University of Colombo, Sri Lanka

University of Colombo School of Computing

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2022— 3^{rd} Year Examination — Semester 6

IT6406 — Network Security and Audit

Structured Question Paper

(2 (Two) hours)

To be completed by the candidate

Index Number □□□□□□□

Important Instructions

- The duration of the paper is **2 (Two) hours**.
- The medium of instructions and questions is English.
- This paper has **4** questions and **11** 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	

Index Number

1. (a). *Packet Filtering Firewall* is one of the firewall types. List down two (2) other types of firewalls.

[2 marks]

Stateful Inspection Firewalls, Application-Level Gateway, Circuit-Level Gateway, Topic 5 Teachers note page 6

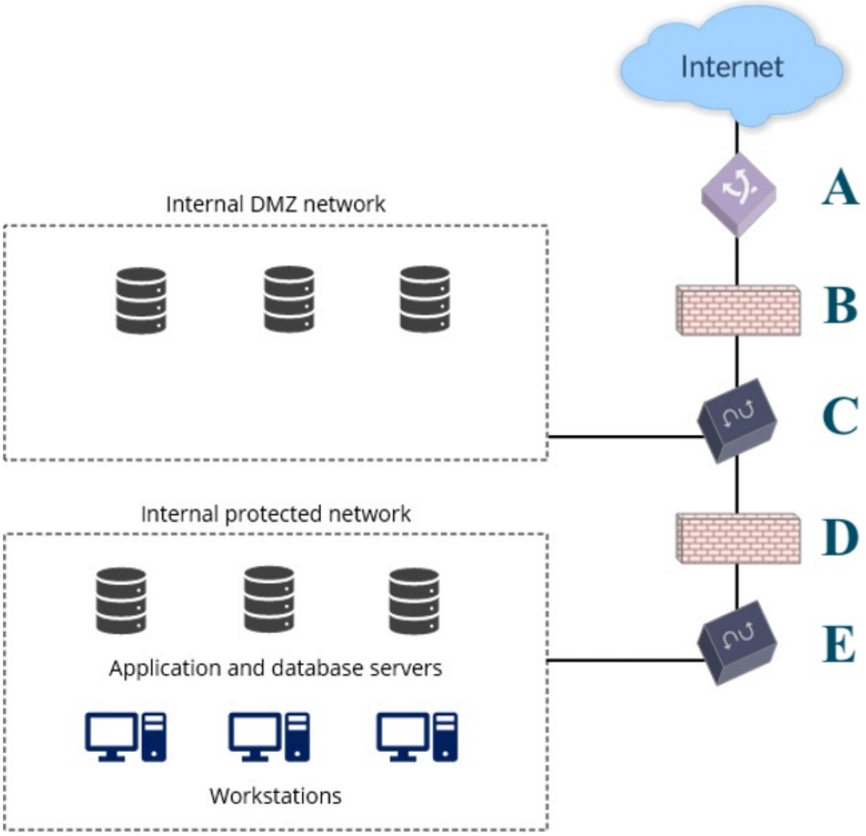
(b). Write down a core functionality of *Packet Filtering Firewalls*.

[4 marks]

ANSWER: Topic 5 Teachers note page 6

Applies a set of rules to each incoming and outgoing IP packets and forward or discard the packet.

(c). The following diagram shows the demilitarised zone (DMZ) network.



i. Name the components labeled as A, B, C, D, and E.

[5 marks]

ANSWER: A- boundary router, B - external firewall, C - LAN switch, D - Internal firewall, E - LAN switch

ii. Write down two (2) servers that can be placed in the Internal DMZ network

[4 marks]

ANSWER: Web servers, email servers, DNS servers

(d). Write the correct Linux commands that can be used to perform the following activities on an Ubuntu machine.

i. Check the status of the Ubuntu Firewall (UFW).

[1 marks]

ANSWER: sudo ufw status

ii. Allow communication through port 71.

[2 marks]

ANSWER: sudo ufw allow 71

iii. Disable the Ubuntu Firewall (UFW).

[2 marks]

ANSWER: sudo ufw disable

(e). List down two (2) security threats to wireless networks and describe one (1) of them.

[5 marks]

ANSWER: page 583-584 ref: 7th edition Accidental association, Malicious association, Ad hoc networks, Nontraditional networks, Identity theft (MAC spoofing), Man-in-the-middle attacks, Denial of service (DoS), Network injection, Eavesdropping, Unauthorized access

2. (a). Name three (3) essential characteristics of cloud computing.

[6 marks]

ANSWER: Broad network access, Rapid elasticity, Measured service, On-demand self-service, Resource pooling

(b). According to the NIST definition, briefly describe what is meant by **Platform as a Service (PaaS)** in a cloud environment?

[5 marks]

ANSWER: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS often provides middleware-style services such as database and component services for use by applications. In effect, PaaS is an operating system in the cloud.

