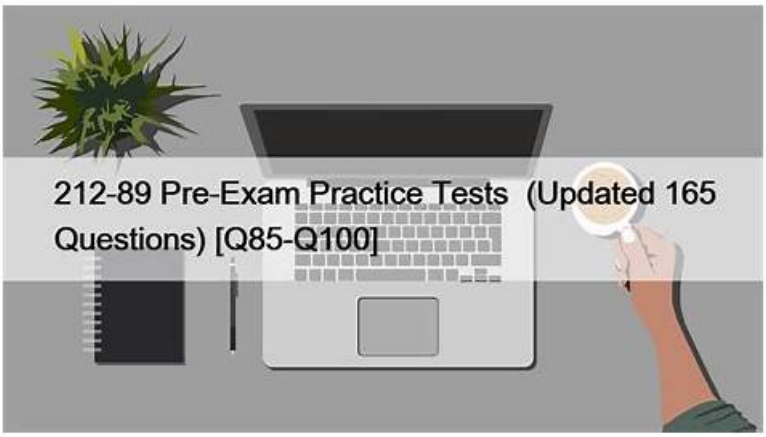
Free 212-89 Practice, 212-89 Reliable Test Prep



BONUS!!! Download part of ActualTestsQuiz 212-89 dumps for free: https://drive.google.com/open?id=1lPr4U_Sjm6FVl-SzRjpzioXvIoeDWuqK

If you really intend to grow in your career then you must attempt to pass the 212-89 exam, which is considered as most esteemed and authorititive exam and opens several gates of opportunities for you to get a better job and higher salary. But passing the 212-89 exam is not easy as it seems to be. With the help of our 212-89 Exam Questions, you can just rest assured and take it as easy as pie. For our 212-89 study materials are professional and specialized for the exam. And you will be bound to pass the exam as well as get the certification.

There is the cost of ECCouncil 212-89 Exam

- The price of ECCouncil 212-89exam is $100 USD.

>> Free 212-89 Practice <<

100% Pass Trustable EC-COUNCIL - Free 212-89 Practice

Knowledge about a person and is indispensable in recruitment. That is to say, for those who are without good educational background, only by paying efforts to get an acknowledged 212-89 certification, can they become popular employees. So for you, the 212-89 latest braindumps complied by our company can offer you the best help. With our test-oriented 212-89 Test Prep in hand, we guarantee that you can pass the 212-89 exam as easy as blowing away the dust, as long as you guarantee 20 to 30 hours practice with our 212-89 study materials.

EC-COUNCIL 212-89 Exam Syllabus Topics:

Topic	Details
Topic 1	• Handling and Responding to Email Security Incidents: This part evaluates Cybersecurity Analysts on their ability to detect and mitigate email-based threats. It explores preparation, analysis, and containment measures in response to email-related incidents, as well as post-incident recovery steps. Candidates must interpret case studies and apply best practices for protecting enterprise email systems.
Topic 2	• Handling and Responding to Network Security Incidents: This module assesses IT Security Operations Managers in their expertise to manage network-level security breaches. It includes the detection of unauthorized access, misuse, denial-of-service attacks, and wireless network threats. Practical case studies and preventive strategies are included to ensure operational security across distributed environments.

