[24/Nov/2018 Updated New PT0-001 Study Guide With Updated Exam Questions From PassLeader

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 (95 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 76A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information? A. MAC address of the client.B. MAC address of the domain controller.C. MAC address of the web server.D. MAC address of the gateway. Answer: D NEW QUESTION 77A penetration tester observes that several high numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend? A. Transition the application to another port.B. Filter port 443 to specific IP addresses.C. Implement a web application firewall.D. Disable unneeded services. Answer: A NEW QUESTION 78A 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 79A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability? A. Randomize the credentials used to log in.B. Install host-based intrusion detection.C. Implement input normalization.D. Perform system hardening. Answer: D NEW QUESTION 80Which of the following properties of the penetration testing engagement agreement will have the largest impact on observing and testing production systems at their highest loads? A. Creating a scope of the critical production systems.B. Setting a schedule of testing access times.C. Establishing a white-box testing engagement.D. Having management sign-off on intrusive testing. Answer: B NEW QUESTION 81A company requested a penetration tester review the security of an in-house-developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Choose two.) A. Convert to JARB. DecompileC. Cross-compile the applicationD. Convert JAR files to DEXE. Re-sign the APKF. Attach to ADB Answer: BC NEW QUESTION 82Consider the following PowerShell command:.....Which of the following BEST describes the actions performed this command? A. Set the execution policyB. Execute a remote scriptC. Run an encoded commandD. Instantiate an object Answer: A NEW QUESTION 83Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Choose two.) A. The tester discovers personally identifiable data on the system.B. The system shows evidence of prior unauthorized compromise.C. The system shows a lack of hardening throughout.D. The system becomes unavailable following an attempted exploit.E. The tester discovers a finding on an out-of-scope system. Answer: CE NEW QUESTION 84A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

www.passleader.com

Which of the following attack strategies should be prioritized from the scan results above? A. Obsolete software may contain exploitable components.B. Weak password management practices may be employed.C. Cryptographically weak protocols may be intercepted.D. Web server configurations may reveal sensitive information. Answer: A NEW QUESTION 85..... 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 (95 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