



PES University, Bengaluru
(Established under Karnataka Act No. 16 of 2013)

Dec 2021: End Semester Assessment
B.TECH. V Semester Elective CSE
UE19CS326: Computer Network SECURITY

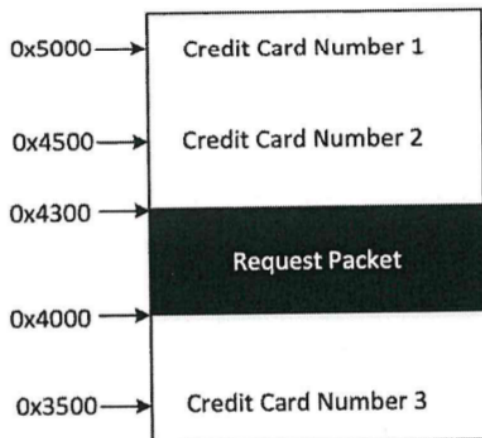
Time: 180 Mins

Answer All Questions

Max Marks: 100

Questions		Marks
Q1A	To establish a TCP connection, Dr. Rama first sends a SYN packet with Seq = 980 to the server and receives a SYN-ACK packet with Seq = 603;Ack = 981. What packet should Dr. Rama include in the next packet to complete the TCP handshake?	2
Q1B	Decide if the following statements are True or False with an explanation of one sentence only. I. Suppose we modified TCP so that the sequence number increases by 2 for every byte sent, but the initial sequence numbers are still randomly chosen. This modified protocol has the same security guarantees as standard TCP. II. If IP spoofing is eliminated from the Internet (all attackers must send messages from their real IP), then an on-path attacker (i.e. attacker can read packets, but can't modify) is no longer more powerful than an of-path attacker (i.e. attacker can't read, can't modify packets) III. TCP is secure against a DoS attack by a man-in-the-middle (MITM) because TCP guarantees delivery and will re-send messages until they are delivered.	6
Q1-C	What is a firewall? List any two firewall design goals. Recall the three important types of firewall depending on the mode of operation.	3 3 6
Q2-A	Decide if the following statements are True or False. I. By default, in a TLS connection, both the server and client are authenticated to each other. II. A DNS lookup for en.wikipedia.org will always force the recursive resolver to send at least 3 DNS queries. III. If Bob is an on-path attacker who can guarantee that his spoofed response arrives before the legitimate response, Bob only needs the victim to make one request for a non-existent domain to successfully execute a Kaminsky attack with 100% probability. IV. Randomizing the client port helps defend TCP against on-path attackers.	4

Q2-B	Dr. Ranga comes to Coffee Bucks and tries to connect to the Wi-Fi network in the coffee shop; He wants to communicate with https://www.pes.edu through TCP. List the protocols used with a justification when Dr. Ranga first connects to the Wi-Fi network and visits https://www.pes.edu ? Assume any caches are empty.	6
Q2-C	Immediately after the TCP handshake, Mallory injects a valid RST packet to the server. Next, Mallory spoofs a SYN packet from Dr. Ranga to the server with headers Seq = X. The server responds with a SYN-ACK packet with Seq = Y ;Ack = X + 1. What is the destination of this packet?	3
Q2-D	Consider the pcap-based sniffer program below. When running this program, we get an error message, saying "NULL: No such device". What is the cause of the error message? Suggest a fix. <pre> handle = pcap_open_live("eth1", BUFSIZ, 1, 1000, errbuf); if (handle == NULL) { perror("NULL"); } Error message: NULL: No such device </pre>	4
Q2-E	Consider the pcap-based sniffer program below. When running this program, we can only capture the packets in or out of our own computer; we are not able to capture the packets among other computers that are on the same network. What is the cause of this problem? <pre> handle = pcap_open_live("eth3", BUFSIZ, 0, 1000, errbuf); if (handle == NULL) { perror("NULL"); } </pre>	3
Q3-A	Define intrusion and how are they detected. Give some examples for intrusion. Where do I put IDS systems on my network?	7
Q3-B	What is WEP and WPA2 in the context of Wi-Fi communication? Which one is better and why?	4
Q3-C	A news report says that company XYZ's network was attacked by outsiders, who apparently sent a lot of spoofed ARP requests/responses from remote machines to	3

	the company's network, trying to launch ARP cache poisoning attacks. Please comment on whether this possible. Justify your answer.	
Q3-D	In a SYN flooding attack, Why do we choose to fill up the memory used for half-open connections, and not the memory used for holding full connections? The latter requires more memory, so the resource is much easier to exhaust.	6
Q4-A	In a discussion at work your co-worker says that Authentication and Authorization are alike. Do you agree? State Yes or NO. If you answer yes, please justify . If your answer is No, please explain.	4
Q4-B	What is Bluetooth? What are the two types of Bluetooth? Give one example for each type.	3
Q4-C	Your friend has been hired by an organization to take care of the security of its computer network. He is feeling a bit nervous as he does not have any money to invest in new hardware / software like firewall/IDS/IPS. He has come to you, knowing that you have studied computer Network security in class. He asks your advice on simple measures that he can take to help prevent/minimise any intrusion attack. Please suggest four simple things that can tremendously help your friend limit the possibility of an intrusion attack?	8
Q4-D	Compared with UDP, what is the chief reason why using TCP for DNS has a higher latency?	2
Q4-E	A malicious Heartbeat request packet is stored in the memory after it is received as shown below. The payload length field contains 0x700. Please describe which credit card numbers will be stolen by the attacker.  <p>The diagram shows a memory layout with five segments: Credit Card Number 1 (0x5000-0x4500), Credit Card Number 2 (0x4500-0x4300), Request Packet (0x4300-0x4000), Credit Card Number 3 (0x4000-0x3500). The Request Packet is highlighted in black and overlaps with the end of Credit Card Number 2 and the beginning of Credit Card Number 3.</p>	3

Q5-A	<p>The attacker is attacking a large network with hundreds of computers, and a detector must be installed as quickly as possible.</p> <p>HIDS or NIDS - Which would you install and Why?</p>	3
Q5-B	<p>The attacker constructs a buffer over-flow attack using shellcode they found online in a database of common attacks.</p> <p>Which is the best detection method for such attack?</p>	3
Q5-C	<p>Decide if the following statements are True or False.</p> <ol style="list-style-type: none"> A stateless firewall can block in-bound TCP connections on destination port 80 to devices on the internal network, while still allowing these devices to make out-bound connections using destination port 80. A stateless firewall can block in-bound UDP connections on destination port 53 to devices on the internal network, while still allowing these devices to make out-bound connections using destination port 53 SYN flooding attacks can be effectively prevented by rate-limiting the number of TCP connections from a given IP address. 	3
Q5-D	<p>A VPN allows Host U on a private network 192.168.60.0/24 to communicate with Host V on another private network 192.168.80.0/24 as shown below.</p> <ol style="list-style-type: none"> Describe the routing entries that should be added to Host U, VPN Client, VPN Server, and Host V? When Host V receives a packet from Host U, what is the source IP address of the packet? When VPN server receives a packet from Host U to Host V, via the VPN tunnel, what is the source and destination IP addresses of the packet? 	<p>6</p> <p>1</p> <p>2</p>
Q5-E	<p>Which encryption algorithm is used in Bluetooth SSP? What is bluejacking?</p>	2