Das neueste 212-89, nützliche und praktische 212-89 pass4sure Trainingsmaterial

Übrigens, Sie können die vollständige Version der ZertFragen 212-89 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1DmEDAjKmFEnihnle-rslqAavRPiNOp7e

Die Fragenkataloge von EC-COUNCIL 212-89 von unserem ZertFragen existieren in der Form von PDF und Stimulationssoftware. Wir aktualisieren unsere Materialien regelmäßig, so dass Sie immer die aktuellen und genauen Informationen über die Fragenkataloge von EC-COUNCIL 212-89 erhalten können. Nach langjährigen Bemühungen haben unsere Erfolgsquote von der EC-COUNCIL 212-89 Zertifizierungsprüfung 100% erreicht.

Die EC-Council Certified Incident Handler (ECIH v2) Zertifizierung soll Fachleuten die Fähigkeiten und Kenntnisse vermitteln, die erforderlich sind, um auf verschiedene Arten von Sicherheitsvorfällen zu reagieren und sie zu behandeln. Dieses Zertifizierungsprogramm wurde vom International Council of E-Commerce Consultants (EC-Council) entwickelt, einer führenden Organisation auf dem Gebiet der Cybersicherheitsschulung und -zertifizierung. Die ECIH v2 Zertifizierung deckt eine breite Palette von Themen ab, einschließlich Incident Handling, Response und Recovery, Netzwerk- und Webanwendungssicherheit sowie Malware-Analyse.

>> 212-89 Examengine <<

212-89 Fragen&Antworten, 212-89 Fragen Beantworten

Wollen Sie gute Leistung in IT-Industrie haben und mehr professioneller anerkannt werden? Melden Sie sich bitte EC-COUNCIL 212-89 IT-Industrie an, um Ihre Fähigkeit zu entwickeln. Wir ZertFragen helfen Ihnen, den Wunsch zu erfüllen. Hier sind sehr professionelle Kenntnisse und starke Dumps über EC-COUNCIL 212-89 Zertifizierungsprüfung, guten Service, die Ihr besseres Beherrschen der Kenntnisse realisieren und die EC-COUNCIL 212-89 Prüfung leichter bestehen und leichter Ihren Erfolg zu erreichen.

EC-COUNCIL EC Council Certified Incident Handler (ECIH v3) 212-89 Prüfungsfragen mit Lösungen (Q160-Q165):

160. Frage
Alex is an incident handler in QWERTY Company. He identified that an attacker created a backdoor inside the company's network by installing a fake AP inside a firewall. Which of the following attack types did the attacker use?

- A. Rogue access point
- B. Ad hoc associations
- C. AP misconfiguration
- D. Wardriving

Antwort: A

Begründung:
When an attacker installs a fake AP (Access Point) within a company's network, especially behind a firewall, this constitutes the deployment of a Rogue Access Point. Rogue APs are unauthorized wireless access points installed within a network without the network administrator's knowledge or consent. They pose a significant security risk because they can be used to intercept sensitive information, bypass network security configurations, and provide a gateway for attackers to enter the network undetected. This type of attack circumvents the security measures put in place by a company, including firewalls, by creating an illicit entry point into the network that is under the control of the attacker.References:Incident Handler (ECIH v3) courses and study materials discuss various network-based attacks and their mitigation strategies, emphasizing the importance of regular network scans to detect and remove rogue access points and thus secure the network from unauthorized access.

161. Frage
In which of the following phases of the incident handling and response (IH&R) process is the identified security incidents analyzed, validated, categorized, and prioritized?

- A. Containment
- B. Notification
- C. Incident triage
- D. Incident recording and assignment

Antwort: C

162. Frage
Dash wants to perform a DoS attack over 256 target URLs simultaneously.
Which of the following tools can Dash employ to achieve his objective?

- A. Ollydbg
- B. IDAPro
- C. HOIC
- D. OpenVAS

Antwort: C

Begründung:
High Orbit Ion Cannon (HOIC) is a tool designed to perform stress testing on networks or servers. It can launch a Distributed Denial of Service (DDoS) attack by enabling an attacker to overwhelm a target with HTTP POST and GET requests. HOIC's distinctive feature is its ability to attack multiple targets (up to 256 URLs simultaneously) with configurable HTTP flood attacks. This capability makes it a preferred choice for attackers aiming to disrupt services on a large scale. Unlike tools designed for debugging or vulnerability scanning (e.g., IDA Pro, Ollydbg, OpenVAS), HOIC is specifically crafted for launching DoS/DDoS attacks, making it the correct answer for Dash's objective.References:The Incident Handler (ECIH v3) courses and study guides delve into

various cyber attack tools, including HOIC, explaining their functionalities and potential impact as part of the comprehensive cybersecurity threat landscape education.

163. Frage
Which of the following is a term that describes the combination of strategies and services intended to restore data, applications, and other resources to the public cloud or dedicated service providers?

