM) attacks
D) DDOS attacks

Question – 4: 1

Which of the following attacks is not a threat to availability?

A) Unauthorized modification attacks
B) Hardware failures
C) Power outages
D) DDOS attacks

...implications

...ions. Provide recommendations on how to address the situation. 2.5

... Which principle among the CIA triad the Bell-LaPadula model is associated with the most? 1.0

CSE-808 CT-1

Question – 5: 1

Which of the followings is true?

A) Information security is a subset of Cyber security
B) Cyber security is a subset of Information security
C) Information security and Cyber security are the same
D) Information security and Cyber security have nothing in common

Question – 6: 1

Which of the following attacks is not a threat to confidentiality?

A) Snooping
B) Social Engineering
C) Unauthorized modification attacks
D) Wiretapping

Question – 7: 1

Consistency in cybersecurity primarily involves:

A) Regularly monitoring network traffic for anomalies
B) Ensuring all users have access to the same level of data protection
C) Implementing measures to prevent data corruption or unauthorized changes
D) Continuously adapting security measures to address evolving threats

Question – 8: 1

Non-repudiation in cybersecurity ensures that:

A) Users can access data securely from any location
B) Data remains unchanged and unaltered during transmission
C) Parties cannot deny their actions or transactions
D) Network traffic is monitored for suspicious activities

Question – 9: 1

Which of the following components is NOT included as a fundamental part of the information security triad?

A) Non-repudiation
B) Integrity
C) Accountability
D) Authorization

University of Dhaka

Dept. of Computer Science and Engineering

Class Test 1 Exam (Batch 2), PMICS

January 2024 Semester

Time: 30 Min CSE 801 - Communication Protocols and Internet Architecture Mark: 15

Answer all the questions. Marks are indicated at the left side of each question.

1. Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates $R_1 = 500$ kbps, $R_2 = 2$ Mbps, and $R_3 = 1$ Mbps.
   (a) (2 points) Assuming no other traffic in the network, what is the throughput for the file transfer?

   (b) (2 points) Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to the Host B?

2. (2 points) List down 3 key differences between a client-server and a peer-to-peer application architecture.

3. (2 points) Suppose Alice, with a web-based e-mail account (such as Hotmail or Gmail), sends a message to Bob, who accesses emails from his mail server using a mail access protocol. Discuss how the message gets from Alice's host to Bob's host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts.

4. (2 points) What is the HOL blocking issue in HTTP/1.1? How does HTTP/2 attempt to solve it? Describe with an example.

=============== THE END ===============