Cyber Security

1. What type of covert computer attack uses devices or computer programs that captures anything the user types or anywhere the user clicks with a mouse?

A. cross-site scripting
B. keylogger
C. buffer overflow
D. macro virus

2. Spoofing is the act of falsely identifying a packet's IP address, MAC address, etWhich of the below are three types of Spoofing?

A. Web Spoofing, DNS Spoofing, and Relay Spoofing
B. ARP Poisoning, Web Spoofing, and DNS Spoofing
C. DNS Spoofing, Relay Spoofing, and ARP Poisoning
D. Web Spoofing, ARP Poisoning, and Relay Spoofing

3. This refers to applications or files that are not classified as viruses or Trojan Horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization. This is done by performing a variety of undesired actions such as irritating users with pop-up windows, tracking user habits, and unnecessarily exposing computer vulnerabilities to attack.

A. Adware
B. Malware
C. Spyware
D. Grayware

4. Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. What are three methods antivirus software use to identify malware?

A. Quarantine-Based Detection, File Emulation, Signature-Based Detection
B. Kernel-Based Detection, Heuristic-Based Detection, File Emulation
C. Signature-Based Detection, Heuristic-Based Detection, File Emulation
D. Signature-Based Detection, Kernel-Based Detection, File Emulation

5. Cloud-computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. What is the primary function of cloud antivirus technology?

A. A technology that uses heuristic to produce quickly enough a solution that is good enough for solving the problem at hand. The solution may not be the best of all the actual solutions, but it is still valuable because finding it does not require a prohibitively long time.

B. A technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure.

C. A technology that prevent unknown programs and processes from accessing the system.

D. A technology that monitors computer systems for suspicious activity in real time, in other words, while the data is loaded into the computer's memory.

6. Your regular bills and account statements do not arrive on time, you never receive bills or collection notices for products or services, or you receive calls from debt collectors about debts that do not belong to you are examples of:

A. Red Flags of Bank Account Hacking

B. Red Flags of Identity Theft

C. Red Flags of Credit Card Theft

D. Red Flags of Postal Fraud

7. What type of Trojan Horses send a copy of itself to all recipients in a user's address book, which causes an outbreak by passing throughout a network?

A. Logic Bomb

B. Spyware

C. Droppers

D. Malware

8. What is considered the first piece of malicious software to have caused significant damage on the Internet?

A. "I Love You" virus

B. Code Red

C. Melissa virus

D. Morris worm

9. A Trojan horse, or Trojan, is a hacking program that is a non-self-replicating type of malware that gains privileged access to the operating system while appearing to perform a desirable function but instead drops a malicious payload. What do Trojans install that create a hidden opening allowing access to a system?

A. Keylogger

B. Malware

C. Backdoor

D. Virus

10. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself into other computer programs, data files, or the boot sector. When this replication succeeds, the affected areas are then said to be infected. This type of virus spreads by infecting USB disks or hard drive disks. The virus is loaded into memory and attempts to infect any and all disks inserted into the computer.

A. Macro
B. File Infector
C. Multipartite
D. Boot Sector

11. Which one of the following is a network attack where the attacker creates an ICMP packet that's larger than the maximum allowed size of 65,535 bytes?
A. Distributed Denial of Service (DDoS)
B. buffer overflow
C. worm
D. Ping of Death

12. Which one of the following is a form of social engineering where an unauthorized person follows closely behind an authorized person into a restricted area?
A. elicitation
B. shoulder surfing
C. keylogging
D. piggybacking

13. Computer software, or just software, is any set of machine-readable instructions that directs a computer's processor to perform specific operations. Changes and improvements to software happen. What is a collection of updates, fixes, or enhancements to a software program delivered in the form of a single installable bundle because installing is easier and less error-prone?
A. Version Update
B. Service Kit
C. Service Pack
D. Security Update

14. This must be regularly updated by a computer's anti-virus program and is used to identify potential malicious software?
A. spam filter
B. signature file
C. white list
D. anti-spyware

15. Which class of brute-force mathematical attack exploits mathematical weaknesses of hash algorithms and one-way hash functions?
A. Dumpster Diving
B. Social Engineering
C. Online Attack
D. Birthday Attack

16. Many legislative Acts affect computer security. Which Act changed computer crime damage assessments, increasing the number of crimes violating federal law?

A. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act)

B. The Privacy Act

C. The Health Insurance Portability and Accountability Act (HIPAA)

D. The Gramm- Leach-Bliley Act (GLBA)

17. TCP/IP provides end-to-end connectivity, specifying how data should be formatted, addressed, transmitted, routed, and received at the destination. The Open Systems Interconnection (OSI) model is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model groups similar communication functions into one of seven logical layers. Which four of the seven layers does TCP/IP operate?

A. Physical, Network, Application, Session

B. Data Link, Transport, Physical, Session

C. Application, Transport, Network, Data Link

D. Transport, Network, Session, Application

18. Which is a set of protocols developed to support the secure exchange of packets and is required in IPv6?

A. IPsec

B. HTTPS

C. TCP/IP

D. Intrusion Detection Systems

19. How do organizations classify information such as client lists, product designs, and organizational strategies?

A. private

B. secure

C. secret

D. sensitive

20. Risk is comprised of what two components?

A. Security and Vulnerability

B. Vulnerability and Threat

C. Security and Threat

D. Target and Threat

21. A security database that contains entries for users and their access rights for files and folders is known as?

A. mandatory access control (MAC)

B. a firewall policy

C. an access control list (ACL)
D. role-based access

22. The Open Systems Interconnection (OSI) model is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model groups similar communication functions into one of seven logical layers. This hardware device operates at the data link layer of the OSI model and can limit hostile sniffing on a LAN (Local Area Network)?

A. Ethernet Hub
B. Ethernet Switch
C. Modem
D. Firewall

23. The purpose of classification is to protect information from being used to damage or endanger national security, research and development, or proprietary information. How do organizations classify information such as client lists, product designs, and organizational strategies?

A. secure
B. sensitive
C. private
D. secret

24. What can an intruder place between two endpoints to capture an entire session?

A. sniffers
B. tunnels
C. gateways
D. spoofers

25. Internet browsers use this to store pages and other multimedia content, such as video and audio files, from websites visited by the user. This allows such websites to load more quickly the next time they are visited.

A. temporary Internet file
B. cache
C. cookie
D. browser history

26. File Transfer Protocol (FTP) uses a client-server architecture and uses separate control and data connections between the client and the server. What do system administrators do to secure a FTP server so only authorized users can access the server?

A. Allow Blind Authentication
B. Redirect FTP to Another Port
C. Disable Anonymous Authentication
D. Initiate Access Control

27. Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) Snort's open source network-based intrusion detection system has the ability to perform real-time traffic analysis and packet logging on IP networks. Snort performs protocol analysis, content searching, and content matching. What is the correct Snort Rule syntex to log TCP traffic from any port going to ports less than or equal to 4000 on the 192.168.1.0 network?

A. log tcp any any -> 192.168.1.0/24 <=4000
B. log udp any any -> 192.168.1.0/24 :4000
C. log tcp any any -> 192.168.1.0/24 :4000
D. log tcp any any -> 192.168.1.0/24 any

28. At what stage of the security system development life cycle do organization's purchase or build security solution?

A. Development Phase
B. Maintenance Phase
C. Physical Design Phase
D. Implementation Phase

29. Some virtual networks may not use encryption to protect the data contents. What process do users initiate when carrying a payload over an incompatible delivery-network, or providing a secure path through an untrusted network?

