Vendor: CompTIA

Exam Code: PT0-001

Exam Name: CompTIA PenTest+ Exam

Version: 13.01

Q & As: 145

QUESTION 1
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

A. Mandate all employees take security awareness training
B. Implement two-factor authentication for remote access
C. Install an intrusion prevention system
D. Increase password complexity requirements
E. Install a security information event monitoring solution.
F. Prevent members of the IT department from interactively logging in as administrators
G. Upgrade the cipher suite used for the VPN solution

Correct Answer: ABD

QUESTION 2
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

Correct Answer: D

QUESTION 3
An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

A. Selection of the appropriate set of security testing tools
B. Current and load ratings of the ICS components
C. Potential operational and safety hazards
D. Electrical certification of hardware used in the test

Correct Answer: A

QUESTION 4
A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.
B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.
C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.

D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

Correct Answer: C

QUESTION 5
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

Correct Answer: A

QUESTION 6
An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A. dig -q any _kerberos._tcp.internal.comptia.net
B. dig -q any _lanman._tcp.internal.comptia.net
C. dig -q any _ntlm._tcp.internal.comptia.net
D. dig -q any _smtp._tcp.internal.comptia.net

Correct Answer: A

QUESTION 7
Which of the following BEST explains why it is important to maintain confidentiality of any identified findings when performing a penetration test?

A. Penetration test findings often contain company intellectual property
B. Penetration test findings could lead to consumer dissatisfaction if made pubic
C. Penetration test findings are legal documents containing privileged information
D. Penetration test findings can assist an attacker in compromising a system

Correct Answer: D

QUESTION 8
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De 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

Correct Answer: C

QUESTION 9
A 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.

Correct Answer: D

QUESTION 10
A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

A. Cleartext exposure of SNMP trap data
B. Software bugs resident in the IT ticketing system
C. S/MIME certificate templates defined by the CA
D. Health information communicated over HTTP
E. DAR encryption on records servers

Correct Answer: DE

QUESTION 11
Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

A. Shodan
B. SET
C. BeEF
D. Wireshark
E. Maltego
F. Dynamo

Correct Answer: AE
Explanation:
https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref
QUESTION 12
During an internal network penetration test, a tester recovers the NTLM password hash tor a user known to have full administrator privileges on a number of target systems Efforts to crack the hash and recover the plaintext password have been unsuccessful Which of the following would be the BEST target for continued exploitation efforts?

A. Operating system Windows 7
   Open ports: 23, 161
B. Operating system Windows Server 2016