[2017 Newest 312-50v9 Exam Questions Free Download From Lead2pass (281-300)

Lead2pass 2017 September New EC-Council 312-50v9 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! How to 100% pass 312-50v9 exam? Lead2pass 312-50v9 dump is unparalleled in quality and is 100% guaranteed to make you pass 312-50v9 exam. All the 312-50v9 exam questions are the latest. Here are some free share of EC-Council 312-50v9 dumps. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 281In order to have an anonymous Internet surf, which of the following is best choice? A. Use SSL sites when entering personal informationB. Use Tor network with multi-nodeC. Use shared WiFiD. Use public VPNAnswer: B QUESTION 282A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below: - Access List should be written between VLANs.- Port security should be enabled for the intranet.- A security solution which filters data packets should be set between intranet (LAN) and DMZ.- A WAF should be used in front of the web applications. According to the section from the report, which of the following choice is true? A. MAC Spoof attacks cannot be performed.B. Possibility of SQL Injection attack is eliminated.C. A stateful firewall can be used between intranet (LAN) and DMZ.D. There is access control policy between VLANs. Answer: CExplanation: QUESTION 283Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol? A. Based on XMLB. Provides a structured model for messagingC. Exchanges data between web servicesD. Only compatible with the application protocol HTTP Answer: DExplanation: QUESTION 284An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next? A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.B. He will activate OSPF on the spoofed root bridge.C. He will repeat the same attack against all L2 switches of the network.D. He will repeat this action so that it escalates to a DoS attack. Answer: A QUESTION 285A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup? A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.B. As long as the physical access to the network elements is restricted, there is no need for additional measures.C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.D. The operator knows that attacks and down time are inevitable and should have a backup site. Answer: A QUESTION 286When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing? A. The amount of time it takes to convert biometric data into a template on a smart card.B. The amount of time and resources that are necessary to maintain a biometric system.C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.D. How long it takes to setup individual user accounts. Answer: C QUESTION 287Due to a slow down of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure? A. All of the employees would stop normal work activitiesB. IT department would be telling employees who the boss isC. Not informing the employees that they are going to be monitored could be an invasion of privacy.D. The network could still experience traffic slow down. Answer: C QUESTION 288In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails? A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.C. A blacklist of companies that have their mail server relays configured to be wide open.D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally. Answer: B QUESTION 289You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes. route add 10.0.0.0 mask 255.0.0.0 10.0.0.1route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes? A. Both static routes indicate that the traffic is external with different gateway.B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.C. Both static routes indicate that the traffic is internal with different gateway.D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway. Answer: DExplanation: QUESTION 290What is the correct process for the TCP three-way handshake connection

establishment and connection termination? A. Connection Establishment: FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACKB. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: ACK, ACK-SYN, SYNC. Connection Establishment: ACK, ACK-SYN, SYNConnection Termination: FIN, ACK-FIN, ACKD. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: FIN, ACK-FIN, ACK Answer: D QUESTION 291Emil uses nmap to scan two hosts using this command. nmap -sS -T4 -O 192.168.99.1 192.168.99.7 He receives this output: Nmap scan report for 192.168.99.1 Host is up (0.00082s latency).Not shown: 994 filtered portsPORT STATE SERVICE21/tcp open ftp23/tcp open telnet53/tcp open domain80/tcp open http161/tcp closed snmpMAC Address: B0:75:D5:33:57:74 (ZTE)Device type: general purposeRunning: Linux 2.6.XOS CPE: cpe:/o:linux:linux_kernel:2.6OS details: Linux 2.6.9 - 2.6.33Network Distance: 1 hop Nmap scan report for 192.168.99.7Host is up (0.000047s latency).All 1000 scanned ports on 192.168.99.7 are closedToo many fingerprints match this host to give specific OS details Network Distance: 0 hops What is his conclusion? A. Host 192.168.99.7 is an iPad.B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.C. Host 192.168.99.1 is the host that he launched the scan from.D. Host 192.168.99.7 is down. Answer: BExplanation: QUESTION 292You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out? A. Scan servers with NmapB. Physically go to each serverC. Scan servers with MBSAD. Telent to every port on each server Answer: A QUESTION 293Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.What just happened? A. PhishingB. WhalingC. TailgatingD. Masquerading Answer: CExplanation: QUESTION 294Which protocol is used for setting up secured channels between two devices, typically in VPNs? A. IPSECB. PEMC. SETD. PPP Answer: A QUESTION 295In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case. Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'? A. NT:LMB. LM:NTC. LM:NTLMD. NTLM:LM Answer: BExplanation: QUESTION 296Which of the following Nmap commands will produce the following output? Output:Starting Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT Nmap scan report for 192.168.1.1Host is up (0.00042s latency).Not shown: 65530 open|filtered ports, 65529 filtered ports PORT STATE SERVICE111/tcp open rpcbind999/tcp open garcon1017/tcp open unknown1021/tcp open exp11023/tcp open netvenuechat2049/tcp open nfs17501/tcp open unknown111/udp open rpcbind123/udp open ntp137/udp open netbios-ns2049/udp open nfs5353/udp open zeroconf17501/udp open|filtered unknown51857/udp open|filtered unknown54358/udp open|filtered unknown56228/udp open|filtered unknown57598/udp open|filtered unknown59488/udp open|filtered unknown60027/udp open|filtered unknown A. nmap -sN -Ps -T4 192.168.1.1B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1C. nmap -sS -Pn 192.168.1.1D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1 Answer: DExplanation: QUESTION 297Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems? A. msfpayloadB. msfcliC. msfencodeD. msfd Answer: C QUESTION 298You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax? A. hping2 host.domain.comB. hping2 --set-ICMP host.domain.comC. hping2 -i host.domain.comD. hping2 -1 host.domain.com Answer: D QUESTION 299Which of the following is a passive wireless packet analyzer that works on Linux-based systems? A. Burp SuiteB. OpenVASC. tsharkD. Kismet Answer: D QUESTION 300The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation? A. RSTB. ACKC. SYN-ACKD. SYN Answer: D More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms Always up-to-date Lead2pass 312-50v9 VCE - everything you need for your EC-Council 312-50v9 exam to pass. Our EC-Council 312-50v9 software allows you to practise exam dumps in real 312-50v9 exam environment. Welcome to choose. 2017 EC-Council 312-50v9 (All 589 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/312-50v9.html [100% Exam Pass Guaranteed]