BCA

(SEM. VI) MODEL PAPER – I

BCA – 6001 : INFORMATION & CYBER SECURITY

Time : 1 :30 Hours *Maximum Marks : 75*

Q.1. What is Cyber Security?
(1) Cyber Security provides security against malware
(2) Cyber Security provides security against cyber-terrorists
(3) Cyber Security protects a system from cyber attacks
(4) All of the mentioned
Ans. (4) All of the mentioned

Q.2. What does cyber security protect?
(1) Cyber security protects criminals
(2) Cyber security protects internet-connected systems
(3) Cyber security protects hackers
(4) None of the mentioned
Ans. (2) Cyber security protects internet-connected systems

Q.3. Who is the father of computer security?
(1) August Kerckhoffs (2) Bob Thomas
(3) Robert (4) Charles
Ans. (1) August Kerckhoffs

Q.4. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
(1) Cyber attack (2) Computer security
(3) Cryptography (4) Digital hacking
Ans. (1) Cyber attack

Q.5. Which of the following is a type of cyber security?
(1) Cloud Security (2) Network Security
(3) Application Security (4) All of the above
Ans. (4) All of the above

Q.6. What are the features of cyber security?
(1) Compliance
(2) Defense against internal threats
(3) Threat Prevention
(4) All of the above
Ans. (4) All of the above

Q.7. Which of the following is the least strong security encryption standard?
(1) WPA3 (2) WPA2
(3) WPA (4) WEP
Ans. (4) WEP

Q.8. Which of the following is a Stuxnet?
(1) Trojan (2) Antivirus
(3) Worm (4) Virus
Ans. (3) Worm

Q.9. Which of the following ethical hacking technique is used for determining which operating system (OS) is running on a remote computer?
(1) Operating System fingerprinting
(2) Operating System penetration testing
(3) Digital-printing
(4) Machine printing
Ans. (1) Operating System fingerprinting

Q.10. Which of the following can diminish the chance of data leakage?
(1) Steganography (2) Chorography
(3) Cryptography (4) Authentication
Ans. (1) Steganography

Q.11. What does the term "cyberspace" refer to?
(1) Virtual reality
(2) The interconnected environment of computer systems
(3) Outer space beyond Earth's atmosphere
(4) Augmented reality
Ans. (2) The interconnected environment of computer systems

Q.12. What is the primary purpose of a firewall in cyberspace?
(1) To block physical access to computers
(2) To prevent unauthorized access to a network
(3) To enhance internet speed
(4) To encrypt data transmission
Ans. (2) To prevent unauthorized access to a network

Q.13. Which of the following is a common cyber threat vector?
(1) Block chain
(2) Trojan horse
(3) JPEG
(4) HTML
Ans. (2) Trojan horse

Q.14. What does the term "phishing" refer to in cyberspace?
(1) Fishing in a virtual environment
(2) A technique to catch malware
(3) Fraudulent attempts to obtain sensitive information
(4) Online gaming strategy
Ans. (3) Fraudulent attempts to obtain sensitive information

Q.15. Which organization is responsible for the global coordination of the Domain Name System (DNS)?
(1) ICANN (Internet Corporation for Assigned Names and Numbers)
(2) NSA (National Security Agency)

(3) WHO (World Health Organization)
(4) NATO (North Atlantic Treaty Organization)
Ans. (1) ICANN (Internet Corporation for Assigned Names and Numbers)

Q.16. What is the purpose of SSL/TLS protocols in cyberspace?
(1) Secure communication over a computer network
(2) Enhance website speed
(3) Block malicious websites
(4) Monitor network traffic
Ans. (1) Secure communication over a computer network

Q.17. What is the role of antivirus software in cyberspace?
(1) To create viruses for testing purposes
(2) To remove malicious software from a computer
(3) To speed up internet connections
(4) To design firewalls
Ans. (2) To remove malicious software from a computer

Q.18. What is the purpose of a VPN (Virtual Private Network) in cyberspace?
(1) To create virtual reality experiences
(2) To securely connect to a private network over the internet
(3) To enhance computer graphics
(4) To optimize website performance
Ans. (2) To securely connect to a private network over the internet

Q.19. What is the main goal of DDoS (Distributed Denial of Service) attacks?
(1) To steal sensitive information
(2) To encrypt data
(3) To overload a website or network, making it unavailable
(4) To create virtual duplicates of a website
Ans. (3) To overload a website or network, making it unavailable

Q.20. Which cybersecurity measure involves the use of two or more authentication factors?
(1) Single sign-on
(2) Multi-factor authentication
(3) Biometric authentication
(4) Captcha verification
Ans. (2) Multi-factor authentication

Q.21. What does the term "Phishing" refer to in the context of the cyber society?
(1) A type of social gathering for cybersecurity professionals
(2) A method of fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity
(3) A new programming language for secure web development
(4) A type of advanced malware
Ans. (2) A method of fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity

Q.50. How does a man-in-the-middle attack work?
(1) By encrypting internet traffic
(2) By intercepting and altering communication between two parties
(3) By blocking websites
(4) By enhancing website design
Ans. (2) By intercepting and altering communication between two parties

Q.51. What is the primary purpose of WPA3 in wireless security?
(1) Data encryption (2) Network monitoring
(3) Device pairing (4) Signal boosting
Ans. (1) Data encryption

Q.52. Which authentication method is more secure than WEP for Wi-Fi networks?
(1) WPA2 (2) MAC filtering
(3) WPA3 (4) WEP2
Ans. (1) WPA2

Q.53. What is the purpose of changing the default username and password on a router?
(1) Enhance performance
(2) Improve range
(3) Prevent unauthorized access
(4) Increase bandwidth
Ans. (3) Prevent unauthorized access

Q.54. What does SSID stand for in the context of wireless networks?
(1) Secure Server Identification (2) System Security Identifier
(3) Service Set Identifier (4) Signal Strength Indicator
Ans. (3) Service Set Identifier

Q.55. Which encryption standard is stronger and more secure for Wi-Fi networks?
(1) Improve internet speed (2) Enhance security
(3) Expand network coverage (4) Boost device compatibility
(5) Signal Strength Indicator
Ans. (2) Enhance security

Q.56. What security feature helps protect against brute force attacks on Wi-Fi passwords?
(1) Firewall (2) Intrusion Detection System (IDS)
(3) CAPTCHA (4) Account lockout
Ans. (4) Account lockout

Q.57. What is the purpose of disabling SSID broadcasting?
(1) Save bandwidth
(2) Improve network speed
(3) Enhance privacy
(4) Prevent unauthorized detection
Ans. (4) Prevent unauthorized detection

Q.58. Which physical security measure is crucial for protecting wireless routers?
(1) Installing antivirus software
(2) Placing routers in a secure location
(3) Enabling two-factor authentication
(4) Using a virtual private network (VPN)
Ans. (2) Placing routers in a secure location

Q.59. How does MAC filtering contribute to wireless network security?
(1) Increases network speed
(2) Restricts access based on device addresses
(3) Enhances data encryption
(4) Improves signal strength
Ans. (2) Restricts access based on device addresses

Q.60. What role does a VPN (Virtual Private Network) play in wireless security?
(1) Signal amplification
(2) Secure data transmission over the internet
(3) MAC address filtering
(4) Firmware updates
Ans. (2) Secure data transmission over the internet

Q.61. Why is it advisable to change the default administrator login credentials on a wireless router?
(1) Boosts internet speed
(2) Prevents unauthorized configuration changes
(3) Increases device compatibility
(4) Enhances network range
Ans. (2) Prevents unauthorized configuration changes

Q.62. What security measure is associated with the term "rogue access points" in wireless networks?
(1) MAC filtering
(2) WPA3 encryption
(3) Intrusion Detection System (IDS)
(4) SSID broadcasting
Ans. (3) Intrusion Detection System (IDS)

Q.63. Which wireless security method involves hiding the network name from unauthorized users?
(1) MAC filtering
(2) WPA3 encryption
(3) SSID broadcasting
(4) Closed network (hidden SSID)
Ans. (4) Closed network (hidden SSID)

Q.64. What is the purpose of a firewall in the context of wireless network security?
(1) Improve signal strength
(2) Block unauthorized access

(3) A type of malware
(4) Deceptive attempts to obtain sensitive information
Ans. (4) Deceptive attempts to obtain sensitive information

Q.36 Which of the following is an example of a strong password?
(1) 123456 (2) Password123
(3) R@inbow$un (4) ABCD
Ans. (3) R@inbow$un

Q.37 What is the purpose of antivirus software?
(1) To speed up the computer
(2) To create backups
(3) To detect and remove malicious software
(4) To organize files
Ans. (3) To detect and remove malicious software

Q.38 What does HTTPS stand for in the context of web browsing?
(1) Hypertext Transfer Protocol Secure
(2) HyperText and Email Security Protocol
(3) High-Efficiency Transfer Protocol for Secure browsing
(4) Home and Entertainment Transfer Protocol with Security
Ans. (1) Hypertext Transfer Protocol Secure