A. Private Networking
B. Tunneling
C. Network Forwarding
D. Channeling

30. When collecting digital evidence from a crime scene, often the best strategy for dealing with a computer that is powered on is to:

A. remove the hard drive
B. transport it while running
C. unplug it
D. perform a clean shutdown

31. This is a non-malicious, yet false message spread by users forwarding to a large number of recipients.

A. phishing
B. e-mail hoax
C. worms
D. keylogger

32. What is the unique number assigned to a message by the e-mail server?

A. IP address

B. e-mail address
C. message ID
D. e-mail ID

33. A cyber attack is a type of offensive maneuver employed by both individuals and whole organizations that target computer information systems, infrastructures, computer networks, and/ or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. What is a Distributed Denial of Service Attack?

A. An attack in which a computer connected to the Internet harvests email addresses from contact forms or guestbook pages.

B. An attack in which a computer connected to the Internet that has been compromised and is used to perform malicious tasks of one sort or another under remote direction.

C. An attack in which incorrect automated bounce messages are repeatedly sent by mail servers, typically as a side effect of incoming spam, thereby filling a user's inbox and possibly shutting down the email server.

D. An attack in which multitudes of compromised systems attack a single target and the flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

34. This protocol is used to encrypt and digitally sign email messages using the X.509 format for certificates.

A. WPA2
B. S/MIME
C. HTTPS
D. SMTP

35. Why is instant messaging dangerous for file transfers?

A. It may not work with all IM clients.
B. It is preferred by spammers.
C. It allows recipients to view all of your files.
D. It bypasses server-based malware protection.

36. What is the difference between SMTP and POP3?

A. The SMTP server listens on port 25, while POP3 listens on port 110.
B. STMP is secure and POP3 isn't.
C. SMTP handles incoming e-mail and POP3 handles outgoing e-mail.
D. There are no differences.

37. Simple Mail Transfer Protocol (SMTP) is an Internet standard for email transmission across Internet Protocol (IP) networks. Your SMTP server is the source of excessive spam emails. What is the most likely cause?

A. The anonymous relays are not disabled
B. The remailer service is not turned off
C. The Domain Name Service root servers are insecure
D. The administrator account is disabled

38. What is the act of making an e-mail message look like it came from someone else or a different location?
A. forging
B. spoofing
C. spamming
D. phishing

39. Attackers have learned to capitalize and take advantage of the human factor in trust relationships. What type of attack uses chat, social media, and email to exploit trust relationships?
A. Chat Attack
B. Cyber Attack
C. Replay Attack
D. Online attack

40. What is the purpose of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003?
A. Allow email marketers to send unsolicited commercial e-mail as long as it adheres to 3 basic types of compliance: unsubscribe, content, and sending behavior compliance
B. Outlines criminal penalties for senders of pornography and SPAM
C. Allow SPAM recipients to sue the sender
D. Require e-mailers to get permission before they send marketing messages

41. What type of email scam involves Internet fraudsters who send seemingly legitimate e-mail messages to trick unsuspecting victims into revealing personal and financial information, such as a Social Security number (SSN), that can be used to steal the victims' identity and gain access to the victim's finances?
A. Snerting
B. Spoofing
C. Phishing
D. Social Engineering

42. What is an attempt to make a machine or network resource unavailable to its intended users by temporarily or indefinitely interrupt or suspend services of a host connected to the Internet?
A. Backscatter
B. DOSNET
C. Traffic Shaping
D. Denial of Service

43. This type of attack is an anomaly where a program, while writing data, overruns the boundary and overwrites adjacent memory. Most security applications and suites are incapable of adequate defense against these kinds of attacks.

