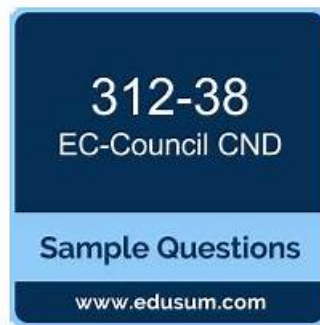


EC-COUNCIL 312-38 Sample Questions - 312-38 Real Dumps Free



BTW, DOWNLOAD part of VCEEngine 312-38 dumps from Cloud Storage: <https://drive.google.com/open?id=1YKK0LeuxDSdKDRoGokHKbsdqrC8Z1v60>

Our 312-38 exam materials can help you stand out in the fierce competition. After using our 312-38 study questions, you have a greater chance of passing the 312-38 certification, which will greatly increase your soft power and better show your strength. Our 312-38 training guide can bring you something. After you have used our 312-38 learning braindump, you will certainly have your own experience. Now let's take a look at why a worthy product of your choice is our 312-38 actual exam.

EC-COUNCIL 312-38 certification is highly regarded in the IT industry as it demonstrates an individual's expertise in protecting an organization's network infrastructure against various cyber threats. EC-Council Certified Network Defender CND certification is designed to equip individuals with the knowledge and skills required to plan, implement, and maintain an organization's network security infrastructure. EC-Council Certified Network Defender CND certification also focuses on developing an individual's ability to detect and respond to network security breaches, and implement appropriate countermeasures.

EC-COUNCIL 312-38 Exam is one of the most sought-after certifications in the field of cybersecurity. EC-Council Certified Network Defender CND certification is particularly useful for network administrators, network security engineers, and other professionals who are responsible for maintaining the security of their organization's computer networks. The EC-Council Certified Network Defender (CND) certification is designed to equip professionals with the knowledge and skills necessary to secure and defend computer networks against cyber attacks.

>> EC-COUNCIL 312-38 Sample Questions <<

EC-COUNCIL 312-38 Real Dumps Free, 312-38 Boot Camp

To do this you just need to enroll in EC-COUNCIL 312-38 exam and strive hard to pass the EC-Council Certified Network Defender CND (312-38) exam with good scores. However, you should keep in mind that the EC-COUNCIL 312-38 certification exam is different from the traditional exam and always gives taught time to their candidates. But with proper EC-Council Certified Network Defender CND (312-38) exam preparation, planning, and firm commitment can enable you to pass the challenging EC-Council Certified Network Defender CND (312-38) exam.

Career Opportunities

The EC-Council 312-38 Exam equips the professionals with the fundamental knowledge and skills in networking concepts. Without a doubt, earning the Certified Network Defender certification has a lucrative career outlook. Some of the positions that the certified individuals can consider include IT Administrators, Network Technicians, Data Analysts, Network Administrators, and Network Engineers, among others. The average remuneration for these titles is \$94,000 per annum.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q522-Q527):

NEW QUESTION # 522

Which of the following is a software tool used in passive attacks for capturing network traffic?

- A. Sniffer
- B. Intrusion prevention system
- C. Intrusion detection system
- D. Warchalking

Answer: A

NEW QUESTION # 523

Which of the following devices helps in connecting a PC to an ISP via a PSTN?

- A. Modem
- B. Repeater
- C. PCI card
- D. Adapter

Answer: A

NEW QUESTION # 524

Peter works as a network administrator at an IT company. He wants to avoid exploitation of the cloud, particularly Azure services. Which of the following is a group of PowerShell scripts designed to help the network administrator understand how attacks happen and help them protect the cloud?

- A. MicroBurst
- B. Sysmon
- C. SecurityPolicyDsc
- D. POSH -Sysmon

Answer: A

Explanation:

MicroBurst is a collection of PowerShell scripts designed to help network administrators understand how attacks occur and to protect cloud environments, particularly Azure services. These scripts aid in detecting vulnerabilities, simulating attacks, and implementing defensive measures to secure the cloud infrastructure.

* POSH-Sysmon: A set of PowerShell scripts for managing Sysmon configurations.

* SecurityPolicyDsc: A module for managing security policies through Desired State Configuration (DSC).