Q.39 Which of the following is an example of a physical security measu for a computer?
(1) Firewall (2) Biometric authentication
(3) Cable locks (4) Encryption
Ans. (3) Cable locks

Q.40 What is the purpose of regular software updates in the context security?
(1) To slow down the computer
(2) To enhance graphics
(3) To fix vulnerabilities and improve security
(4) To increase storage space
Ans. (3) To fix vulnerabilities and improve security

Q.41 What is the role of a CAPTCHA in online security?
(1) To prevent spam
(2) To increase website traffic
(3) To improve website design
(4) To enhance internet speed
Ans. (1) To prevent spam

Q.42 What is the purpose of a cookie in the context of web security?
(1) To store website design elements
(2) To track user preferences and login information
(3) To block ads
(4) To increase internet speed
Ans. (2) To track user preferences and login information

Q.43 What does the term "zero-day vulnerability" refer to?
(1) A software bug that occurs every day
(2) A security flaw that is exploited before a fix is available
(3) The first day of a cyber attack
(4) A virus with no known cure
ns. (2) A security flaw that is exploited before a fix is available

) 44 What is the purpose of biometric authentication in Internet security?
(1) To increase download speed
(2) To block websites
(3) To verify a user's identity based on unique physical or behavioral traits
(4) To improve device performance
ns. (3) To verify a user's identity based on unique physical o behavioral traits

) 45 What is the main goal of ransom are attacks?
(1) To steal personal information
(2) To slow down internet speed
(3) To encrypt files and demand a ransom for their release
(4) To improve search engine rankings
ns. (3) To encrypt files and demand a ransom for their release

) 46 What is the purpose of a WAF (Web Application Firewall) in Internet security?
(1) To increase internet speed
(2) To block unauthorized access to web applications
(3) To organize files
(4) To enhance website design
ns. (2) To block unauthorized access to web applications

) 47 Which of the following is a social engineering attack?
(1) Firewall breach (2) Brute-force attack
(3) Phishing attack (4) DDoS attack
ns. (3) Phishing attack

) 48 What is the purpose of multi-factor authentication (MFA)?
(1) To increase download speed
(2) To encrypt internet traffic
(3) To verify a user's identity using multiple credentials
(4) To improve device performance
ns. (3) To verify a user's identity using multiple credentials

) 49 What does DNS (Domain Name System) do in the context of Internet security?
(1) Encrypts internet traffic
(2) Resolves domain names to IP addresses
(3) Blocks unauthorized access
(4) Improves search engine rankings
ns. (2) Resolves domain names to IP addresses

Q.22 Which of the following is a fundamental principle of cybersecurity the cyber society?
(1) Least privilege (2) Online anonymity
(3) Data hoarding (4) Unrestricted access
Ans. (1) Least privilege

Q.23 Which of the following is not a steganography tool?
(1) Crypture (2) SteganographX Plus
(3) rSteg (4) Burp Suite
Ans. (4) Burp Suite

Q.24 What does the term "IoT" stand for in the context of the cybe society?
(1) Internet of Things
(2) Input Output Technology
(3) Intelligent Online Tracking
(4) Internet over Transmission
Ans. (1) Internet of Things

Q.25 What is the role of a firewall in the context of cyber society?
(1) To prevent physical break-ins
(2) To block unauthorized access to a computer network
(3) To protect against earthquakes
(4) To regulate internet speed
Ans. (2) To block unauthorized access to a computer network

Q.26 In the context of cyber society, what is the primary purpose encryption?
(1) To create strong passwords
(2) To hide the identity of internet users
(3) To secure data by converting it into a code
(4) To slow down cyber attacks
Ans. (3) To secure data by converting it into a code.

Q.27 What is a "Zero-Day Exploit" in the realm of cyber society?
(1) A software bug that occurs every day
(2) An exploit that takes zero days to execute
(3) An attack that targets undisclosed vulnerabilities before patch is available
(4) A strategy for zeroing in on cybercriminals
Ans. (3) An attack that targets undisclosed vulnerabilities before patch is available.

Q.28 What does the term "Digital Footprint" refer to in the cyb society?
(1) A shoe brand for tech enthusiasts
(2) Traces of an individual's online activity and presence
(3) A virtual reality game
(4) A type of cyber attack
Ans. (2) Traces of an individual's online activity and presence

Q.29 What is the significance of two-factor authentication (2FA) in the cyber society?
(1) To double the internet speed
(2) To provide multiple online identities
(3) To add an extra layer of security by requiring two forms of identification
(4) To facilitate dual-screen displays
Ans. (3) To add an extra layer of security by requiring two forms of identification

Q.30 What is the primary purpose of a CAPTCHA in the cyber society?
(1) To prevent robots from taking over the internet
(2) To slow down internet speed
(3) To create digital artwork
(4) To enhance virtual reality experiences
Ans. (1) To prevent robots from taking over the internet

Q.31 What is the primary purpose of a firewall in the context of Internet security?
(1) To block unauthorized access
(2) To increase internet speed
(3) To enhance website design
(4) To improve search engine rankings
Ans. (1) To block unauthorized access

Q.32 What is the most common method of authentication for online accounts?
(1) Biometric authentication
(2) Two-factor authentication
(3) Single-factor authentication
(4) No authentication required
Ans. (2) Two-factor authentication

Q.33 Which of the following is a common phishing attack vector?
(1) Denial-of-Service (DoS) attacks
(2) Brute-force attacks
(3) Spoofed emails
(4) SQL injection attacks
Ans. (3) Spoofed emails

Q.34 What is the purpose of using a VPN (Virtual Private Network) in Internet security?
(1) To block websites
(2) To increase download speed
(3) To encrypt internet traffic
(4) To improve device performance
Ans. (3) To encrypt internet traffic

Q.35 What does the term "phishing" refer to in the context of Internet security?
(1) Fishing for compliments
(2) Fishing for data

(3) Increase network speed
(4) Encrypt data transmission
Ans (2) Block unauthorized access

Q.65 How does social engineering pose a threat to wireless security?
(1) By physically damaging routers
(2) Through manipulation to gain access credentials
(3) Enhancing signal interference
(4) Improving encryption standards
Ans (2) Through manipulation to gain access credentials

Q.66 Which security measure involves limiting the number of devices that can connect to a wireless network simultaneously?
(1) MAC filtering (2) Network segmentation
(3) Bandwidth throttling (4) Device pairing
(2) MAC filtering

Q.67 What is the primary purpose of using WPA3-Personal over WPA3-Enterprise in wireless security?
(1) Increased data encryption
(2) Simplified home network setup
(3) Advanced authentication for business networks
(4) Improved signal strength
Ans. (2) Simplified home network setup

Q.68 How does a strong passphrase contribute to wireless security?
(1) Enhances network speed
(2) Prevents brute force attacks
(3) Improves signal strength
(4) Increases device compatibility
Ans (2) Prevents brute force attacks

Q.69 Which security feature helps protect against packet sniffing in wireless networks?
(1) WPA3 encryption
(2) VPN tunneling
(3) MAC filtering
(4) Intrusion Prevention System (IPS)
Ans. (1) WPA3 encryption

Q.70 Which international organization is responsible for the development of cybersecurity standards?
(1) United Nations (UN)
(2) International Telecommunication Union (ITU)
(3) World Health Organization (WHO)
(4) International Monetary Fund (IMF)
Ans. (2) International Telecommunication Union (ITU)

Q.71 What is the primary goal of the General Data Protection Regulation (GDPR)?
(1) Regulating internet service providers
(2) Protecting individuals' privacy and personal data

(3) Controlling social media content
(4) Restricting online financial transactions
ns. (2) Protecting individuals' privacy and personal data

.72 Which law primarily addresses the privacy of electronic communications?
(1) Children's Online Privacy Protection Act (COPPA)
(2) Electronic Communications Privacy Act (ECPA)
(3) Computer Fraud and Abuse Act (CFAA)
(4) Digital Millennium Copyright Act (DMCA)
s. (2) Electronic Communications Privacy Act (ECPA)

73. ISO/IEC 27001 is a standard related to:
(1) Cloud computing (2) Information security management
(3) Social media usage (4) Mobile app development
s. (2) Information security management

74. What is the primary objective of the Children's Online Privacy Protection Act (COPPA)?
(1) Regulating online freedom of speech
(2) Privacy protection for children under 13
(3) Regulation of e-commerce transactions
(4) Security measures for online banking
s. (2) Privacy protection for children under 13

75. Which law is focused on preventing unauthorized access to computer systems?
(1) Health Insurance Portability and Accountability Act (HIPAA)
(2) Computer Fraud and Abuse Act (CFAA)
(3) General Data Protection Regulation (GDPR)
(4) Electronic Communications Privacy Act (ECPA)
s. (2) Computer Fraud and Abuse Act (CFAA)

