# [2017 New Lead2pass 2017 100% Real 312-49v9 Exam Questions

2017 July EC-Council Official New Released 312-49v9 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
We are all well aware that a major problem in the IT industry is that there is a lack of quality study materials. Our exam preparation material provides you everything you will need to take a certification examination. Our EC-Council 312-49v9 Exam will provide you with exam questions with verified answers that reflect the actual exam. These questions and answers provide you with the experience of taking the actual test. High quality and value for the 312-49v9 Exam. 100% guarantee to pass your EC-Council 312-49v9 exam and get your EC-Council certification. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-49v9.html QUESTION 1You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers: http://172.168.4.131/level/99/exec/show/config After typing in this URL, you are presented with the entire configuration file for that router.What have you discovered? A. URL Obfuscation Arbitrary Administrative Access VulnerabilityB. HTML Configuration Arbitrary Administrative Access VulnerabilityC. Cisco IOS Arbitrary Administrative Access Online VulnerabilityD. HTTP Configuration Arbitrary Administrative Access Vulnerability Answer: Answer: D QUESTION 2Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network? A. Block access to TCP port 171B. Change the default community string namesC. Block all internal MAC address from using SNMPD. Block access to UDP port 171 Answer: B QUESTION 3When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers? A. Time-Sync ProtocolB. SyncTime ServiceC. Network Time ProtocolD. Universal Time Set Answer: C QUESTION 4When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel? A. Avoid over-saturation of wireless signalsB. So that the access points will work on different requenciesC. Avoid cross talkD. Multiple access points can be set up on the same channel without any issues Answer: C QUESTION 5You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour.Why were these passwords cracked so Quickly? A. Passwords of 14 characters or less are broken up into two 7-character hashesB. A password Group Policy change takes at least 3 weeks to completely replicate throughout a networkC. Networks using Active Directory never use SAM databases so the SAM database pulled was emptyD. The passwords that were cracked are local accounts on the Domain Controller Answer: A QUESTION 6Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports? A. FilteredB. ClosedC. OpenD. Stealth Answer: C QUESTION 7What is the target host IP in the following command? C:> firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP A. 10.10.150.1B. This command is using FIN packets, which cannot scan target hostsC. Firewalk does not scan target hostsD. 172.16.28.95 Answer: D QUESTION 8Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet? A. Poison the switch's MAC address table by flooding it with ACK bitsB. Crash the switch with aDoS attack since switches cannot send ACK bitsC. Enable tunneling feature on the switchD. Trick the switch into thinking it already has a session with Terri's computer Answer: Answer: D QUESTION 9When is it appropriate to use computer forensics? A. If copyright and intellectual property theft/misuse has occurred B. If employees do not care for their boss?management techniquesC. If sales drop off for no apparent reason for an extended period of timeD. If a financial institution is burglarized by robbers Answer: A QUESTION 480You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the

company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different.What area of the law is the employee violating? A. Copyright lawB. Brandmark lawC. Trademark lawD. Printright law Answer: C QUESTION 11What feature of Windows is the following command trying to utilize? A. White spaceB. AFSC. ADSD. Slack file Answer: C QUESTION 12You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as other members of your team collect it. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case? A. All forms should be placed in an approved secure container because they are now primary evidence in the caseB. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should beplaced in the report fileC. All forms should be placed in the report file because they are now primary evidence in the caseD. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container Answer: D QUESTION 13When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to _____ A. Automate collection from image filesB. Avoiding copying data from the boot partitionC. Acquire data from the host-protected area on a diskD. Prevent contamination to the evidence drive Answer: D QUESTION 14Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, reQuested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use? A. Social ValidationB. Friendship/LikingC. ReciprocationD. Scarcity Answer: C QUESTION 15You are working as a computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact local law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject computer. You inform the officer that you will not be able to comply with thatnetwork sniffer on your network and monitor all traffic to the subject? computer. You inform the officer that you will not be able to comply with that request because doing so would: A. Violate your contractB. Cause network congestionC. Make you an agent of law enforcementD. Write information to the subject hard drive Write information to the subject hard drive Answer: C QUESTION 16What is kept in the following directory? HKLMSECURITYPolicySecrets A. IAS account names and passwordsB. Service account passwords in plain textC. Local store PKI Kerberos certificatesD. Cached password hashes for the past 20 users Answer: B The EC-Council 312-49v9 questions and answers in PDF on Lead2pass are the most reliable study guide for 312-49v9 exam. Comparing with others', our 312-49v9 dump is more authoritative and complete. We provide the latest full version of 312-49v9 PDF and VCE dumps with new real questions and answers to ensure your 312-49v9 exam 100% pass. EC-Council 312-49v9 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDUDdCdEVMbkJER1U 2017 **EC-Council 312-49v9** exam dumps (All 505 Q&As) from Lead2pass: https://www.lead2pass.com/312-49v9.html [100% Exam Pass Guaranteed]