U.S.N.										

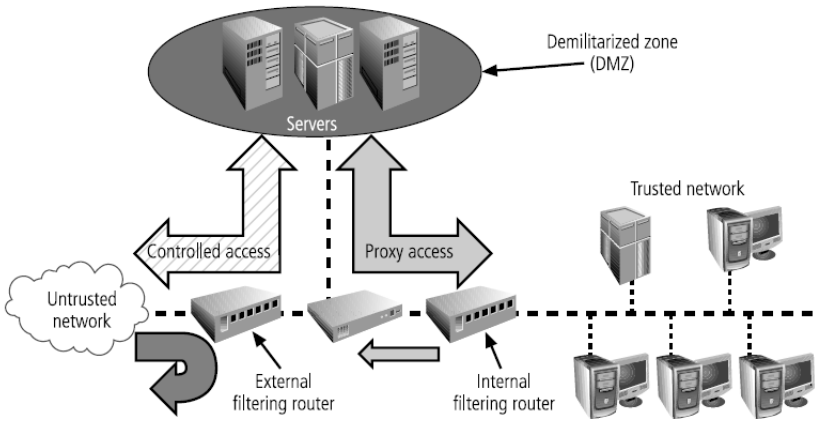
B.M.S. College of Engineering, Bengaluru-560019

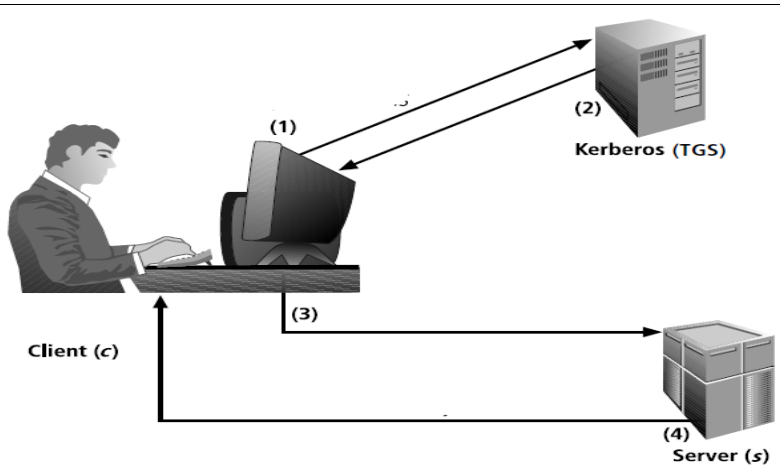
Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E. **Semester: VII**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 22IS7PEISF **Max Marks: 100**
Course: Information Security and Forensics

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

		UNIT – I	*CO*	*PO*	Marks
1	a)	Discuss the mechanisms of access control systems that determine whether to admit a user into a trusted area of an organization, emphasizing their role in ensuring security.	*CO1*	*PO1*	**8**
	b)	Discuss the relationship between different types of firewalls (e.g., application gateways, circuit gateways, packet filtering, and MAC layer firewalls) and their corresponding layers in the OSI model, explaining the functionality that is provided at its respective layer.	*CO1*	*PO1*	**9**
	c)	Outline the key factors to consider when selecting the best firewall for an organization.	*CO1*	*PO1*	**3**
		OR			
2	a)	Identify and explain the given firewall architecture with its merits.  	*CO1*	*PO2*	**7**

		b)	Summarize the best practices for configuring and maintaining firewalls to ensure optimal security and performance in an organization's network infrastructure.	*CO1*	*PO1*	**5**
		c)	 Identify the purpose of the given diagram by providing details of steps (1- 4) listed in it.	*CO1*	*PO2*	**8**
			UNIT – II			
	3	a)	A XYZ Bank experiences unusual traffic patterns, such as a sudden spike in inbound connections from unfamiliar IP addresses. Suggest various detection methods that IDPS can use to effectively monitor, evaluate and identify potential threats in the network traffic to ensure security and prevent unauthorized access.	*CO1*	*PO2*	**9**
		b)	Illustrate the importance of scanning and analysis tools by elaborating any one tool of your choice.	*CO1*	*PO1*	**5**
		c)	An organization needs to adopt biometric authentication for its employee access to secure areas. Identify and elaborate the three fundamental criteria's to be used by the organization to evaluate the effectiveness of the biometric technology in terms of accuracy, reliability and user acceptance in prior to actual access to these secure systems.	*CO1*	*PO1*	**6**
			OR			
	4	a)	A healthcare organization experiences repeated unauthorized access attempts on its critical patient database. It needs a security mechanism that can be implemented to redirect attackers away from sensitive systems, monitor their activities and keep them engaged long enough for security teams to document their behavior and plan an appropriate response. Suggest and explain a suitable technology that can be implemented for the above scenario.	*CO1*	*PO2*	**6**

