



University of Colombo, Sri Lanka

University of Colombo School of Computing



**DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY
(EXTERNAL)**

Academic Year 2026— 3rd Year Examination — Semester 6

IT6406 — Network Security and Audit

Structured Question Paper

(Two (2) hours)

To be completed by the candidate

Index Number

--	--	--	--	--	--	--

Important Instructions

- The duration of the paper is **Two (2) hours**.
- The medium of instructions and questions is English.
- This paper has **4** questions and **10** pages.
- Answer **All** questions. **All** questions carry **equal** marks.
- **Write your answers in English** using the space provided **in this question paper**.
- Do not tear off any part of this answer book.
- Under no circumstances may this book (or any part of this book), used or unused, be removed from the Examination Hall by a candidate.
- Questions appear on both sides of the paper. If a page is not printed, please inform the supervisor immediately.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries and mobile phones, are **not allowed**.
- Non Programmable Calculators may be used.
- *All rights reserved.*

**To be completed by
the examiners**

1	
2	
3	
4	
Total	

--	--	--	--	--	--	--

1. (a). State the primary objective of an intruder when targeting an information system.

[4 marks]

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system
Topic 5 Teachers note page 9

- (b). Identify two (2) statistical anomaly detection methodologies utilised within Intrusion Detection Systems (IDS).

[4 marks]

Threshold detection
Profile based
Topic 5 Teachers note page 12

- (c). Explain the concept of **rule-based anomaly detection** in an Intrusion Detection System (IDS)

[5 marks]

Rule-based techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
Topic 5 Teachers note page 12/ 18

Index Number

--	--	--	--	--	--	--

- (d). Describe the underlying mechanism of a **Packet Filtering Firewall** and identify the specific network parameters upon which its filtering rules are constructed.

[6 marks]

applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. Filtering rules are based on, Source IP address, Destination IP address, Source and destination transport-level address, IP protocol field, and Interface.

Topic 5 Teachers note page 27

- (e). Explain how **S/MIME** (Secure/Multipurpose Internet Mail Extensions) achieves the security services such as **Authentication** and **Confidentiality** in email communication.

[6 marks]

Authentication -Provides by digital signature. Most commonly RSA with SHA-256. Confidentiality - Provides confidentiality by encrypting messages. Use AES- 128 with CBC

Topic 6 Teachers note page 11

--	--	--	--	--	--	--

2. (a). What is **MAC Address Spoofing**?

[4 marks]

MAC spoofing is the technique of changing a device's factory-assigned Media Access Control (MAC) address to imitate another device or to disguise your own. Topic 7 Teachers note page 4

(b). Explain the security threats associated with **MAC Address Spoofing** in wireless environments.

[6 marks]

MAC spoofing threatens wireless security by allowing attackers to bypass MAC filtering, hijack active user sessions, and execute Man-in-the-Middle attacks. By masking their identity as a trusted device, attackers gain unauthorized network access, intercept sensitive data, disrupt operations via Denial of Service, and evade forensic tracking.

Topic 7 Teachers note page 4

(c). Suggest a technical control that can be implemented to remediate security risks arising from MAC address spoofing.

[4 marks]

avoid mac based filtering and use advanced authentication mechanisms.

Securing wireless access points. Securing wireless networks. Use encryption etc

Topic 7 Teachers note page 5

--	--	--	--	--	--	--

- (d). Explain why **Wired Equivalent Privacy (WEP)** has been deprecated and is considered obsolete by the modern wireless networking industry.

[3 marks]

because of fundamental architectural flaws that make it easy to crack using standard, readily available packet-sniffing tools. Topic 7 Teachers note page 11

- (e). Specify the expected trust levels and access privileges granted to each of the following groups in an organisation: Employees, Contractors, and Guests.

