EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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

NEW QUESTION 2
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 3
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

NEW QUESTION 4
Management wants to calculate the risk factor for their organization. Kevin, a network administrator in the organization knows how to calculate the risk factor. Certain parameters are required before calculating risk factor. What are they? (Select all that apply) Risk factor =.............X...............X...........

A. Vulnerability
B. Impact
C. Attack
D. Threat

Answer: ABD

NEW QUESTION 5
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

NEW QUESTION 6
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

NEW QUESTION 7
The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.
Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)

A. Complying with the company's security policies
B. Implementing strong authentication schemes
C. Implementing a strong password policy
D. Install antivirus software

Answer: D

NEW QUESTION 8
Mark is monitoring the network traffic on his organization's network. He wants to detect a TCP and UDP ping sweep on his network. Which type of filter will be used to detect this on the network?

A. Tcp.srcport==7 and udp.srcport==7
B. Tcp.srcport==7 and udp.dstport==7
C. Tcp.dstport==7 and udp.srcport==7
D. Tcp.dstport==7 and udp.dstport==7

Answer: D

NEW QUESTION 9
A company wants to implement a data backup method which allows them to encrypt the data ensuring its security as well as access at any time and from any location. What is the appropriate backup method that should be implemented?

A. Onsite backup
B. Hot site backup
C. Offsite backup
D. Cloud backup

Answer: D

NEW QUESTION 10
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

NEW QUESTION 10
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

NEW QUESTION 12
You are an IT security consultant working on a contract for a large manufacturing company to audit their entire network. After performing all the tests and building your report, you present a number of recommendations to the company and what they should implement to become more secure. One recommendation is to install a network-based device that notifies IT employees whenever malicious or questionable traffic is found. From your talks with the company, you know that they do not want a device that actually drops traffic completely, they only want notification. What type of device are you suggesting?

A. The best solution to cover the needs of this company would be a HIDS device.
B. A NIDS device would work best for the company
C. You are suggesting a NIPS device
D. A HIPS device would best suite this company

Answer: B

NEW QUESTION 15
The agency Jacob works for stores and transmits vast amounts of sensitive government data that cannot be compromised. Jacob has implemented Encapsulating Security Payload (ESP) to encrypt IP traffic. Jacob wants to encrypt the IP traffic by inserting the ESP header in the IP datagram before the transport layer protocol header. What mode of ESP does Jacob need to use to encrypt the IP traffic?

A. He should use ESP in transport mode.
B. Jacob should utilize ESP in tunnel mode.
C. Jacob should use ESP in pass-through mode.
D. He should use ESP in gateway mode

Answer: B

NEW QUESTION 17
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 20
An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. An attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts. Which of the following password cracking techniques is the attacker trying?

A. Bruteforce
B. Rainbow table
C. Hybrid
D. Dictionary

Answer: D

NEW QUESTION 22
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

A. The type of scan she is usinq is called a NULL scan.
B. Cindy is using a half-open scan to find live hosts on her network.
C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
D. She is utilizing a RST scan to find live hosts that are listening on her network.

Answer: B

NEW QUESTION 23
Michael decides to view the-----------------to track employee actions on the organization's network.

A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set

Answer: B

NEW QUESTION 27
Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is
encapsulated. As the traffic passes though the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the _____ implementation of a VPN.

A. Full Mesh Mode
B. Point-to-Point Mode
C. Transport Mode
D. Tunnel Mode

Answer: D

NEW QUESTION 28
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

NEW QUESTION 32
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 33
Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

A. Kyle purchased a Ferro resonant Standby UPS.
B. Kyle purchased a Line-Interactive UPS
C. He has bought a Standby UPS
D. He purchased a True Online UPS.

Answer: C

NEW QUESTION 35
Management wants to bring their organization into compliance with the ISO standard for information security risk management. Which ISO standard will management decide to implement?

A. ISO/IEC 27004
B. ISO/IEC 27002
C. ISO/IEC 27006
D. ISO/IEC 27005

Answer: D

NEW QUESTION 36
Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method that works where one key is public and the other is private. What encryption method did Ivan settle on?

A. Ivan settled on the private encryption method.
B. Ivan settled on the symmetric encryption method.
C. Ivan settled on the asymmetric encryption method
D. Ivan settled on the hashing encryption method

Answer: C

NEW QUESTION 40
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

NEW QUESTION 44
Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this source address signify?

A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
B. This source address is IPv6 and translates as 13.1.68.3
C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
D. This means that the source is using IPv4

Answer: D

NEW QUESTION 47
......

Relate Links

100% Pass Your 312-38 Exam with Exambible Prep Materials

https://www.exambible.com/312-38-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/