- A. Eradication
- B. Cloud recovery
- C. Mitigation
- D. Analysis

Antwort: B

Begründung:
The term that describes the combination of strategies and services intended to restore data, applications, and other resources to the public cloud or dedicated service providers is "Cloud recovery." This term encompasses disaster recovery efforts focused on ensuring that an organization's digital assets can be quickly and effectively restored or moved to cloud environments in the event of data loss, system failure, or a disaster.
Cloud recovery strategies are part of a broader disaster recovery and business continuity planning, ensuring minimal downtime and data loss by leveraging cloud computing's scalability and flexibility. Mitigation, analysis, and eradication are terms associated with other aspects of incident response and risk management, not specifically with the restoration of resources to cloud environments.
References:The Incident Handler (ECIH v3) curriculum includes discussions on disaster recovery and business continuity planning, highlighting cloud recovery as a vital component of ensuring organizational resilience against disruptions.

164. Frage
Smith employs various malware detection techniques to thoroughly examine the network and its systems for suspicious and malicious malware files. Among all techniques, which one involves analyzing the memory dumps or binary codes for the traces of malware?

- A. Intrusion analysis
- B. Dynamic analysis
- C. Static analysis
- D. Live system

Antwort: C

Begründung:
Static analysis involves examining the malware's memory dumps or binary codes without executing the code.
This technique is used to find traces of malware by analyzing the code to understand its purpose, functionality, and potential impact. Static analysis allows for the identification of malicious signatures, strings, or other indicators of compromise within the malware's code. This method is contrasted with dynamic analysis, which studies the malware's behavior during execution, live system analysis, which examines running systems, and intrusion analysis, which focuses on detecting and analyzing breaches.References:The ECIH v3 certification program includes malware analysis techniques, highlighting static analysis as a key method for investigating malware without the risk of executing it on a live system.

165. Frage
.....

www.pass4test.de } Öffnen und suchen Sie ⇛ 212-89 ⇚ Kostenloser Download □212-89 Online Prüfung

- 212-89 Prüfungsfrage □ 212-89 Dumps □ 212-89 Prüfungsfragen □ Erhalten Sie den kostenlosen Download von ➠ 212-89 □ mühelos über ⇛ www.itzert.com ⇚ □212-89 Simulationsfragen
- 212-89 Übungstest: EC Council Certified Incident Handler (ECIH v3) - 212-89 Braindumps Prüfung □ Sie müssen nur zu （ www.pass4test.de ） gehen um nach kostenloser Download von ▶ 212-89 ◀ zu suchen □212-89 Dumps
- 212-89 Testing Engine □ 212-89 Online Prüfung □ 212-89 Prüfungsmaterialien □ Sie müssen nur zu ➠ www.itzert.com □ gehen um nach kostenloser Download von 「 212-89 」 zu suchen □212-89 Zertifikatsfragen
- 212-89 Übungsmaterialien - 212-89 realer Test - 212-89 Testvorbereitung □ Sie müssen nur zu ➽ www.zertfragen.com □ gehen um nach kostenloser Download von { 212-89 } zu suchen □212-89 Online Praxisprüfung
- 212-89 zu bestehen mit allseitigen Garantien □ URL kopieren ➥ www.itzert.com □ Öffnen und suchen Sie ✔ 212-89 □✔□ Kostenloser Download □212-89 Simulationsfragen
- 212-89 Übungsmaterialien □ 212-89 Testing Engine □ 212-89 Online Prüfung □ Suchen Sie auf der Webseite “ www.pass4test.de ” nach ➥ 212-89 □ und laden Sie es kostenlos herunter □212-89 Pruefungssimulationen
- 212-89 Prüfungsfrage □ 212-89 Prüfungsfrage □ 212-89 Prüfungsfrage ✳ Öffnen Sie 【 www.itzert.com 】 geben Sie ✔ 212-89 □✔□ ein und erhalten Sie den kostenlosen Download □212-89 Prüfungsmaterialien
- 212-89 Übungsmaterialien □ 212-89 Online Praxisprüfung □ 212-89 Prüfungsfragen □ Öffnen Sie die Webseite 《 www.zertpruefung.ch 》 und suchen Sie nach kostenloser Download von 《 212-89 》 □212-89 Prüfungsfrage
- EC-COUNCIL 212-89 Quiz - 212-89 Studienanleitung - 212-89 Trainingsmaterialien □ URL kopieren （ www.itzert.com ） Öffnen und suchen Sie “ 212-89 ” Kostenloser Download □212-89 Zertifizierung
- 212-89 Zertifizierung □ 212-89 Online Prüfung □ 212-89 Prüfungsmaterialien □ Sie müssen nur zu ✔ www.zertpruefung.ch □✔□ gehen um nach kostenloser Download von ▷ 212-89 ◁ zu suchen □212-89 Prüfungsfrage
- interncertify.com, ncon.edu.sa, academia.clinicaevolve.ro, 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, elearnzambia.cloud, mcq24.in, paraschessacademy.com, shortcourses.russellcollege.edu.au, 106.15.58.108, www.stes.tyc.edu.tw, Disposable vapes

P.S. Kostenlose und neue 212-89 Prüfungsfragen sind auf Google Drive freigegeben von ZertFragen verfügbar: https://drive.google.com/open?id=1DmEDAjKmFEnihnle-rslqAavRPiNOp7e