NESA NATIONAL EXAMINATION AND SCHOOL INSPECTION AUTHORITY

SPE - Cyber Security

T2-145

Thursday, 10 July 2025
8:30 AM to 11:30 AM

Names:.....

Index number:.....

TSS NATIONAL EXAMINATIONS, LEVEL 5, 2024-2025

QUESTIONS and ANSWERS BOOKLET

TRADE (s) : SOFTWARE PROGRAMMING AND EMBEDDED SYSTEMS (SPE)

SUBJECT: CYBER SECURITY

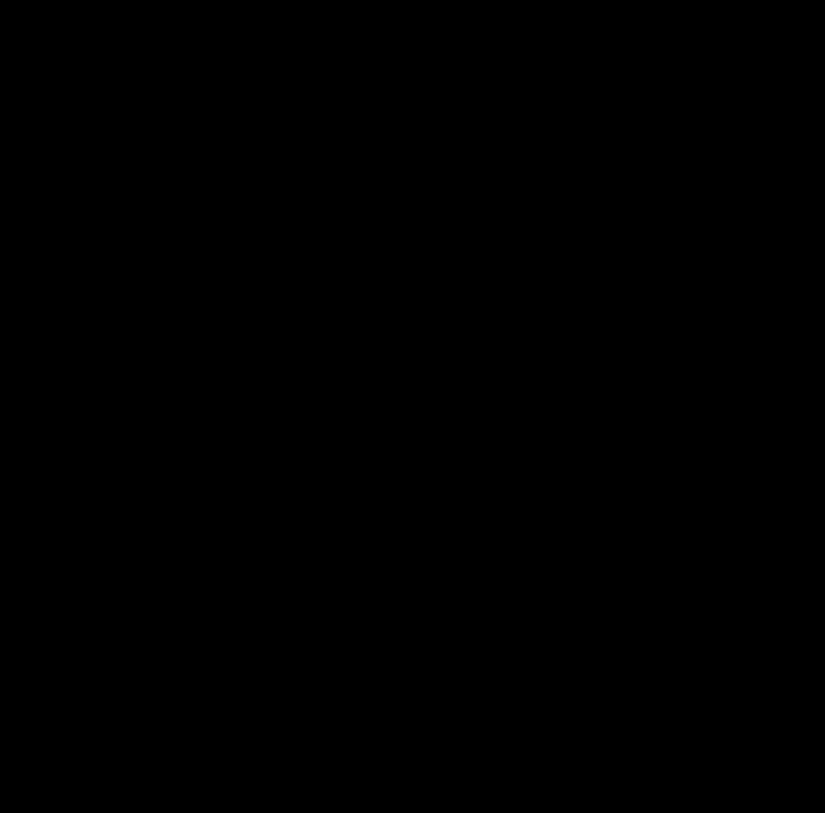
DURATION: 3 Hours

Read carefully the instructions on page 3

TOTAL MARKS...../100

FOR EXAMINER'S USE ONLY

QUESTIONS	1	2	3	4	5	6	7	8	9	10	Total
Marks											
QUESTIONS	11	12	13	14	15	16	17	18	19	20	Total
Marks											
QUESTIONS	21	22	23	24	25	26	27	28	29	30	Total
Marks											



T2-145_Cyber Security

TSS NATIONAL EXAMINATIONS, LEVEL 5, 2024-2025

TRADE: SOFTWARE PROGRAMMING AND EMBEDDED SYSTEMS (SPE)

SUBJECT: CYBER SECURITY

DURATION: 3 HOURS

INSTRUCTIONS TO CANDIDATES:

1. This Exam paper is composed of **three sections (A, B and C).** Follow the instructions given below and answer the indicated questions for a total of **100 marks.**

   Section **A:** Fourteen (14) questions which are **Compulsory** **55 marks**

   Section **B:** Among the five (5) questions, attempt any three (3) **30 marks**

   Section **C:** Among the two (2) questions, attempt anyone (1) **15 marks**

2. Fill in your actual **names** and **Index number** on the provided space (Cover).
3. Do not remove or tear any page or part of this Questions and Answers Booklet.
4. Answer in the language in which the Examination is set.
5. In section **A**, answer questions in the provided space. In case of multiple-choice questions, just **circle** the letter corresponding to the correct option.
6. In section **B** and **C**, answer questions in the provided space after section C questions.
7. **Allowed materials:**
   - Blue or Black pen.
   - Geometrical Instruments
   - Silent non-programmable calculators

