# EC-Council

## Exam Questions 312-38

Certified Network Defender

**NEW QUESTION 1**
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

A. Bollards
B. Fence
C. Video surveillance
D. Mantrap

**Answer:** B

**NEW QUESTION 2**
Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?

A. Behavior-based IDS
B. Anomaly-based IDS
C. Stateful protocol analysis
D. Signature-based IDS

**Answer:** D

**NEW QUESTION 3**
Assume that you are working as a network administrator in the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server. How will you prioritize these two incidents?

A. Based on approval from management
B. Based on a first come first served basis
C. Based on a potential technical effect of the incident
D. Based on the type of response needed for the incident

**Answer:** C

**NEW QUESTION 4**
George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the _________.

A. Archived data
B. Deleted data
C. Data in transit
D. Backup data

**Answer:** D

**NEW QUESTION 5**
Which OSI layer does a Network Interface Card (NIC) work on?

A. Physical layer
B. Presentation layer
C. Network layer
D. Session layer

**Answer:** A

**NEW QUESTION 6**
------------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15
B. 802.16
C. 802.15.4
D. 802.12

**Answer:** B

**NEW QUESTION 7**
Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?

A. Scans and probes
B. Malicious Code
C. Denial of service
D. Distributed denial of service

**Answer:**

B

**NEW QUESTION 8**
Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?

A. Confidentiality
B. Availability
C. Data Integrity
D. Usability

**Answer:** C

**NEW QUESTION 9**
The network admin decides to assign a class B IP address to a host in the network. Identify which of the following addresses fall within a class B IP address range.

A. 255.255.255.0
B. 18.12.4.1
C. 172.168.12.4
D. 169.254.254.254

**Answer:** C

**NEW QUESTION 10**
What command is used to terminate certain processes in an Ubuntu system?

A. #grep Kill [Target Process}
B. #kill-9[PID]
C. #ps ax Kill
D. # netstat Kill [Target Process]

**Answer:** C

**NEW QUESTION 11**
Alex is administrating the firewall in the organization's network. What command will he use to check all the remote addresses and ports in numerical form?

A. Netstat -o
B. Netstat -a
C. Netstat -ao
D. Netstat -an

**Answer:** D

**NEW QUESTION 12**
Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?

A. Extreme severity level
B. Low severity level
C. Mid severity level
D. High severity level

**Answer:** B

**NEW QUESTION 13**
Which of the information below can be gained through network sniffing? (Select all that apply)

A. Telnet Passwords
B. Syslog traffic
C. DNS traffic
D. Programming errors

**Answer:** ABC

**NEW QUESTION 14**
Kyle is an IT consultant working on a contract for a large energy company in Houston. Kyle was hired on to do contract work three weeks ago so the company could prepare for an external IT security audit. With suggestions from upper management, Kyle has installed a network-based IDS system. This system checks for abnormal behavior and patterns found in network traffic that appear to be dissimilar from the traffic normally recorded by the IDS. What type of detection is this network-based IDS system using?

A. This network-based IDS system is using anomaly detection.
B. This network-based IDS system is using dissimilarity algorithms.
C. This system is using misuse detection.
D. This network-based IDS is utilizing definition-based detection.

**Answer:** A

**NEW QUESTION 15**
Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

A. Mitigation
B. Assessment
C. Remediation
D. Verification

**Answer:** C

**NEW QUESTION 16**
Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?

A. Containment
B. Assign eradication
C. A follow-up
D. Recovery

**Answer:** C

**NEW QUESTION 17**
Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level. Which of the following is the correct order in the risk management phase?

A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification
D. Risk Identificatio
E. Risk Assessmen
F. Risk Monitoring & Review, Risk Treatment

**Answer:** A

**NEW QUESTION 18**
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach

**Answer:** A

**NEW QUESTION 19**
Which of the following VPN topologies establishes a persistent connection between an organization's main office and its branch offices using a third-party network or the Internet?

A. Star
B. Point-to-Point
C. Full Mesh
D. Hub-and-Spoke

**Answer:** D

**NEW QUESTION 20**
James was inspecting ARP packets in his organization's network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating. Which type of attack is James analyzing?

A. ARP Sweep
B. ARP misconfiguration
C. ARP spoofinq
D. ARP Poisioning

**Answer:** A

**NEW QUESTION 21**
......