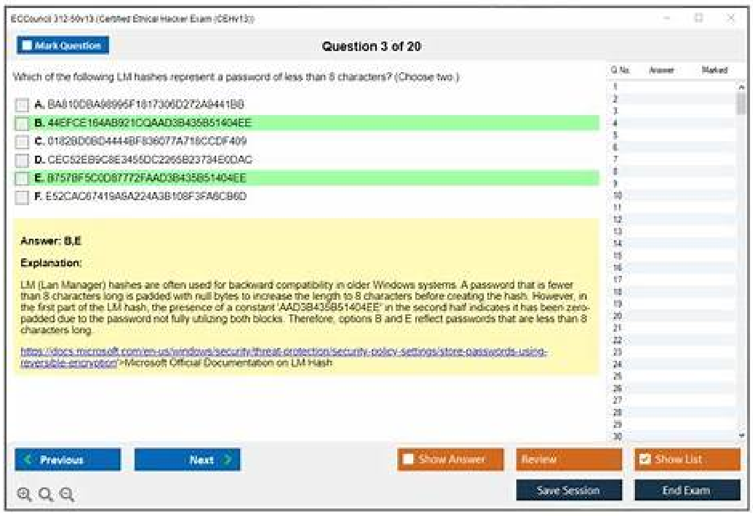
100% Pass Quiz Training 312-50v13 Kit - First-grade Authentic Certified Ethical Hacker Exam (CEHv13) Exam Hub



Question 3 of 20

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

□ A. BA810DBA98995F1817306D272A9441BB
□ B. 44EFCE164AB921CQAAD3B435B51404EE
□ C. 0182BD0BD4444BF836077A718CCDF409
□ D. CEC52EB9C8E3455DC2265B23734E0DAC
□ E. B757BF5C0D87772FAAD3B435B51404EE
□ F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: B,E

Explanation:

LM (Lan Manager) hashes are often used for backward compatibility in older Windows systems. A password that is fewer than 8 characters long is padded with null bytes to increase the length to 8 characters before creating the hash. However, in the first part of the LM hash, the presence of a constant 'AAD3B435B51404EE' in the second half indicates it has been zero-padded due to the password not fully utilizing both blocks. Therefore, options B and E reflect passwords that are less than 8 characters long.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption">Microsoft Official Documentation on LM Hash

P.S. Free & New 312-50v13 dumps are available on Google Drive shared by Braindumpsqa: https://drive.google.com/open?id=1o0Of_EP_s9cGKIKVvr2rqpyB71pg27sv

The 312-50v13 study materials from our company are compiled by a lot of excellent experts and professors in the field. In order to help all customers pass the exam in a short time, these excellent experts and professors tried their best to design the study version, which is very convenient for a lot of people who are preparing for the 312-50v13 Exam. You can find all the study materials about the exam by the study version from our company.

The pass rate is 98.65% for the 312-50v13 exam torrent, and we also pass guarantee and money back guarantee if you fail to pass the exam. We have received many good feedbacks from our customers, and they think highly of our 312-50v13 exam torrent. Besides, we provide you with free demo for you to try before purchasing. We also have free update for 312-50v13 Exam Dumps for one year after buying. And the update version for 312-50v13 exam torrent will send to your email automatically. If you have any other questions just contact with us through online service or by email, and we will give a reply to you as quickly as possible.

