CHEAPTRY

QUESTION & ANSWER

Accurate study guides, High passing rate!

CHEAPTRY provides update free of charge in one year!

Exam : **PT0-001**

Title : CompTIA PenTest+ Certification Exam

Version : DEMO

1.A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 100.
Which of the following levels of difficulty would be required to exploit this vulnerability?
A. Very difficult; perimeter systems are usually behind a firewall
B. Somewhat difficult, would require significant processing power to exploit
C. Trivial, little effort is required to exploit this finding
D. Impossible; external hosts are hardened to protect against attacks
Answer:C

2.A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained.
Which of the actions should the penetration tester use to maintain persistence to the device? (Select TWO)
A. Place an entry in HKLM\Software Microsoft\CurrentVersion\Run to call au57d.ps1.
B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com
C. Place a script in C:\users\%username\local\appdata\roaming\templau57d.ps1
D. Create a fake service in Windows called RTAudio to execute manually
E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.
F. Create a schedule task to call C:\wwindows\system32\drivers\etc\hosts
Answer:AB

3.Which of the following tools is used to perform a credential brute force attack?
A. Hydra
B. John the Ripper
C. Hashcat
D. Peach
Answer:A

4.Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select 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:BE

5.A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the remediate to immediately remediate all vulnerabilities.
Under such circumstances which of the following would be the BEST suggestion for the client?
A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation
B. Identify the issues that can be remediated most quickly and address them first.

C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities
D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long time.
Answer:D