Exam	**PT0-001**
Title	**CompTIA PenTest+ Certification**
Version	**6.0**
Product Type	**244 Q&A with explanations**

QUESTION 1
DRAG DROP
Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.
Select and Place:

Correct Answer:

Section: (none)
Explanation
Explanation/Reference:

QUESTION 2
DRAG DROP
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:
#!/usr/bin/python
s = ?Administrator?
The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.
Select and Place:

Correct Answer:

Section: (none)
Explanation
Explanation/Reference:

QUESTION 3
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 4
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 5
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 6
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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://nvd.nist.gov/vuln-metrics/cvss

QUESTION 7
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: A,C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 8
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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-totackle-
such-attacks

QUESTION 9
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: B,D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 10
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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 11
Which of the following is the reason why a penetration tester would run the chkconfig --del servicename command at the end of an engagement?

A. To remove the persistence
B. To enable persistence
C. To report persistence
D. To check for persistence

Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 12
A penetration tester wants to target NETBIOS name service. Which of the following is the MOST likely command to exploit the NETBIOS name service?

A. arpspoof
B. nmap
C. responder
D. burpsuite

Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/

QUESTION 13
A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

A. Rules of engagement
B. Request for proposal
C. Master service agreement
D. Business impact analysis