U.S.N.										

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

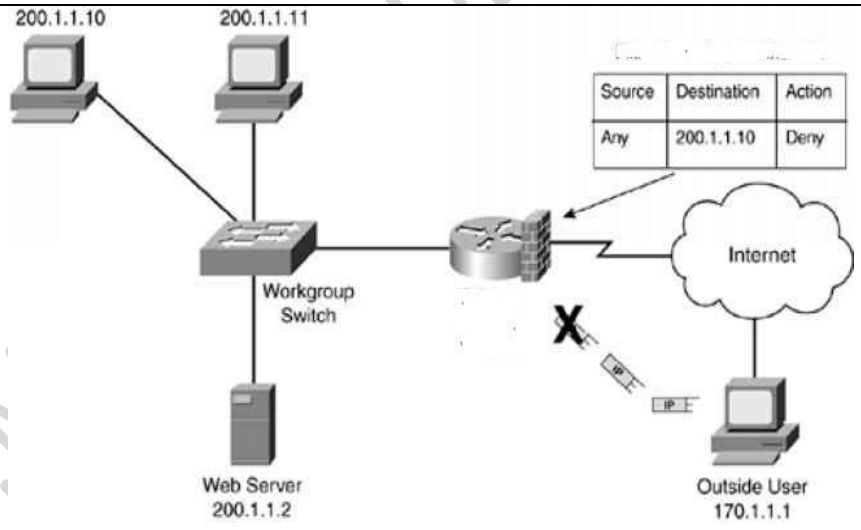
Autonomous Institute Affiliated to VTU

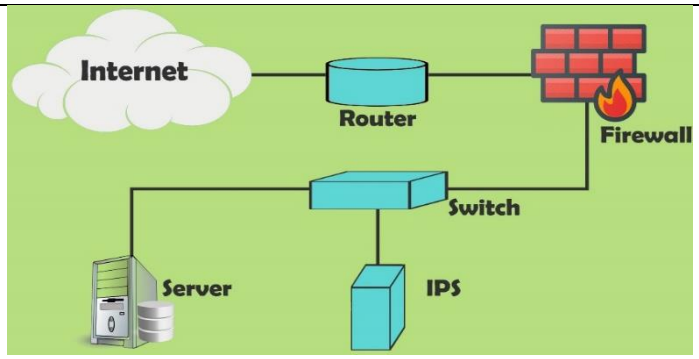
January 2024 Semester End Main Examinations

Programme: B.E. **Semester: VII**
Branch: Information Science and Engineering **Duration: 3 hrs.**
Course Code: 20IS7PCISF **Max Marks: 100**
Course: Information Security and Digital Forensics

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

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	CO	PO	Marks
1	a)	Illustrate sample Firewall Rules and their Format.	CO2	PO1	**06**
	b)	Why firewall is required? Based on what criteria you select the firewall. Justify with your answer.	CO3	PO2	**06**
	c)	What is a VPN? Explain Transport Mode VPN and Tunnel Mode VPN.	CO1		**08**
		OR			
2	a)	 Figure 1 Identify the type of firewall used in Figure 1. Illustrate how it decides whether to drop or forward the packet to the next network connection.	CO2	PO1	**06**
	b)	Distinguish between: i) Authentication and Authorization ii) RADIUS and TACACS.	CO1		**06**
	c)	How various types of firewalls interact with the network traffic at various levels of the OSI model? Provide your answer.	CO2	PO1	**08**

			UNIT - II			
	3	a)	 Figure 3(a) i) Identify the type of IDPS for monitoring and analysing the internals of computing system in the above diagram ii) Provide the advantages and disadvantages of the identified IDPS.	*CO2*	*PO1*	**08**
		b)	Explain the scanning and analysis tools that are commonly used in an organization to monitor the attacks.	*CO2*	*PO1*	**06**
		c)	The Safe Deposit Locker system in XYZ bank has upgraded from Traditional Access of Lockers to a Biometric Access Control System to use Safe Deposit Locker by their customers securely. Now, the bank needs to assess the effectiveness of Biometric implemented in a bank before it can be used in real-time by customers. Illustrate with an example how the following criteria can be assessed • The percentage of users who are in fact authorized users but are denied access. • The percentage of users who are unauthorized but are granted access. • The level at which both the above errors can be equalized.	*CO2*	*PO1*	**06**
			OR			
	4	a)	Identify the Strengths and Limitations of IDPSs.	*CO1*		**06**
		b)	Why honeypots are designed? What are the advantages and disadvantages of using the honeypot?	*CO2*	*PO1*	**08**
		c)	Summarize the possible Biometric authentication technologies. How certain biometrics rank in terms of effectiveness and acceptance.	*CO2*	*PO1*	**08**
			UNIT - III			
	5	a)	Define Network forensics. Identify the methods that are used by Network intruders to enter a system.	*CO3,1*	*PO2*	**08**
		b)	Signify the importance of Log files in network forensics? Illustrate the legal issues involved with creating and using logs that organizations and investigators must keep in mind.	*CO3,1*	*PO2*	**08**

		c)	A financial company "XYZ Payment Systems", has suffered a network security breach wherein the customer's debit and credit card data are leaked resulting in the compromise of Personal Identifiable Information impacting 2,200 people. The company needs to perform a forensic investigation to determine the cause and extent of the breach. i) Identify the series of steps to be taken in the investigation process ii) List the various sources for evidence collection	*CO1,2,3*	*PO1,2*	**06**
			UNIT - IV			
	6	a)	Explain any four network attacks.	*CO1*		**08**
		b)	Can you tell the effect of DNS spoofing? Illustrate the types of DNS poisoning techniques.	*CO3*	*PO2*	**08**
		c)	Identify the three fundamentals of reconstruction for investigating a crime.	*CO1*		**06**
			UNIT - V			
	7	a)	What are the indications of a web attack?	*CO1*		**04**
		b)	Explain Cross-site scripting (XSS), cookie poisoning and cookie snooping attacks.	*CO1*		**08**
		c)	Identify are the tools that can be used to find the static IP address of a particular host. Also, Interpret the checklist of an investigator or administrator for Web security.	*CO2*	*PO1*	**08**

****