6. The acronym DMCA stands for:
(1) Digital Millennium Copyright Act
(2) Data Management and Control Act
(3) Domain Name Certification Authority
(4) Distributed Multi-channel Content Aggregation
(1) Digital Millennium Copyright Act

7. What does the NIST Cybersecurity Framework provide guidelines for?
(1) International trade regulations
(2) Software development methodologies
(3) Cybersecurity risk management
(4) Social media etiquette and guidelines
(3) Cybersecurity risk management

8. Which standard is associated with cryptographic protocols used for secure communication?
(1) SSL/TLS (2) HTTP (3) FTP (4) ICMP
(1) SSL/TLS

Q.79 The Electronic Communications Privacy Act (ECPA) prim addresses the privacy of:
(1) Financial transactions (2) Electronic communications
(3) Online advertisements (4) Social media content
Ans. (2) Electronic communications

Q.80 ISO/IEC 27001 is a standard related to:
(1) Cloud computing
(2) Information security management
(3) Social media usage
(4) Mobile app development
Ans. (2) Information security management

Q.81 What is the main purpose of ISO/IEC 27001?
(1) Regulating internet service providers
(2) Ensuring the quality of software development
(3) Providing guidelines for ethical hacking
(4) Establishing an information security management sy (ISMS)
Ans. (4) Establishing an information security management sy (ISMS)

Q.82 In the ISO/IEC 27001 framework, what does the acronym I stand for?
(1) International Security Management System
(2) Information Security Monitoring System
(3) Information Security Management System
(4) Integrated Security Measurement System
Ans. (3) Information Security Management System

Q.83 Which phase of the ISO/IEC 27001 implementation inv identifying and assessing information security risks?
(1) Planning (2) Implementation
(3) Monitoring and review (4) Risk assessment
Ans. (4) Risk assessment

Q.84 What is the purpose of the Statement of Applicability (So ISO/IEC 27001?
(1) Summarizing financial statements
(2) Identifying applicable security controls
(3) Describing software application features
(4) Listing employee roles and responsibilities
Ans. (2) Identifying applicable security controls

Q.85 In the context of ISO/IEC 27001, what does the term "risk treat refer to?
(1) Removing all identified risks
(2) Accepting identified risks without mitigation
(3) Mitigating or avoiding identified risks
(4) Ignoring identified risks
Ans. (3) Mitigating or avoiding identified risks

Q.86 Which of the following is a key benefit of ISO/IEC 27001 certification?
(1) Higher internet speed
(2) Enhanced information security
(3) Increased social media engagement
(4) Improved mobile app performance
Ans. (2) Enhanced information security

Q.87 What is the significance of the ISO/IEC 27001 Annex A?
(1) Providing templates for project documentation
(2) Listing controls for information security management
(3) Describing procedures for software development
(4) Specifying hardware requirements
Ans. (2) Listing controls for information security management

Q.88 What role does top management play in ISO/IEC 27001 implementation?
(1) Writing code for security controls
(2) Conducting penetration testing
(3) Providing leadership and commitment
(4) Reviewing IT support tickets
Ans. (3) Providing leadership and commitment

Q.89 How often should an organization conduct internal audits according to ISO/IEC 27001?
(1) Every month
(2) Once a year
(3) As needed, but at least annually
(4) Only during a security breach
Ans. (3) As needed, but at least annually

Q.90 What is the primary goal of a firewall in network security?
(1) Data encryption
(2) User authentication
(3) Network monitoring
(4) Controlling and filtering network traffic
Ans. (4) Controlling and filtering network traffic

Q.91 Which cryptographic algorithm is commonly used for secure communication over the internet?
(1) MD5 (2) DES (3) RSA (4) SHA-1
Ans. (3) RSA

Q.92 What does the term "biometric authentication" refer to?
(1) Using passwords
(2) Using physical characteristics
(3) Two-factor authentication
(4) Public key authentication
Ans. (2) Using physical characteristics

Q.93 What is the purpose of an Intrusion Detection System (IDS)?
(1) Preventing unauthorized access
(2) Detecting and responding to suspicious activities

(3) Encrypting data at rest
(4) Filtering spam emails
Ans. (2) Detecting and responding to suspicious activities

Q.94 Which of the following is an example of a preventive security control?
(1) Antivirus software
(2) Firewall
(3) Encryption
(4) Intrusion Prevention System (IPS)
Ans. (2) Firewall

Q.95 What is the main goal of a risk assessment in security management?
(1) Identify and mitigate security risks
(2) Implement encryption techniques
(3) Monitor network traffic
(4) Authenticate users
Ans. (1) Identify and mitigate security risks

Q.96 What is the term for the practice of tricking individuals into divulging confidential information?
(1) Hacking (2) Spoofing
(3) Phishing (4) Denial of Service (DoS)
Ans. (3) Phishing

Q.97 Which security concept involves assigning access levels to different categories of data?
(1) Encryption (2) Authorization
(3) Authentication (4) Confidentiality
Ans. (2) Authorization

Q.98 What is the purpose of a Virtual Private Network (VPN) in network security?
(1) Monitor system performance
(2) Control network traffic
(3) Provide a secure communication channel over the internet
(4) Prevent physical access
Ans. (3) Provide a secure communication channel over the internet

Q.99 Which security best practice involves using unique passwords for each account?
(1) Password sharing (2) Password reuse
(3) Password rotation (4) Password hygiene
Ans. (4) Password hygiene

Q.100 What is the primary goal of disaster recovery in information security?
(1) Preventing disasters
(2) Minimizing the impact of disasters
(3) Ignoring disasters
(4) Enhancing network performance
Ans. (2) Minimizing the impact of disasters

BCA

(SEM. VI) MODEL PAPER – II

BCA – 6001 : INFORMATION & CYBER SECURITY

Time : 1 :30 Hours *Maximum Marks : 75*

Q.1. Which of the following is an objective of network security?
(1) Confidentiality (2) Integrity
(3) Availability (4) All of the above
Ans. (4) All of the above

Q.2. Which of the following is not a cybercrime?
(1) Denial of Service (2) Man in the Middle
(3) Malware (4) AES
Ans. (4) AES

Q.3. Which of the following is a component of cyber security?
(1) Internet of Things (2) AI
(3) Database (4) Attacks
Ans. (1) Internet of Things

Q.4. Which of the following is a type of cyber attack?
(1) Phishing (2) SQL Injections
(3) Password Attack (4) All of the above
Ans. (4) All of the above

Q.5. Which of the following is not an advantage of cyber security?
(1) Makes the system slower
(2) Minimizes computer freezing and crashes
(3) Gives privacy to users
(4) Protects system against viruses
Ans. (1) Makes the system slower

Q.6. "Cyberspace" was coined by _____
(1) Richard Stallman (2) William Gibson
(3) Andrew Tannenbaum (4) Scott Fahlman
Ans. (2) William Gibson

Q.7. In which year has hacking become a practical crime and a matter of concern in the field of cyber technology?
(1) 1991 (2) 1983
(3) 1970 (4) 1964
Ans. (3) 1970

Q.8. Governments hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _____
(1) Nation / State sponsored hackers
(2) CIA triad

(3) Special Hackers
(4) Government Hackers

Ans. (1) Nation / State sponsored hackers

Q.9. Which of the following act violates cyber security?
(1) Exploit (2) Attack
(3) Threat (4) Vulnerability

Ans. (2) Attack

Q.10 What is the term for a malicious software that, once installed, allows unauthorized access and control of a computer?
(1) Spyware
(2) Ransomware
(3) Trojan Horse
(4) Worm

Ans. (3) Trojan Horse

Q.11. What is the purpose of a Distributed Denial of Service (DDoS) attack in the context of the cyber society?
(1) To steal sensitive information
(2) To overload a network or website with traffic, making it unavailable
(3) To encrypt data for ransom
(4) To spread fake news

Ans. (2) To overload a network or website with traffic, making it unavailable

Q.12 What does the acronym "DNS" stand for in the cyber society?
(1) Digital Network System
(2) Domain Name System
(3) Data and Network Security
(4) Dynamic Networking Service

Ans. (2) Domain Name System

Q.13 Which of the following is a common method for enhancing password security in the cyber society?
(1) Using easily guessable passwords
(2) Changing passwords once a year
(3) Multi-factor authentication
(4) Writing passwords on sticky notes

Ans. (3) Multi-factor authentication

Q.14 What is the primary purpose of an antivirus program in the cyber society?
(1) To speed up computer performance
(2) To create backups of files
(3) To detect and remove malicious software
(4) To organize files on the computer

