**QUESTION 174**
Which tool provides a full packet capture from network traffic?

A. Nagios
B. CAINE
C. Hydra
D. Wireshark

**Correct Answer:** D

**QUESTION 175**
A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders After further investigation, the analyst learns that customers claim that they cannot access company servers According to NIST SP800-61, in which phase of the incident response process is the analyst?

A. post-incident activity
B. detection and analysis
C. preparation
D. containment, eradication, and recovery

**Correct Answer:** B

**QUESTION 176**
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

**Correct Answer:** B

**QUESTION 177**
Which security principle is violated by running all processes as root or administrator?

A. principle of least privilege
B. role-based access control
C. separation of duties
D. trusted computing base

**Correct Answer:** A

**QUESTION 178**
Which two components reduce the attack surface on an endpoint? (Choose two.)

A. secure boot

B. load balancing
C. increased audit log levels
D. restricting USB ports
E. full packet captures at the endpoint

**Correct Answer:** AD

**QUESTION 179**
A company encountered a breach on its web servers using IIS 7 5 Dunng the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1 2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters. Which action does the engineer recommend?

A. Upgrade to TLS v1 3.
B. Install the latest IIS version.
C. Downgrade to TLS 1.1.
D. Deploy an intrusion detection system

**Correct Answer:** B

**QUESTION 180**
What describes the concept of data consistently and readily being accessible for legitimate users?

A. integrity
B. availability
C. accessibility
D. confidentiality

**Correct Answer:** B

**QUESTION 181**
Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic
B. indirect
C. best
D. corroborative

**Correct Answer:** D

**QUESTION 182**
What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. least privilege
B. need to know

C. integrity validation
D. due diligence

**Correct Answer:** A

**QUESTION 183**
What is the relationship between a vulnerability and a threat?

A. A threat exploits a vulnerability
B. A vulnerability is a calculation of the potential loss caused by a threat
C. A vulnerability exploits a threat
D. A threat is a calculation of the potential loss caused by a vulnerability

**Correct Answer:** A

**QUESTION 184**
Which artifact is used to uniquely identify a detected file?

A. file timestamp
B. file extension
C. file size
D. file hash
**Correct Answer:** D

**QUESTION 185**
Which metric is used to capture the level of access needed to launch a successful attack?

A. privileges required
B. user interaction
C. attack complexity
D. attack vector

**Correct Answer:** D

**QUESTION 186**
What is the difference between the ACK flag and the RST flag?

A. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.
B. The ACK flag confirms the received segment, and the RST flag terminates the connection.
C. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent
D. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

**Correct Answer:** B

**QUESTION 187**
What is the function of a command and control server?

A. It enumerates open ports on a network device

B. It drops secondary payload into malware
C. It is used to regain control of the network after a compromise
D. It sends instruction to a compromised system

**Correct Answer:** D

**QUESTION 188**
Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative
B. true positive
C. true negative
D. false positive

**Correct Answer:** D

**QUESTION 189**
How does an attacker observe network traffic exchanged between two users?

A. port scanning
B. man-in-the-middle
C. command injection
D. denial of service

**Correct Answer:** B

**QUESTION 190**
How does a certificate authority impact security?

A. It validates client identity when communicating with the server.
B. It authenticates client identity when requesting an SSL certificate.
C. It authenticates domain identity when requesting an SSL certificate.
D. It validates the domain identity of the SSL certificate.

**Correct Answer:** D

**QUESTION 191**
An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external penmeter data flows contain records, writings, and artwork Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age. The engineer must identify protected data. Which two types of data must be identified'? (Choose two.)

A. SOX
B. PII
C. PHI
D. PCI
E. copyright

**Correct Answer:** BC

**QUESTION 192**
An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

A. Recovery
B. Detection
C. Eradication
D. Analysis

**Correct Answer:** B

**QUESTION 193**
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

**Correct Answer:** D

**QUESTION 194**
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

A. detection and analysis
B. post-incident activity
C. vulnerability management
D. risk assessment
E. vulnerability scoring

**Correct Answer:** AB

**QUESTION 195**
Which type of data collection requires the largest amount of storage space?

A. alert data
B. transaction data
C. session data
D. full packet capture

**Correct Answer:** D

**QUESTION 196**
What is a benefit of using asymmetric cryptography?

A. decrypts data with one key