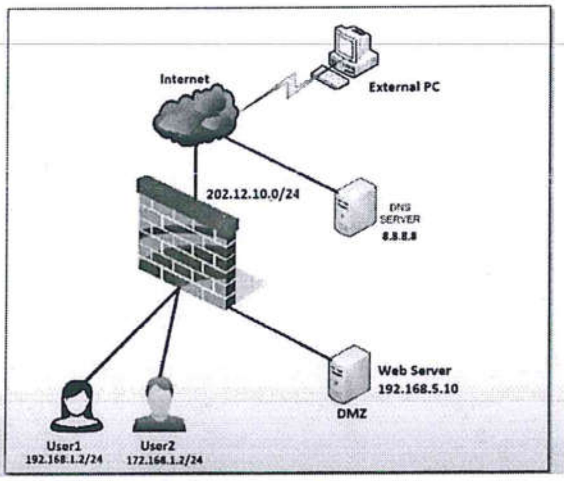
PES UNIVERSITY, BENGALURU-560085 **UE17CS331**

(Estd. Under Karnataka Act 10 of 2013)

DECEMBER 2020: END-SEMESTER ASSESSMENT (ESA) B.Tech – VI SEMESTER
UE17CS331 –COMPUTER NETWORK SECURITY

Time: 3 Hrs Answer All Questions Max Marks: 100

1.	a)	Define Information Security. What are the assets of a computer system?	4
	b)	What is Packet sniffing? How packets are received in promiscuous mode and in monitor mode?	10
	c)	Differentiate between a Vulnerability, a risk and a threat. What is CIA Triad?	6
2.	a)	What is a firewall? Describe in detail about the three important types of firewall depending on the mode of operation.	10
	b)	Describe the working of local DNS Cache Poisoning attack.	10
3.	a)	You have intrusion detection software that can monitor the activity and identify suspicious activity based on past experience. What type of analysis is being performed? Explain in detail.	6
	b)	What is the purpose and role of DMZ in network security?	7
	c)	What is a Three-way handshake? How can it be used to create a DoS attack? State the countermeasure for DoS attack.	7
4.	a)	An ACL protects access to objects in your system by ensuring that only authorized users can access certain functions and stored objects. An access control list consists of a set of ACL rules. An ACL rule is the combination of one user ID or one user group and one privilege set. Consider yourself as the System Administrator of PES University. Create a complete set of ACLs for PES University.	6
	b)	You are the Chief Information Officer (CISO) for ABC company. The recent security audit report shows the deficiencies in the organization personnel security controls. Apart from employee awareness training and security policy document, what principles would you implement to improve the personnel security of your organization?	6

	c)	The security administrator has installed a new firewall which implements an implicit DENY policy by default click on the firewall and configure it to allow ONLY the following communication. Tabulate the rules for the following firewall requirements (include Rule#, Source, Destination, Port, Protocol and Action).  Internet External PC 202.12.10.0/24 DNS SERVER 8.8.8.8 Web Server 192.168.5.10 DMZ User1 192.168.1.2/24 User2 172.168.1.2/24 1. **Allow all HTTP traffic to a web server with an IP of 192.168.5.10.** Note that while HTTP traffic typically uses TCP, it can also use UDP. Because of this IP is used instead of TCP or UDP. 2. **Allow all HTTP and HTTPS traffic to a web server with an IP of 192.168.5.10. This requires two rules. One rule allows HTTP traffic by allowing port 80, and the second rule allows HTTPS traffic by allowing port 443.** 3. **Allow DNS queries from User1 to a computer with an IP of 8.8.8.8. DNS name resolution queries use UDP port 53.** 4. **Block DNS zone transfer traffic from any source to any destination. DNS zone transfers use TCP port 53.** 5. **Allow DNS queries from User2 to a computer with an IP of 8.8.8.8. DNS name resolution queries use UDP port 53.**	8
5.	a)	What is Bluetooth? Describe the different flavors of Bluetooth technology in detail.	10
	b)	Write a short note on IEEE 802.11i robust security standard concepts and architecture for wireless LANs.	10