

➤ **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](#))**

[Visit Braindump2go and Download Full Version 312-38 Exam Dumps](#)

QUESTION 406

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 Identification. Risk Assessment. Risk Monitoring & Review, Risk Treatment

Answer: A

QUESTION 407

John has implemented _____ in the network to restrict the limit of public IP addresses in his organization and to enhance the firewall filtering technique.

- A. DMZ
- B. Proxies
- C. VPN
- D. NAT

Answer: D

QUESTION 408

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

QUESTION 409

Consider a scenario consisting of a tree network. The root Node N is connected to two main nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?

- A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
 - B. Does not cause any disturbance to the child nodes or its transmission
- Fail

[312-38 Exam Dumps](#) [312-38 Exam Questions](#) [312-38 PDF Dumps](#) [312-38 VCE Dumps](#)

<https://www.braindump2go.com/312-38.html>

ure
of
the
mai
n
no
de
will
aff
ect
all
rel
ate
d
chil
d
no
des
con
nec
ted
to
the
mai
n
no
de

D. Affects the root node only

Answer: C

QUESTION 410

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

QUESTION 411

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

- A. Install a CCTV with cameras pointing to the entrance doors and the street
- B. Use fences in the entrance doors
- C. Use lights in all the entrance doors and along the company's perimeter
- D. Use an IDS in the entrance doors and install some of them near the corners

Answer: A

QUESTION 412

Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including

[312-38 Exam Dumps](#) [312-38 Exam Questions](#) [312-38 PDF Dumps](#) [312-38 VCE Dumps](#)

<https://www.braindump2go.com/312-38.html>

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

QUESTION 413

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

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

Answer: D

QUESTION 414

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

QUESTION 415

Rick has implemented several firewalls and IDS systems across his enterprise network. What should he do to effectively correlate all incidents that pass through these security controls?

- A. Use firewalls in Network Address Transition (NAT) mode
- B. Implement IPsec
- C. Implement Simple Network Management Protocol (SNMP)
- D. Use Network Time Protocol (NTP)

Answer: D

QUESTION 416

Management asked their network administrator to suggest an appropriate backup medium for their backup plan that best suits their organization's need. Which of the following factors will the administrator consider when deciding on the appropriate backup medium?

- A. Capability
- B. Accountability
- C. Extensibility
- D. Reliability

Answer: ACD

QUESTION 417

Which of the following network monitoring techniques requires extra monitoring software or hardware?

- A. Non-router based
- B. Switch based
- C. Hub based
- D. Router based

Answer: A

QUESTION 418

Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?

- A. Steven should use a Demilitarized Zone (DMZ)
- B. Steven should use Open Shortest Path First (OSPF)
- C. Steven should use IPsec
- D. Steven should enabled Network Address Translation(NAT)

Answer: D

QUESTION 419

What is the name of the authority that verifies the certificate authority in digital certificates?

- A. Directory management system
- B. Certificate authority
- C. Registration authority
- D. Certificate Management system

Answer: D

QUESTION 420

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the dat

- A. Which RAID level is used here?
- B. RAID 3
- C. RAID 1
- D. RAID 5
- E. RAID 0

Answer: B

QUESTION 421

You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region. You suspect a DoS incident on the network. What will be your first reaction as a first responder?

- A. Avoid Fear, Uncertainty and Doubt
- B. Communicate the incident
- C. Make an initial assessment

D. Disable Virus Protection

Answer: A

QUESTION 422

If a network is at risk from unskilled individuals, what type of threat is this?

- A. External Threats
- B. Structured Threats
- C. Unstructured Threats
- D. Internal Threats

Answer: C

QUESTION 423

According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication. What needs to happen to force this server to use Windows Authentication?

- A. Edit the ADLIN file.
- B. Edit the shadow file.
- C. Remove the /var/bin/localauth.conf file.
- D. Edit the PAM file to enforce Windows Authentication

Answer: D

QUESTION 424

Kelly is taking backups of the organization's data. Currently, he is taking backups of only those files which are created or modified after the last backup. What type of backup is Kelly using?

- A. Full backup
- B. Incremental backup
- C. Differential Backup
- D. Normal Backup

Answer: B

QUESTION 425

John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

- A. `Tcp.flags==0x2b`
- B. `Tcp.flags=0x00`
- C. `Tcp.options.mss_val<1460`
- D. `Tcp.options.wscale_val==20`

Answer: ABC

QUESTION 426

A company has the right to monitor the activities of their employees on different information systems according to the _____ policy.

- A. Information system
- B. User access control

- C. Internet usage
- D. Confidential data

Answer: B

QUESTION 427

Liza was told by her network administrator that they will be implementing IPsec VPN tunnels to connect the branch locations to the main office. What layer of the OSI model do IPsec tunnels function on?

- A. The data link layer
- B. The session layer
- C. The network layer
- D. The application and physical layers

Answer: C

QUESTION 428

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

Answer: D

QUESTION 429

Which VPN QoS model guarantees the traffic from one customer edge (CE) to another?

- A. Pipe Model
- B. AAA model
- C. Hub-and-Spoke VPN model
- D. Hose mode

Answer: A

QUESTION 430

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 spoofing
- D. ARP Poisoning

Answer: A

QUESTION 431

Alex is administrating the firewall in the organization's network. What command will he use to check the ports applications open?

- A. Netstat -an
- B. Netstat -o

- C. Netstat -a
- D. Netstat -ao

Answer: A

QUESTION 432

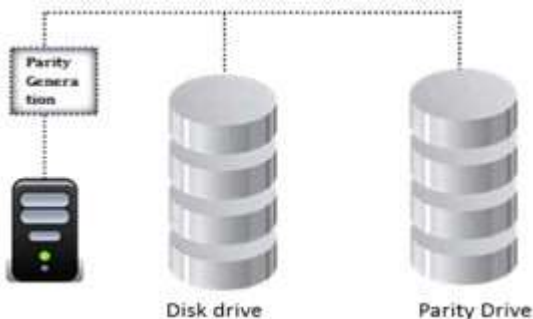
The risk assessment team in Southern California has estimated that the probability of an incident that has potential to impact almost 80% of the bank's business is very high. How should this risk be categorized in the risk matrix?

- A. High
- B. Medium
- C. Extreme
- D. Low

Answer: C

QUESTION 433

Identify the minimum number of drives required to setup RAID level 5.



- A. Multiple
- B. 3
- C. 4
- D. 2

Answer: B

QUESTION 434

Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a _____ as it separates the storage units from the servers and the user network.

- A. SAN
- B. SCSA
- C. NAS
- D. SAS

Answer: A

QUESTION 435

A local bank wants to protect their card holder data. The bank should comply with the _____ standard to ensure the security of card holder data.

- A. HIPAA
- B. ISEC
- C. PCI DSS

D. SOAX

Answer: C

QUESTION 436

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