- **Vendor: EC-Council**
- **Exam Code: 312-38**
- **Exam Name: EC-Council Certified Network Defender Certification Exam**
- **New Updated Questions from Braindump2go (Updated in October/2021)**

QUESTION 499
Jason has set a firewall policy that allows only a specific list of network services and deny everything else. This strategy is known as a_____.

A. Default allow
B. Default deny
C. Default restrict
D. Default access

Answer: B

QUESTION 500
You are responsible for network functions and logical security throughout the corporation. Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in BarcelonA. These laptops contained proprietary company information. While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

A. You should have used 3DES.
B. You should have implemented the Distributed File System (DFS).
C. If you would have implemented Pretty Good Privacy (PGP).
D. You could have implemented the Encrypted File System (EFS)

Answer: D

QUESTION 501
Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?

A. Bus
B. Star
C. Ring
D. Mesh

Answer: B

QUESTION 502

Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented.
What is the correct hierarchy for a security policy implementation?

A. Laws, Policies, Regulations, Procedures and Standards
B. Regulations, Policies, Laws, Standards and Procedures
C. Laws, Regulations, Policies, Standards and Procedures
D. Procedures, Policies, Laws, Standards and Regulations

Answer: C

QUESTION 503
An organization needs to adhere to the_____rules for safeguarding and protecting the electronically stored health information of employees.

A. HI PA A
B. PCI DSS
C. ISEC
D. SOX

Answer: A

QUESTION 504
Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization. Why is Chris calculating the KRI for his organization? It helps Chris to:

A. Identifies adverse events
B. Facilitates backward
C. Facilitates post Incident management
D. Notifies when risk has reached threshold levels

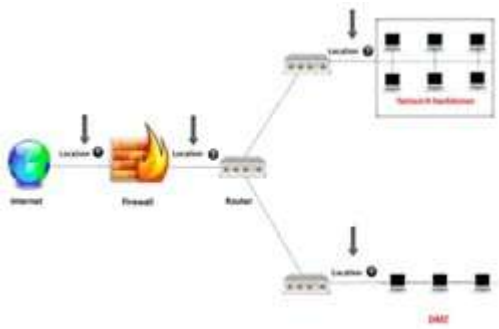
Answer: AD

QUESTION 505
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a_____and it has to adhere to the_____

A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix

Answer: A

QUESTION 506
An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



A. Location 2
B. Location 3
C. Location 4
D. Location 1

Answer: A

QUESTION 507
Which of the following is a best practice for wireless network security?

A. Enabling the remote router login
B. Do not changing the default SSID
C. Do not placing packet filter between the AP and the corporate intranet
D. Using SSID cloaking

Answer: D

QUESTION 508
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

QUESTION 509
Which IEEE standard does wireless network use?

A. 802.11
B. 802.18
C. 802.9
D. 802.10

Answer: A

QUESTION 510
Which of the following acts as a verifier for the certificate authority?

A. Certificate Management system
B. Certificate authority
C. Directory management system

D. Registration authority

Answer: D

QUESTION 511
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

QUESTION 512
A network administrator is monitoring the network traffic with Wireshark. Which of the following filters will she use to view the packets moving without setting a flag to detect TCP Null Scan attempts?

A. TCRflags==0x000
B. Tcp.flags==0X029
C. Tcp.dstport==7
D. Tcp.flags==0x003

Answer: A

QUESTION 513
Bryson is the IT manager and sole IT employee working for a federal agency in California. The agency was just given a grant and was able to hire on 30 more employees for a new extended project. Because of this, Bryson has hired on two more IT employees to train up and work. Both of his new hires are straight out of college and do not have any practical IT experience. Bryson has spent the last two weeks teaching the new employees the basics of computers, networking, troubleshooting techniques etc. To see how these two new hires are doing, he asks them at what layer of the OSI model do Network Interface Cards (NIC) work on. What should the new employees answer?

A. NICs work on the Session layer of the OSI model.
B. The new employees should say that NICs perform on the Network layer.
C. They should tell Bryson that NICs perform on the Physical layer
D. They should answer with the Presentation layer.

Answer: C

QUESTION 514
Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the----------authentication technique to satisfy the management request.

A. Two-factor Authentication
B. Smart Card Authentication
C. Single-sign-on
D. Biometric

Answer: C

QUESTION 515
John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?

A. Application level gateway
B. Circuit level gateway
C. Stateful Multilayer Inspection
D. Packet Filtering

Answer: B

QUESTION 516
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. High severity level
B. Extreme severity level
C. Mid severity level
D. Low severity level

Answer: D

QUESTION 517
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

QUESTION 518
----------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

QUESTION 519
As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's_____integrity check mechanism provides security against a replay attack

A. CBC-32
B. CRC-MAC
C. CRC-32
D. CBC-MAC

Answer: D

QUESTION 520
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. Usability
B. Data Integrity
C. Availability
D. Confidentiality

Answer: B

QUESTION 521
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

QUESTION 522
Identify the correct statements regarding a DMZ zone:

A. It is a file integrity monitoring mechanism
B. It is a Neutral zone between a trusted network and an untrusted network
C. It serves as a proxy
D. It includes sensitive internal servers such as database servers

Answer: B

QUESTION 523
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

QUESTION 524
Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm's partners have asked that a secure wireless network be implemented in the office so employees can move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment. What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?

A. The IEEE standard covering wireless is 802.9 and they should follow this.
B. 802.7 covers wireless standards and should be followed
C. They should follow the 802.11 standard
D. Frank and the other IT employees should follow the 802.1 standard.

Answer: C

QUESTION 525
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. Which step should Malone list as the last step in the incident response methodology?

A. Malone should list a follow-up as the last step in the methodology
B. Recovery would be the correct choice for the last step in the incident response methodology
C. He should assign eradication to the last step.
D. Containment should be listed on Malone's plan for incident response.

Answer: B

QUESTION 526
Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?

A. Just Enough Administration (EA)
B. User Account Control (UAC)
C. Windows Security Identifier (SID)
D. Credential Guard

Answer: A

QUESTION 527
How is application whitelisting different from application blacklisting?

A. It allows all applications other than the undesirable applications
B. It allows execution of trusted applications in a unified environment
C. It allows execution of untrusted applications in an isolated environment
D. It rejects all applications other than the allowed applications

Answer: D

QUESTION 528
Which of the following security models enable strict identity verification for every user or device attempting to access the network resources?
1. Zero-trust network model
2. Castle-and-Moat model

A. Both 1 and 2
B. 1 only
C. 2 only
D. None

Answer: B

QUESTION 529
If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the company's Linux systems, which directory should he access?

A. /etc/logrotate.conf
B. /etc/hosts.allow
C. /etc/crontab
D. /etc/login.defs

Answer: D

QUESTION 530
Which of the Windows security component is responsible for controlling access of a user to Windows resources?

A. Network Logon Service (Netlogon)
B. Security Accounts Manager (SAM)
C. Security Reference Monitor (SRM)
D. Local Security Authority Subsystem (LSASS)

Answer: D