Name: Enrolment No:	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2018

Programme Name: B. Tech. (CS+CSF) **Semester :** ODD-2018-19 (VII)
Course Name : IT Network Security **Time :** 03 hrs
Course Code : CSIB442 **Max. Marks :** 100
Nos. of page(s) : 02

Instructions: Attempt all questions

SECTION A

S. No.		Marks	CO
Q 1	Define Security Policy. What are common security policies, regulations and standards? Discuss Internet access policies in detail.	4	CO1
Q 2	What do you understand by Physical Security? List various factors affecting physical security. Differentiate various physical security controls: administrative controls, physical controls and technical controls.	4	CO3
Q 3	Describe some of the physical security measures in your university. Express them in terms that could be implemented in a computerized door locking system.	4	CO4
Q 4	List common threats specific to host security. What are the sources of these threats? Discuss various baseline security measures that you will take to protect your host from these threats.	4	CO2
Q 5	Compare and contrast wireless network threats: war driving, rogue access point attack, denial-of-service attack and WEP cracking.	4	CO1

SECTION B

Q 6	What is an Intrusion Detection System? List various functions of Intrusion detection. Differentiate between Host and Network Intrusion detection systems. Give examples of few attacks detected by network and host intrusion detection systems.	10	CO4
Q 7	Explain each of the following security concepts: confidentiality, privacy, trust and assurance. Why is it necessary to prevent forgery of capabilities in capability systems to meet reference monitor guarantees? Specify the conditions under which it is necessary to weaken (reduce) the permissions available to a capability.	10	CO3
Q 8	What is Redundant Array of Independent Drives (RAID)? Discuss advantages of RAID briefly. List and briefly explain various RAID levels.	10	CO2 & CO3
Q 9	What are viruses? How do viruses spread? What are some controls that could be implemented for viruses? What are the different types of virus detection techniques? **OR**	10	CO1, CO2 & CO3

	Write short note on various IDS approaches: signature-based detection, anomaly-based detection, misuse detection, behavior-based detection, protection-based detection, structure-based detection and analysis timing based detection.		
	SECTION-C		
Q 10	How is Virtual Private Network (VPN) connection better than a conventional point-to-point connection? What are the benefits of choosing an internet-based VPN over a point-to-point T1 connection? Discuss the process of establishing a VPN connection. Suppose you are working from home via a Virtual Private Network connection. From your remote internet connection you enters an ISP's login page. Once logged in, the ISP's owned device creates a secure tunnel straight to the main offices enterprise network. What kind of VPN is this? **OR** Write short notes (maximum 100 words) on each of the following topics a) Risk Management Phases: Identification, assessment and tracking and review. b) Internal and external vulnerability assessments. c) Redundant Array of Independent Disks (RAID) Technology. d) Types of Network Security Attacks: reconnaissance, access, denial-of-service and malware attacks. e) Types of authentication: password, two-factor, biometrics, smart card and single sign on (SSO).	**20**	**CO1, CO2, CO4**
Q 11	Answer the following questions: a) Differentiate between internal, external, unstructured and structured threats with the help of neat and clean diagram. b) How an administrator analyzes network traffic using monitoring and analysis tool. Differentiate between various router and non-router based monitoring techniques. c) Compare and contrast a worm and a virus. List various controls for worms? When comparing the source code for the worm to the virus, what do you notice?	**20**	**CO1, CO2 & CO3**

Name: Enrolment No:	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2018

Programme Name: B. Tech. (CS+CSF) **Semester :** ODD-2018-19 (VII)
Course Name : IT Network Security **Time :** 03 hrs
Course Code : CSIB442 **Max. Marks :** 100
Nos. of page(s) : 02

Instructions: **Attempt all questions**

SECTION A

S. No.		Marks	CO
Q 1	How hierarchy of security policy is helpful in meeting organization's security requirements? Discuss with an example and give two good policy statements.	4	CO1
Q 2	Differentiate between RAID 3 and RAID 5. How many minimum disk drives are needed for R1, R3, R5, R10 and R01?	4	CO3
Q 3	What kind of network security policies, do we need for a university. Explain with an example.	4	CO4
Q 4	Differentiate between Enterprise Information Security Policy (EISP), Issue Specific Security Policy (ISSP) and System Specific Security Policy (SSSP).	4	CO2
Q 5	How much harmful are reconnaissance, access, denial-of-service and malware attacks. Discuss each of these attack with a scenario.	4	CO1
	SECTION B		
Q 6	Define Intrusion. What are different indications of an intrusions? Why do we need an intrusion detection and prevention system? List various activities of IDS. Draw an IDS working architecture with neat and clean diagram. Differentiate between various components of an IDS system.	10	CO1 & CO2
Q 7	What is firewall? Explain different types of firewall. List various design goals for a firewall. Discuss various techniques used by firewalls to control access and enforce a security policy.	10	CO3
Q 8	Does location and architecture considerations, fire-fighting systems, physical barriers, security personnel, physical locks, concealed weapon/contraband detection devices, mantrap, alarm system, video surveillance and lighting system falls under physical security controls? If yes, elaborate these controls with their features.	10	CO2 & CO3
Q 9	What is meant by Risk Management? List the components of Risk Management. Explain Risk control strategies in detail. **OR** What is a worm? What is the main difference between a worm and a virus? What are some controls for worms? When comparing the source code for the worm to the	10	CO1, CO2 & CO4

	virus, what do you notice?		
SECTION-C (Attempt any one)			
Q 10	Differentiate between following categories: a) Wireless network threats: war driving, rogue access point attack, denial-of-service attack and WEP cracking. b) Wireless antennas: directional antenna, omnidirectional antenna, parabolic grid antenna, yogi antenna, dipole antenna, reflector antennas. c) WPA2 Encryption: WPA2-Personal and WPA2-Enterprise. d) Wifi Authentication Methods: Open System Authentication and Shared Key Authentication. e) Deploying a Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS). **OR** Answer the following questions: a) Is network traffic monitoring and analysis ethical? Discuss its advantages. Differentiate between router and non-router based monitoring techniques. b) How bandwidth monitoring different from network monitoring. List various best practices for an administrators considering current and future bandwidth needs. c) Define Risk Management. Discuss various key roles and responsibilities in risk management. Give examples of few key risk indicators.	**20**	**CO1, CO2, CO3**
Q11	Why Virtual Private Network (VPN) connection is better than a conventional point-to-point connection? Discuss the benefits of choosing an internet-based VPN over a point-to-point T1 connection? Identify and explain the process of establishing a VPN connection. Suppose you are working from home via a Virtual Private Network connection. From your remote internet connection you enters an ISP's login page. Once logged in, the ISP's owned device creates a secure tunnel straight to the main offices enterprise network. What kind of VPN is this?	**20**	**CO1, CO2, CO4**