Network Security | Question Bank | Questions

#	Question
1	Describe CIA security principles.
2	We breach into computer systems, deal with sensitive data and reveal vulnerabilities to help institutions/companies mitigate them. Who are we?
3	What is cybersecurity?
4	When should we say there is confidentiality between the sender and the receiver of a message?
5	An event, natural or man-made, able to cause a negative impact to an organization in terms of cybersecurity is known as:
6	Vulnerabilities are weaknesses in a system that can be exploited. List at least TWO most common ways in which vulnerabilities are introduced to a system?
7	A flaw, loophole, oversight, or error that can be exploited to violate system security policy in terms of cybersecurity is known as:
8	Explain the term “Non-repudiation”
9	Demonstrate how to hack into a device behind NAT using Netcat in three main steps.
10	Why is Kali Linux a popular choice in testing the network security of an organization? A) It is a network scanning tool that prioritizes security risks. B) It can be used to intercept and log network traffic. C) It can be used to test weaknesses by using only malicious software. D) It is an open source Linux security distribution and contains over 300 tools.
11	An administrator of a small data center wants a flexible, secure method of remotely connecting to servers. (i) Which protocol would be best to use? A)Telnet B) Secure Copy

#	Question
	C) Remote Desktop D) Secure Shell (ii) Explain your choice.
12	Which method tries all possible passwords until a match is found? A) rainbow tables B) brute force C) cloud D) cryptographic E) birthday F) dictionary
13	(i) What is SQL injection? (ii) What is best practice in defending against SQL injection?
14	The information gathered during the stage of footprinting revealed that on 14th April 2022 the admin was celebrating his 32th birthday. He always says his passwords must be 10 no more no less. Some of his other passwords were found to contain his birth year combined with one special character that can be either an at sign, underscore or dollar sign, and the name of the capital of Japan where he brags he was born. There is always only one UPPERCASE in his passwords. Guess three possible combinations of passwords from the information provided above. The admin's username is "pi" (without quotation marks), the default username for a Raspberry Pi. Least two vulnerabilities that you have found and provide your advice on how to improve the security measures.
15	Define the term Spyware in cybersecurity?
16	White hat hackers, gray hat hackers, and black hat hackers try to break into websites and computer networks. However white hat hackers have at least four protocols that they have to stick to. Which ones?
17	A common approach that organizations use to detect cyber attacks is security information and event management (SIEM) tools. Explain: a) Security Incident Detection b) Threat response workflow
18	Provide two mechanisms that help detect security incidents

#	Question
19	You decide to purchase concert tickets online. Alas, the website doesn't seem to be working as you cannot get through, which is often the case. This is commonly the result of a Distributed Denial of Service (DDoS). Explain this attack behavior.
20	Explain five handshake steps involved when a browser tries to connect to the web server secured with SSL.
21	What does system hardening mean?
22	Server hardening is a general system hardening process that involves securing the data, ports, components, functions, and permissions of a server. List at least FOUR measures to harden the security of a server
23	Your computer has just been infected with Ransomware and the hacker is demanding only Frw12,000 before releasing it. What do you do?
24	What is Zero-Trust architecture?
25	What's the definition of a backdoor in Cybersecurity ?
26	Man-in-the-Middle (MitM) Attack occurs when an attacker intercepts a two-party transaction, inserting themselves in the middle. Elaborate a diagram showing victim devices, switches and the attacker's position.
27	What is Data encryption and decryption process?
28	Firewalls contribute to the security of your network in which three (3) ways?
29	Explain the term Defense in depth.
30	What cryptographic transport algorithm is considered to be significantly more secure than SSL? A) AES B) HTTPS C) ESSL D) TLS