

New 312-38 Braindumps | 312-38 Discount Code



BTW, DOWNLOAD part of Pass4sures 312-38 dumps from Cloud Storage: <https://drive.google.com/open?id=1FjgVLQxMoTD6AOtR8Dkaiil7jHa4VYri>

If you buy Pass4sures EC-COUNCIL 312-38 Exam Training materials, you will solve the problem of your test preparation. You will get the training materials which have the highest quality. Buy our products today, and you will open a new door, and you will get a better future. We can make you pay a minimum of effort to get the greatest success.

With the aid of our EC-COUNCIL 312-38 exam preparation to improve your grade and change your states of life and get amazing changes in career, everything is possible. It all starts from our EC-COUNCIL 312-38 learning questions. Our EC-COUNCIL 312-38 training questions are the accumulation of professional knowledge worthy practicing and remembering.

>> New 312-38 Braindumps <<

312-38 Discount Code & Free 312-38 Exam

Do you still have the ability to deal with your job well? Do you think whether you have the competitive advantage when you are compared with people working in the same field? If your answer is no, you are a right place now. Because our 312-38 exam torrent will be your good partner and you will have the chance to change your work which you are not satisfied with, and can enhance your ability by our 312-38 Guide questions, you will pass the exam and achieve your target.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q549-Q554):

NEW QUESTION # 549

Which of the following honeypots provides an attacker access to the real operating system without any restriction and collects a vast amount of information about the attacker?

- A. High-interaction honeypot
- B. Low-interaction honeypot
- C. Honeyd
- D. Medium-interaction honeypot

Answer: A

Explanation:

A high-interaction honeypot offers a vast amount of information about attackers. It provides an attacker access to the real operating system without any restriction. A high-interaction honeypot is a powerful weapon that provides opportunities to discover new tools, to identify new vulnerabilities in the operating system, and to learn how blackhats communicate with one another.

Answer option D is incorrect. A low-interaction honeypot captures limited amounts of information that are mainly transactional data and some limited interactive information. Because of simple design and basic functionality, low-interaction honeypots are easy to install, deploy, maintain, and configure. A low-interaction honeypot detects unauthorized scans or unauthorized connection attempts. A low-interaction honeypot is like a one-way connection, as the honeypot provides services that are limited to listening ports. Its role is very passive and does not alter any traffic. It generates logs or alerts when incoming packets match their patterns.

Answer option B is incorrect. A medium-interaction honeypot offers richer interaction capabilities than a low-interaction honeypot, but does not provide any real underlying operating system target. Installing and configuring a medium-interaction honeypot takes more time than a low-interaction honeypot. It is also more complicated to deploy and maintain as compared to a low-interaction honeypot. A medium-interaction honeypot captures a greater amount of information but comes with greater risk. Answer option C is incorrect. Honeyd is an example of a low-interaction honeypot.

NEW QUESTION # 550

Which of the following firewalls are used to track the state of active connections and determine the network packets allowed to enter through the firewall? Each correct answer represents a complete solution. Choose all that apply.

- A. Stateful
- B. Circuit-level gateway
- C. Dynamic packet-filtering
- D. Proxy server

Answer: A,C

Explanation:

A dynamic packet-filtering firewall is a fourth generation firewall technology. It is also known as a stateful firewall. It tracks the state of active connections and determines which network packets are allowed to enter through the firewall. It records session information, such as IP addresses and port numbers to implement a more secure network. The dynamic packet-filtering firewall operates at Layer3, Layer4, and Layer5.

Answer option A is incorrect. A circuit-level gateway is a type of firewall that works at the session layer of the OSI model between the application layer and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks. Circuit-level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.

Answer option C is incorrect. A proxy server firewall intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

NEW QUESTION # 551

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

- A. NetWitness
- **B. Wireshark**
- C. Bridle
- D. None
- E. NetResident

Answer: B

Explanation:

Wireshark is an open source protocol analyzer that can capture traffic in real time. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.

Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features:

Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.

Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.

Captured files can be programmatically edited or converted via command-line switches to the "editcap" program

Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.

Answer option C is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures.

Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Answer option D is incorrect. NetWitness is used to analyze and monitor the network traffic and activity.

Answer option A is incorrect. Netresident is used to capture, store, analyze, and reconstruct network events and activities.

NEW QUESTION # 552

Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?

- A. DCAP
- B. BOOTP
- **C. NNTP**
- D. NTP

Answer: C

Explanation:

The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read.

Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces.

In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

NEW QUESTION # 553

Which of the following filters can be applied to detect an ICMP ping sweep attempt using Wireshark?