SECTION A: Attempt all questions **(55 marks)**

---

01. Which of the following statements accurately describe IPv4 and IPv6? **(4marks)**
(Circle all that apply)

a) IPv4 uses 32-bit addresses which were getting lesser as the internet demand grows, while IPv6 uses 128-bit addresses
b) IPv6 includes built-in security features like encryption and authentication, whereas IPv4 was simply built without security prioritization
c) IPv4 supports more devices than IPv6 due to its larger address space.
d) IPv6 addresses are written in hexadecimal notation, while IPv4 addresses are written in dotted-decimal notations
e) IPv6 supports auto-configuration without DHCP, while IPv4 requires additional configurations

02. For each of the following sub-questions circle the letter corresponding to right option. **(4marks)**

a) How many bits are used in each segment in an IPv4 address?

i. 4 bits
ii. 8 bits
iii. 12 bits

b) How many hexadecimal digits are in the full IPv6 address?

i. 64
ii. 32
iii. 16

c) How many possible hosts can be on 192.168.0.1/24 subnet in IPv4?

i. 258
ii. 252
iii. 254

d) What is the compressed form of the IPv6 address 2001:0db8:0000:0000:0000:0000:0000:0001 ?

i. 2001:db8:0:0:0:0:0:1
ii. 2001:db8::1
iii. 2001::1
iv. 2001:db8::0001

03. A network administrator is configuring an IP addressing scheme for a growing enterprise network. The administrator is considering using Classless Inter-Domain Routing (CIDR) instead of traditional Classful IP addressing to optimize address allocation and improve scalability. Understanding the benefits of CIDR is essential for choosing the most effective addressing method for the network. **(4marks)**

Question:

Why is Classless Inter-Domain Routing (CIDR) preferred over Classful IP addressing in modern networks?

(Circle all that apply)

a) CIDR allows for more efficient IP address allocation by using variable-length subnet masks (VLSM).
b) Classful IP addressing provides better security than CIDR.
c) CIDR is only used in IPv6 networks, while classful addressing is for IPv4 networks.
d) Classful IP addressing is more flexible and scalable than CIDR.

04. A network administrator configured VLANs on multiple switches to segment traffic within the network. However, the administrator notices that hosts in the same VLAN on different switches cannot communicate with each other. The administrator is now troubleshooting the issue to identify the root cause and resolve the problem. **(4marks)**

Question:

Which of the following is the most likely cause of the issue where hosts in the same VLAN on different switches cannot communicate? (Circle all that apply)

a) The trunk ports between switches are not properly configured.
b) The VLAN was not assigned an IP address on the switch.
c) The STP protocol is blocking VLAN traffic.
d) The switch does not support multiple VLAN configurations.

05. **Assertion (A):** Passive reconnaissance is a crucial step in web application penetration testing as it helps attackers gather intelligence without alerting the target system. **(2marks)**

Reason (R): Passive reconnaissance involves actively scanning the target's network for open ports and services. (Circle the right answer)

A) Both A and R are true
B) A is true, but R is false.
C) A is false, but R is true.

06. For each of the following sub-questions circle the letter corresponding to right option. **(2marks)**

a) Which Android tool is most suitable for extracting the APK of a mobile application for static analysis?

i) ADB (Android Debug Bridge)
ii) OWASP ZAP
iii) METASPLOIT
iv) HYDRA

b) Which of the following is a risk when mobile apps store sensitive data in plaintext on the device?

i) Brute-force attacks on the server
ii) Root privilege escalation
iii) Local data leakage
iv) Remote code execution

07. Match each term in List A (OSI Model Components) with its correct description, network device, or protocol in List B (Functions/Protocols/Devices). **(5marks)**

Answer	***List A: OSI Model Components***	***List B: Functions/Protocols/Devices***
1 = ...	a) OSI Model History	1. A device used to connect different networks, making forwarding decisions based on IP addresses and routing tables.
2 = ...	b) Transport Protocol (TCP)	2. This protocol is connection- oriented, ensures reliable data transmission, and performs error checking
3 = ...	c) End Devices	3. The OSI reference model was developed to standardize network communication functions and support interoperability between different networking technologies.
4 = ...	d) Router	4. A protocol that provides faster communication with no connection setup, often used for real- time applications like video streaming
5 = ...	e) Transport Protocol (UDP)	5. These devices are like computers, printers, and phones that interface directly with the network and run applications.