* Sysmon: A Windows system service and device driver that logs system activity to the Windows event log, not specifically focused on cloud protection.

References:

* EC-Council Certified Network Defender (CND) Study Guide

* Azure security documentation and MicroBurst resources

NEW QUESTION # 525

Which of the following refers to the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an

organization's infrastructure?

- A. Key risk indicators
- B. Indicators of exposure
- **C. Indicators of compromise**
- D. Indicators of attack

Answer: C

Explanation:

Indicators of Compromise (IoCs) are clues, artifacts, or evidence that suggest a potential intrusion or malicious activity within an organization's infrastructure. IoCs are used to identify and respond to security breaches and can include log entries, file hashes, unusual network traffic, or specific patterns that match known threats.

Indicators of Attack (IoA): Focus on detecting the methods and techniques used by attackers.

Key Risk Indicators: Metrics that indicate increased risk levels.

Indicators of Exposure: Signs that reveal vulnerabilities or weaknesses in the system.

NEW QUESTION # 526

Arman transferred some money to his friend's account using a net banking service. After a few hours, his friend informed him that he hadn't received the money yet. Arman logged on to the bank's website to investigate and discovered that the amount had been transferred to an unknown account instead. The bank, upon receiving Arman's complaint, discovered that someone had established a station between Arman's and the bank server's communication system. The station intercepted the communication and inserted another account number replacing his friend's account number. What is such an attack called?

- A. DNS Poisoning
- B. Privilege Escalation
- **C. Man-in-the-Middle Attack**
- D. DNS Cache Poisoning

Answer: C

Explanation:

The scenario described is a classic example of a Man-in-the-Middle (MitM) attack. In this type of cyberattack, the attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. The attacker has inserted themselves between the two parties, in this case, Arman and the bank's server, and has intercepted the communication to redirect the funds to a different account. This type of attack can occur in various forms, such as eavesdropping on or altering the communication over an insecure network service, but it is characterized by the attacker's ability to intercept and modify the data being exchanged without either legitimate party noticing.

NEW QUESTION # 527

.....

312-38 Real Dumps Free: <https://www.vceengine.com/312-38-vce-test-engine.html>

- EC-COUNCIL 312-38 Sample Questions: EC-Council Certified Network Defender CND - www.examcollectionpass.com Providers you Best Real Dumps Free ☐ Open ⇒ www.examcollectionpass.com ⇐ enter ➡ 312-38 ☐ and obtain a free download ☐ 312-38 Test Guide
- 312-38 Examcollection Free Dumps ☐ 312-38 Certification Exam ☐ Exam 312-38 Score ☐ Open ✓ www.pdfvce.com ☐ ✓ ☐ and search for ▶ 312-38 ◀ to download exam materials for free ☐ 312-38 Clear Exam
- Try Desktop EC-COUNCIL 312-38 Practice Test Software For Self-Assessment ☐ ➤ www.vce4dumps.com ☐ is best website to obtain ⇒ 312-38 ⇐ for free download ☐ 312-38 Valid Test Review
- EC-COUNCIL 312-38 Sample Questions: EC-Council Certified Network Defender CND - Pdfvce Providers you Best Real Dumps Free ☐ Search for ☼ 312-38 ☐ ☼ ☐ and easily obtain a free download on ▷ www.pdfvce.com ◁ ☐ ☐ Certification 312-38 Book Torrent
- Reliable 312-38 Dumps Sheet ↘ Reliable 312-38 Dumps Sheet ☐ Certification 312-38 Book Torrent ☐ Search for [312-38] and download exam materials for free through ✓ www.practicevce.com ☐ ✓ ☐ ☐ Sure 312-38 Pass
- Test 312-38 Discount Voucher ☐ 312-38 Certification Exam ☐ Reliable 312-38 Real Test ☐ Search for ➡ 312-38 ☐ ☐ and download it for free immediately on ➡ www.pdfvce.com ☐ ☐ 312-38 Reliable Brindumps Ebook
- Pass 312-38 Exam with EC-COUNCIL's Exam Questions and Achieve 100% Success on Your First Try ☐ Search for ☼

[illegible]

What's more, part of that VCEEngine 312-38 dumps now are free: <https://drive.google.com/open?id=1YKK0LeuxDSdKDRoGokHKbsdqrC8Z1v60>