- A. `icmp.type==15`
- B. `icmp.type==17`
- C. `icmp.type==8`
- D. `icmp.type==13`

Answer: C

Explanation:

In Wireshark, the filter `icmp.type==8` is used to detect ICMP Echo requests, which are commonly used in ping sweep attempts. A ping sweep is a network scanning technique used to determine which of a range of IP addresses map to live hosts. It involves sending ICMP Echo requests (type 8) to multiple hosts and listening for Echo replies (type 0). If an Echo reply is received, it indicates that the host is active. Therefore, the filter `icmp.type==8` can be applied to capture these ICMP Echo requests and detect a ping sweep attempt.

NEW QUESTION # 554

.....

Pass4sures are specialized in providing our customers with the most reliable and accurate 312-38 exam guide and help them pass their 312-38 exams by achieve their satisfied scores. With our 312-38 study materials, your exam will be a piece of cake. We have a lasting and sustainable cooperation with customers who are willing to purchase our 312-38 Actual Exam. We try our best to renovate and update our 312-38 study materials in order to help you fill the knowledge gap during your learning process, thus increasing your confidence and success rate.

312-38 Discount Code: <https://www.pass4sures.top/CertifiedEthicalHacker/312-38-testking-braindumps.html>

EC-COUNCIL New 312-38 Braindumps Copy the font file to another directory, EC-COUNCIL New 312-38 Braindumps We have a group of experienced employees aiming to offer considerable and warm customer service, Pass4sures 312-38 Discount Code has a reliable customer service and has problems finding or using any product, You can free download part of Pass4sures's simulation test questions and answers about EC-COUNCIL certification 312-38 exam as a try.

Greensburger via Wikimedia Commons What are the major improvements New 312-38 Braindumps to cellular networks that have enabled faster data rates, Use macOS Recovery, Copy the font file to another directory.

We have a group of experienced employees aiming to offer considerable 312-38 and warm customer service, Pass4sures has a reliable customer service and has problems finding or using any product.

New 312-38 Braindumps | High Pass-Rate 312-38 Discount Code: EC-Council Certified Network Defender CND

You can free download part of Pass4sures's simulation test questions and answers about EC-COUNCIL certification 312-38 exam as a try, Everyone knows the regular pass rate of 312-38 is low, that's why these certifications are being valued.

- New 312-38 Braindumps Exam Pass at Your First Attempt | EC-COUNCIL 312-38 Discount Code Go to website www.troytecdumps.com open and search for « 312-38 » to download for free Valid Dumps 312-38 Files
- Valid Dumps 312-38 Files 312-38 Valid Test Practice Study 312-38 Reference Search for 312-38 and download exam materials for free through www.pdfvce.com 312-38 Reliable Test Labs
- Latest Braindumps 312-38 Ebook 312-38 Exam Dumps Pdf Valid 312-38 Mock Exam Search for 312-38 and obtain a free download on (www.testkingpass.com) Valid 312-38 Mock Exam
- 2026 Trustable EC-COUNCIL 312-38: New EC-Council Certified Network Defender CND Braindumps Search for « 312-38 » and easily obtain a free download on www.pdfvce.com 312-38 Reliable Test Labs
- New 312-38 Braindumps Exam Pass at Your First Attempt | EC-COUNCIL 312-38 Discount Code Immediately open www.troytecdumps.com and search for [312-38] to obtain a free download Excellect 312-38 Pass Rate
- New 312-38 Braindumps Exam Pass at Your First Attempt | EC-COUNCIL 312-38 Discount Code The page for free

- download of 「 312-38 」 on www.pdfvce.com will open immediately 312-38 Exam Simulator Free
- 312-38 Exam Dumps Pdf [Study 312-38 Reference](#) [312-38 Valuable Feedback](#) Search for ➡ 312-38 and obtain a free download on www.exam4labs.com 312-38 Exam Dumps Pdf
 - 100% Pass Quiz 2026 EC-COUNCIL - New 312-38 Braindumps Search for ➡ 312-38 on 「 www.pdfvce.com 」 immediately to obtain a free download 312-38 Exam Dumps Pdf
 - Penetration Testing: 312-38 Pre-assessment Test Enter ▶ www.examdisscuss.com and search for ➡ 312-38 to download for free 312-38 Exam Simulator Free
 - Use EC-COUNCIL 312-38 Exam Dumps To Ace Exam Quickly Search for 312-38 and download exam materials for free through ▶ www.pdfvce.com 312-38 Valid Exam Discount
 - Penetration Testing: 312-38 Pre-assessment Test Easily obtain free download of 312-38 by searching on ▶ www.easy4engine.com Study 312-38 Reference
 - brianiwca308748.blogpayz.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, mysocialguides.com, mariamupfo662243.topbloghub.com, faygdur343042.homewikia.com, www.callcentersindia.co.in, freeurldirectory.com, 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, myportal.utt.edu.tt, Disposable vapes

DOWNLOAD the newest Pass4sures 312-38 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1FjgVLQxMoTD6AOtR8Dkiaif7jHa4VYri>