

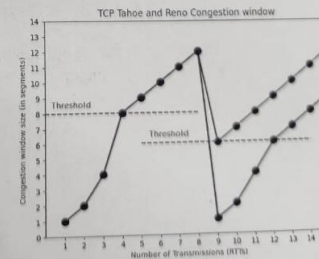


University of Dhaka
Dept. of Computer Science and Engineering
PMICS Midterm Exam (Batch 1)
July 2023 Semester

Time: 1.5 Hr. CSE 801 - Communication Protocols and Internet Architecture Mark: 30

Answer any **THREE** questions. Marks are indicated at the left side of each question.

1. (a) (6 points) An ISP wants to generate a block of addresses starting with 171.81.0.0/16 and it wants to distribute these blocks to 1152 business customers as follows. The first group has 128 medium-sized businesses; each needs 128 addresses. The second group has 1024 small businesses; each needs 32 addresses. Design the subblocks by giving the network address and address range in the form of a.b.c.d/x for each subblock. Finally, analyze how many addresses are still available after these allocations.
(b) (4 points) Can we use HTTP cookies to track user behavior across multiple websites? Explain the process with the help of a figure and state its security concerns.
2. (a) (6 points) A resource record of DNS is a four-tuple that contains the following fields: $(Name, Value, Type, TTL)$. Describe the contents of other fields when $Type = A$, $Type = NS$, and $Type = CNAME$ and their practical usages.
(b) (4 points) How do you define DNS cache? Suppose you can access the caches in the local DNS servers of your department. How can you determine the Web servers (outside your department) that are most popular among the users in your department? Explain.
3. (a) (4 points) How does SMTP mark the end of a message body? How about HTTP? Can HTTP use the same method as SMTP to mark the end of a message body? Explain.
(b) (6 points) Suppose, you purchase a wireless modem and connect it to your cable modem. Also, suppose that your ISP dynamically assigns your wireless router one IP address and you have five hosts at your home that use 802.11 to wireless connect to your wireless router. How are IP addresses assigned to the devices? Does the wireless router use NAT? Analyze your answer.
4. Considering the congestion control behavior shown in the figure below, and answer the following questions.
(a) (2 points) Define Cumulative Acknowledgment.
(b) (2 points) State the effects of setting TIME-OUT period too small or too large.
(c) (3 points) Assuming a packet loss is detected in TCP Reno after round 6 by the receipt of a triple duplicate ACK, what will be the values of the congestion window size and of ssthresh at round 7? Explain the rule.
(d) (3 points) Describe how 'fast retransmit' can increase data transfer performance.



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

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) Describe how a TCP SYN flooding attack can be mounted. Discuss the damages caused by TCP SYN flooding attack with IP spoofing. 3+2=5
- (b) Suppose a machine X in the same LAN with machine A wants to establish a connection with a server Y executing code. Machine X wants to establish a TCP connection with Y pretending to be A. Discuss how this attack can be mounted. 3.5
- (c) In IP spoofing, an adversary X wants a remote host to believe that the incoming packets are coming from a trusted client. So, to initiate a connection with the remote host, X sends a SYN packet with the client's IP address in it. What problems can X expect to encounter? 1.5
2. (a) What is meant by poisoning the DNS cache? Explain how one can mount a DNS cache poisoning attack. 2+4=6
- (b) Consider the following snapshot of an email header. Write on the anomaly found in the email routing path. 2

```
Return-Path: cossackerg1@ralve29.vnet.ibm.com
Delivery-Date: Sun Apr 4 12:36:10 2010
Received: from m503.ecn.purdue.edu [m503.ecn.purdue.edu (128.46.105.218)]
by rvl4.ecn.purdue.edu (8.14.4/8.14.4) with ESMTP id o34GaaED13679
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT)
for <kak@rvl4.ecn.purdue.edu>; Sun, 4 Apr 2010 12:36:10 -0400 (EDT)
Received: from 114.24.88.69 [114.24.88.69] with ESMTP id 114-24-88-69.dynamic.hinet.net (114.24.88.69)
by m503.ecn.purdue.edu (8.14.4/8.14.4) with ESMTP id o34GZ2k8020095;
Sun, 4 Apr 2010 12:35:23 -0400
Received: from 114.24.88.69 by e33.co.us.ibm.com; Mon, 5 Apr 2010 00:34:59 +0800
Message-ID: <000601c4d4148c46040408080000ScO0cossackerg1>
From: "Miguel A. Souza" <cossackerg1@ralve29.vnet.ibm.com>
To: <kat@ecn.purdue.edu>
Subject: ecn.purdue.edu account notification
Date: Mon, 5 Apr 2010 00:34:59 +0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-----_TextPart_000_0006_01CAD414.C4404060"
X-Priority: 3
X-MNMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
X-ECN-MailServer-VirusScanned: by anavind-new
X-ECN-MailServer-Originator: 114-24-88-69.dynamic.hinet.net (114.24.88.69)
X-ECN-MailServer-SpanScanAdvice: DoScan
Status: RD
```

