[4/Sep/2018 Updated PassLeader Offer 75q PT0-001 PDF and VCE Dumps With New Update Questions

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 (75 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 1 A software development team recently migrated to new application software on the on-premises environment. Penetration test findings show that multiple vulnerabilities exist. If a penetration tester does not have access to a live or test environment, a test might be better to create the same environment on the VM. Which of the following is MOST important for confirmation? A.   Unsecure service and protocol configuration. B.   Running SMB and SMTP service. C.   Weak password complexity and user account. D.   Misconfiguration. Answer: A NEW QUESTION 2 While prioritizing findings and recommendations for an executive summary, which of the following considerations would be MOST valuable to the client? A.   Levels of difficulty to exploit identified vulnerabilities. B.   Time taken to accomplish each step. C.   Risk tolerance of the organization. D.   Availability of patches and remediations. Answer: C NEW QUESTION 3 A penetration tester successfully exploits a DM2 server that appears to be listening on an outbound port. The penetration tester wishes to forward that traffic back to a device. Which of the following are the BEST tools to use few this purpose? (Choose two.) A.   Tcpdump B.   Nmap C.   Wiresrtark D.   SSH E.   Netcat F.   Cain and Abel Answer: CD NEW QUESTION 4 When performing compliance-based assessments, which of the following is the MOST important key consideration? A.   Additional rate B.   Company policy C.   Impact tolerance D.   Industry type Answer: A NEW QUESTION 5 A security consultant found a SCADA device in one of the VLANs in scope. Which of the following actions would be the BEST to create a potentially destructive outcome against device? A.   Launch an SNMP password brute force attack against the device. B.   Launch a Nessus vulnerability scan against the device. C.   Launch a DNS cache poisoning attack against the device. D.   Launch an SMB exploit against the device. Answer: A NEW QUESTION 6 A 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 7 After 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.   SOW B.   NDA C.   EULA D.   BRA Answer: D NEW QUESTION 8 An 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 attack B.   Impersonation attack C.   Spear phishing attack D.   Drive-by download attack Answer: B NEW QUESTION 9 A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify compliance with the baseline? A.   Discovery scan B.   Stealth scan C.   Full scan D.   Credentialed scan Answer: A NEW QUESTION 10 Which of the following CPU register does the penetration tester need to overwrite in order to exploit a simple butter overflow? A.   Stack pointer register B.   Index pointer register C.   Stack base pointer D.   Destination index register Answer: D NEW QUESTION 11 A 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 12 A 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 13 ..... 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 (75 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