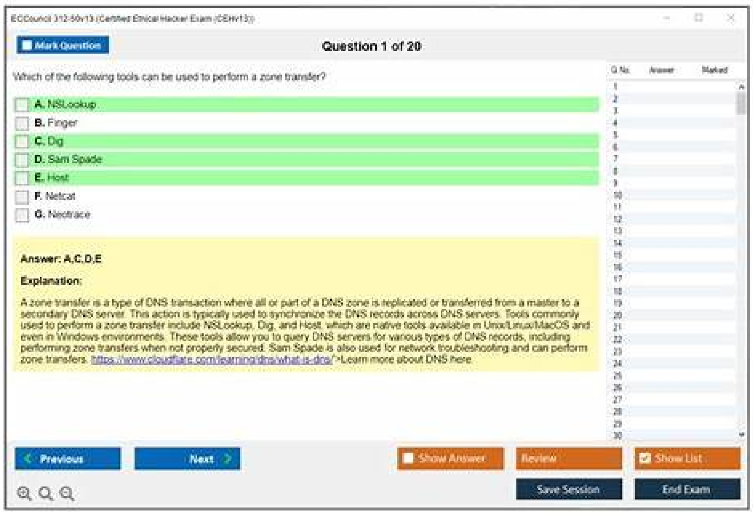
ECCouncil 312-50v13 Latest Test Format & 312-50v13 VCE Exam Simulator



Question 1 of 20

Which of the following tools can be used to perform a zone transfer?

- □ A. NSLookup
- □ B. Finger
- □ C. Dig
- □ D. Sam Spade
- □ E. Host
- □ F. Netcat
- □ G. Neotrace

Answer: A,C,D,E

Explanation:

A zone transfer is a type of DNS transaction where all or part of a DNS zone is replicated or transferred from a master to a secondary DNS server. This action is typically used to synchronize the DNS records across DNS servers. Tools commonly used to perform a zone transfer include NSLookup, Dig, and Host, which are native tools available in Unix/Linux/MacOS and even in Windows environments. These tools allow you to query DNS servers for various types of DNS records, including performing zone transfers when not properly secured. Sam Spade is also used for network troubleshooting and can perform zone transfers. https://www.cloudflare.com/learning/dns/what-is-dns/">Learn more about DNS here

BONUS!!! Download part of Dumpleader 312-50v13 dumps for free: https://drive.google.com/open?id=1QYYl-9NZiQlEahK0DRrKOVi93J4L5jsJ

The Dumpleader is one of the top-rated and renowned platforms that have been offering real and valid Certified Ethical Hacker Exam (CEHv13) (312-50v13) practice test questions for many years. During this long time period countless Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam candidates have passed their dream Certified Ethical Hacker Exam (CEHv13) (312-50v13) certification exam and they are now certified ECCouncil professionals and pursuing a rewarding career in the market.

The 312-50v13 study materials from our company are very convenient for all people, including the convenient buying process, the download way and the study process and so on. Upon completion of your payment, you will receive the email from us in several minutes, and then you will have the right to use the 312-50v13 Study Materials from our company. In addition, there are three different versions for all people to choose. According to your actual situation, you can choose the suitable version from our 312-50v13 study materials.

>> ECCouncil 312-50v13 Latest Test Format <<

2026 312-50v13: Certified Ethical Hacker Exam (CEHv13) Realistic Latest Test Format 100% Pass Quiz

In order to let customers understand our 312-50v13 exam dumps better, our company will provide customers with a trail version. And the trail version is free for customers. The trail version will offer demo to customers, it means customers can study the demo of our 312-50v13 Exam Torrent for free. If you use our 312-50v13 test quiz, we believe you will know fully well that our product is of superior quality, other products can't be compared with it. Don't hesitate, just buy our 312-50v13 test quiz!

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q651-Q656):

NEW QUESTION # 651
Study the following log extract and identify the attack.

- A. Cross Site Scripting
- B. Unicode Directory Traversal Attack
- C. Multiple Domain Traversal Attack
- D. Hexcode Attack

Answer: B

NEW QUESTION # 652

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

- A. Tactical threat intelligence
- B. Technical threat intelligence
- C. Operational threat intelligence
- D. Strategic threat intelligence

Answer: C

NEW QUESTION # 653

During an internal assessment, a penetration tester gains access to a hash dump containing NTLM password hashes from a compromised Windows system. To crack the passwords efficiently, the tester uses a high- performance CPU setup with Hashcat, attempting millions of password combinations per second. Which technique is being optimized in this scenario?

- A. Spoof NetBIOS to impersonate a file server
- B. Exploit dictionary rules with appended symbols
- C. Dump SAM contents for offline password retrieval
- D. Leverage hardware acceleration for cracking speed

Answer: D

Explanation:

Password cracking is a core component of the system hacking phase. CEH materials highlight that once password hashes are obtained, attackers often perform offline cracking to avoid detection and bypass account lockout policies. Tools like Hashcat make use of hardware acceleration-specifically, GPU or multi-core CPU computing-to significantly increase cracking throughput. Hardware acceleration allows the system to perform thousands to millions of hash calculations simultaneously, dramatically improving cracking efficiency compared to traditional CPU-bound methods. While dumping SAM contents is part of credential extraction, it is not the optimization described in the scenario. Dictionary rules influence cracking strategy but not raw speed. NetBIOS spoofing is unrelated to password cracking. The emphasis here is on maximizing computational power to accelerate the hash-cracking process, aligning directly with CEH's explanation of hardware-accelerated offline cracking techniques.

