Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES (SCES)
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END-OF-SEMESTER EXAMINATION
CNS3105: NETWORK SECURITY

DATE: 24/7/2023 Time: 2 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One [30 Marks]

A. Explain the following attacks which can occur during communication across the network.

[8 Marks]

- **i.** Disclosure
- **ii.** Traffic analysis
- **iii.** Masquerade
- **iv.** Content modification
- **v.** Sequence modification
- **vi.** Timing modification
- **vii.** Source repudiation
- **viii.** Destination repudiation

B. Briefly describe any four system security standards. **[6 Marks]**

C. Explain any two common techniques that can be used to protect a password file.

[4 Marks]

D. Explain any three design goals for network firewalls. **[6 Marks]**

E. Explain the four SSL protocols. **[6 Marks]**

Question Two [15 Marks]

A. Explain the different phases of a virus's lifetime. **[6 Marks]**

B. Using a well-labeled diagram, explain the protocols used to provide IP security.

[9 Marks]

Question Three [15 Marks]

A. Using a diagram, illustrate a simple implementation of an Intrusion Detection System.

[6 Marks]

B. Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets. The strategy is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way. Consider the diagram in Figure 1. Provide a security in-depth analysis of the network.

[9 Marks]

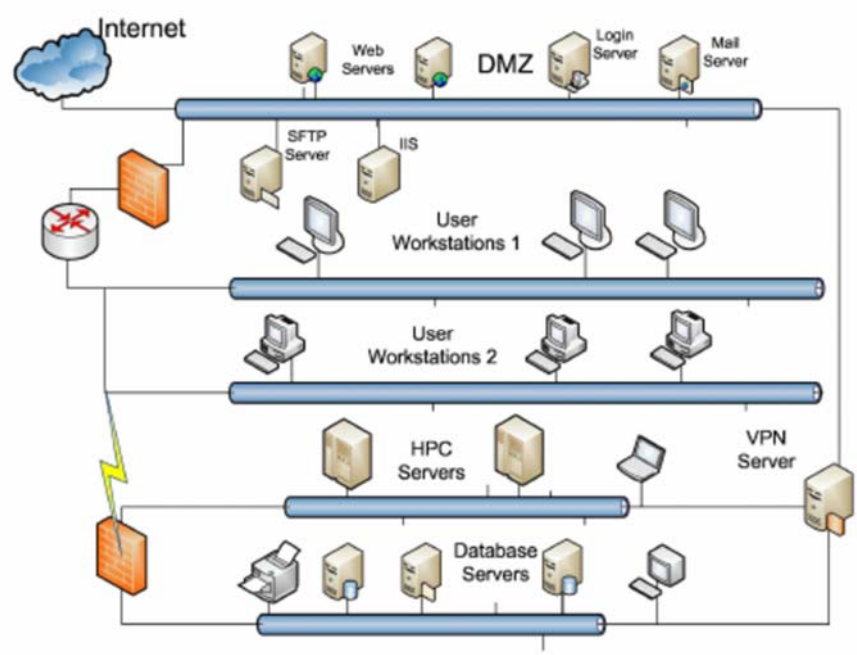

Figure 1: Corporate Network

Question Four [15 Marks]

A. An Indicator of Compromise (IOC) is often described in the forensics world as evidence on a computer that indicates that the security of the network has been breached. Explain any six Indicators of Compromise (IOC) Companies should monitor. **[9 Marks]**

B. Man-in-the-middle attack (MITM) attack is a common attack in computer networks. Explain any three prevention techniques for the MITM attack. **[6 Marks]**

Question Five [15 Marks]

A. A brute force attack is a trial-and-error approach used by attackers to determine the correct credentials by repeatedly attempting all possible combinations. Explain any three prevention measures for the attack on computer networks. **[6 Marks]**

B. A port scan is a technique for identifying which ports are open on a network. Port scanning is similar to knocking on doors to determine whether somebody is home since ports on a computer are where information is transferred and received. A port scan on a network or server indicates which ports are open and listening (receiving data), as well as the presence of security measures like firewalls between the sender and the destination. It is also a popular reconnaissance starting point for attackers looking for a weak point of entry to hack into the network/device. Explain any six of the most often used port scanning techniques. **[9 Marks]**