## Topic- Cyber Security

1. **What is the purpose of a firewall in cybersecurity?**
    a) Network monitoring
    b) Malware detection
    c) Intrusion prevention
    d) Access control
    e) Data encryption

**Answer Access Control**

2. **What is the most common type of cyber attack?**
    a) Phishing
    b) DDoS
    c) SQL Injection
    d) Ransomware
    e) Man in the middle

**Answer Phishing**

3. **Which of the following is NOT a best practice for creating strong passwords?**
    a) Use Password Manager
    b) Using easy and simple passwords
    c) Using Pass phrases
    d) Using unique phrases
    e) Using upper and lower case letters, numbers and symbols

**Answer Using easy and simple passwords**

4. **Which encryption protocol is widely used for securing web traffic?**
    a) SSL: Secure Sockets Layer
    b) TLS: Transport Layer Security
    c) SSH:Secure Socket Shell
    d) PGP: Pretty Good Privacy
    e) Ipsec:Internet Protocol Security

**Answer TLS**

5. **What does VPN stand for in the context of cybersecurity?**
    a) Virtual Private Network
    b) Very Private Network
    c) Valid Public Network
    d) Virtual Protection Network
    e) Verified Private Network

**Answer Virtual Private Network**

6. **What is the primary purpose of a penetration test?**
    a) Test software
    b) Test security
    c) Test usability
    d) Test compatibility
    e) Test performance

**Answer Test Security**

7. **Which of the following is NOT a common authentication factor when we talk about Cyber Security?**
    a) Something you have
    b) Something you know
    c) Something you are
    d) Something you desire
    e) Something you wear

**Answer Something you desire**

8. **What does the term "phishing" refer to in cybersecurity?**
    a) Malicious software
    b) Social Engineering
    c) Physical Intrusion
    d) Denial of Service
    e) Unauthorised Access

**Answer Social Engineering**

9. **What type of cyber attack involves flooding a network with excessive requests to overload it??**
    a) Phishing
    b) DDoS
    c) Spoofing
    d) Bruteforce
    e) Cross side scripting

**Answer DDoS**

10. **What is the purpose of a honeypot in cybersecurity?**
    a) Gather data
    b) Detect Intrusions
    c) Encrypt Data
    d) Block Access
    e) Filter traffic

**Answer Detect Intrusions**

11. **Which of the following is NOT a potential consequence of a data breach?**
    a) Financial Loss
    b) Reputational Damage
    c) Legal Penalties
    d) Improved Security
    e) Identity Theft

**Answer Improved Security**

12. **What is the term for a piece of software that appears legitimate but actually carries out malicious activities?The term describes software that, like its ancient namesake, disguises itself as harmless while secretly carrying out harmful actions?**
    a) Trojan
    b) Worm
    c) Spyware
    d) Rootkit
    e) Ransomware

**Answer Trojan**

## Topic- Cyber Security

13. What does the "S" stand for in the abbreviation "HTTPS"??
    a) Secret
    b) Secure
    c) Software
    d) Session
    e) Storage

**Answer Secure**

14. Which of the following is a common method for protecting sensitive data in transit?
    a) Encrytion
    b) Compression
    c) Obfuscation
    d) Redundancy
    e) Fragmentation

**Answer Encryption**

15. What does IDS stand for in the context of cybersecurity??
    a) Intrusion Detection System
    b) Internet Defense System
    c) Internal Data Scanner
    d) Intruder Deterrent System
    e) Information Defense System

**Answer Intrusion Detection System.**

16. What is a common method for protecting against SQL injection attacks??
    a) Parameterized queries
    b) Captcha
    c) Two factor authentication
    d) Session management
    e) Biometric Authentication

**Answer Parameterized Queries**

17. **What type of cyber attack involves manipulating users into performing actions or divulging confidential information?**
    a) Social Engineering
    b) Ransomware
    c) DDoS
    d) Man in the Middle
    e) Phishing

**Answer Social Engineering**

18. **Which of the following is a characteristic of a strong cybersecurity culture within an organization?**
    a) Blaming individuals
    b) Reactive approach
    c) Proactive approach
    d) Lack of Training
    e) Ignoring Incidents

**Answer Proactive Approach**

19. **What is a zero-day vulnerability?**
    a) Known and Patched Vulnerability
    b) Previously unknown vulnerability
    c) Expired Vulnerability
    d) Vulnerability with no fix.
    e) Temporary Vulnerability

**Answer Previously Unknown Vulnerability**

20. **What is the purpose of multi-factor authentication (MFA)?**
    a) Increase security
    b) Decrease Usability
    c) Decrease Cost
    d) Increase Speed
    e) Decrease complexity

**Answer With recourse**

## Topic- Cyber Security

**21. Which of the following is NOT a common cyber threat actor??**

a) Hactivist
b) Insider Threat.
c) Script Kiddie
d) Black Hat Hacker.
e) Marketing Manager

**Answer Marketing Manager**

**22. What is the primary objective of a security policy in an organization?.**

a) Secure the network
b) Secure the Data
c) Secure the premises
d) Secure the employees
e) Secure the finances

**Answer Secure the Data**

**23. Which of the following is a common method for securing IoT devices?**

a) Weak passwords
b) Regular Updates.
c) Network Segmentation.
d) Firmware downgrades
e) Public Access Points.

**Answer Network Segmentation**

**24. What is the main purpose of encryption in cybersecurity?**

a) Protect data at rest
b) Protect data in transit
c) Protect data in use
d) Protect data at risk
e) Protect data at storage

**Answer Protect data at transit**

**25. What does the term "malware" refer to in cybersecurity?**

a) Malicious software
b) Security hardware
c) Network protocol
d) Encryption algorithm
e) Secure Authentication

**Answer Malicious Software**

**26. Which of the following is NOT a component of the CIA triad in cybersecurity?**

a) Confidentiality
b) Integrity
c) Authentication
d) Availability
e) All the above

**Answer Authentication**

**27. What is a common method for protecting against ransomware attacks?**

a) Regular backups
b) Anti-virus software
c) Strong passwords
d) Public Wi-Fi
e) Data sharing

**Answer Regular Backups**

**28. Which of the following is NOT a common type of malware?**

a) Virus
b) Trojan
c) Worm
d) Firewall
e) Spyware

**Answer Firewall**

## Topic- Cyber Security

**29. What does the term "botnet" refer to in cybersecurity?**

a) Network of infected devices
b) Secure network
c) Group of security experts
d) Network of automated tasks
e) Virtual private network

**Answer Network of Infected Devices**

**30. What is the purpose of a security audit in cybersecurity?**

a) Identify weaknesses
b) Test software
c) Secure the network
d) Encrypt data
e) Monitor traffic

**Answer Identify weaknesses**