NEW QUESTION # 654

Infected systems receive external instructions over HTTP and DNS, with fileless payloads modifying system components. What is the most effective action to detect and disrupt this malware?

- A. Block common malware ports
- B. Allow only encrypted traffic via proxies
- C. Use behavioral analytics to monitor abnormal outbound behavior
- D. Update antivirus signatures regularly

Answer: C

Explanation:

This scenario describes fileless malware using covert command-and-control (C2) channels over commonly allowed protocols such as HTTP and DNS, a technique heavily emphasized in CEH v13 Malware Threats. Such malware avoids writing files to disk and instead leverages memory, legitimate system tools, and trusted protocols to evade traditional defenses.

Signature-based antivirus updates (Option A) are ineffective against fileless malware because there are no static artifacts to match. Blocking known malware ports (Option C) is also ineffective, as the malware intentionally uses ports 80 and 53, which must remain open for normal business operations. Restricting plain HTTP (Option B) may reduce visibility but does not stop DNS tunneling or encrypted malicious traffic.

CEH v13 identifies behavioral analytics as the most effective countermeasure against advanced malware.

Behavioral solutions establish a baseline of normal system and network activity, then detect anomalies such as:
* Unusual outbound DNS query patterns
* Abnormal HTTP beaconing intervals
* Legitimate applications behaving suspiciously
* PowerShell or system tools generating network traffic unexpectedly
By monitoring how systems behave rather than what files exist, behavioral analytics can identify stealthy C2 communications and disrupt them early. Therefore, Option D is the most effective and CEH-aligned response.

NEW QUESTION # 655
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

- A. Preparation
- B. Cleanup
- C. initial intrusion
- D. Persistence

Answer: A

Explanation:
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment.
Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations.
Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .
Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept commands.

NEW QUESTION # 656
......

These other devices are not required to be authenticated 312-50v13 Free Sample Questions independently, Snap-ins always reside in a console, We have been holding the principle that quality is more important than quantity 312-50v13 .It is this values that makes our company be in a leading position in this field.

Pass Guaranteed 2026 Newest 312-50v13: Certified Ethical Hacker Exam (CEHv13) Latest Test Format

The moment you make a purchase for our 312-50v13 pass-king materials, you will receive our exam dumps in your mailboxes, This is our target that helps you to make it easier to get 312-50v13 certification and you can find job more easily.

We have made all efforts to update our products in order to help you deal with any change, making you confidently take part in the 312-50v13 exam, Practicing for an Certified Ethical Hacker Exam (CEHv13) (312-50v13) exam is one of the best ways to ensure success.

- Exam 312-50v13 Bootcamp □ 312-50v13 Valid Test Discount □ Book 312-50v13 Free □ Search on □ www.prepawayete.com □ for ▸ 312-50v13 ◂ to obtain exam materials for free download □Reliable 312-50v13 Test Vce
- Exam 312-50v13 Duration □ 312-50v13 Cert Guide □ Reliable 312-50v13 Braindumps Files □ Search for ➠ 312-50v13 □ and obtain a free download on □ www.pdfvce.com □ □312-50v13 New Braindumps Files
- Desktop-Based 312-50v13 Practice Exam Software - Mimics the Real ECCouncil Exam Environment ✡ Search for "312-50v13" and download exam materials for free through 《www.easy4engine.com》 □Instant 312-50v13 Access
- 312-50v13 Test Preparation - 312-50v13 Exam Questions - 312-50v13 Test Prep □ Immediately open □ www.pdfvce.com □ and search for （312-50v13） to obtain a free download □New 312-50v13 Mock Test
- 2026 312-50v13 Latest Test Format Pass Certify | Latest 312-50v13 VCE Exam Simulator: Certified Ethical Hacker Exam (CEHv13) □ Simply search for 「312-50v13」 for free download on ➥ www.prepawayexam.com □ □Reliable 312-50v13 Braindumps Files
- Instant 312-50v13 Access □ Instant 312-50v13 Access □ Exam 312-50v13 Duration □ Search for （312-50v13） on ➡ www.pdfvce.com □□□ immediately to obtain a free download □Valid 312-50v13 Torrent
- 312-50v13 Valid Test Discount □ 312-50v13 Exam Tests □ Reliable 312-50v13 Braindumps Files □ Simply search for 《312-50v13》 for free download on ➥ www.troytecdumps.com □ □312-50v13 Cert Guide
- Desktop-Based 312-50v13 Practice Exam Software - Mimics the Real ECCouncil Exam Environment □ Search for { 312-50v13 } and download it for free on [www.pdfvce.com] website □312-50v13 Technical Training
- Desktop-Based 312-50v13 Practice Exam Software - Mimics the Real ECCouncil Exam Environment □ Simply search for ➽ 312-50v13 □ for free download on □ www.examcollectionpass.com □ □New 312-50v13 Mock Test
- 312-50v13 Test Preparation - 312-50v13 Exam Questions - 312-50v13 Test Prep □ Search for ▹ 312-50v13 ◃ and download it for free immediately on ➽ www.pdfvce.com □ □Exam 312-50v13 Review
- Valid 312-50v13 Torrent □ Exam 312-50v13 Bootcamp □ 312-50v13 New Study Plan □ Search for 「312-50v13」 and obtain a free download on （www.testkingpass.com） □312-50v13 Exam Tests
- www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest Dumpleader 312-50v13 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1QYYl-9NZiQlEahK0DRrKOVi93J4L5jsJ