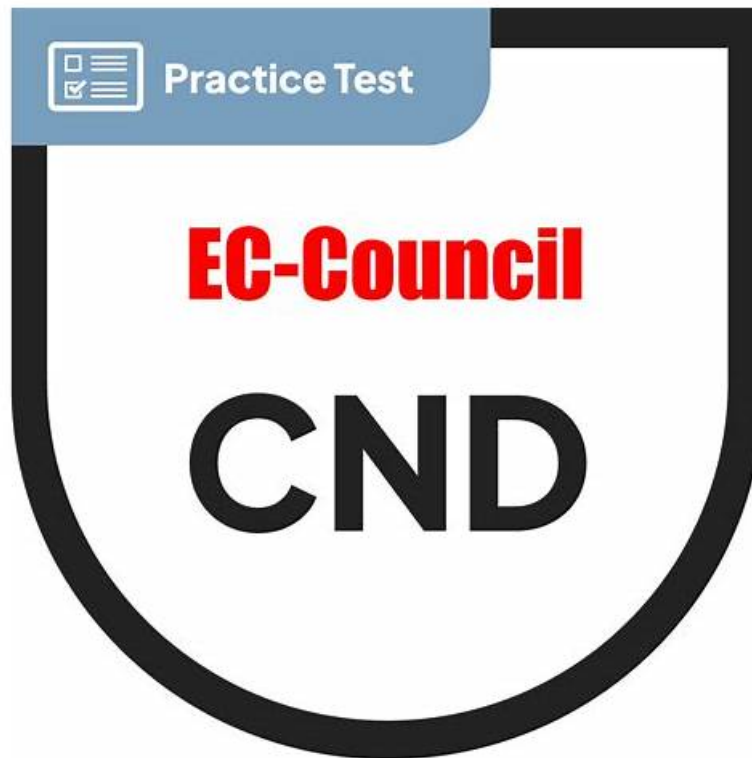


312-38 PrüfungGuide, EC-COUNCIL 312-38 Zertifikat - EC-Council Certified Network Defender CND



Außerdem sind jetzt einige Teile dieser ExamFragen 312-38 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1kJbQsYPBg7i5mpbVHwB_SiTEa7AYop0H

Wir sind der Schnellste, der das EC-COUNCIL 312-38 Zertifikat erhält; wir sind noch der höchste, der Ihre Interessen schützt. Wir sind ExamFragen. ExamFragen kann Ihnen versprechen, dass die Testaufgaben von EC-COUNCIL 312-38 Zertifizierungsprüfung 100% richtig und ganz umfassend sind. Nachdem Sie die Testfragen zur EC-COUNCIL 312-38 Zertifizierung gekauft haben, werden Sie kostenlos die einjährige Aktualisierung genießen.

EC-Council 312-38 (C-Council Certified Network Defender CND) Zertifizierungsprüfung ist eine der gefragtesten Zertifizierungen im Cybersecurity-Bereich. Die Zertifizierung soll die Fähigkeiten und Kenntnisse von Kandidaten in verschiedenen Bereichen der Netzwerkverteidigung bewerten, einschließlich Risikomanagement, Vorfälle, Netzwerksicherheit und Bedrohungsanalyse.

Die Prüfung von EC-Council 312-38 deckt ein breites Spektrum von Themen ab, darunter Netzwerksicherheit, Netzwerkprotokolle, Netzwerkschwachstellen und Netzwerkverteidigungstechnologien. Kandidaten, die die Prüfung bestehen, zeigen ein umfassendes Verständnis der Netzwerkverteidigung und sind ausgestattet, um Angriffe auf die Netzwerkinfrastruktur ihres Unternehmens zu identifizieren und zu mildern.

>> 312-38 Fragenkatalog <<

EC-COUNCIL 312-38 Tests, 312-38 Testantworten

Unser ExamFragen ist eine Website, die eine lange Geschichte hinter sich hat. So genießt ExamFragen einen guten Ruf in der IT-Branche. Und wir haben vielen Kandidaten geholfen, die EC-COUNCIL 312-38 Prüfung zu bestehen. Die Fragen und Antworten zur EC-COUNCIL 312-38 Zertifizierungsprüfung von ExamFragen werden von den erfahrungsreichen Expertenteams nach ihren Kenntnissen und Erfahrungen bearbeitet. Wenn Sie an der EC-COUNCIL 312-38 Zertifizierungsprüfung teilnehmen wollen, ist ExamFragen zweifellos eine gute Wahl.

Die CND-Zertifizierungsprüfung (C-Council Certified Network Defender) ist eine strenge Prüfung, die eine umfassende Vorbereitung und Studie erfordert. Die Prüfung besteht aus 100 Multiple-Choice-Fragen und hat eine Zeitlimit von 4 Stunden. Um die Prüfung zu bestehen, müssen die Kandidaten mindestens 70% erzielen.