A. BotNet
B. Malware
C. Buffer Overflow
D. Denial of Service

44. What type of intrusion detection system takes action after intruder detection?

A. dynamic
B. static
C. active
D. passive

45. What is a false positive?

A. An event signaling an intrusion detection system to produce an alarm when no attack has taken place
B. An event when no attack has taken place and no alarm is raised
C. A legitimate attack that triggers an intrusion detection system to produce an alarm
D. A failure of an intrusion detection system to detect an actual attack

46. The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. Which encryption scheme does PKI use?

A. Quantum Encryption
B. Elliptical Curve Encryption
C. Symmetric Encryption
D. Asymmetric Encryption

47. What is the process of recovering passwords from data that has been stored in or transmitted by a computer system?

A. Password Reversing
B. Password Distributing
C. Password Shadowing
D. Password Cracking

48. The purpose of this is to help you make more-informed decisions about which security measures to adopt?

A. Detection Assessment
B. Threat Assessment
C. Vulnerability Assessment

D. Security Assessment

49. This type of assessment answers the following questions: What to protect? Who/What are the threats and vulnerabilities? What are the implications of damage or loss? What is the value to the organization? What can minimize exposure to the loss or damage?

A. vulnerability assessment
B. risk assessment
C. detection assessment
D. security assessment

50. What are groups of rigorous methods for finding bugs or errors in code related to computer security. These methods are used for testing purposes and are very important for ensuring that potential vulnerabilities are prevented.

A. Attack Conditions
B. Attack Patterns
C. Attack Mitigation
D. Attack Vulnerabilities

51. Heuristic scanning is a:

A. security device that sets black lists and white lists for all Internet traffic as it enters or leaves a network
B. process for reviewing all e-mail for spam as it enters or leaves a network
C. form of penetration testing that detects malicious programs on specific computer systems
D. method of detecting potentially malicious behavior by examining what a program does or how it acts

52. In cryptography, a key is a piece of information that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. What is the primary principle of encryption using a key?

A. All functions are public, only the key is secret. The key contains the parameters used for the encryption responsible for decryption.
B. The key indicates which function is used for encryption. Thereby it is more difficult to decrypt an intercepted message as the function is unknown.
C. The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
D. The key contains the secret function for encryption including parameters. Only a password can activate the key.

53. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. What is the primary role of the Certificate Authority?

A. To track self-signed certificates and third party attestations of those certifications

B. To review critical transactions communications between two or more parties
C. To digitally sign and publish the public key bound to a given user
D. To use a random number generator to create public keys

54. What is the primary role of the Certificate Authority?
A. to use a random number generator to create public keys
B. to review critical transactions communications between two or more parties
C. to digitally sign and publish the public key bound to a given user
D. to track self-signed certificates and third party attestations of those certifications

55. In a Public Key infrastructure, this provides nonrepudiation:
A. symmetric keys
B. digital signature
C. e-mail signature
D. electronic certificates

56. The digital signature scheme consists of which three algorithms?
A. a key generation algorithm, an asymmetric key algorithm, and a signing algorithm
B. a symmetric key algorithm, a signing algorithm, and a signature verification algorithm
C. a key generation algorithm, a signing algorithm, and a hash-and-decrypt algorithm
D. a key generation algorithm, a signing algorithm, and a signature verification algorithm

57. In computer security, challenge-response authentication is a family of protocols in which one party presents a question/challenge and another party must provide a valid answer/response to be authenticated. The simplest example of a challenge-response protocol is password authentication, where the challenge is asking for the password and the valid response is the correct password. Which technology issues a challenge/response test as a means of ascertaining that a user is a human and not a computer program?
A. CAPTCHA
B. Site Key
C. Munging
D. CHAP

58. This security principle describes the requirement that different people should perform different portions of a critical process.
A. segregation of duties
B. job rotation
C. defense in depth
D. least privilege

59. What type of authentication methodology uses a person's physical characteristic for identification?
A. Voice Analysis

B. Behaviometrics
C. Biometrics
D. Facial Recognition

60. When withdrawing money from an automated teller machine, a user inserts a card (something he has) and enters a pin code (something he knows) into a keypad. What type of authentication is this?
A. Two-factor Authentication
B. Common Authentication
C. Two-factor Authorization
D. Multi-Factor Authentication

61. In networking, the Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. What authentication method is used in conjunction with PPP to validate the identify of a client?
A. Password Authentication Protocol (PAP)
B. Extensible Authentication Protocol (EAP)
C. Challenge-Handshake Authentication Protocol (CHAP)
D. Routing Internet Protocol (RIP)

