PT1-002 Q&As

CompTIA PenTest+ Certification Exam

QUESTION 1

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact

B. Try to take down the attackers

C. Call law enforcement officials immediately

D. Collect the proper evidence and add to the final report

Correct Answer: A

QUESTION 2

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding

B. Session riding

C. Cybersquatting

D. Side channel

Correct Answer: B

Reference: https://www.iotcentral.io/blog/the-top-cloud-computing-vulnerabilities-and-threats

QUESTION 3

A security team is switching firewall vendors. The director of security wants to scope a penetration test to satisfy requirements to perform the test after major architectural changes. Which of the following is the BEST way to approach the project?

A. Design a penetration test approach, focusing on publicly released firewall DoS vulnerabilities.

B. Review the firewall configuration, followed by a targeted attack by a read team.

C. Perform a discovery scan to identify changes in the network.

D. Focus on an objective-based approach to assess network assets with a red team.

Correct Answer: D

QUESTION 4

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee\\'s birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?

A. Phishing

B. Tailgating

C. Baiting

D. Shoulder surfing

Correct Answer: C

QUESTION 5

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.

B. Implement multifactor authentication on all corporate applications.

C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.

D. Implement an email security gateway to block spam and malware from email communications.

Correct Answer: A

Reference: https://resources.infosecinstitute.com/topic/top-9-free-phishing-simulators/

QUESTION 6

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work

B. The correct user accounts and associated passwords

C. The expected time frame of the assessment

D. The proper emergency contacts for the client

Correct Answer: C

QUESTION 7

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

C. Attestation of findings and delivery of the report

D. Review of the lessons learned during the engagement

Correct Answer: A

QUESTION 8

An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client\\'s information?

A. Follow the established data retention and destruction process

B. Report any findings to regulatory oversight groups

C. Publish the findings after the client reviews the report

D. Encrypt and store any client information for future analysis

Correct Answer: D

QUESTION 9

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost

B. To guide them through the building entrances

C. To validate the billing information with the client

D. As proof in case they are discovered

Correct Answer: D

Reference: https://hub.packtpub.com/penetration-testing-rules-of-engagement/

QUESTION 10

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

A. Halt the penetration test.

B. Conduct an incident response.

C. Deconflict with the penetration tester.

D. Assume the alert is from the penetration test.

Correct Answer: B

QUESTION 11

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A.