08. An ISP assigns a 192.168.10.0/28 network to a small business. The administrator wants to determine the available subnet ranges. **(4marks)**

Which of the following are valid subnets for this network? (Circle all that apply)

a) 192.168.10.0 – 192.168.10.15
b) 192.168.10.16 – 192.168.10.31
c) 192.168.10.64 – 192.168.10.127
d) 192.168.10.240 – 192.168.10.255

09. Determine whether each of the following statements is ***True***(T) or ***False***(F) based on the understanding of WLAN devices, including access points, WLAN bridges, and controllers. **(5marks)**

a) Access points are devices that connect wireless devices to a wired network and typically require a controller for centralized management. .....
b) WLAN bridges are used to connect two separate wired networks, allowing wireless devices to communicate across them. .....
c) A controller is an optional device in a WLAN setup that helps manage multiple access points, providing features such as load balancing and security management. .....
d) WLAN devices such as access points and bridges should only be configured using command-line interfaces (CLI); graphical user interfaces (GUIs) are not supported for configuration. .....
e) In a WLAN, access points can be configured to support multiple SSIDs, allowing them to provide different wireless networks for different user groups. .....

10. Cybersecurity analyst is implementing encryption mechanisms to secure communications between two remote offices. The analyst decides to use asymmetric encryption to ensure secure data transmission over an untrusted network. **(4marks)**

Question:
Assertion (A): Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption.

Reason (R): In asymmetric encryption, the private key is used to encrypt while the public key is used to decrypt data.

Circle the correct option among the following.

a) Both A and R are true
b) A is true, but R is false.
c) A is false, but R is true.

11. A network engineer is tasked with designing an efficient subnetting plan for a large enterprise. The company requires internal secure networks, optimized IP allocation, and efficient routing. The engineer must apply the subnetting scheme following the best practices based on this. Which of the following is ***NOT*** a correct application of subnetting principles? **(4marks)**

a) Using a /28 subnet mask (255.255.255.240) to create 16 subnets in a Class C network.
b) Assigning an IP from the 172.16.0.0/12 range for a public-facing web server.
c) Using VLSM (Variable Length Subnet Masking) to optimize IP address allocation for different network segments.
d) Subnetting a 192.168.0.0/23 network to allow more than 254 hosts in a single subnet.

12. A network administrator has implemented a Router-on-a-Stick setup to enable Inter-VLAN Routing between VLAN 30 and VLAN 40. However, devices in VLAN 30 cannot communicate with devices in VLAN 40. Below is the router's configuration: **(4marks)**

```
interface g0/0
no shutdown
interface g0/0.30
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0

interface g0/0.40
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0
```

Question: Which skills should be applied to fix the issue?
(Circle all that apply)

a) Enable IP routing on the router.
b) Assign VLANs to the switch ports where end devices are connected.
c) Add a default route on the router.
d) Enable encapsulation on the physical interface instead of sub-interfaces.

13. A hacker gains access to a Wi-Fi network by exploiting weak encryption protocols or using a brute-force attack on the network's password, allowing the attacker to connect and access data transmitted over the network. Match the exploitation technique applied to the term described below in the following table: **(5marks)**

Description	Exploitation Technique	Answer
1) Capturing network traffic to analyze or steal data.	a) Man-in-the-Middle (MitM)	1=.....
2) Intercepting and altering communication between two parties.	b) Wi-Fi Hacking	2 =.....
3) Overloading a system or network to make it unavailable.	c) Packet Sniffing	3 =.....
4) A victim executes the attacker's script that allows a remote control of a system using a backdoor.	d) Denial of Service (DOS)	4 =.....
5) Exploiting weak encryption or passwords to access networks.	e) Reverse Shell	5 =.....

