

**UCSC****University of Colombo, Sri Lanka***University of Colombo School of Computing***DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY
(EXTERNAL)**Academic Year 2025 — 3rd Year Examination — Semester 6**IT6406 — Network Security and Audit***Structured Question Paper*

(2 Hours)

To be completed by the candidate**Index Number**

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

Important Instructions

- The duration of the paper is **2 hours**.
- The medium of instructions and questions is English. Students should answer in the medium of English language only.
- This paper has **4 questions** on **10 pages**. Answer **all** questions.
- All questions carry **equal** marks.
- Write your answers **only on the space provided** on this question paper.
- Do not tear off any part of this question paper. Under no circumstances may this paper (or any part of this paper), used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper. If a page or part of a page is not printed, please inform the supervisor/invigilator immediately.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries, smartwatches, and mobile phones, is not allowed.
- Non Programmable Calculators may be used.
- *All Rights Reserved*. This question paper can NOT be used without proper permission from the University of Colombo School of Computing.

**To be completed by
the examiners**

1	
2	
3	
4	
Total	

Index Number

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

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

[4 marks]

--

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

[4 marks]

--

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

[5 marks]

--

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]

--

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

[6 marks]

--

Index Number

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

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

[4 marks]

--

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

[6 marks]

--

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

[4 marks]

--

Index Number

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

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

[3 marks]

--

- (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]

--

- (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]

--

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]

--

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

[5 marks]

--

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

[4 marks]

--

Index Number

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

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

[3 marks]

--

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

[5 marks]

--

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

[6 marks]

--

Index Number

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

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

[5 marks]

--

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

[5 marks]

--

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

[2 marks]

--

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]

--

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

[3 marks]

--

Index Number

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

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

[5 marks]

--