Ans. (3) To detect and remove malicious software

15 In the context of social engineering, what does "pretexting" involve?
(1) Creating a false identity to deceive individuals
(2) Posting fake news on social media
(3) Hacking into social media accounts
(4) Encrypting online conversations

s. (1) Creating a false identity to deceive individuals

16. What is the role of a bug bounty program in the cyber society?
(1) To spread computer viruses
(2) To reward individuals for finding and reporting security vulnerabilities
(3) To create intentional software bugs
(4) To track online user behavior

s. (2) To reward individuals for finding and reporting security vulnerabilities

17. What does the term "Blockchain" refer to in the context of the cyber society?
(1) A type of computer virus
(2) A decentralized and secure ledger technology
(3) A new programming language
(4) A method of encrypting emails

s. (2) A decentralized and secure ledger technology

18. What is the primary purpose of the General Data Protection Regulation (GDPR) in the cyber society?
(1) To encourage data sharing without restrictions
(2) To regulate the use of virtual reality technology
(3) To protect the privacy and personal data of individuals
(4) To increase internet speed globally

s. (3) To protect the privacy and personal data of individuals

19. What is the concept of "Net Neutrality" in the context of the cyber society?
(1) The idea that the internet should be free of charge
(2) The principle that internet service providers should treat all data on the internet the same
(3) The belief that cyber attacks are inevitable and cannot be prevented
(4) The practice of limiting internet access for certain users

s. (2) The principle that internet service providers should treat all data on the internet the same

20. People will normally think it as a normal/regular file and your secret message will pass on without any _____
(1) suspicion (2) decryption
(3) encryption (4) cracking

s. (1) suspicion

Q.21 What is the term for the practice of concealing messages information within another non-secret text or data?
(1) Decryption (2) Cryptography
(3) Steganography (4) Obfuscation
Ans. (3) Steganography

Q.22 In the context of cybersecurity, what does the acronym "VPN" sta for?
(1) Virtual Private Network
(2) Very Personal Navigation
(3) Virtual Public Network
(4) Visual Processing Node
Ans. (1) Virtual Private Network

Q.23 Which of the following is a common method of social engineering t involves manipulating individuals into divulging confiden information?
(1) Spoofing (2) Phishing
(3) Brute force attack (4) DDoS attack
Ans. (2) Phishing

Q.24 What is the role of biometric authentication in the cyber society?
(1) To analyze online behavior
(2) To secure data using biological samples
(3) To track GPS coordinates
(4) To create virtual reality environments
Ans. (2) To secure data using biological samples

Q.25 What is the purpose of penetration testing in the context cybersecurity?
(1) To launch cyber attacks on competitors
(2) To identify vulnerabilities in a system or network
(3) To create secure passwords
(4) To encrypt communication
Ans. (2) To identify vulnerabilities in a system or network

Q.26 What does the term "Social Media Engineering" refer to in the cy society?
(1) Creating new social media platforms
(2) Manipulating social media algorithms
(3) Exploiting human psychology to gain access to information
(4) Developing software for social networking
Ans. (3) Exploiting human psychology to gain access to information

Q.27 Which of the following is a potential cybersecurity threat associat with Internet of Things (IoT) devices?
(1) Increased network speed
(2) Device vulnerabilities leading to security breaches
(3) Improved battery life
(4) Enhanced data storage capacity
Ans. (2) Device vulnerabilities leading to security breaches

Q.28 What is the primary purpose of the "Dark Web" in the cyber society?
(1) A space for ethical hacking
(2) To conduct legal and transparent transactions
(3) An encrypted and anonymous part of the internet for illicit activities
(4) A platform for open access to information
Ans. (3) An encrypted and anonymous part of the internet for illicit activities

Q.29 What is the concept of "Cybersecurity Awareness Training" aiming to achieve in organizations?
(1) To slow down internet speed
(2) To educate employees about potential cybersecurity threats and best practices
(3) To promote hacking skills
(4) To develop new cybersecurity technologies
Ans. (2) To educate employees about potential cybersecurity threats and best practices

Q.30 What is the primary purpose of a CAPTCHA?
(1) To encrypt website data
(2) To prevent automated bots from accessing a website
(3) To enhance virtual reality experiences
(4) To increase internet speed
Ans. (2) To prevent automated bots from accessing a website

Q.31 What is the purpose of a VPN kill switch?
(1) To enhance internet speed
(2) To block unauthorized access
(3) To terminate internet connections in case the VPN connection fails
(4) To organize files
Ans. (3) To terminate internet connections in case the VPN connection fails

Q.32 What is the role of a security token in authentication?
(1) To increase download speed
(2) To encrypt internet traffic
(3) To generate one-time codes for authentication
(4) To improve device performance
Ans. (3) To generate one-time codes for authentication

Q.33 What is the primary purpose of encryption in Internet security?
(1) To block websites
(2) To organize files
(3) To hide sensitive information by converting it into a secure format
(4) To improve search engine rankings
Ans. (3) To hide sensitive information by converting it into a secure format

Q.34 What is the significance of the term "sandboxing" in the context of security?
(1) To slow down internet speed
(2) To create backups
(3) To run untrusted programs in an isolated environment
(4) To block unauthorized access
Ans. (3) To run untrusted programs in an isolated environment

Q.35 What is the purpose of a security audit in an organization?
(1) To improve website design
(2) To increase internet speed
(3) To assess and enhance the overall security posture
(4) To organize files
Ans. (3) To assess and enhance the overall security posture

Q.36 What is the primary purpose of encryption in cybersecurity?
(1) Authentication (2) Data Integrity
(3) Confidentiality (4) Availability
Ans. (3) Confidentiality

Q.37 Which type of malware is designed to spread from one computer to another by attaching itself to legitimate programs?
(1) Trojan Horse (2) Worm
(3) Spyware (4) Ransomware
Ans. (2) Worm

Q.38 What is the main function of a firewall in a network security system?
(1) Encryption (2) Access Control
(3) Intrusion Detection (4) Virus Scanning
Ans. (2) Access Control

Q.39 In a phishing attack, what is the typical goal of the attacker?
(1) Stealing sensitive information
(2) Disrupting network services
(3) Installing malware
(4) Conducting a DDoS attack
Ans. (1) Stealing sensitive information

Q.40 Which of the following is an example of something you have in the context of 2FA?
(1) Password (2) PIN
(3) Security Token (4) Biometric Data
Ans. (3) Security Token

Q.41 What is the primary goal of an incident response plan in cybersecurity?
(1) Preventing all cyberattacks
(2) Recovering data after an incident
(3) Identifying vulnerabilities in the system
(4) Training employees on cybersecurity
Ans. (2) Recovering data after an incident

Q.42 Which authentication protocol is commonly used for secure transmission of passwords over a network?
(1) HTTP (2) FTP
(3) SSH (4) Kerberos
Ans. (3) SSH

Q.43 What is the purpose of a vulnerability assessment in cybersecurity?
(1) Identify and mitigate security vulnerabilities
(2) Block unauthorized access to the network
(3) Encrypt sensitive data
(4) Monitor network traffic
Ans. (1) Identify and mitigate security vulnerabilities

Q.44 Which social engineering technique involves pretending to be a trustworthy entity in order to obtain sensitive information?
(1) Spoofing (2) Phishing
(3) Eavesdropping (4) Sniffing
Ans. (2) Phishing

Q.45 What does the term "zero-day" cybersecurity?
(1) An attack that occurs at midnight
(2) A vulnerability that is exploited before a patch is available
(3) The first day of a security awareness training program
(4) A type of antivirus software
Ans. (2) A vulnerability that is exploited before a patch is available

Q.46 Which of the following is a common method to secure wireless networks?
(1) MAC Filtering (2) Firewall
(3) Encryption (4) Antivirus Software
Ans. (3) Encryption

Q.47 Which cybersecurity framework is developed by the National Institute of Standards and Technology (NIST)?
(1) ISO/IEC 27001
(2) COBIT
(3) CIS Controls
(4) NIST Cybersecurity Framework
Ans. (4) NIST Cybersecurity Framework

Q.48 What is the primary purpose of regularly backing up data in cybersecurity?
(1) Enhancing network speed
(2) Preventing unauthorized access
(3) Recovering data in case of loss or corruption
(4) Updating antivirus definitions
Ans. (4) Recovering data in case of loss or corruption

Q.49 What is the main goal of a penetration test?
(1) Test the speed of network connections
(2) Identify and exploit vulnerabilities

(3) Monitor network traffic in real-time
(4) Encrypt sensitive data
Ans. (2) Identify and exploit vulnerabilities

Q.50. What does an insider threat refer to in cybersecurity?
(1) Cyberattacks originating from external sources
(2) Malicious activities carried out by employees or associates
(3) Software vulnerabilities within the system
(4) Denial-of-Service (DoS) attacks
Ans. (2) Malicious activities carried out by employees or associates

Q.51. How does regularly monitoring network traffic contribute to wirele security?
(1) Increases signal strength
(2) Identifies unauthorized access or suspicious activity
(3) Boosts device compatibility
(4) Enhances data encryption
Ans. (2) Identifies unauthorized access or suspicious activity

Q.52. Which type of attack involves an attacker intercepting and alteri communication between two parties in a wireless network?
(1) Man-in-the-Middle (MitM)
(2) Brute force
(3) Denial of Service (DoS)
(4) Spoofing
Ans. (1) Man-in-the-Middle (MitM)

Q.53. What security measure involves limiting the range of a Wi-Fi signal prevent unauthorized access from outside a specific area?
(1) MAC filtering
(2) Signal masking
(3) VLAN segmentation
(4) Physical access controls
Ans. (2) Signal masking

Q.54. How does network segmentation enhance wireless security?
(1) Increases network speed
(2) Simplifies device configuration
(3) Limits the impact of a security breach
(4) Boosts signal strength
Ans. (3) Limits the impact of a security breach

Q.55. What is the primary purpose of implementing two-fact authentication on a wireless network?
(1) Enhances data encryption
(2) Provides additional login security
(3) Improves signal strength
(4) Prevents physical tampering
Ans. (2) Provides additional login security

Q.56. Which security measure involves separating a wireless network int different virtual networks to enhance security and manage traffic?

