212-82 Download Demo & Exam 212-82 Certification Cost

P.S. Free & New 212-82 dumps are available on Google Drive shared by Real4exams: https://drive.google.com/open?id=11vMUzEf8le1_izfNUj9TWxk8IfwTAqIs

The latest 212-82 dumps collection covers everything you need to overcome the difficulty of real questions and certification exam. Accurate 212-82 test answers are tested and verified by our professional experts with the high technical knowledge and rich experience. You may get answers from other vendors, but our 212-82 briandumps pdf are the most reliable training materials for your exam preparation.

ECCouncil 212-82 Exam is an excellent choice for entry-level cybersecurity professionals who want to gain a strong foundation in cybersecurity. Passing the exam demonstrates the ability to protect organizations from cyber threats and vulnerabilities. Certified Cybersecurity Technician certification is recognized globally and is essential for professionals who want to work in government agencies.

>> 212-82 Download Demo <<

Valid 212-82 training materials | 212-82 exam prep: Certified Cybersecurity Technician - Real4exams

Our Certified Cybersecurity Technician (212-82) questions PDF version is great for busy candidates who like to learn on the go with their smartphones or tablets. The Certified Cybersecurity Technician (212-82) dumps PDF format's portability making it ideal for on-the-go studying from any smart device. Studying in PDF format is convenient since it can be printed out and used as a hard copy if you do not have access to a smart device at the moment.

ECCouncil Certified Cybersecurity Technician Sample Questions (Q25-Q30):

NEW QUESTION # 25
An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.
Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

- A. 20.20.10.60
- B. 20.20.10.180
- C. 20.20.10.59
- D. 20.20.10.19

Answer: D

Explanation:
20.20.10.19 is the source IP address of the SYN flooding attack in the above scenario. SYN flooding is a type of denial-of-service (DoS) attack that exploits the TCP (Transmission Control Protocol) three-way handshake process to disrupt the network and gain advantage over the network to bypass the firewall. SYN flooding sends a large number of SYN packets with spoofed source IP addresses to a target server, causing it to allocate resources and wait for the corresponding ACK packets that never arrive. This exhausts the server's resources and prevents it from accepting legitimate requests . To determine the source IP address of the SYN flooding attack, one has to follow these steps:
Navigate to the Documents folder of Attacker-1 machine.
Double-click on Synflood.pcapng file to open it with Wireshark.
Click on Statistics menu and select Conversations option.
Click on TCP tab and sort the list by Bytes column in descending order.
Observe the IP address that has sent the most bytes to 20.20.10.26 (target server).
The IP address that has sent the most bytes to 20.20.10.26 is 20.20.10.19 , which is the source IP address of the SYN flooding attack.

NEW QUESTION # 26
Bob was recently hired by a medical company after it experienced a major cyber security breach.
Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. HIPPA/PHI
- B. ISO 2002
- C. PCIDSS
- D. PII

Answer: A

Explanation:
HIPPA/PHI is the regulation that is mostly violated in the above scenario. HIPPA (Health Insurance Portability and Accountability Act) is a US federal law that sets standards for protecting the privacy and security of health information. PHI (Protected Health Information) is any information that relates to the health or health care of an individual and that can identify the individual, such as name, address, medical records, etc. HIPPA/PHI requires covered entities, such as health care providers, health plans, or health care clearinghouses, and their business associates, to safeguard PHI from unauthorized access, use, or disclosure.In the scenario, the medical company experienced a major cyber security breach that exposed the personal medical records of many patients on the

internet, which violates HIPPA/PHI regulations. PII (Personally Identifiable Information) is any information that can be used to identify a specific individual, such as name, address, social security number, etc. PII is not specific to health information and can be regulated by various laws, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. PCI DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. ISO 2002 (International Organization for Standardization 2002) is not a regulation, but a standard for information security management systems that provides guidelines and best practices for organizations to manage their information security risks.

