Vendor: CompTIA

Exam Code: PT0-001

Exam Name: CompTIA PenTest+ Exam: PT0-001 Exam

Version: DEMO

QUESTION 1
A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

A. schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run
B. net session server | dsquery -user | net use c$
C. powershell && set-executionpolicy unrestricted
D. reg save HKLM\System\CurrentControlSet\Services\Sv.reg

Answer: D

QUESTION 2
A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

A. The physical location and network ESSIDs to be tested
B. The number of wireless devices owned by the client
C. The client's preferred wireless access point vendor
D. The bands and frequencies used by the client's devices

Answer: D

QUESTION 3
Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

A. ICS vendors are slow to implement adequate security controls.
B. ICS staff are not adequately trained to perform basic duties.
C. There is a scarcity of replacement equipment for critical devices.
D. There is a lack of compliance for ICS facilities.

Answer: B

QUESTION 4
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 10.0. 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

QUESTION 5
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 following 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\temp\au57d.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:\windows\system32\drivers\etc\hosts.

Answer: AC

QUESTION 6
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

QUESTION 7
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: BD

QUESTION 8
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 resources 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 lime.

Answer: D

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**