[Lead2pass New Free Lead2pass EC-Council 312-50v9 PDF Dumps With New Update Exam Questions (301-320)

Lead2pass 2017 November New EC-Council <u>312-50v9 Exam Dumps!</u> <u>100% Free Download!</u> <u>100% Pass Guaranteed!</u> Are you struggling for the 312-50v9 exam? Good news, Lead2pass EC-Council technical experts have collected all the questions and answers which are updated to cover the knowledge points and enhance candidates' abilities. We offer the latest 312-50v9 PDF and VCE dumps with new version VCE player for free download, and the new 312-50v9 dump ensures your 312-50v9 exam 100% pass. Following questions and answers are all new published by EC-Council Official Exam Center: https://www.lead2pass.com/312-50v9.html QUESTION 301Internet Protocol Security IPSec is actually a suite of protocols. Each

protocol within the suite provides different functionality. Collective IPSec does everything except. A. Protect the payload and the headersB. AuthenticateC. EncryptD. Work at the Data Link LayerAnswer: D QUESTION 302Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system? A. A biometric system that bases authentication decisions on behavioral attributes.B. A biometric system that bases authentication decisions system that creates one-time passwords that are encrypted with secret keys.D.

An authentication system that uses passphrases that are converted into virtual passwords. Answer: C QUESTION 303An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack? A. Only using OSPFv3 will mitigate this risk.B. Make sure that legitimate network routers are configured to run routing protocols with authentication.C. Redirection of the traffic cannot happen unless the admin allows it explicitly.D. Disable all routing protocols and only use static routes. Answer: B QUESTION 304Look at the following output. What did the hacker accomplish?; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105;; global options: +cmddomain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400 3600 domain.com. 600 IN A 192.168.1.102domain.com. 600 IN A 192.168.1.105domain.com. 3600 IN NS srv1.domain.com.domain.com. 3600 IN NS srv2.domain.com.vpn.domain.com. 3600 IN A 192.168.1.1server.domain.com. 3600 IN A 192.168.1.30ffice.domain.com. 3600 IN A 192.168.1.4remote.domain.com. 3600 IN A 192.168. 1.48support.domain.com. 3600 IN A 192.168.1.47ns1.domain.com. 3600 IN A 192.168.1.41ns2.domain.com. 3600 IN A 192.168.1.42ns3.domain.com. 3600 IN A 192.168.1.34ns4.domain.com. 3600 IN A 192.168.1.45srv1.domain.com. 3600 IN A 192.168.1.102srv2.domain.com. 1200 IN A 192.168.1.105domain.com. 3600 INSOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400 3600 ;; Ouery time: 269 msec;; SERVER: 192.168.1.105#53(192.168.1.105);; WHEN: Sun Aug 11 20:07:59 2013;; XFR size: 65 records (messages 65, bytes 4501) A. The hacker used whois to gather publicly available records for the domain.B. The hacker used the "fierce" tool to brute force the list of available domains.C. The hacker listed DNS records on his own domain.D. The hacker successfully transfered the zone and enumerated the hosts. Answer: DExplanation: QUESTION 305What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities? A. Security through obscurityB. Host-Based Intrusion Detection SystemC. Defense in depthD. Network-Based Intrusion Detection System Answer: C QUESTION 306Scenario: 1. Victim opens the attacker's web site.2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'.3. Victim clicks to the interesting and attractive content url.4. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make \$1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario? A. HTTP Parameter PollutionB. HTML InjectionC.

Session FixationD. ClickJacking Attack Answer: DExplanation: QUESTION 307If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used? A. Spoof ScanB. TCP Connect scanC. TCP SYND. Idle Scan Answer: C QUESTION 308What is correct about digital signatures? A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.B. Digital signatures may be used in different documents of the same type.C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.D. Digital signatures are issued once for each user and can be used everywhere until they expire. Answer: A QUESTION 309What is not a PCI compliance recommendation? A. Limit access to card holder data to as few individuals as possible.B. Use encryption to protect all transmission of card holder data over any public network.C. Rotate employees handling credit card transactions on a yearly basis to different departments.D. Use a firewall between the public network and the payment card data. Answer: B QUESTION 310Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive

network segments? A. Network-based intrusion detection system (NIDS)B. Host-based intrusion detection system (HIDS)C. FirewallsD. Honeypots Answer: A QUESTION 311An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps? A. The sequence does not matter. Both steps have to be performed against all hosts.B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.C. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.D. The port scan alone is adequate. This way he saves time. Answer: CExplanation: OUESTION 312What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script? A. User Access Control (UAC)B. Data Execution Prevention (DEP)C. Address Space Layout Randomization (ASLR)D. Windows firewall Answer: B QUESTION 313Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms? A. ScalabilityB. SpeedC. Key distributionD. Security Answer: B QUESTION 314By using a smart card and pin, you are using a two-factor authentication that satisfies A. Something you know and something you areB. Something you have and something you knowC. Something you have and something you areD. Something you are and something you remember Answer: B QUESTION 315What is the difference between the AES and RSA algorithms? A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.C. Both are symmetric algorithms, but AES uses 256-bit keys.D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data. Answer: B QUESTION 316Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism? Code:#include <string.h>int main(){char buffer[8];strcpy(buffer, ""11111111111111111111111111111"");} Output:Segmentation fault A. C#B. PythonC. JavaD. C++ Answer: A QUESTION 317The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network? access-list 102 deny tcp any anyaccess-list 104 permit udp host 10.0.0.3 anyaccess-list 110 permit tcp host 10.0.0.2 eq www anyaccess-list 108 permit tcp any eq ftp any A. The ACL 110 needs to be changed to port 80B. The ACL for FTP must be before the ACL 110C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the routerD. The ACL 104 needs to be first because is UDP Answer: CExplanation: OUESTION 318Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"". Which statement below is true? A. This is probably a legitimate message as it comes from a respectable organization.B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.D. This is a scam because Bob does not know Scott. Answer: C QUESTION 319In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this? A. Port ScanningB. Hacking Active DirectoryC. Privilege EscalationD. Shoulder-Surfing Answer: C QUESTION 320Which of the following will perform an Xmas scan using NMAP? A. nmap -sA 192.168.1.254B. nmap -sP 192.168.1.254C. nmap -sX 192.168.1.254D. nmap -sV 192.168.1.254 Answer: C More free Lead2pass 312-50v9 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDTVZJRHRvblhycms We ensure our new version 312-50v9 PDF and VCE dumps are 100% valid for passing exam, because Lead2pass is the top IT certification study training materials vendor. Many candidates have passed exam with the help of Lead2pass's VCE or PDF dumps. Lead2pass will update the study materials timely to make them be consistent with the current exam. Download the free demo on Lead2pass, you can pass the exam easily. 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]