62. Your boss does not want anyone else to have the ability to read an email except the intended recipient. What type of security ensures only the intended recipient can read your email?
A. Confidentiality
B. Authentication
C. Integrity
D. Availability

63. A binary code represents text or computer processor instructions using the binary number system's two binary digits - 0 and 1. What is added to the end of a string of binary code that indicates whether the number of bits in the string with the value one is even or odd?
A. Modular Sum
B. Parity Bit
C. Checksum
D. Parity Word

64. What is a credential issued by the Authentication Service that supplies valid authentication credentials?
A. Security Ticket
B. Server Certificate
C. User Certificate
D. Server Ticket

65. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. What setup should an administrator use for regularly testing the strength of user passwords

A. A networked workstation so the password database can easily be copied locally and processed by the cracking program.

B. A networked workstation so the cracking program can access the live password database.

C. A standalone workstation on which the password database is copied and processed by the cracking program.

D. A standalone workstation so that the live password database can be accessed and processed by the cracking program.

66. In computing, the Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. When does CHAP perform the handshake process?

A. When establishing a connection and after disconnecting the session

B. Only when establishing the initial connection

C. Only after the connection is established

D. When establishing a connection and at any time after the connection is established

67. Which one of the following is not an effect of a natural disaster on a computer?

A. water damage

B. smoke damage to the hard drive

C. static electricity

D. power fluctuations

68. What is the best reason water isn't used to suppress fires in a data center?

A. It's too expensive compared to other methods.

B. Water may not be able to reach all servers in a rack.

C. Water would ruin the electronics in computers and network equipment.

D. Water cannot put out electrical fires.

69. This provides duplication of server data storage by using multiple hard drive volumes.

A. Disk Striping

B. Mirroring

C. Hot Swapping

D. Parity

70. What RAID level uses disk striping?

A. RAID 0+1

B. RAID 5

C. RAID 1

D. RAID 0

71. This term refers to the ability to maintain data and operational processing despite a disrupting event?

A. high availability
B. high definition
C. disaster planning
D. business continuity

72. Regarding Business Continuity Planning and Disaster Recovery Planning, which one of the following determines the recovery cost balancing?

A. cost of impact and the cost of resources
B. maximum allowable outage and the cost to recover
C. cost of disruption and the cost to recover
D. cost of system inoperability and the cost of resources to recover

73. The CEO wants to determine the feasibility of the IT recovery process, verify the compatibility of backup facilities, and ensuring the adequacy of procedures relating to the various teams working in the recovery process. These tasks are examples of what?

A. Disaster Recovery Plan Maintenance
B. Disaster Recovery Plan Training
C. Disaster Recovery Plan Testing
D. Disaster Recovery Plan Authentication

74. This type of plan contains the steps for implementing critical business functions using alternate mechanisms until normal operations can be resumed at the primary site or elsewhere on a permanent basis.

A. Incremental Recovery Plan
B. Disaster Recovery Plan
C. Incident Recovery Plan
D. Business Continuity Plan

75. What are the three primary strategies when developing a disaster recovery plan?

A. Corrective Measures, Detective Measures, and Risk Assessment
B. Risk Assessment, Independent Verification and Validation, and Management Support
C. Management Support, Detective Measures, and Preventative Measures
D. Preventive Measures, Detective Measures, and Corrective Measures

76. Which one of the following configurations of elements represents the most complete disaster recovery plan?

A. vendor contract for alternate processing site, names of persons on the disaster recovery team, and offsite storage procedures
B. vendor contract for alternate processing site, backup procedures, and names of persons on the disaster recovery team

C. off-site storage procedures, identification of critical applications, and test of the plan

D. alternate processing site, backup and off-site storage procedures, identification of critical applications, and test of the plan

77. Which one of the following IT contingency solutions provides recovery time objectives ranging from minutes to several hours?