(1) MAC filtering
(2) WPA3 encryption
(3) VLAN segmentation
(4) Closed network (hidden SSID)
Ans. (3) VLAN segmentation

Q.57. What is the primary purpose of conducting regular security audits on a wireless network?
(1) Improving signal strength
(2) Identifying and fixing security vulnerabilities
(3) Enhancing device compatibility
(4) Increasing network speed
Ans. (2) Identifying and fixing security vulnerabilities

Q.58. Which security measure involves limiting the amount of data a device can send or receive over a wireless network?
(1) Traffic shaping
(2) Signal masking
(3) Intrusion Detection System (IDS)
(4) WPA3 encryption
Ans. (1) Traffic shaping

Q.59. How does a captive portal enhance wireless security?
(1) Prevents physical tampering
(2) Improves signal strength
(3) Requires user authentication before accessing the network
(4) Enhances device compatibility
Ans. (3) Requires user authentication before accessing the network

Q.60. Why is it important to disable unnecessary services and ports on a wireless router?
(1) Improves network speed
(2) Reduces the attack surface and potential vulnerabilities
(3) Enhances device compatibility
(4) Boosts signal strength
Ans. (2) Reduces the attack surface and potential vulnerabilities

Q.61. How does firmware integrity verification contribute to wireless security?
(1) Improves signal strength
(2) Prevents unauthorized firmware modifications
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Prevents unauthorized firmware modifications

Q.62. What is the purpose of using a strong, unique password for the router's admin interface?
(1) Improves signal strength
(2) Enhances device compatibility
(3) Prevents unauthorized access to router settings
(4) Increases network speed
Ans. (3) Prevents unauthorized access to router settings

Q.63. How does regular backup of router configuration settings contribu to security?
(1) Improves signal strength
(2) Facilitates faster data transmission
(3) Ensures quick device compatibility
(4) Facilitates quick recovery after a security incident
Ans. (4) Facilitates quick recovery after a security incident

Q.64. What security measure involves updating and patching not only t router but also connected devices?
(1) Device pairing
(2) Network segmentation
(3) Regular security patching
(4) MAC filtering
Ans. (3) Regular security patching

Q.65. How does disabling unused wireless interfaces contribute security?
(1) Improves signal strength
(2) Reduces the attack surface
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Reduces the attack surface

Q.66. What is the purpose of implementing a guest network in wirele security?
(1) Increases network speed
(2) Enhances device compatibility
(3) Provides a separate network for guest devices
(4) Boosts signal strength
Ans. (3) Provides a separate network for guest devices

Q.67. How does encryption in transit contribute to the security of wirele communication?
(1) Enhances signal strength
(2) Prevents unauthorized access during data transmission
(3) Increases device compatibility
(4) Improves network speed
Ans. (2) Prevents unauthorized access during data transmission

Q.68. What is the primary purpose of implementing security awarene training for users on a wireless network?
(1) Improves signal strength
(2) Enhances device compatibility
(3) Reduces the risk of social engineering attacks
(4) Increases network speed
Ans. (3) Reduces the risk of social engineering attacks

Q.69. How does physical security awareness contribute to overall wirele network security?
(1) Improves signal strength
(2) Prevents physical tampering and unauthorized access

(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Prevents physical tampering and unauthorized access

Q.70. What is the purpose of implementing intrusion detection and prevention systems in wireless networks?
(1) Improves signal strength
(2) Identifies and responds to suspicious activities or attacks
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Identifies and responds to suspicious activities or attacks

Q.71. The Information Technology Act, 2000 was enacted to:
(1) Regulate the postal service
(2) Facilitate electronic transactions
(3) Control traditional media outlets
(4) Monitor international telecommunications
Ans. (2) Facilitate electronic transactions

Q.72. What does the Information Technology Act, 2000 define in the context of electronic records?
(1) Digital cameras (2) Computer systems
(3) Fax machines (4) Photocopy machines
Ans. (2) Computer systems

Q.73. According to the IT Act, 2000, what is the legal status of electronic documents?
(1) Not recognized as evidence
(2) Equivalent to paper documents
(3) Only valid for financial transactions
(4) Acceptable only in criminal cases
Ans. (2) Equivalent to paper documents

Q.74. The IT Act, 2000 provides legal recognition for:
(1) Cryptocurrency transactions
(2) Social media profiles
(3) Electronic signatures
(4) Online gaming accounts
Ans. (3) Electronic signatures

Q.75. What offense is addressed under Section 43 of the Information Technology Act, 2000?
(1) Unauthorized access to computer systems
(2) Copyright infringement
(3) Defamation on social media
(4) Hacking financial databases
Ans. (1) Unauthorized access to computer systems

Q.76. Under the IT Act, 2000, what does "intermediary" refer to?
(1) Middleman in e-commerce transactions
(2) Third party facilitating communication
(3) Government regulatory body

(4) Software used for data encryption
Ans. (2) Third party facilitating communication

Q.77 What does Section 66A of the IT Act, 2000 specifically address?
(1) Cyber terrorism
(2) Data breaches
(3) Online defamation
(4) Unauthorized interception of communication
Ans. (3) Online defamation

Q.78 The IT Act, 2000 empowers the government to issue directions for:
(1) Internet shutdowns
(2) Social media content creation
(3) Online shopping discounts
(4) Mobile app development
Ans. (1) Internet shutdowns

Q.79 In the context of the IT Act, 2000, what does "digital signature certificate" mean?
(1) A software for digital forensics
(2) A secure key for online gaming
(3) A unique identifier for electronic transactions
(4) A code to unlock encrypted files
Ans. (3) A unique identifier for electronic transactions

Q.80 What is the penalty for the offense of cyber terrorism under the IT Act, 2000?
(1) Fine and imprisonment
(2) Community service
(3) Warning letter
(4) Revocation of internet access
Ans. (1) Fine and imprisonment

Q.81 Which international organization is responsible for developing and publishing the ISO/IEC 27001 standard for information security management systems?
(1) International Telecommunication Union (ITU)
(2) International Organization for Standardization (ISO)
(3) Internet Engineering Task Force (IETF)
(4) International Electrotechnical Commission (IEC)
Ans. (2) International Organization for Standardization (ISO)

Q.82 The NIST Cybersecurity Framework is developed by which U.S. government agency?
(1) National Security Agency (NSA)
(2) Central Intelligence Agency (CIA)
(3) National Institute of Standards and Technology (NIST)
(4) Federal Bureau of Investigation (FBI)
Ans. (3) National Institute of Standards and Technology (NIST)

Q.83 Which international standard provides guidelines for implementing an IT service management system?
(1) ISO/IEC 27001 (2) ISO/IEC 20000
(3) ISO 9001 (4) ISO 14001
Ans. (2) ISO/IEC 20000

Q.84 The Common Criteria (ISO/IEC 15408) is primarily associated with:
(1) Cloud computing security
(2) Secure software development
(3) Evaluation of IT security products
(4) Network encryption protocols
Ans. (3) Evaluation of IT security products

Q.85 Which international standard provides guidelines for the management of information security risks?
(1) ISO/IEC 27005 (2) ISO/IEC 27002
(3) ISO/IEC 27032 (4) ISO/IEC 27017
Ans. (1) ISO/IEC 27005

Q.86 ISO/IEC 27002 focuses on
(1) Risk management
(2) Information security controls
(3) Cryptographic protocols
(4) Incident response
Ans. (2) Information security controls

Q.87 Which organization publishes the CIS Controls, a set of best practices for cybersecurity?
(1) Center for Internet Security (CIS)
(2) Cybersecurity and Infrastructure Security Agency (CISA)
(3) International Cybersecurity Institute (ICI)
(4) Cybersecurity Information Sharing Partnership (CISP)
Ans. (1) Center for Internet Security (CIS)

Q.88 The Payment Card Industry Data Security Standard (PCI DSS) is designed to:
(1) Regulate online advertising
(2) Secure credit card transactions
(3) Control social media content
(4) Manage international trade regulations
Ans. (2) Secure credit card transactions

