1. What is Integrity in pillars of information security?
   Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional. There are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data or during the storage of the document in the database or collection. Integrity pillar is responsible for maintaining the original characteristics of the data, as they were configured in their creation. In this way, the information cannot be changed without authorization. If there is an improper change in the data, it means there was a loss of integrity, so it is necessary to implement control mechanisms in order to prevent unauthorized alteration of information.

2. What are the types of hacking?
   a) Phishing –
      In this type of hacking, hackers' intention is to steal critical information of users like account passwords, MasterCard detail, etc. For example, hackers can replicate an original website for users' interaction and can steal critical information from the duplicate website the hacker has created.
   b) Cookie theft –
      Hackers access the net website exploitation malicious codes and steal cookies that contain tips, login passwords, etc. Get access to your account then will do any factor besides your account.
   c) Social Engineering –
      Social engineering is an attempt to manipulate you to share personal info, sometimes by impersonating a trustworthy supply.
   d) Cracking Password –
      Hackers will get your credentials through a technique known as key-logging.
   e) Missing Security Patches –
      Security tools will become outdated as a result of the hacking landscape advancement and needs frequent updates to protect against new threats.
   f) Malware-Injection Devices –
      Cyber-criminals will use hardware to sneak malware onto your pc. You would have detected infected USB sticks which can allow hackers remote access to your device when it is connected to your pc.

3. Mention 5 popular known ports?

Port Number	Usage
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH)
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web
110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

4. What is SYN flood attack?
   A SYN flood (half-open attack) is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (SYN) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.
   A SYN flood can occur in three different ways:
   a) **Direct attack:** A SYN flood where the IP address is not spoofed is known as a direct attack. In this attack, the attacker does not mask their IP address at all. As a result of the attacker using a single source device with a real IP address to create the attack, the attacker is highly vulnerable to discovery and mitigation. In order to create the half-open state on the targeted machine, the hacker prevents their machine from responding to the server's SYN-ACK packets.
   b) **Spoofed Attack:** A malicious user can also spoof the IP address on each SYN packet they send in order to inhibit mitigation efforts and make their identity more difficult to discover. While the packets may be spoofed, those packets can potentially be traced back to their source. It's difficult to do this sort of detective work but it's not impossible, especially if Internet service providers (ISPs) are willing to help.

c) **Distributed attack (DDoS):** If an attack is created using a botnet the likelihood of tracking the attack back to its source is low. For an added level of obfuscation, an attacker may have each distributed device also spoof the IP addresses from which it sends packets. If the attacker is using a botnet such as the Mirai botnet, they generally won't care about masking the IP of the infected device.

By using a SYN flood attack, a bad actor can attempt to create denial-of-service in a target device or service with substantially less traffic than other DDoS attacks. Instead of volumetric attacks, which aim to saturate the network infrastructure surrounding the target, SYN attacks only need to be larger than the available backlog in the target's operating system. If the attacker is able to determine the size of the backlog and how long each connection will be left open before timing out, the attacker can target the exact parameters needed to disable the system, thereby reducing the total traffic to the minimum necessary amount to create denial-of-service.

5. What is DHCP flood attack?
   A DHCP starvation attack is a malicious digital attack that targets DHCP servers. During a DHCP attack, a hostile actor floods a DHCP server with bogus DISCOVER packets until the DHCP server exhausts its supply of IP addresses. Once that happens, the attacker can deny legitimate network users service, or even supply an alternate DHCP connection that leads to a Man-in-the-Middle (MITM) attack.

6. What is DHCP snooping?
   DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.
   The DHCP Snooping feature performs the following activities:
   a) Validates DHCP messages from untrusted sources and filters out invalid messages.
   b) Builds and maintains the DHCP Snooping binding database, which contains information about untrusted hosts with leased IP addresses.
   c) Utilizes the DHCP Snooping binding database to validate subsequent requests from untrusted hosts.

7. How can you spoof a MAC address?
   Step 1- Go to the control panel or simply click Windows key X on your keyboard and open ‘device manager’.
   Step 2- Click to expand ‘Network Adapters’ and right-click the Ethernet or the adapter for which you want to change the MAC address for and choose ‘Properties’
   Step 3- Go to the Advanced tab and in the property box, click either the ‘Network Address’ or ‘Locally administered Address’.
   Step 4- In the ‘Value’ box you will see the MAC address. Clear its contents then enter a new address.
   Step 5- Click OK and restart your computer after entering the new MAC address
   Step 6- You can check by opening ‘Command Prompt’, and then click Run as administrator. At the command prompt, type: ipconfig/all and then hit Enter to check the physical address.

8. What is command to get the MAC address from ARP cache?
   Arp command (address resolution protocol) is used to view and manage the arp cache. The arp cache contains a dynamic list of IP addresses of the devices (computers, routers) your computer communicated with recently. More importantly, along with the IP address, the MAC address (the 6-byte 'burned-in' physical/hardware address) of the device is also stored in the cache.
   arp -a: This command is used to display the ARP table for a particular IP address. It also shows all the entries of the ARP cache or table.
   arp -g: This command works the same as the arp -a command.
   arp -d: This command is used when you want to delete an entry from the ARP table for a particular interface. To delete an entry, write arp -d command along with the IP address in a command prompt you want to delete.

9. What is use of IP scanner? Mention any one tool name or command?
   IP scanning is the ongoing IT task of analysing a business network to discover IP addresses and identify relevant information associated with those IP addresses and devices.
   Armed with an IP range scanner, admins can set a specified range of addresses to discover any IP addresses within that range.
   An IP address scanner tool can help:
   a) Avoid human errors and prevent network issues.
   b) Perform scans to receive up-to-date insights.
   c) Manage IPv4 and IPv6 from a single platform.
   d) Easily search a range of IP addresses e. Create and scan network subnets
   IP Scanning Tool:
   Auvik SolarWinds Network Device Scanner

10. What is sequence number in TCP handshake?

    The client on either side of a TCP session maintains a 32-bit sequence number it uses to keep track of how much data it has sent. This sequence number is included on each transmitted packet, and acknowledged by the opposite host as an acknowledgement number to inform the sending host that the transmitted data was received successfully. When a host initiates a TCP session, its initial sequence number is effectively random; it may be any value between 0 and 4,294,967,295, inclusive.

    The sequence number is a counter used to keep track of every byte sent outward by a host. If a TCP packet contains 1400 bytes of data, then the sequence number will be increased by 1400 after the packet is transmitted. At offset 64 is the acknowledgement number. Sequence number in a 3-way handshake is a random 32 bits(in the range of 0 to (2^32 -1)) number which is assigned to the first bit of the data. Generally, a sequence number is used only once in one connection. For other data transmission in the same connection, some other random sequence number can be used.