A. single location disk replication

B. asynchronous shadowing

C. synchronous mirroring

D. multiple location disk replications

78. Organizations use contingency plans for an outcome other than the usual (expected) outcome. Which one of the following IT contingency solutions provides recovery time objectives ranging from minutes to several hours?

A. single location disk replication

B. asynchronous shadowing

C. synchronous mirroring

D. multiple location disk replications

79. Which one of the following configurations of elements represents the most complete disaster recovery plan?

A. vendor contract for alternate processing site, names of persons on the disaster recovery team, offsite storage procedures

B. alternate processing site, backup and off-site storage procedures, identification of critical applications, and test of the plan

C. off-site storage procedures, identification of critical applications, test of the plan

D. vendor contract for alternate processing site, backup procedures, names of persons on the disaster recovery team

80. What maintains a historical record of all the changes make to data by constantly monitor all data written on a hard drive and thus provide backups that can be restored immediately?

A. Continuous Data protection (CDP)

B. Backup Data Plan (BDP)

C. Synchronous backups

D. Disk to Disk (D2D) backups

81. This is the maximum length of time that an organization can tolerate between backups.

A. Recovery Time Objective (RTO)

B. Recovery Point Objective (RPO)

C. Service Establishment Point (SEP)

D. Business Recovery Time (BRT)

82. This type of attack is to directly attach conductors to the circuit(s) being protected so that the information can be obtained from and/or changes injected into the system under attack.

A. Shape Charge Attack
B. Probe Attack
C. Machine Attack
D. Circuit Disruption Attack

83. The abbreviation RAID stands for?

A. Resistant Architecture of Interdependent Drives
B. Repository Array of Inexpensive Disks
C. Redundant Array of Independent Drives
D. Replacement Archive for Identical Disks

84. What is an effective technique in ventilation systems that forces air outward from a facility to help guard against dust and other pollutants?

A. Adaptive Support Pressurization
B. Positive Pressurization
C. Negative Pressurization
D. Supply Only Pressurization

85. Half of employees admit to taking corporate data when they leave a job, and 40 percent say they plan to use the data in their new job. How do you prevent this?

A. Tag Sensitive Information, Monitor Technology, Enforce Non-Disclosure Agreements
B. Employee Education, Enforce Non-Disclosure Agreements, Monitor Technology
C. Enforce Non-Disclosure Agreements, Monitor Technology, Secure Intellectual Property
D. Monitor Technology, Secure Intellectual Property, Education Employees

86. Which one of the following type of attacks requires physical access to a computer system?

A. scanning the network for open ports and IP addresses
B. cracking passwords
C. using a bootdisk to load an alternate operating systems
D. exploiting vulnerabilities in web servers

87. What process takes a variable sized long input of bits and produces a fixed, small sequence of bits that is effectively unique?

A. Decoy Protocol
B. Public Key Encryption
C. Hashing
D. Cascading

88. What process takes a variable sized long input of bits and produces a fixed, small sequence of bits that is effectively unique?

A. decoy protocol
B. public key encryption
C. hashing
D. cascading

89. This is a method of hiding nearly undetectable messages in images, documents, or other file types.
A. cryptography
B. steganography
C. symmetric encryption
D. cryptanalysis

90. In which way does the Combined Encryption combine symmetric and asymmetric encryption?
A. First, the message is encrypted with symmetric encryption and then it is encrypted asymmetrically together with the key.
B. The secret key is symmetrically transmitted, the message itself asymmetrically.
C. First, the message is encrypted with asymmetric encryption and then it is encrypted symmetrically together with the key
D. The secret key is asymmetrically transmitted, the message itself symmetrically.