Q.89 What does the acronym IEC stand for in the context of international standards?
(1) International Electromagnetic Compatibility
(2) International Energy Conservation
(3) International Environmental Compliance
(4) International Electrotechnical Commission
Ans. (4) International Electrotechnical Commission

Q.90 The GDPR (General Data Protection Regulation) is a regulation of the European Union related to

(1) Cybersecurity best practices
(2) Data protection and privacy
(3) Internet domain registration
(4) Regulation of e-commerce transactions

Ans. (2) Data protection and privacy

Q.91. Which disaster recovery phase involves returning operations to normal after a disruption?
(1) Mitigation (2) Preparedness
(3) Response (4) Recovery

Ans. (4) Recovery

Q.92. What is the purpose of a tabletop exercise in disaster recovery planning?
(1) Physical fitness training
(2) Testing the effectiveness of the disaster recovery plan
(3) Encrypting sensitive information
(4) Conducting security audits

Ans. (2) Testing the effectiveness of the disaster recovery plan

Q.93. Which factor is critical in determining the Recovery Time Objective (RTO)?
(1) The cost of the disaster recovery plan
(2) The severity of the disaster
(3) The time if takes to restore normal operations
(4) The number of employees in the organization

Ans. (3) The time it takes to restore normal operations

Q.94. What is the purpose of a data escrow in disaster recovery?
(1) Data destruction
(2) Storing data with a third party for safekeeping
(3) Data encryption
(4) Data compression

Ans. (2) Storing data with a third party for safekeeping

Q.95. What is a digital signature in the context of cybersecurity?
(1) A scanned image of a handwritten signature
(2) An encrypted hash value of a document
(3) A physical signature on a digital document
(4) A unique username and password combination

Ans. (2) An encrypted hash value of a document

Q.96. Which key is used for creating a digital signature?
(1) Public key (2) Private key
(3) Session key (4) Symmetric key

Ans. (2) Private key

Q.97. What is the primary purpose of a digital signature?
(1) Encrypting data
(2) Verifying the integrity and authenticity of a message
(3) Hiding the identity of the sender
(4) Controlling network traffic

Ans. (2) Verifying the integrity and authenticity of a message

98. Which cryptographic algorithm is commonly used in digital signatures?
(1) MD5 (2) DES
(3) RSA (4) SHA-1

ns. (3) RSA

99. How does a recipient verify the digital signature of a message?
(1) Using the sender's public key
(2) Using the sender's private key
(3) Comparing the hash value with a known value
(4) Decrypting the message with a shared secret key

ns. (1) Using the sender's public key

100. What is the role of a Certificate Authority (CA) in digital signatures?
(1) Generating digital signatures
(2) Verifying the identity of the sender
(3) Creating public keys
(4) Encrypting messages

ns. (2) Verifying the identity of the sender

❑❑

BCA

(SEM. VI) MODEL PAPER – III

BCA – 6001 : INFORMATION & CYBER SECURITY

Time : 1 :30 Hours Maximum Mar

Q.1. Which of the following actions compromise cyber security?
(1) Vulnerability (2) Attack
(3) Threat (4) Exploit
Ans. (2) Attack

Q.2. Which of the following is the hacking approach where criminals design fake websites or pages for tricking or additional traffic?
(1) Pharming (2) Website-Duplication
(3) Mimicking (4) Spamming
Ans. (1) Pharming

Q.3. Which of the following is not a type of peer-to-peer cyber-crime
(1) MiTM
(2) Injecting Trojans to a target victim
(3) Credit card details leak in the deep web
(4) Phishing
Ans. (3) Credit card details leak in the deep web

Q.4. A cyber-criminal or penetration tester uses the additional da stores certain special instructions in the memory for activi break the system in which of the following attack?
(1) Clickjacking (2) Buffer-overflow
(3) Phishing (4) MiTM
Ans. (2) Buffer-overflow

Q.5. Which of the following do Cyber attackers commonly tar fetching IP address of a target or victim user?
(1) ip tracker (2) emails
(3) websites (4) web pages
Ans. (2) emails

Q.6. Which of the following is defined as an attempt to harm, dam cause threat to a system or network?
(1) Digital crime (2) Threats
(3) System hijacking (4) Cyber Attack
Ans. (4) Cyber Attack

Q.7. They are nefarious hackers, and their main motive is to gain fi profit by doing cyber crimes. Who are "they" referred to here?
(1) White Hat Hackers (2) Black Hat Hackers
(3) Hactivists (4) Gray Hat Hackers
Ans. (2) Black Hat Hackers

IT security in any firm or organization is maintained and handled by _____
(1) Software Security Specialist
(2) CEO of the organization
(3) Security Auditor
(4) IT Security Engineer
(4) IT Security Engineer

Where did the term "hacker" originate?
(1) MIT (2) New York University
(3) Harvard University (4) Bell's Lab
(1) MIT

What is the existence of weakness in a system or network is known as?
(1) Attack (2) Exploit
(3) Vulnerability (4) Threat
(3) Vulnerability

Which of the following is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.
(1) MiTM attack (2) Phishing attack
(3) Website attack (4) DoS attack
(2) Phishing attack

Which of the following is not a step followed by cyber-criminals in data breaching?
(1) Exfiltration
(2) Research and info-gathering
(3) Attack the system
(4) Fixing the bugs
(4) Fixing the bugs

Which of the following online service's privacy cannot be protected using Tor?
(1) Browsing data (2) Instant messaging
(3) Login using ID (4) Relay chats
(2) Instant messaging

Which of the following term refers to a group of hackers who are both white and black hat?
(1) Yellow Hat hackers (2) Grey Hat hackers
(3) Red Hat Hackers (4) White-Black Hat Hackers
(2) Grey Hat hackers

Which of the following is not an email-related hacking tool?
(1) Mail Password (2) Email Finder Pro
(3) Mail PassView (4) Sendinc
(4) Sendinc

Q.17 Which of the following DDoS in mobile systems wait for the own trigger the cyber attack?
(1) botnets (2) programs
(3) virus (4) worms
Ans (1) botnets

Q.18 In the context of cybersecurity, what does the term "White Hacker" refer to?
(1) A hacker who wears a white hat while working
(2) A hacker who uses their skills for ethical and legal purpose
(3) A hacker who focuses on attacking government systems
(4) A hacker who specializes in spreading malware
Ans (2) A hacker who uses their skills for ethical and legal purpose

Q.19 What does the term "Two-Factor Authentication" (2FA) involve?
(1) Using two different internet browsers simultaneously
(2) Authenticating with two different devices
(3) Providing two forms of identification to access an account
(4) Using two different passwords for the same account
Ans. (3) Providing two forms of identification to access an account

Q.20 What is the primary purpose of an Intrusion Detection System (ID
(1) To create a secure network
(2) To identify and respond to suspicious activities or sec incidents
(3) To increase internet speed
(4) To generate secure passwords
Ans. (2) To identify and respond to suspicious activities or sec incidents

Q.21 What is the term for a cybersecurity attack that involves tri individuals into divulging confidential information through ema other communication channels?
(1) Spoofing
(2) Ransomware
(3) Social Engineering
(4) Encryption
Ans. (3) Social Engineering

Q.22 What does the term "Ransomware" refer to in the context of t society?
(1) Software that increases the speed of internet connections
(2) Malicious software that encrypts files and demands a ra for their release
(3) A type of antivirus program
(4) Software used for ethical hacking
Ans. (2) Malicious software that encrypts files and demands a ra for their release

Q.23 Which of the following is a potential security risk associated public Wi-Fi networks?