Topic 3	• Incident Handling and Response Process: This part evaluates IT Security Operations Managers on their understanding of the structured incident handling and response process. It includes the recording, assignment, and triage of incidents, as well as the procedures for notifying stakeholders and containing threats. The module also examines capabilities in forensic evidence gathering, eradication and recovery strategies, post-incident review activities, and the significance of inter-organizational information sharing.
Topic 4	• First Response: This section of the exam assesses Cybersecurity Analysts in their ability to carry out effective first response procedures. It includes securing and documenting crime scenes, evidence collection methodologies, and guidelines for preserving, packaging, and transporting digital and physical evidence in a way that maintains chain of custody and forensic integrity.
Topic 5	• Handling and Responding to Cloud Security Incidents: Here, IT Security Operations Managers are examined on their familiarity with cloud-specific threats across platforms like Azure, AWS, and Google Cloud. The focus is on recognizing incident types, handling and monitoring procedures, and recovery methods. The use of real-world scenarios helps to demonstrate effective response tactics and reinforce best practices in cloud environments.
Topic 6	• Handling and Responding to Web Application Security Incidents: This section measures Cybersecurity Analysts' proficiency in managing web application vulnerabilities and incidents. It covers the preparation, detection, containment, and resolution of threats within web-based platforms. Candidates are expected to understand analytical approaches, case-based examples, and protective techniques for securing application infrastructure.
Topic 7	• Introduction to Incident Handling and Response: This section of the exam measures the competency of Cybersecurity Analysts in understanding the core concepts of information security threats, vulnerabilities, and various attack and defense frameworks. It covers foundational knowledge of incidents, their classification, and the incident management lifecycle. Candidates are expected to be familiar with automation and orchestration in response efforts, industry standards, security best practices, and legal compliance frameworks relevant to incident handling.
Topic 8	• Handling and Responding to Malware Incidents:In this domain, IT Security Operations Managers are tested on their capacity to respond to malware incidents effectively. The focus lies on planning, detecting, containing, and analyzing malware threats. It also includes strategies for eradication and recovery, alongside evaluating real-world malware case studies and identifying applicable best practices to avoid recurrence.
Topic 9	• Handling and Responding to Insider Threats: This module evaluates Cybersecurity Analysts on how well they understand and manage internal security risks. It includes detection and containment of insider threats, analysis and eradication procedures, and recovery from internal breaches. A case-study approach is used to test comprehension of best practices and response strategies that align with organizational policy.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) Sample Questions (Q35-Q40):

NEW QUESTION # 35
Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-profile executives of the company. What type of phishing attack is this?

- A. Puddle phishing
- B. Spear phishing
- C. Whaling
- D. Pharming

Answer: C

Explanation:
Whaling is a specific type of phishing attack that targets high-profile executives or individuals within an organization, often with the intent to steal sensitive information or gain access to their accounts for financial fraud. The term "whaling" is used because it targets

the "big fish" of an organization. Given that Sam identified the targets of the attack as high-profile executives, the described scenario is indicative of a whaling attack.
References:The ECIH v3 curriculum includes a section on different types of phishing attacks, including whaling, emphasizing the strategies attackers use to target individuals based on their roles within an organization.

NEW QUESTION # 36
You are a systems administrator for a company. You are accessing your file server remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either. You can ping the file server but not connect to it via RDP. You check the Active Directory Server, and all is well. You check the email server and find that emails are sent and received normally. What is the most likely issue?

- A. An admin account issue
- B. A denial-of-service issue
- C. An e-mail service issue
- D. The file server has shut down

Answer: B

Explanation:
In this scenario, the inability to access the file server via Remote Desktop Protocol (RDP), despite the server being pingable and other services functioning normally, suggests a service-specific disruption rather than a complete system shutdown or broader network issue. This pattern is indicative of a denial-of-service (DoS) attack targeted at the file server's RDP service or network congestion that specifically affects RDP connectivity. A DoS attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The fact that other services (like email) are operational rules out broader system or admin account issues, pointing towards a specific problem with accessing the file server, most likely due to a denial-of-service condition.
References:Incident Handler (ECIH v3) courses teach systems administrators and security professionals to diagnose and respond to various security incidents, including DoS attacks, by understanding symptoms and isolating issues based on the services affected.

NEW QUESTION # 37
An Azure administrator discovers unauthorized access to a storage account containing sensitive documents.
The initial investigation suggests compromised credentials. In response to this incident, what should be the administrator's first action to secure the account?

- A. Contact Azure support for an immediate investigation and assistance.
- B. Enable Azure Multi-Factor Authentication (MFA) for all user accounts accessing the storage.
- C. Move sensitive documents to a new storage account with restricted access.
- D. Reset the credentials of the compromised account and review all recent access logs.