		b)	Illustrate the role of a Network-based Intrusion Detection and Prevention System (IDPS) in monitoring network traffic and detecting potential attacks.	*CO1*	*PO1*	**6**
		c)	A large retail chain is monitoring its network across multiple locations, and it needs to have all its IDPS control functions implemented and managed from a central location which impacts the efficiency and effectiveness of detecting and responding to potential security threats in real-time. Suggest the IDPS Control strategy that can be incorporated for above needs and describe the same with a relevant diagram.	*CO1*	*PO2*	**8**
			UNIT – III			
	5	a)	Justify the statement "Audit logs are important in investigations".	*CO2*	*PO1*	**5**
		b)	An organization is concerned about the security of their IIS logs and wants to ensure that they are maintained in a credible state. Identify the steps to be considered to ensure that their IIS logs are credible and can be used as evidence in an investigation.	*CO2*	*PO1*	**10**
		c)	Describe the basic procedures of End-to-end forensic investigation.	*CO4*	*PO1*	**5**
			OR			
	6	a)	Define Network Forensics. Explore the methods used by network intruders to enter a system.	*CO2*	*PO1*	**10**
		b)	"In the event of a ransomware attack on an organization's network, identifying log files to review for insights into the breach and using this data to trace the attack's origin and enhance protection against future threats is vital", Elaborate the above statement by depicting the source and traces of attack with suitable reasoning with respect to log file as evidence of proof in legal terms.	*CO2*	*PO2*	**10**
			UNIT – IV			
	7	a)	List and describe any three primary types of network attacks and justify the need for investigators to analyze network traffic.	*CO3*	*PO1*	**8**
		b)	A customer of PQR Bank is trying to log into his bank's website by entering the URL in browser. Instead of reaching the official website, its unknowingly redirected to a fake site that looks identical to bank's website. Believing it to be genuine, he enter his login credentials, which are instantly captured by attackers. Explore in detail the techniques with its relevant diagrams that the attackers might use to manipulate the DNS system to create such scenarios, redirecting users to fraudulent websites and leading to stolen credentials or financial losses.	*CO3*	*PO2*	**12**
			OR			
	8	a)	An analyst of an organization found a broken system when the hackers posted the user identities of about 700 million people. Later, he	*CO3*	*PO2*	**10**

			collected several log files as proof. Now the analyst needs to authenticate the collected evidence so that it is admissible in court. Elaborate the challenges he should look towards for gathering evidence for a network inquiry from all technical sources.			
		b)	Mention the difficulty in reconstructing evidence for a network investigation. Review the three types of analysis that an investigator must perform during evidence reconstruction.	***CO4***	***PO1***	**10**
			UNIT – V			
	9	a)	Identify the potential types of web attacks (Any Five)	***CO4***	***PO1***	**5**
		b)	A cybersecurity analyst is investigating a data breach at a news website. Users report that malicious pop-ups and phishing pages appear whenever they view the comment section of articles. Upon investigation, analyst discovers that an attacker has injected a harmful script into the user-generated comments, targeting visitors with unauthorized actions and stealing sensitive information. Based on the above situation • Identify the cause of a problem • Suggest prevention method to this type of attack from reoccurring.	***CO4***	***PO2***	**8**
		c)	Discuss the conditions under which a buffer overflow takes place. Provide its potential impact on a system and the methods used to detect it.	***CO4***	***PO1***	**7**
			OR			
	10	a)	Illustrate the web attack by “Parameter Tampering”.	***CO4***	***PO1***	**5**
		b)	You are responsible for maintaining a university’s online portal where students can log into view their grades. A student reports that by entering specific characters into the login form, they were able to access another student’s records. Upon investigation, you find suspicious database queries being executed in the logs, containing unexpected inputs like ' OR '1'='1. • Identify the cause of this vulnerability, • Suggest measures need to be considered to secure the portal.	***CO4***	***PO2***	**10**
		c)	Provide measures that need to be considered to increase web security by an investigator or administrator as a part of checklist in his daily routine.	***CO4***	***PO1***	**5**

****