EC-COUNCIL EC-Council Certified Network Defender CND 312-38 Prüfungsfragen mit Lösungen (Q647-Q652):

647. Frage

Which of the following statements is not true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.

- A. It does not support file protection.
- B. It supports the Linux operating system.
- C. It supports task compression files.
- D. It works well with large disk, because the cluster size increases as the disk partition size increases.

Antwort: C,D

648. Frage

Match the following NIST security life cycle components with their activities:

1. Implement	i. Applies tailoring guidance and supplemental controls as needed
2. Authorize	ii. Determines security control effectiveness
3. Categorize	iii. Determines risk to organizational operations and assets
4. Select	iv. Sets security controls within an enterprise architecture
	v. Defines criticality of information system according to potential worst-case

- A. 1-i, 2-v, 3-iii, 4-ii
- B. 1-iii, 2-iv, 3-v, 4-i
- C. 1-ii, 2-i, 3-v, 4-iv
- D. 1-iv, 2-iii, 3-v, 4-i

Antwort: D

Begründung:

The NIST security life cycle components and their activities are correctly matched in option C:

* Implement (1) corresponds with iv. Sets security controls within an enterprise architecture. This involves integrating the selected security controls into the enterprise architecture during the implementation phase.

* Authorize (2) matches with iii. Determines risk to organizational operations and assets. Authorization involves assessing the risks to the organization's operations and assets and determining if the implemented controls are adequate.

* Categorize (3) aligns with v. Defines criticality of information system according to potential worst-case.

Categorization is the process of determining the criticality of information systems based on the potential impact of worst-case scenarios.

* Select (4) is associated with i. Determines security control effectiveness. Selection involves choosing the appropriate security controls and determining their effectiveness in protecting the system.

References: The information provided is based on the NIST guidelines for the system development life cycle, which include security considerations as an integral part of the process 1234.

649. Frage

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=0x00`
- B. `Tcp.options.mss_val<1460`

- C. `Tcp.options.wscale_val=20`
- D. `Tcp.flags=0x2b`

Antwort: A,B,D

650. Frage

Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?

- A. Discretionary access control
- B. Non-discretionary access control
- C. Role-based access control
- D. Mandatory access control

Antwort: A

Begründung:

Ross implemented Discretionary Access Control (DAC) in the organization's peer-to-peer network. DAC is a type of access control where the data owner has the authority to decide who can access their data and what permissions they have. In a peer-to-peer network, where each peer can act as both a client and a server, DAC allows individual users to set access controls for their own files and folders. This is consistent with Ross allowing employees to set their own control measures, which aligns with the principles of DAC where owners or creators of the resources have the discretion to grant or restrict access to other users based on their own criteria.

651. Frage

Which among the following is used to limit the number of cmdlets or administrative privileges of administrator, user, or service accounts?

- A. Just Enough Administration (JEA)
- B. Windows Security Identifier (SID)
- C. User Account Control (UAC)
- D. Credential Guard

Antwort: A

Begründung:

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. JEA helps in reducing the number of administrators on your machines by using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users. It limits what users can do by specifying which cmdlets, functions, and external commands they can run. This ensures that users have just enough access to perform their jobs without having unnecessary administrative privileges, which aligns with the principle of least privilege¹²³.

References: The information about JEA and its role in limiting cmdlets and administrative privileges is detailed in the Microsoft documentation and training modules on Just Enough Administration (JEA), as well as in the PowerShell-Docs on GitHub¹²³. These sources provide comprehensive guidance on how JEA is used to control administrative privileges and are aligned with the objectives and documents of the EC-Council's Certified Network Defender (CND) program.

652. Frage

.....

312-38 Tests: <https://www.examfragen.de/312-38-pruefung-fragen.html>

- 312-38 Exam ☉ 312-38 Prüfungs ☐ 312-38 Zertifikatsdemo ☐ Öffnen Sie « www.zertpruefung.de » geben Sie ► 312-38 ◀ ein und erhalten Sie den kostenlosen Download ☐ 312-38 Prüfungsfragen
- 312-38 Exam ☐ 312-38 Exam ☐ 312-38 Prüfungsfragen ☐ Öffnen Sie die Webseite ➡ www.itzert.com ☐ und suchen Sie nach kostenloser Download von ► 312-38 ◀ ☐ 312-38 Testfragen
- 312-38 PDF ☐ 312-38 Exam ☐ 312-38 Zertifizierungsprüfung ☐ Suchen Sie jetzt auf“ www.pruefungfrage.de ” nach ► 312-38 ☐ und laden Sie es kostenlos herunter ☐ 312-38 PDF