(1) Increased internet speed
(2) Enhanced data encryption
(3) Man-in-the-Middle attacks
(4) Improved network stability
Ans. (2) Man-in-the-Middle attacks

Q.24 What is the primary purpose of the "Cookie" files used in web browsers?
(1) To store website preferences
(2) To track users' physical locations
(3) To increase internet speed
(4) To encrypt online communications
Ans. (1) To store website preferences

Q.25 In the context of cybersecurity, what does the term "Zero Trust" refer to?
(1) Trusting all devices and users by default
(2) A security model that requires verification from everyone trying to access resources, regardless of their location
(3) A belief in the inevitability of cyber attacks
(4) Trusting only government agencies for cybersecurity
Ans. (2) A security model that requires verification from everyone trying to access resources, regardless of their location

Q.26 What is the primary purpose of a vulnerability assessment in cybersecurity?
(1) To test the speed of internet connections
(2) To identify weaknesses in a system or network
(3) To create secure passwords
(4) To develop new software applications
Ans. (2) To identify weaknesses in a system or network

Q.27 What does the term "Social Media Algorithm" refer to in the context of the cyber society?
(1) A set of rules governing online etiquette
(2) A mathematical formula used to encrypt messages
(3) A set of instructions for creating social media accounts
(4) A computational process that determines the content shown to users on social media platforms
Ans. (4) A computational process that determines the content shown to users on social media platforms

Q.28 In the context of cybersecurity, what is the purpose of a honeypot?
(1) To attract bees to the internet
(2) To detect and analyze cyber threats by mimicking vulnerable systems
(3) To store large amounts of honey for online transactions
(4) To enhance the flavor of online content
Ans. (2) To detect and analyze cyber threats by mimicking vulnerable systems

Q.29 What is the term for a cybersecurity attack that involves overwhelming a system or network with traffic to make it unavailable?
(1) Phishing
(2) DDoS (Distributed Denial of Service) attack
(3) Spoofing
(4) Zero-Day Exploit
Ans. (2) DDoS (Distributed Denial of Service) attack

Q.30 What is the concept of "Metadata" in the context of cyber society?
(1) Data that describes other data, providing information about it
(2) A type of computer virus
(3) Encrypted messages exchanged between users
(4) An online forum for discussing cybersecurity issues
Ans. (1) Data that describes other data, providing information about it

Q.31 Which of the following is a common method of protecting sensitive information during online communication?
(1) Using unsecured Wi-Fi networks
(2) Sending information via plain text emails
(3) Employing end-to-end encryption
(4) Increasing the font size of messages
Ans. (3) Employing end-to-end encryption

Q.32 What is the role of a Security Information and Event Management (SIEM) system in cybersecurity?
(1) To manage social media accounts
(2) To monitor and analyze security events in real-time
(3) To create secure passwords
(4) To design secure websites
Ans. (2) To monitor and analyze security events in real-time

Q.33 In the context of cybersecurity, what is the significance of the "Principle of Least Privilege"?
(1) Giving everyone maximum access to data
(2) Restricting access rights to the minimum necessary for tasks
(3) Allowing unlimited access to network resources
(4) Encouraging password sharing among colleagues
Ans. (2) Restricting access rights to the minimum necessary for tasks

Q.34 What does the term "Cybersecurity Framework" refer to?
(1) A blueprint for constructing physical security barriers
(2) A set of guidelines and best practices for managing cybersecurity risk
(3) A programming language for developing cybersecurity software
(4) A virtual reality environment for cybersecurity training
Ans. (2) A set of guidelines and best practices for managing cybersecurity risk

35 What is the primary purpose of a security patch in the cyber society?
(1) To increase the speed of internet connections
(2) To repair vulnerabilities in software and improve security
(3) To create secure passwords
(4) To detect and analyze cyber threats
ns (2) To repair vulnerabilities in software and improve security

36 What is the primary purpose of cybersecurity awareness training for employees?
(1) To install security patches
(2) To prevent all cyberattacks
(3) To educate employees on security best practices
(4) To block unauthorized access to the network
ns. (3) To educate employees on security best practices

37 What does a VPN provide in the context of cybersecurity?
(1) Anonymity on the internet
(2) Protection against physical theft
(3) Antivirus scanning
(4) Biometric authentication
ns (1) Anonymity on the internet

38 Which cryptographic algorithm is commonly used for secure communication over the internet, such as HTTPS?
(1) RSA (2) AES
(3) DES (4) SHA
ns. (2) AES

39 What is the purpose of a cybersecurity policy within an organization?
(1) Ensure compliance with environmental regulations
(2) Define the organization's approach to managing cybersecurity risks
(3) Schedule regular software updates
(4) Monitor employee productivity
ns. (2) Define the organization's approach to managing cybersecurity risks

40 Why is it important to regularly apply security patches to software and systems?
(1) To increase network speed
(2) To prevent all cyberattacks
(3) To fix known vulnerabilities and weaknesses
(4) To encrypt sensitive data
ns (3) To fix known vulnerabilities and weaknesses

41 In the context of incident response, what does the term "downtime" refer to?
(1) The time taken to identify a security incident
(2) The time during which a system or service is unavailable
(3) The time required to update antivirus definitions
(4) The time allocated for employee cybersecurity training
ns. (2) The time during which a system or service is unavailable

Q.42 Which of the following is an example of something you know i multi-factor authentication (MFA)?
(1) Fingerprint
(2) One-Time Password (OTP)
(3) Smart Card
(4) Personal Identification Number (PIN)
Ans. (4) Personal Identification Number (PIN)

Q.43 What is the primary goal of cyber threat intelligence in cybersecurity
(1) To secure physical facilities
(2) To gather information on competitors
(3) To provide insights into potential cyber threats
(4) To monitor employee emails
Ans. (3) To provide insights into potential cyber threats

Q.44 What is a key consideration for ensuring security in cloud computin environments?
(1) Physical access control
(2) Network speed optimization
(3) Data encryption during transmission
(4) User account creation
Ans. (3) Data encryption during transmission

Q.45 Which international standard focuses on information securi management systems?
(1) ISO/IEC 27001 (2) NIST SP 800-53
(3) COBIT (4) CIS Controls
Ans. (1) ISO/IEC 27001

Q.46 What is the main goal of a pretexting attack in social engineering?
(1) To gain unauthorized access to a system
(2) To impersonate a legitimate entity
(3) To spread malware
(4) To launch a denial-of-service attack
Ans. (2) To impersonate a legitimate entity

Q.47 What is the purpose of network scanning in cybersecurity?
(1) Encrypting sensitive data
(2) Identifying vulnerabilities and open ports
(3) Monitoring employee emails
(4) Ensuring compliance with cybersecurity policies
Ans. (2) Identifying vulnerabilities and open ports

Q.48 What is the primary objective of a ransomware attack?
(1) Stealing sensitive information
(2) Disrupting network services
(3) Encrypting files and demanding payment for decryption
(4) Impersonating a legitimate entity
Ans. (3) Encrypting files and demanding payment for decryption

Q.49 What is a common security measure for protecting mobile devices?
(1) MAC Filtering (2) Disk Encryption
(3) Firewalls (4) Network Segmentation
Ans. (2) Disk Encryption

Q.50 Why is ongoing security awareness training important for employees?
(1) To install security patches
(2) To prevent all cyber attacks
(3) To adapt to evolving cyber threats and risks
(4) To encrypt sensitive data
Ans. (3) To adapt to evolving cyber threats and risks

Q.51 What is the primary purpose of endpoint security?
(1) Protecting network infrastructure
(2) Securing data in transit
(3) Ensuring the security of individual devices (endpoints)
(4) Monitoring network traffic
Ans. (3) Ensuring the security of individual devices (endpoints)

Q.52 What is the first step in the cybersecurity risk management process?
(1) Risk assessment (2) Risk mitigation
(3) Risk acceptance (4) Risk analysis
Ans. (1) Risk assessment

Q.53 What is a common security concern associated with IoT devices?
(1) Slow network speed
(2) Lack of encryption
(3) Overuse of firewalls
(4) Too many security patches
Ans. (2) Lack of encryption

Q.54 What is the purpose of IAM in cybersecurity?
(1) Monitoring network traffic
(2) Managing user identities and controlling access to resources
(3) Encrypting sensitive data
(4) Conducting penetration tests
Ans. (2) Managing user identities and controlling access to resources

Q.55 What is a fundamental principle of secure coding?
(1) Maximizing code complexity
(2) Input validation and sanitization
(3) Ignoring error handling
(4) Avoiding version control
Ans. (2) Input validation and sanitization

Q.56 _____ is a type of software designed to help the user's computer detect viruses and avoid them.
(1) Malware (2) Adware
(3) Antivirus (4) Both 2 and 3
Ans. (3) Antivirus

Q.57 What is the purpose of conducting periodic wireless site surveys for security?
(1) Improves signal strength
(2) Identifies and mitigates signal interference
(3) Enhances device compatibility

(4) Increases network speed

Ans. (2) Identifies and mitigates signal interference

Q.58 How does the use of a strong firewall contribute to wireless network security?
(1) Improves signal strength
(2) Blocks unauthorized access and malicious traffic
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Blocks unauthorized access and malicious traffic

Q.59 What is the role of a security log in wireless network protection?
(1) Improves signal strength
(2) Records and monitors security-related events
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Records and monitors security-related events

Q.60 Why is it important to implement a strong physical access control policy for server rooms housing wireless infrastructure?
(1) Improves signal strength
(2) Prevents unauthorized physical access to critical infrastructure
(3) Enhances device compatibility
(4) Increases network speed.