- (c) How is TTL used in a DNS cache? Write on the security aspect of TTL. 2
3. (a) Discuss the pros and cons of Cipher Block Chaining (CBC) along with its working procedure. 4
- (b) Perform encryption and decryption using the RSA algorithm with the following information: 3
 $p = 17, q = 11, e = 7$ and $M = 88$

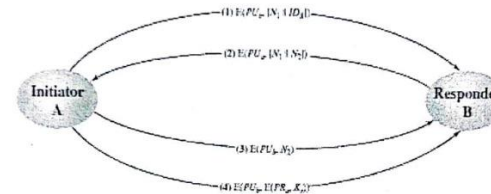
University of Dhaka
Department of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS)
Mid Term Examination
CSE 802: Information Security Fundamentals

Total Mark: 30

Total Time: 1 Hour 30 Minutes

Answer any Three (3) Questions

- (c) How is public key cryptography used to achieve digital signature? 3
4. (a) Discuss different applications of a cryptographic hash functions. 3
- (b) Consider the scenario shown in the figure below. Here, A wants to establish a secure secret key with B for safe communication. Messages passed between A and B are shown in the figure. You should explain the purpose of each message involved in the communication. 4



- (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, 29th September 2023
Course 804: Network Security

Full Marks: 15

Time: 1.5 Hours

Answer any 3 (three) of the following questions

- 1) Imagine you're the newly hired IT director for a renowned university with a sprawling campus. The university boasts a diverse student body with over 20,000 students, numerous research facilities, multiple libraries, and several off-campus affiliates. 2+ 1.5+ 1.5

Recently, the university experienced a cyber incident where researchers' data was compromised, causing distress in the academic community. The board is alarmed and urges an overhaul of the network security systems. You're asked to evaluate the current setup and implement additional measures.

The university has an existing firewall and a basic network monitoring system. The IT team provides you with network logs that indicate multiple unauthorized access attempts in the past few months, though not all were successful. Moreover, with the diverse needs of students, faculty, and research facilities, the network experiences high traffic, often needing rapid access to vast amounts of data, making minimal latency crucial. The Board of Trustees has allocated a budget to enhance cybersecurity but wants your recommendation on whether to invest in an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS).

- a) Outline the key considerations that should be factored into your decision on whether to implement an IDS or IPS in the university setting, taking into account the diverse user base and the different types of data processed.
- b) Discuss the potential advantages and limitations of deploying an IDS in this scenario.
- c) Discuss the potential advantages and limitations of deploying an IPS in this scenario.

- 2) What does "Cyber Kill Chain" mean? A large organization has experienced security breaches in their critical services and data breaches. Now the threat actors have demanded ransom from the organization. Please re-construct the scenario and explain steps in "Cyber Kill Chain". 5

- 3) A bank has recently launched its online banking service, which mandates the use of Multi-Factor Authentication (MFA) for user access. The platform is currently accessible through HTTP and operates on a single instance hosted in the bank's Data Center. 1+ 1+ 1+ 1+ 1

- a) What do the terms Confidentiality, Integrity, and Availability mean in the context of cybersecurity?
- b) How does using Multi-Factor Authentication (MFA) contribute to the confidentiality of the online banking platform?
- c) Are there any confidentiality concerns arising from the use of HTTP instead of HTTPS? Please elaborate.
- d) How does MFA help in maintaining the integrity of transactions and user data?
- e) What are the possible integrity risks associated with running a single instance of the application?

