[25/Jan/2019 Updated Valid 133q PT0-001 Practice Test with Free PDF Study Guide Download

New Updated PT0-001 Exam Questions from PassLeader PT0-001 PDF dumps! Welcome to download the newest PassLeader PT0-001 VCE dumps: https://www.passleader.com/pt0-001.html (133 Q&As) Keywords: PT0-001 exam dumps, PT0-001 exam questions, PT0-001 VCE dumps, PT0-001 PDF dumps, PT0-001 practice tests, PT0-001 study guide, PT0-001 braindumps, CompTIA PenTest+ Certification Exam P.S. Free PT0-001 dumps download from Google Drive: https://drive.google.com/open?id=1Xvl7jQbsLhLfR0jZSB8jZLBFffBsoW1g NEW QUESTION 101A company contracted a firm specializing in penetration testing to assess the security of a core business application. The company provided the firm with a copy of the Java bytecode. Which of the following steps must the firm take before it can run a static code analyzer? A. Run the application through a dynamic code analyzer.B. Employ a fuzzing utility.C. Decompile the application.D. Check memory allocations. Answer: D NEW QUESTION 102A financial institution is asking a penetration tester to determine if collusion capabilities to produce wire fraud are present. Which of the following threat actors should the penetration tester portray during the assessment? A. Insider threatB. Nation stateC. Script kiddieD. Cybercrime organization Answer: D NEW QUESTION 103 Which of the following has a direct and significant impact on the budget of the security assessment? A. ScopingB. SchedulingC. Compliance requirementD. Target risk Answer: A NEW QUESTION 104After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable. The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation? A. SOWB. NDAC. EULAD. BRA Answer: D NEW QUESTION 105During an internal network penetration test, a tester recovers the NTLM password hash tor a user known to have full administrator privileges on a number of target systems efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts? A. Operating system Windows 7Open ports: 23, 161B. Operating system Windows Server 2016Open ports: 53, 5900C. Operating system Windows 8 1Open ports: 445, 3389D. Operating system Windows 8Open ports: 514, 3389 Answer: C NEW QUESTION 106A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor? A. Advanced persistent threatB. Script kiddieC. HacktivistD. Organized crime Answer: A NEW QUESTION 107Which of the following types of physical security attacks does ...? A. Lock pickingB. ImpersonationC. Shoulder surfingD. Tailgating Answer: D NEW QUESTION 108Which of the following reasons does penetration tester needs to have a customer's point-of-contact information available at all time? (Choose three.) A. To report indicators of compromiseB. To report findings that cannot be exploitedC. To report critical findingsD. To report the latest published exploitsE. To update payment informationF. To report a server that becomes unresponsiveG. To update the statement of workH. To report a cracked password Answer: ACF NEW QUESTION 109While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective? A. Letter of engagement and attestation of findingsB. NDA and MSAC. SOW and final reportD. Risk summary and executive summary Answer: D NEW QUESTION 110An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email to obtain the CEO's login credentials. Which of the following types of attacks is this an example of? A. Elicitation attackB. Impersonation attackC. Spear phishing attackD. Drive-by download attack Answer: C NEW QUESTION 111During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests? A. EttercapB. TcpdumpC. ResponderD. Medusa Answer: C NEW QUESTION 112In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following as a potential NEXT step to extract credentials from the device? A. Brute force the user's password.B. Perform an ARP spoofing attack.C. Leverage the BeEF framework to capture credentials.D. Conduct LLMNR/NETBIOS-ns poisoning. Answer: D NEW QUESTION 113A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profiles. For which of the following types of attack would this information be used? A. Exploit chainingB. Session hijackingC. DictionaryD. Karma Answer: C NEW QUESTION 114A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability? A. RID cycling to enumerate users and groups.B. Pass the hash to relay credentials.C. Password brute forcing to log into the host.D. Session hijacking to impersonate a system account. Answer: C NEW QUESTION 115Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe is looking for a method that will enable him to enter the building during business hours or when there are no employee on-site. Which of the following would be MOST effective in accomplishing this? A. Badge cloningB. Lock pickingC.

TailgatingD. Piggybacking Answer: A NEW QUESTION 116A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of following BEST describes the types of adversaries this would identify? A. Script kiddiesB. APT actorsC. Insider threatsD. Hacktrvist groups Answer: B NEW QUESTION 117 Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple butter overflow? A. Stack pointer registerB. Index pointer registerC. Stack base pointerD. Destination index register Answer: D NEW QUESTION 118After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms? A. Expand the password length from seven to 14 charactersB. Implement password history restrictionsC. Configure password filtersD. Disable the accounts after five incorrect attemptsE. Decrease the password expiration window Answer: A NEW QUESTION 119A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these? A. Attempt to crack the service account passwords.B. Attempt DLL hijacking attacks.C. Attempt to locate weak file and folder permissions.D. Attempt privilege escalation attacks. Answer: D NEW QUESTION 120A penetration tester is preparing to conduct API testing. Which of the following would be MOST helpful in preparing for this engagement? A. NiktoB. WARC. W3AFD. Swagger Answer: D NEW QUESTION 121Drag and Drop..... Download the newest PassLeader PT0-001 dumps from passleader.com now! 100% Pass Guarantee! PT0-001 PDF dumps & PT0-001 VCE dumps: https://www.passleader.com/pt0-001.html (133 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. Free PT0-001 Exam Dumps Collection On Google Drive: https://drive.google.com/open?id=1Xvl7jQbsLhLfR0jZSB8jZLBFffBsoW1g