NEW QUESTION # 27
You are the Lead Cybersecurity Specialist at GlobalTech, a multinational tech conglomerate renowned for its avant-garde technological solutions in the aerospace and defense sector. The organization's reputation stands on the innovative technologies it pioneers, many of which are nation's top secrets.
Late on a Sunday night, you are alerted about suspicious activities on a server holding the schematics and project details for a groundbreaking missile defense system. The indicators suggest a complex, multi-stage cyberattack that managed to bypass traditional security measures. Preliminary investigations reveal that the cybercrlmlnals might have used an Insider's credentials, further complicating the breach. Given the extremely sensitive nature of the data involved, a leak could have severe national security implications and irreparably tarnish the company's reputation. Considering the potential gravity and intricacies of this security incident, what immediate action should you undertake to handle this situation effectively, safeguard crucial data, and minimize potential fallout?

- A. Engage with an external specialized cybersecurity firm to conduct a parallel investigation, leveraging its expertise to identify the culprits and understand the breach's modus operandi.
- B. Notify federal agencies about the potential breach of national security. Work in tandem with them to ensure all necessary measures are taken to prevent further data exfiltration and protect national interests.
- C. Initiate the incident response protocol, focusing on immediate containment by isolating the impacted server. Concurrently, assess the breadth and depth of the breach by examining network logs and affected systems.
- D. Inform the top executive board and legal team about the breach. Prepare a public statement to ensure shareholders and clients are kept in the loop about the incident and the measures being undertaken.

Answer: C

Explanation:
In the event of a cyberattack involving highly sensitive data, such as a missile defense system, the immediate focus should be on containing the breach and understanding its scope. Here's a step-by-step approach:
* Incident Response Protocol:
* Containment: Isolate the impacted server to prevent further unauthorized access or data exfiltration. This helps to limit the damage and secure sensitive information.
* Assessment: Examine network logs, affected systems, and user activities to determine the extent of the breach. This includes identifying how the attackers gained access and what data might have been compromised.
* Minimize Fallout:
* Preservation of Evidence: Ensure that all logs and forensic data are preserved for a detailed investigation.
* Internal Coordination: Inform key stakeholders within the organization, including the executive board and legal team, about the breach and ongoing response efforts.
* Collaboration:
* Federal Agencies: Depending on the severity and national security implications, notifying federal agencies might be necessary after initial containment and assessment.
* External Experts: If required, engage external cybersecurity firms to assist with the investigation and provide additional expertise.
References:
* NIST Computer Security Incident Handling Guide:NIST SP 800-61r2
* SANS Institute Incident Handling Handbook: SANS Reading Room

NEW QUESTION # 28
Hotel Grande offers luxury accommodations and emphasizes top-notch service for its guests. One such service is secure, high-speed Wi-FI access In every room. The hotel wishes to deploy an authentication method that would give individual guests a seamless experience without compromising security. This method should ideally provide a balance between convenience and strong security. Which of the following should Hotel Grande use?

- A. MAC address filtering
- B. Open Authentication
- C. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)
- D. PSK (Pre-Shared Key)

Answer: C

Explanation:
* Strong Security:
* EAP-TLS provides strong security by using certificate-based authentication. This ensures that both the client and server are authenticated before a connection is established.

NEW QUESTION # 29
An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.
Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

- A. 20.20.10.60
- B. 20.20.10.180
- C. 20.20.10.59
- D. 20.20.10.19

Answer: D

NEW QUESTION # 30
.....

Nowadays the competition in the society is fiercer and if you don't have a specialty you can't occupy an advantageous position in the competition and may be weeded out. Passing the test 212-82 certification can help you be competent in some area and gain the competition advantages in the labor market. If you buy our 212-82 Study Materials you will pass the 212-82 exam smoothly. You will feel grateful for choosing us!

www.real4dumps.com" open and search for （ 212-82 ） to download for free □212-82 Free Exam Questions

- mikemil988.blogmazing.com, haot1.com, tedcole945.theblogfairy.com, club.gslxtfc.com.cn, cecapperu.com, hightechtrainingcenter.com, tedcole945.blogsvila.com, shortcourses.russellcollege.edu.au, cresc1ta.store, study.stcs.edu.np, Disposable vapes

BONUS!!! Download part of Real4exams 212-82 dumps for free: https://drive.google.com/open?id=11vMUzEf8le1_izfNUj9TWxk8IfwTAqIs