14. A security administrator is tasked with ensuring the authenticity of digital communications within a corporate network. The administrator is reviewing the components of a digital certificate to make sure that it contains all the necessary elements for secure communication. Which of the following components must be present in a digital certificate? **(4marks)**

(Circle all that apply)

a) The certificate authority's (CA) public key

b) A private key corresponding to the certificate's public key

c) The certificate holder's identity (e.g., organization name, common name)

d) A cryptographic hash of the certificate holder's public key, signed by the CA

Section B: Attempt any three (3) questions **(30 marks)**

---

15. A growing enterprise has recently expanded its network infrastructure and has implemented multiple VLANs to segment traffic. The network must support a large number of users and provide robust security measures. As network engineer, you have been tasked with choosing the most appropriate method for inter-VLAN routing to ensure performance, scalability, and security while minimizing costs. **(10marks)**

Question:

a) Analyze the advantages, limitations, and security of the following inter-VLAN routings:

i) Traditional inter-VLAN routing:
ii) Router-on-a-stick:
iii) Layer-3 switch inter-VLAN routing:

b) Provide a well-reasonable recommendation

16. You are an ethical hacker tasked with conducting a comprehensive vulnerability assessment for a large organization. The company is concerned about protecting its sensitive data, ensuring that its systems remain operational, and maintaining the integrity of its communications. **(10marks)**

Question:

a) Analyze how the following core principles of information security (CIA) align with the phases of ethical hacking.

i) Confidentiality:
ii) Integrity:
iii) Availability:

b) List only two (2) vulnerabilities based on nature

17. You are tasked with assessing the security posture of a web application used by a financial institution. The application handles sensitive customer data, including account information, transaction history, and personally identifiable information (PII). During your security audit, you identify that the application is vulnerable to both SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks. **(10marks)**

Question:

a) Analyze how the combination of SQL Injection (SQLi) and Cross-Site Scripting (XSS) vulnerabilities can be exploited together in a web application attack

b) What impact would such attacks have on both the integrity and confidentiality of the web application?

c) Discuss the potential risks and consequences for the application's security.

18. You are a network administrator and your task is to design the IP addressing scheme and routing protocol for a large corporate network consisting of multiple subnets with varying size requirements. You need to select an appropriate routing protocol to ensure optimal routing performance, scalability, and efficient IP address utilization. You also need to evaluate classful and classless routing protocols to determine the most suitable solution. The three routing protocols: RIPv2, EIGRP, and OSPF are considered. **(10marks)**

Question:

a) Assess the differences between classful and classless routing protocols, focusing on their impact on IP addressing and network design.

b) Considering the need for multiple subnets of varying sizes, how would you evaluate the suitability of RIPv2, EIGRP, and OSPF for this network?

c) Discuss how factors such as scalability, summarization and protocol efficiency influence the decision-making process.

19. You are setting up a company network using multiple switches and VLANs (Virtual Local Area Network). To make the network faster, secure and organized, you will use: **(10marks)**

- VLANs to separate traffic
- VTP (VLAN Trunking Protocol) to share VLAN info
- STP (Spanning Tree Protocol) to prevent loops

a) Explain the role of VLANs, VTP, and STP in improving the efficiency and security of a network

b) Mention Two (2) measures for each step that can be taken to protect the network from attacks like VLAN hopping and MAC flooding

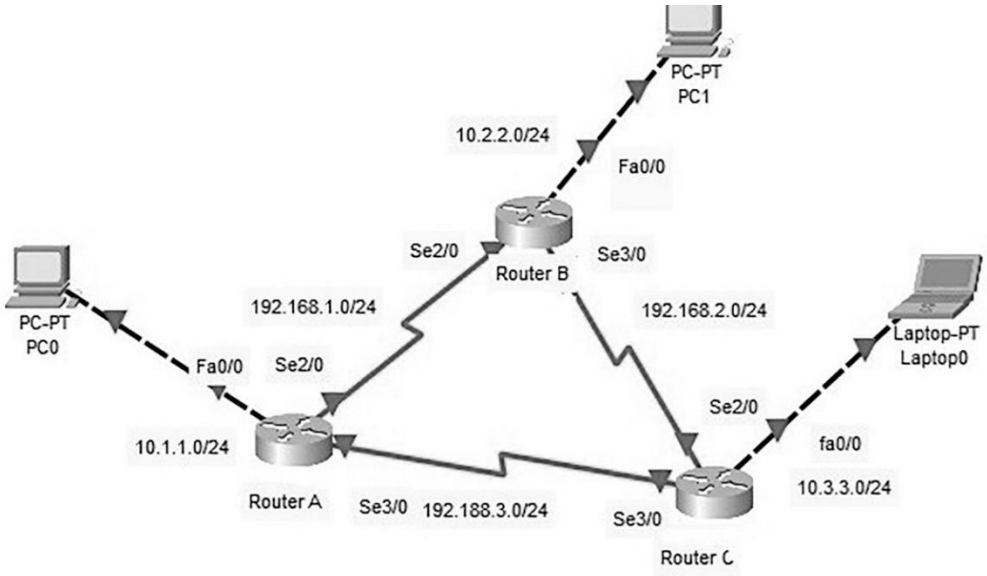
Section C: Attempt only one (1) question **(15 marks)**