(c). The **abuse and nefarious use** is a threat to cloud security. Briefly describe what it is.

[5 marks]

ANSWER: For many cloud providers, it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service.

(d). Name two (2) countermeasures that can be taken to minimise the threat in question (c).

[4 marks]

ANSWER: stricter initial registration and validation processes, enhanced credit card fraud monitoring and coordination, comprehensive introspection of customer network traffic, monitoring public blacklists for one's own network blocks (e). Using an appropriate diagram, illustrate how encryption can be used in a cloud environment to protect a database.

[5 marks]

ANSWER: Any appropriate diagram that indicates that the data stored in the database are encrypted. It is important to show that the cloud user needs to perform data encryption and decryption through the help of data owner's APIs where the cryptographic keys are maintained at the data owner's infrastructure (not in the cloud itself).

Index Number | | | | | | | |

3. (a). Threats on web applications can be categorized based on **confidentiality, integrity, and authentication**. Write one example of such threat for each category and for each threat write one consequence and one countermeasure with respect to web security to lessen the affect of such threat.

[9 marks]

ANSWER: Confidentiality: Eavesdropping on net (encryption), Thief of info from server (encryption), Theft of data from client (encryption) : Cons: Unintended information reveal
Integrity: Modification of user data (Using Hash verification), Modification of memory (Using Hash verification), Modification of message traffic (Using Hash verification) : Cons: Unauthorized modification
Authentication: Impersonation of legitimate users (Multiple means of authentication) : Cons: Identity theft

(b). Transport Layer Security (TLS) is not a single protocol but rather two layers of protocols above TCP.

i. Write three (03) sub protocols of Transport Layer Security (TLS).

[6 marks]

ANSWER: TLS Record protocol
Change Cipher Spec protocol
Alert protocol
Handshake protocol

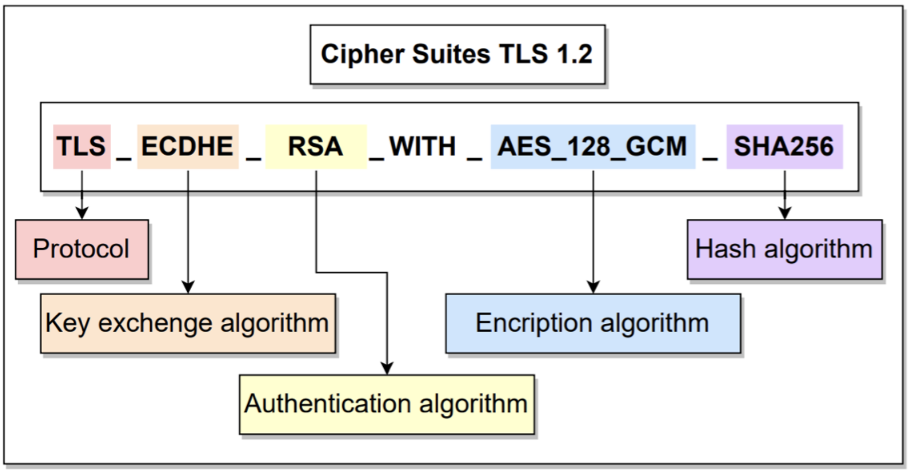
ii. Name the components of the given Cipher Spec.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Example answer: TLS denotes the protocol

[6 marks]

ANSWER:



(c). Write two (02) authentication methods supported by **User Authentication Protocol of Secure Shell (SSH)** .

[4 marks]

ANSWER: public key, host based, password

Index Number □□□□□□□

4. (a). Multiple factors or means of authentication are used to strengthen user authentication. Write four (04) means of authentication with one (01) example for each.

[8 marks]

ANSWER:
Something the individual knows: password, personal identification number (PIN)
Something the individual possesses: cryptographic keys, electronic keycards
Something the individual is (static biometrics): fingerprint, retina
Something the individual does (dynamic biometrics): recognition by voice pattern, handwriting characteristics

(b). Virtual Private Network (VPN) can be described as a logical communication link that carries private traffic over public network.

i. Write two (02) practical applications of VPNs.

[5 marks]

ANSWER:
Need of accessing private cooperate services from remote locations
Controlled/Private Access needed from many locations by different parties
Infrastructure requirements such as extended LANs

ii. Write two (02) VPN protocols that do not provide confidentiality.

[2 marks]

ANSWER:
MPLS, GRE Tunnels, L2TP

iii. Write the two (02) Security protocols defined in IP Security.

[2 marks]

ANSWER:
Authentication Header
Encapsulated Security Payload

(c). Write four (04) techniques used by crackers/hackers in learning passwords.

[8 marks]

ANSWER:
Try default passwords used with standard accounts
Exhaustively try all short passwords
Try words in the system's online dictionary
Collect information about users and try generating passwords
Tap the line between a remote user and the host system
Use a Trojan horse to bypass restrictions on access

______________ ********************** ______________