Ans. (2) Prevents unauthorized physical access to critical infrastructure

Q.61 What is the purpose of a honey pot in wireless network security?
(1) Improves signal strength
(2) Attracts and identifies attackers
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Attracts and identifies attackers

Q.62 How does regular network monitoring contribute to wireless security?
(1) Improves signal strength
(2) Identifies abnormal patterns and potential security threats
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Identifies abnormal patterns and potential security threats

Q.63 What is the primary purpose of securing DNS (Domain Name System) in wireless networks?
(1) Improves signal strength
(2) Prevents DNS spoofing and hijacking
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Prevents DNS spoofing and hijacking

Q.64 Why is it important to educate users about the risks of connecting to unsecured public Wi-Fi networks?
(1) Improves signal strength
(2) Reduces the risk of data interception and unauthorized access

(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Reduces the risk of data interception and unauthorized access

Q.65 What is the purpose of conducting regular security assessments on wireless networks?
(1) Improves signal strength
(2) Identifies vulnerabilities and weaknesses
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Identifies vulnerabilities and weaknesses

Q.66 How does implementing a strong password policy for wireless networks contribute to security?
(1) Improves signal strength
(2) Prevents unauthorized access through strong authentication
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Prevents unauthorized access through strong authentication

Q.67 What role does firmware validation play in the security of wireless routers and access points?
(1) Improves signal strength
(2) Ensures the authenticity and integrity of device firmware
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Ensures the authenticity and integrity of device firmware

Q.68 Why is it crucial to disable unnecessary network services on wireless devices?
(1) Improves signal strength
(2) Reduces the attack surface and potential vulnerabilities
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Reduces the attack surface and potential vulnerabilities

Q.69 What security measure involves using network address translation (NAT) for internal devices?
(1) Improves signal strength
(2) NAT prevents direct access to internal IP addresses
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) NAT prevents direct access to internal IP addresses

Q.70 How does implementing secure boot processes contribute to the overall security of wireless devices?
(1) Improves signal strength
(2) Ensures only authenticated and authorized firmware is loaded
(3) Enhances device compatibility
(4) Increases network speed

Ans. (2) Ensures only authenticated and authorized firmware is loaded

Q.71 What is the role of a security token in two-factor authentication for wireless networks?
(1) Improves signal strength
(2) Generates temporary authentication codes for enhanced security
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Generates temporary authentication codes for enhanced security

Q.72 How does implementing port security on switches contribute to wireless network security?
(1) Improves signal strength
(2) Prevents unauthorized devices from connecting to the network
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Prevents unauthorized devices from connecting to the network

Q.73 What is the purpose of using a VPN (Virtual Private Network) for remote access to a wireless network?
(1) Improves signal strength
(2) Encrypts data for secure transmission over the internet
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Encrypts data for secure transmission over the internet

Q.74 How does implementing a security-focused BYOD (Bring Your Own Device) policy contribute to wireless network security?
(1) Improves signal strength
(2) Establishes guidelines for secure use of personal devices on the network
(3) Enhances device compatibility
(4) Increases network speed
Ans. (2) Establishes guidelines for secure use of personal devices on the network

Q.75 What is the primary goal of a digital forensic investigation?
(1) To recover lost passwords
(2) To analyze and preserve electronic evidence
(3) To monitor online activities in real-time
(4) To enhance computer system performance
Ans. (2) To analyze and preserve electronic evidence

Q.76 In a criminal investigation, what is the role of the investigating agency in gathering evidence?
(1) Only collecting physical evidence
(2) Collecting both physical and digital evidence
(3) Relying solely on eyewitness accounts
(4) Ignoring digital evidence as it is less reliable
Ans. (2) Collecting both physical and digital evidence

Q.77 What is the significance of chain of custody in a forensic investigation?
(1) It determines the investigator's expertise
(2) It establishes the chronological documentation of evidence handling
(3) It specifies the types of evidence that can be collected
(4) It outlines the legal process for obtaining a search warrant
Ans. (2) It establishes the chronological documentation of evidence handling

Q.78 What does the term "volatile data" refer to in a forensic investigation?
(1) Data stored on external hard drives
(2) Data that is easily tampered with or lost
(3) Encrypted data requiring a key for access
(4) Data accessed during regular business operations
Ans. (2) Data that is easily tampered with or lost

Q.79 What is the primary purpose of a search warrant in a digital forensic investigation?
(1) To validate the credentials of the investigating team
(2) To authorize the seizure of electronic devices for evidence
(3) To track the location of suspects in real-time
(4) To obtain access to private online communications
Ans. (2) To authorize the seizure of electronic devices for evidence

Q.80 In a computer crime investigation, what is the term for the unauthorized access of computer systems?
(1) Cyberbullying (2) Cyberstalking
(3) Hacking (4) Phishing
Ans. (3) Hacking

Q.81 What is the primary role of digital imaging in forensic investigations?
(1) Capturing crime scene photos for documentation
(2) Creating duplicate copies of digital evidence
(3) Enhancing images for facial recognition
(4) Analyzing fingerprints on digital surfaces
Ans. (2) Creating duplicate copies of digital evidence

Q.82 In a financial fraud investigation, what is the purpose of tracing transactions?
(1) Identifying potential witnesses
(2) Tracking the movement of funds
(3) Collecting physical evidence from crime scenes
(4) Analyzing social media activities of suspects
Ans. (2) Tracking the movement of funds

Q.83 What does the term "steganography" refer to in the context of digital investigations?
(1) Unauthorized access to computer systems
(2) Concealing information within digital files
(3) Tracing financial transactions

(4) Monitoring online activities in real-time
Ans. (2) Concealing information within digital files

Q.84 What is the purpose of conducting a forensic analysis of net logs?
(1) Monitoring employee productivity
(2) Identifying network vulnerabilities
(3) Assessing the physical security of servers
(4) Recovering lost passwords
Ans. (2) Identifying network vulnerabilities

Q.85 What is the primary purpose of multi-factor authentication (MFA)?
(1) To restrict internet access
(2) To enhance the speed of data transmission
(3) To verify user identity using multiple credentials
(4) To encrypt stored data
Ans. (3) To verify user identity using multiple credentials

Q.86 Which one of the following is a type of antivirus program?
(1) Quick heal (2) Mcafee
(3) Kaspersky (4) All of the above
Ans. (4) All of these

Q.87 Which of the following refers to exploring the appropriate, et behaviors related to the online environment and digital m platform?
(1) Cyber low (2) Cyberethics
(3) Cybersecurity (4) Cybersafety
Ans. (2) cyberethics

Q.88 What is the primary purpose of Endpoint Protection in cybersecu
(1) To secure physical access to servers
(2) To regulate internet traffic within an organization
(3) To protect individual devices (endpoints) from malware other cyber threats
(4) To monitor employee emails
Ans. (3) To protect individual devices (endpoints) from malware other cyber threats

Q.89 What is the role of encryption in cybersecurity?
(1) To block access to specific websites
(2) To encode data in a way that only authorized parties access it
(3) To regulate e-commerce transactions
(4) To secure physical access to computer networks
Ans. (2) To encode data in a way that only authorized parties access it

Q.90 What is the purpose of Security Information and Event Manage (SIEM) systems in cybersecurity?
(1) To manage access control lists
(2) To analyze and correlate security event data from va sources

(3) To regulate online advertising
(4) To secure physical access to data centers
Ans. (2) To analyze and correlate security event data from various sources

Q.91 Which property of digital signatures ensures that they cannot be altered once applied?
(1) Non-repudiation (2) Confidentiality
(3) Availability (4) Integrity
Ans. (4) Integrity

Q.92 What is the term for a digital signature that is verified by a trusted third party, such as a Certificate Authority?
(1) Self-signed signature (2) Public signature
(3) Certified signature (4) Private signature
Ans. (3) Certified signature

Q.93 In which phase of a digital signature process is the hash value encrypted with the sender's private key?
(1) Signature creation (2) Signature verification
(3) Key generation (4) Key distribution
Ans. (1) Signature creation

Q.94 What is the benefit of using a digital signature in email communication?
(1) Increased download speed
(2) Enhanced visual appeal
(3) Authentication and integrity verification
(4) Improved network performance
Ans. (3) Authentication and integrity verification

Q.95 Which phase of computer forensics involves collecting and preserving evidence in a way that maintains its integrity?
(1) Analysis (2) Reporting
(3) Examination (4) Preservation
Ans. (4) Preservation

Q.96 What is the role of a write blocker in computer forensics?
(1) Encrypting data
(2) Identifying malware
(3) Preventing changes to evidence during the imaging process
(4) Conducting network scans
Ans. (3) Preventing changes to evidence during the imaging process

Q.97 Which file system metadata is commonly examined during a computer forensics investigation?
(1) RAM (2) Registry files
(3) Swap files (4) Firewall logs
Ans. (2) Registry files

Q.98 What is steganography in the context of computer forensics?
(1) Recovering lost data

(2) Hiding information within other data
(3) Decrypting encrypted files
(4) Analyzing network traffic

Ans. (2) Hiding information within other data

Q.99.What is the purpose of timeline analysis in computer forensics?
(1) Identifying the sequence of events on a computer system
(2) Encrypting communication channels
(3) Recovering deleted files
(4) Conducting network scans

Ans. (1) Identifying the sequence of events on a computer system

Q.100.What is the term for the process of converting raw digital evidence into a readable format for analysis?
(1) Imaging (2) Hashing
(3) Decryption (4) Parsing

Ans. (4) Parsing

❑❑