---

20. You have a network with three routers: Router A, Router B, and Router C. Each router is connected to different networks. **(15marks)**

Your task is:

i) To assign IP addresses to devices interfaces (including PCs).
ii) To configure both EIGRP and Static Routing to enable communication between all networks and test.
iii) To check the EIGRP neighbors.
iv) To check the routing tables to test connectivity between networks from the work stations in LAN A, B and C .



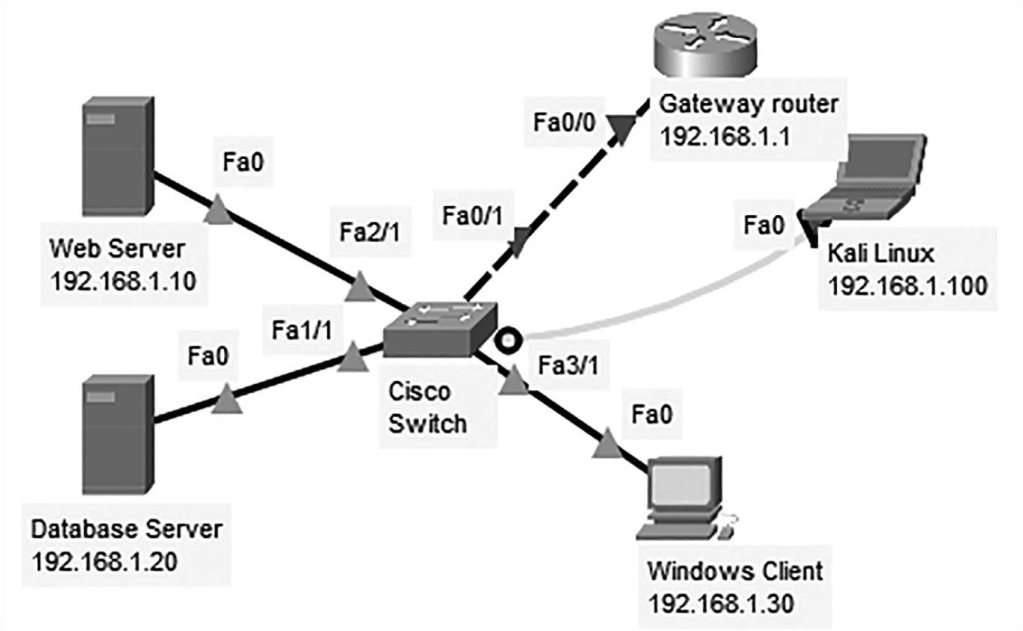
IP Addressing Scheme:

Network	**IP Address Range**	**Subnet Mask**	**Connected Routers**
Network 1	192.168.1.0/24	255.255.255.0	Router A - Router B
Network 2	192.168.2.0/24	255.255.255.0	Router B - Router C
Network 3	192.168.3.0/24	255.255.255.0	Router A - Router C
LAN A	10.1.1.0/24	255.255.255.0	Connected to Router A
LAN B	10.2.2.0/24	255.255.255.0	Connected to Router B
LAN C	10.3.3.0/24	255.255.255.0	Connected to Router C

21. You are a penetration tester assigned to perform reconnaissance on a company's internal network. The network administrator provided a guest subnet (192.168.1.0/24) to test security vulnerabilities. Your task is to: **(15marks)**

1. Gather information about the network (Passive Reconnaissance)
2. Identify active devices, open ports, and running services (Active Reconnaissance & Scanning)

Network Topology



Company Network Setup:

- Router (Gateway: 192.168.1.1)
- Web Server (192.168.1.10) – Hosting the company's website
- Database Server (192.168.1.20) – Storing user data
- Windows Client (192.168.1.30) – Employee workstation
- Kali Linux Attacker Machine (192.168.1.100) – Your PenTesting machine.

END

RESERVED SPACE FOR SECTION B AND C ANSWERS

Do not write in this margin

Do not write in this margin

Do not write in this margin

Do not write in this margin

Do not write in this margin

Do not write in this margin

Do not write in this margin

Do not write in this margin