- 4) Consider a scenario where you are entrusted with the investigation of Command and Control (C2) traffic originating from your enterprise Local Area Network (LAN) towards external entities beyond your organization's perimeter. Your objective is to identify the compromised machine within your network and conduct a comprehensive analysis to determine the root cause of the compromise. It has come to your attention that an employee received a phishing email containing a link to a malicious domain, which, when clicked, triggered the execution of a malware instance, subsequently initiating HTTP communications with a malevolent server. 1+ 1.5+ 1.5

In this context, you possess knowledge of various data formats used for network monitoring and threat detection purposes. Among these formats, your assignment requires you to scrutinize and assess the suitability of the following three types of data formats:

- a) Netflow
- b) Layer 7 metadata: Network service logs
- c) Full packet capture (PCAP)

Your job is to explain which type of data format is the **best choice** for your investigation and why. You should also highlight the **advantages and disadvantages** of each data format to help make a well-informed decision.



University of Dhaka

Department of Computer Science and Engineering

Professional Masters in Information and Cyber Security (PMICS) Program, July 2023

CSE 808 – Information Infrastructure Protection

Mid Term – 1, Date: September 23, 2023

Marks: 30

Time: 1 Hour 30 Minutes

Answer any THREE out of the following four questions.

✓ Question – 1:

"Suppose you are the Chief Information Security Officer (CISO) of a large, multinational company with diverse operations. You have decided to implement the NIST Cybersecurity Framework (CSF) to enhance your organization's cybersecurity posture.

- Briefly describe the NIST CSF before the board of directors and senior management to get the required budget and proper support. 4.0
- Explain the relationship between the NIST CSF and international cybersecurity standards, such as ISO 27001. How effectively these can be integrated? 2.0
- Write down the significance of developing a Target Profile and a Current Profile. How they are related to NIST Framework implementation? 2.0
- What are the common cyber security layers? In which layers NIST CSF need to be implemented? 2.0

✓ Question – 2:

- A cybersecurity researcher discovers a critical vulnerability in a widely used software application. This vulnerability could potentially lead to data breaches and significant harm to users if exploited. The researcher promptly reports the vulnerability to the software company but receives no response or action to fix the issue. As a result, the researcher decided to disclose the vulnerability publicly to raise awareness. Explore the potential consequences the researcher may face from both legal and ethical standpoints. 2.0
- Which one is more important – Integrity or Consistency? Justify your choice. 1.5
- Write down the differences between hashing and encryption. 2.0
- CCTV is detective control, and antivirus is a preventive control. Explain the common categories of cyber security controls. 2.5
- Discuss the concept of "zero-day attack" in the context of cyber kill chain? 2.0

Question – 3:

Consider an e-commerce platform facing the problem of traffic management as well as security issues. The authority hires you as a security consultant. The authority planning to run the following applications.

i) Online retail stores, ii) Supplier portals, iii) Online payment systems, iv) Online auction, v) Online Inventory, vi) Online Market Research Survey, vii) Crowdfunding, viii) e-commerce Backend system

- How does a Next-generation firewall deep inspect TLS/SSL encrypted packets? 1.5
- You have to design a Network Access Control. Please describe the key factors to consider. Also, suggest the Access Control Policy. 3.5
- You have to place the applications into the DMZ network and internal protected network. The selection of each application into a particular network requires well justification. Also, provide a diagram with the required devices. 5.0

✓ Question – 4:

- "Confidential data can never be public." Agree or disagree, justify with examples. 1.5
- How can multi-factor authentication (MFA) enhance access security, and what are some common factors used in MFA? 1.5
- As an Information Security official, how, many classification layers will you suggest to your organization, explain with justification. 2.5
- How does COBIT 5 support organizations in aligning IT goals with business objectives and improving overall business performance? 2.5
- What are the primary types of backups, and how do they differ from each other? 2.0