91. What does the "dd" Unix/Linux command do as part of computer forensics?
A. creates a hash of all of the contents of a drive
B. creates an exact duplicate of a disk image
C. copies the hard drive to a solid state drive
D. duplicates the slackspace on a hard disk

92. What are the two primary types of computer forensic investigations?
A. when a computer was the target of a crime and the computer itself was stolen
B. when a computer was used to commit a crime and when a computer was the target of a crime
C. when a computer was the target of a crime and when the computer was used by a criminal
D. when a computer was used to commit a crime and the crime involved medical records

93. What is the name of the special container used to hold electronic evidence that blocks the radio signals?
A. Faraday bag
B. Radio Frequency Identification (RFID)
C. cell phone holder
D. signal blocking box

94. Verifying the authentication of digital images is one form of forensic security. What are forensic techniques used to complete this verification?
A. Use an image's compression history after erasing its associated compression fingerprints
B. Use an image's compression history and its associated compression fingerprints

C. Erase an image's compression history and its associated compression fingerprints
D. Erase an image's compression history and use its associated compression fingerprints

95. Prosecuting cybercrimes is difficult because most of the evidence is digital. Forensic investigators must leverage a forensic investigation life cycle to ensure the confidentiality, integrity, or availability of digital evidence. Steps in the forensic investigation life cycle are:
A. Requirement Analysis, Inaccuracy, Destruction of Evidence
B. Review of Evidence, Destruction of Evidence, Representation of Evidence
C. Requirement Analysis, Representation of Evidence, Repository of Data
D. Representation of Evidence, Retrieval of Data, Inaccuracy

96. What standard company policy outlines what the organization considers to be the appropriate use of all computer resources?
A. Internet Usage Policy (IUP)
B. Acceptable Use Policy (AUP)
C. End User License Agreement (EULA)
D. Data Communication Standard (DCS)

97. U.S. Presidents use this power to set policy directives that implement or interpret federal statutes, a constitutional provision, or a treaty.
A. Executive Orders
B. Public Law
C. Joint Resolution
D. Legislation

98. This Act intended to enhance the security and resiliency of the cyber and communications infrastructure of the United States.
A. Cybersecurity Act of 2012
B. Federal Information Security Management Act of 2002
C. Confidential Information Protection and Statistical Efficiency Act of 2002
D. Computer Security Act of 1987

99. This is the mission of what federal organization - to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
A. National Institute of Standards and Technology (NIST)
B. Department of Homeland Security (DHS)
C. Office of Management and Budget (OMB)
D. Department of Commerce (DOC)

100. What are the three primary goals of the Comprehensive National Cybersecurity Initiative (CNCI)?

A. To establish a front line of defense against today's immediate threats; To defend against the full spectrum of threats; To develop and implement a government-wide cyber counterintelligence (CI) plan.

B. To establish a front line of defense against today's immediate threats; To defend against the full spectrum of threats; To strengthen the future cybersecurity environment

C. To strengthen the future cybersecurity environment; To build cybersecurity capability in the electricity sector; To protect the nation's communication grid from cyber threats

D. To defend against the full spectrum of threats; To coordinate and redirect research and development (R&D) efforts; To develop and implement a government-wide cyber counterintelligence (CI) plan

Answers

1. B
2. B
3. D
4. C
5. B
6. B
7. C
8. D
9. C
10. D
11. D
12. D
13. C
14. B
15. D
16. A
17. C
18. A
19. D
20. B
21. C
22. B
23. B
24. A
25. A
26. C
27. C
28. D
29. B
30. C
31. B
32. C
33. D
34. B
35. D
36. A
37. A
38. B
39. D
40. A
41. C
42. D
43. C
44. C
45. A
46. D
47. D
48. D
49. B
50. B
51. D
52. A
53. C
54. C
55. B
56. D
57. A
58. A
59. C
60. A
61. C
62. B
63. B
64. A
65. C
66. D
67. C
68. C
69. B
70. D
71. A
72. D
73. C
74. B
75. D
76. D
77. C
78. C
79. B
80. A
81. B
82. B
83. C
84. B
85. B
86. C
87. C
88. C
89. B
90. D
91. B
92. B
93. A
94. B
95. C
96. B
97. A
98. A
99. A
100. B