[3 marks]

Employees - most trusted, fully access
 Contractors - some trust is necessary, partial access
 Guests/third parties - least trusted, limited access Topic 10 Teachers note page 8

- (f). An organisation houses its web server inside a Demilitarised Zone (DMZ). The firewall is configured to block all traffic except HTTP and HTTPS. The internal router is configured with an outdated routing protocol (RIPv1), which broadcasts routing updates in plaintext across the local subnet without authentication. Identify a **Network Asset**, a **Network Vulnerability** present in this topology, and a potential **Network based Threat**.

[5 marks]

Network Asset (Any one of the following): -The web server inside the DMZ, internal router.
 Network Vulnerability: use of RIPv1
 Threat: A malicious actor conducting a packet sniffing or routing table poisoning attack
 Topic 10 Teachers note page 20

Index Number

--	--	--	--	--	--	--

3. (a). Transport Layer Security (TLS) is a combination of protocols working together to secure information communication.
- i. What is the Phase I of Handshake Protocol in TLS?

[2 marks]

ANSWER:

Establish Security Capabilities [TLS note slide 21]

- ii. Explain the objective of the Phase I of TLS Handshake protocol and list four (04) outcomes of it.

[5 marks]

ANSWER: Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers [TLS note slide 22]

- (b). What is the problem addressed by Kerberos Protocol?

[4 marks]

Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

[User Authentication slide 17]

Index Number

--	--	--	--	--	--	--

(c). Write down three (03) environmental shortcomings of **Kerberos V4**.

[3 marks]

Encryption system dependence, Internet protocol dependence, Message byte ordering, Ticket lifetime, Authentication forwarding, Inter-realm authentication
[User Authentication slide 28]

(d). Write down five (05) services provided by a **federated identity management system**.

[5 marks]

Point of contact, SSO protocol services, Trust services, Key services, Identity services, Authorization, Provisioning, Management [User Authentication slide 34]

(e). Write down three (03) authentication methods of **Extensible Authentication Protocol (EAP)**.

[6 marks]

EAP-TLS (EAP Transport Layer Security), EAP-TTLS (EAP Tunneled TLS), EAP-GPSK (EAP Generalized Pre-Shared Key), EAP-IKEv2 [User Authentication slide 37]

Index Number

--	--	--	--	--	--	--

4. (a). Using an example, explain why the communication in a **Virtual Private Network (VPN)** may not necessarily be encrypted.

[5 marks]

ANSWER: By definition Virtual Private Network can be described as a logical communication link that carries private traffic over public network. Examples for VPNs without encryption are MPLS, GRE Tunnels, L2TP, and IP Security Authentication Header protocol

[Virtual Private Networks slide 7, 9]

- (b). Write down five (05) selectors determining a **Security Policy Database (SPD)** entry in an IP Security VPN.

[5 marks]

ANSWER: Remote IP Address, Local IP Address, Next Layer Protocol, Name, Local and Remote Ports [Virtual Private Networks slide 27]

- (c). What is the IP Security protocol that provides your confidentiality for the communication.

[2 marks]

ANSWER: IP Security Encapsulated Security Payload (ESP) [Virtual Private Networks slide 30]

Index Number

--	--	--	--	--	--	--

- (d). Use the IPv4 packet structure to explain how **IP Security tunneling mode** can be distinguished from **IP Security transport mode**.

[5 marks]

ANSWER: Tunnel mode always has a new header in addition to old header

In Tunnel mode the IP Security header is placed between new IP header and old IP header where in transport mode the IP security header is placed between Original IP header and TCP header. [Virtual Private Networks slide 32]

- (e). What is referred to as **ISAKMP** in IP Security and what is the purpose of it?

[3 marks]

ANSWER: Internet Security Association and Key Management Protocol

The default automated key management protocol for IPsec [Virtual Private Networks slide 33]

Index Number

--	--	--	--	--	--	--

(f). Explain the difference between **internal compliance** and **external compliance**.

[5 marks]

ANSWER: Internal compliance refers to an organization's ability to follow its own rules, which are typically based on defined policies

External compliance refers to the need or desire for an organization to follow rules a [IT Infrastructure Auditing Concepts slide 14]