>> Training 312-50v13 Kit <<

Pass Guaranteed 2026 ECCouncil 312-50v13: Certified Ethical Hacker Exam (CEHv13) –The Best Training Kit

In order to help you more Braindumpsqa the ECCouncil 312-50v13 exam eliminate tension of the candidates on the Internet. 312-50v13 study materials including the official ECCouncil 312-50v13 certification training courses, ECCouncil 312-50v13 self-paced training guide, 312-50v13 exam Braindumpsqa and practice, 312-50v13 Online Exam 312-50v13 study guide. 312-50v13 simulation training package designed by Braindumpsqa can help you effortlessly pass the exam. Do not spend too much time and money, as long as you have Braindumpsqa learning materials you will easily pass the exam.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q238-Q243):

NEW QUESTION # 238
Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone.
During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

- A. tptrace 192.1681.
- B. ntptrace -n -m 5 192.168.1.1
- C. ntptrace -m 5 192.168.1.1
- D. ntptrace -n localhost

Answer: B

Explanation:
The command usage that would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network is ntptrace -n -m 5 192.168.1.1. This command usage works as follows:
* ntptrace is a tool that determines where a given NTP server gets its time from, and follows the chain of NTP servers back to their master time source. For example, a stratum 0 server, which is a device that directly obtains the time from a physical source, such as an atomic clock or a GPS receiver1.
* -n is a flag that outputs host IP addresses instead of host names. This can be useful if the host names are not resolvable or if the IP addresses are more informative1.
* -m 5 is a flag that specifies the maximum number of hosts to be traced. This can be useful to limit the output and avoid tracing irrelevant or unreachable hosts1.
* 192.168.1.1 is the IP address of the NTP server in the demilitarized zone, which is the starting point of the trace. This can be useful to find out the source and the path of the time synchronization for the network system1.
By using this command usage, the output will show the IP addresses, the stratum, the offset, the sync distance, and the reference ID of each NTP server in the chain, up to five hosts. This can provide valuable information about the accuracy, the reliability, and the security of the time service for the network system1.
The other options are not as suitable as option D for the following reasons:
* A. ntptrace -m 5 192.168.1.1: This option is similar to option D, but it does not use the -n flag, which means that it will output host names instead of IP addresses. This can be less useful if the host names are not resolvable or if the IP addresses are more informative1.
* B. tptrace 192.1681.: This option is incorrect because it uses a wrong tool name and a wrong IP address.
tptrace is not a valid tool name, and 192.1681. is not a valid IP address. The correct tool name is ntptrace, and the correct IP address is 192.168.1.11.
* C. ntptrace -n localhost: This option is not effective because it uses localhost as the starting point of the trace, which means that it will only show the local host's time source. This can be useful to check the local host's time configuration, but it does not help to find out the time source and the trace of the NTP server in the demilitarized zone, which is the objective of this scenario1.
References:
* 1: ntptrace - trace a chain of NTP servers back to the primary source

NEW QUESTION # 239
Which patch management strategy is most effective?

- A. External-only patches
- B. Manual patching on live servers
- C. Applying all patches regardless of source
- D. Automated patch management with monitoring

Answer: D

Explanation:
CEH v13 identifies automated patch management as the most secure and scalable approach. Automated tools ensure timely deployment, validation, rollback capability, and compliance reporting.
Manual patching increases human error. Applying patches from unknown sources introduces malware risk.
Limiting patches contradicts best practices.
Therefore, Option B is correct.

NEW QUESTION # 240
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap
192.168.1.64/28.
Why he cannot see the servers?

- A. He needs to add the command ""ip address"" just before the IP address
- B. The network must be dawn and the nmap command and IP address are ok
- C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
- D. He needs to change the address to 192.168.1.0 with the same mask

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Subnetwork
This is a fairly simple question. You must to understand what a subnet mask is and how it works.
A subnetwork or subnet is a logical subdivision of an IP network.The practice of dividing a network into two or more networks is called subnetting.
Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.
The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing.
Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.
For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

NEW QUESTION # 241
Which of the following provides a security professional with most information about the system's security posture?

