Name:

Enrolment No:

UPES

UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2021

Course: IT Network Security **Semester: IV**

Program: B.Tech CSE with spz in CSF **Time 03 hrs.**

Course Code: CSSF2008 **Max. Marks: 100**

Instructions: Use headings, quotation, and paragraphs to support your explanations if possible.

SECTION A

S. No.		**Marks**
Q 1	2. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former. a) True b) False	**CO1 5**
	3. What are two problems that can be caused by a large number of ARP request and reply messages? a. All ARP request messages must be processed by all nodes on the local network. b. A large number of ARP request and reply messages may slow down the switching process, leading the switch to make many changes in its MAC table. c. The network may become overloaded because ARP reply messages have a very large payload due to the 48-bit MAC address and 32-bit IP address that they contain. d. The ARP request is sent as a broadcast, and will flood the entire subnet. e. Switches become overloaded because they concentrate all the traffic from the attached subnets.	
Q 2	1.Which network monitoring tool saves captured network frames in PCAP files? a) NetFlow b) Wireshark c) SNMP d) SIEM	**CO1 5**
	2.A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as ___________ a) Chock point b) Meeting point c) Firewall point d) Secure point	

	3.Which of the following statements is NOT true concerning VPNs? a) Financially rewarding compared to leased lines b) Allows remote workers to access corporate data c) Allows LAN-to-LAN connectivity over public networks d) Is the backbone of the Internet	
Q 3	1.Which protocol is used by the traceroute command to send and receive echo-requests and echo-replies? a. SNMP b. ICMP c. Telnet d. TCP	**CO2** **5**
	2.Network layer firewall works as a ___________ a) Frame filter b) Packet filter c) Content filter d) Virus filter	
	3.Traffic in a VPN is NOT _____________ a) Invisible from public networks b) Logically separated from other traffic c) Accessible from unauthorized public networks d) Restricted to a single protocol in IPsec	
Q 4	1.A network security specialist is tasked to implement a security measure that monitors the status of critical files in the data center and sends an immediate alert if any file is modified. Which aspect of secure communications is addressed by this security measure? a. origin authentication b. data integrity c. nonrepudiation d. data confidentiality	**CO3** **5**
	2.What are the three-impact metrics contained in the CVSS 3.0 Base Metric Group? (Choose three.) a. confidentiality b. remediation level c. integrity d. attack vector e. exploit f. availability	
Q 5	1. What is a purpose of entering the nslookup cisco.com command on a Windows PC? a. to check if the DNS service is running b. to connect to the Cisco server c. to test if the Cisco server is reachable d. to discover the transmission time needed to reach the Cisco server	**CO4** **5**

	2.What tells a firewall how to reassemble a data stream that has been divided into packets? a) The source routing feature b) The number in the header’s identification field c) The destination IP address d) The header checksum field in the packet header	
Q 6	1.Use Caesar’s Cipher to decipher the “HQFUBSWHG WHAW” a) ABANDONED LOCK b) ENCRYPTED TEXT c) ABANDONED TEXT d) ENCRYPTED LOCK	**CO1** **5**
	2.At which two traffic layers do most commercial IDSes generate signatures? a) Application layer and Network layer b) Network layer and Session Layer c) Transport layer and Application layer d) Transport layer and Network layer	
	SECTION B	
Q 7	What protocol or technology defines a group of routers, one of them defined as active and another one as standby?	**CO1** **10**
Q 8	What are the two types of VPN connections? (Briefly explain each of them)	**CO2** **10**
Q 9	What are the 3 As of security functions in AAA server ?	**CO3** **10**
Q 10	Where is the domain controller?	**CO3** **10**
Q 11	What are the steps in the DORA process for implementing a fixed IP address through a DHCP server?	**CO4** **10**
	SECTION-C	
Q 12	Regarding the TCP / IP model, explain the layers to be protected, and give two examples of known attacks and the ways in which these attacks can be protected (select attacks from different layers in the model) OR Explain the NAT service, its characteristics and methods of operation, then explain how it relates to the limitations of IPV4 and what are the characteristics of IPV6 that do not require NAT.	**CO1** **20**