1. **What is cyber security**

Cybersecurity refers to protection of internet connected systems such as hardware, software, and data from cyber threats.

1. **What are the elements of cyber security?**

application security

Information security

Network security

Operational

End-user security

1. **What are the advantages of cyber security?**

data protection from unauthorized access

Preventing financial fraud

Improves customer confidence

1. **Define cryptography**

cryptography refers to provision of secure communication in the presence of malicious third parties

1. **Differentiate between IDS and IPS**

IDS alerts about a potential incident which enables operations (security) while IPS takes action itself to block the attempted intrusion.

1. **What is CIA?**
2. **What is a firewall?**

a firewall is a network security device that monitors and filters incoming and out coming network traffic based on an organization’s previously established security policies

1. **Explain trace route.**

traceroute is a utility that records the routes through the internet between computer and a specified destination computer.

1. **Differentiate between HIDS and NIDS.**
2. **Explain SSL**

SSL- Secure Socket Layer is the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems

11**.What do you mean by data leakage?**

Data leakage is unauthorized transmission of data from an organization to any external source

12.**Explain the brute force attack. How to prevent it.**

**13. what is port scanning?**

port scanning is a technique hackers use to discover open doors/ weak points in a network.

**14.name the different layers of OSI model.**

**15. What is VPN**

VPN- Virtual Private Network is an encrypted connection over the internet from a device to a network.

16.What are black hat hackers?

black hat hackers violate computer security for their own personal profit.

17.what are white hat hackers?

white hat hackers are hackers who identify security vulnerabilities in hardware, software/network.

18.what are grey hat hackers?

grey hat hackers violate laws but usually don’t have the malicious intent typical of a black hat hacker

19. how to reset a password protected BIOS configuration?

Turn off the computer and disconnect the power cable from the computer

Locate the password reset jumper on the system board

Remove the jumper plug from the password jumper pins

Power on without the jumper plug to clear the password

Wait until the desktop is loaded and then shut down the computer and replace the jumper plug in its original location

20.What is MITM attack?

MITM- Man In The Middle attack is a general term for when a perpetrator positions himself in a conversation between a user and an application.

21.Define ARP and its working process.

ARP- Address Resolution Protocol is a protocol or procedure that connects an ever-changing internet protocol(IP) address to a fixed physical machine address know as media access control in a local area network.

When a new computer joins a LAN, is assigned a unique IP address to use for identification and communication when an incoming packet destined for a machine on a particular LAN arrives at a gateway, the gateway asks ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

22.botnet is a collection of internet connected devices, which may include personal computers (PCs), servers, mobile devices and internet of things(IoT) devices, that are infected and controlled by a common type of malware.

23.SSL- Secure Socket Layer is a standard security protocol for establishing an encrypted link between a web server and a browser while TLS is a protocol that provides communication security between client/server applications that communicate with each other over the internet.

24.CSRF-Cross Site Request Forgery

25.2FA-Two Factor Authentication is an identity and access management security method that requires two forms of identification to access resource and data. It is used to give business the ability to monitor and help safeguard their most vulnerable information and networks.

26.asymmetric encryption uses public key for encryption and a private key for decryption while symmetric encryption uses one key for both encryption and decryption.

27.XSS- Cross Site Scripting

28.WAF- Web Application Firewall protects web applications from a variety of application layer attacks such as cross site scripting(XSS), SQL injection and cookie poisoning.

29.Hacking is gaining an unauthorized access to data in a system or computer

30.Hackers are individuals who use computer networking skills to overcome a technical problem

31. network sniffing is the process of monitoring and capturing all the packets passing through a given network

32.DNS ensures the internet is not only user friendly but works smoothly, loading whatever content we ask for quickly and efficiently. Without it, we would be stuck memorizing long lists of numbers (ID addresses) to access the content we want.

33. salting is a technique to protect passwords stored in databases by adding a string of 32/ more characters and then hashing them

34.SSH- Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

35.SSL is great, but it is simply not enough. The interception the data packets flowing between visitor and website is only one-way internet criminals gain access to sensitive information.

36.Black box testing is a test that only considers the external behavior of the system, the internal workings of the software is not taken into account and white box testing is a method used to test a software taking into consideration its internal functioning.

37.Explain vulnerabilities in network security.

38.Explain TCP three-way handshake.