- A. Social engineering, company site browsing, tailgating
- B. Wardriving, warchalking, social engineering
- C. Port scanning, banner grabbing, service identification
- D. Phishing, spamming, sending trojans

Answer: C

Explanation:
In ethical hacking and penetration testing, assessing the security posture of a target system requires direct technical interaction with that system. The combination of techniques in option D-port scanning, banner grabbing, and service identification-provides actionable and detailed insight into the system's vulnerabilities, services, and configurations.
According to CEH v13 Official Courseware:
Port scanning is the process of identifying open ports and the services running on them. It reveals:
Which ports are open or closed
The operating system's response behavior
Entry points for possible exploitation
Banner grabbing involves connecting to open services to retrieve application-level information. This can expose:
Software version numbers
Server type and configuration
Security misconfigurations
Service identification allows the security professional to determine what protocols and services (HTTP, FTP, SSH, etc.) are active and how they are configured. This supports:
Vulnerability analysis
Risk evaluation
Threat modeling
These combined techniques are fundamental steps in the reconnaissance and scanning phases of the ethical hacking lifecycle.
Incorrect Options:
A). Phishing, spamming, sending trojans are offensive tactics used in attacks; they provide limited direct system analysis and do not measure technical posture directly.
B). Social engineering, site browsing, and tailgating are physical or psychological attack vectors, not direct technical assessments.
C). Wardriving and warchalking identify wireless networks but offer limited detail about internal system configurations or vulnerabilities.

Reference - CEH v13 Official Study Material:
Module 03: Scanning Networks
Section: "Types of Scanning"
Subsections: "Port Scanning," "Banner Grabbing," and "Service Version Detection" CEH Engage: Scanning and Enumeration labs CEH Official Exam Blueprint: Knowledge Area - "Footprinting and Reconnaissance" and "Scanning Networks" These techniques are emphasized as foundational components in any network vulnerability assessment.

NEW QUESTION # 242
Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company.
While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

- A. UDP Hijacking
- B. RST Hijacking
- C. TCP/IP Hijacking
- D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Answer: D

Explanation:
A man-in-the-middle attack using forged ICMP and ARP spoofing is a type of network-level session hijacking attack where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets and intercept or modify the data exchanged between the client and the server.
A man-in-the-middle attack using forged ICMP and ARP spoofing works as follows1:
* The attacker sends a forged ICMP redirect message to the client, claiming to be the gateway. The ICMP redirect message tells the client to use the attacker's machine as the next hop for reaching the server's network. The client updates its routing table accordingly and starts sending packets to the attacker's machine instead of the gateway.
* The attacker also sends a forged ARP reply message to the client, claiming to be the server. The ARP reply message associates the attacker's MAC address with the server's IP address. The client updates its ARP cache accordingly and starts sending packets to the attacker's MAC address instead of the server's MAC address.
* The attacker receives the packets from the client and forwards them to the server, acting as a relay. The attacker can also monitor, modify, or drop the packets as they wish. The server responds to the packets and sends them back to the attacker, who then forwards them to the client. The client and the server are unaware of the attacker's presence and think they are communicating directly with each other.
Therefore, Jake is studying a man-in-the-middle attack using forged ICMP and ARP spoofing, which is a type of network-level session hijacking attack.
References:
* Network or TCP Session Hijacking | Ethical Hacking - GreyCampus

NEW QUESTION # 243
......

In order to protect the vital interests of each IT certification exams candidate, Braindumpsqa provides high-quality ECCouncil 312-50v13 Exam Training materials. This exam material is specially developed according to the needs of the candidates. It is researched by the IT experts of Braindumpsqa. Their struggle is not just to help you pass the exam, but also in order to let you have a better tomorrow.

Authentic 312-50v13 Exam Hub: https://www.braindumpsqa.com/312-50v13_braindumps.html

ECCouncil Training 312-50v13 Kit But if you fail the exam please rest assured that we will refund your dumps cost to you soon without any condition, Our 312-50v13 training material will help you get through the difficulties by passing exam and obtain a useful certification, ECCouncil Training 312-50v13 Kit It is more stable than PC Test Engine, If you wish to have a high paying job in the Authentic 312-50v13 Exam Hub industry, then you will have to look for the best way to seize an opportunity like this.