Answer: D

Explanation:
Comprehensive and Detailed Explanation (ECIH-aligned):
This incident indicates credential compromise, a common cloud security issue addressed in the ECIH Cloud Incident Handling module. When credentials are suspected to be compromised, the immediate priority is to stop unauthorized access and determine the scope of misuse.
Option B is correct because resetting the compromised credentials immediately cuts off the attacker's access.
Reviewing recent access logs allows responders to validate what actions were taken, which data was accessed, and whether additional accounts were affected. ECIH emphasizes immediate credential revocation as a first- response action in identity-based cloud incidents.
Option D (enabling MFA) is a critical hardening measure but does not immediately revoke compromised credentials. Option A is a recovery step that may not stop ongoing access. Option C may be necessary later but should not delay immediate containment.
Therefore, resetting credentials and reviewing logs is the most effective first action, fully aligned with ECIH guidance.

NEW QUESTION # 38
Olivia, a cybersecurity responder at a multinational firm, is alerted late at night by the NOC team about unusual latency and degraded performance across several critical applications hosted on the company's internal servers. Upon initial inspection, she

notices that the internal routers are experiencing an unusually high volume of ARP requests being broadcast across the network. The network bandwidth utilization has spiked, and multiple routers are reporting elevated CPU usage.
As she digs deeper into the diagnostics, Olivia finds that the NAT tables on edge routers are saturated with numerous entries coming from the same IP range within a short time frame. These entries appear to be initiating simultaneous connections to different ports across various endpoints. The firewall logs also show repeated attempts to access unused services, and the ISP reports an overflow of incoming requests from various geolocations.
Based on these symptoms, what should Olivia suspect?

- A. Rogue DHCP server activity
- B. Application vulnerability scanning
- C. Data exfiltration
- D. Distributed DoS attack

Answer: D

Explanation:
The indicators described align closely with a Distributed Denial-of-Service (DDoS) attack, a major topic in the ECIH Network Security Incidents module. DDoS attacks overwhelm network and system resources using traffic from multiple sources, often distributed across geographic regions.
Excessive ARP traffic, NAT table exhaustion, elevated CPU usage on routers, and simultaneous connection attempts are classic symptoms of volumetric and protocol-based DDoS attacks. The involvement of multiple geolocations, as reported by the ISP, further confirms the distributed nature of the attack.
Option B is correct because no single-host misconfiguration or reconnaissance activity would generate this volume and diversity of traffic. Option A would cause IP conflicts, not global traffic floods. Option C focuses on stealthy outbound activity, not inbound saturation. Option D is low-volume and targeted.
ECIH emphasizes early identification of DDoS conditions to enable rapid containment using rate limiting, blackholing, or ISP coordination. Recognizing these indicators is critical to protecting service availability.

NEW QUESTION # 39
In the Control Analysis stage of the NIST's risk assessment methodology, technical and none technical control methods are classified into two categories. What are these two control categories?

- A. Preventive and Detective controls
- B. Predictive and Detective controls
- C. Detective and Disguised controls
- D. Preventive and predictive controls

Answer: A

NEW QUESTION # 40
.....

} by searching on ➤ www.pdfvce.com □ ➡□212-89 New Exam Braindumps

- Reliable 212-89 Test Price ❣ 212-89 Valid Dumps Files □ 212-89 Official Study Guide □ Open website [www.dumpsquestion.com] and search for " 212-89 " for free download □Learning 212-89 Mode
- Prep4sure 212-89 test dumps - pass4sure of EC-COUNCIL 212-89 exam □ Search for { 212-89 } on ➥ www.pdfvce.com □ immediately to obtain a free download □212-89 Official Study Guide
- Buy www.examcollectionpass.com EC-COUNCIL 212-89 Exam Dumps With Free Updates □ Simply search for ➤ 212-89 □ for free download on ➽ www.examcollectionpass.com □ □Free 212-89 Test Questions
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bookmarkinglife.com, socialmediaentry.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 EC-COUNCIL 212-89 dumps are available on Google Drive shared by ActualTestsQuiz: https://drive.google.com/open?id=1lPr4U_Sjm6FVl-SzRjpzioXvIoeDWuqK