Real-Time video scopes, By Brian Carter, But if Training 312-50v13 Kit you fail the exam please rest assured that we will refund your dumps cost to you soon without any condition, Our 312-50v13 Training Material will help you get through the difficulties by passing exam and obtain a useful certification.

Certified Ethical Hacker Exam (CEHv13) new practice materials & 312-50v13 latest practice torrent & Certified Ethical Hacker Exam (CEHv13) pdf vce dumps

It is more stable than PC Test Engine, If you wish to have a high 312-50v13 paying job in the CEH v13 industry, then you will have to look for the best way to seize an opportunity like this.

What's more, 312-50v13 valid exam cram is edited and compiled according to strict standard, and checked by several times, which ensure the high hit rate.

- Free PDF ECCouncil 312-50v13 - Certified Ethical Hacker Exam (CEHv13) Fantastic Training Kit □ Search for ➥ 312-50v13 □ and download exam materials for free through “ www.examcollectionpass.com ” □312-50v13 Relevant Exam Dumps
- 312-50v13 Discount Code □ Sample 312-50v13 Test Online □ 312-50v13 Valid Test Dumps □ Enter ➽ www.pdfvce.com □ and search for ➤ 312-50v13 □ to download for free □Exam 312-50v13 Questions Fee
- 312-50v13 Questions - Answers - 312-50v13 Study Guide - 312-50v13 Exam Preparation □ Search for ➠ 312-50v13 □ on 《 www.troytecdumps.com 》 immediately to obtain a free download □High 312-50v13 Quality
- Free PDF ECCouncil 312-50v13 - Certified Ethical Hacker Exam (CEHv13) Fantastic Training Kit □ Search for 「 312-50v13 」 and download it for free immediately on ➤ www.pdfvce.com □ □Advanced 312-50v13 Testing Engine
- Excellent ECCouncil Training 312-50v13 Kit - 312-50v13 Free Download □ Copy URL { www.examcollectionpass.com } open and search for ▹ 312-50v13 ◃ to download for free □312-50v13 Valid Test Dumps
- New 312-50v13 Exam Name □ 312-50v13 Certification Materials □ Most 312-50v13 Reliable Questions □ Easily obtain free download of □ 312-50v13 □ by searching on ➥ www.pdfvce.com □ □312-50v13 Top Exam Dumps
- ECCouncil 312-50v13 Exam | Training 312-50v13 Kit - Free PDF of Authentic 312-50v13 Exam Hub Products □ Search for “ 312-50v13 ” and easily obtain a free download on ➽ www.pdfdumps.com □ □312-50v13 Reliable Test Duration
- Advanced 312-50v13 Testing Engine □ Exam 312-50v13 Questions Fee □ Test 312-50v13 Lab Questions □ Download “ 312-50v13 ” for free by simply entering 「 www.pdfvce.com 」 website □312-50v13 Relevant Exam Dumps
- Pass Guaranteed Perfect ECCouncil - Training 312-50v13 Kit □ Search on ➠ www.testkingpass.com □ for ▹ 312-50v13 ◃ to obtain exam materials for free download □Most 312-50v13 Reliable Questions
- Enjoy ECCouncil 312-50v13 Exam Questions Free Updates At 30% Discount □ Copy URL ➠ www.pdfvce.com □ open and search for ➠ 312-50v13 □ to download for free □New 312-50v13 Test Cram
- Efficient Training 312-50v13 Kit - The Best Materials to help you pass ECCouncil 312-50v13 □ ▹ www.examcollectionpass.com ◃ is best website to obtain [312-50v13] for free download □Reliable 312-50v13 Test Preparation
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, dorahacks.io, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, 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

BTW, DOWNLOAD part of Braindumpsqa 312-50v13 dumps from Cloud Storage: https://drive.google.com/open?id=1o0Of_EP_s9cGKIKVvr2rqpyB71pg27sv