PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following components should a penetration tester include in an assessment report?

A. User activities

B. Customer remediation plan

C. Key management

D. Attack narrative

Correct Answer: D

An attack narrative provides a detailed account of the steps taken during the penetration test, including the methods used, vulnerabilities exploited, and the outcomes of each attack. This helps stakeholders understand the context and

implications of the findings.

Components of an Assessment Report:

Importance of Attack Narrative:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 2

During an engagement, a penetration tester needs to break the key for the Wi-Fi network that uses WPA2 encryption. Which of the following attacks would accomplish this objective?

A. ChopChop

B. Replay

C. Initialization vector

D. KRACK

Correct Answer: D

KRACK (Key Reinstallation Attack) exploits a vulnerability in the WPA2 protocol to decrypt and inject packets, potentially allowing an attacker to break the encryption key and gain access to the Wi-Fi network.

Understanding KRACK:

Attack Steps:

Impact:

Mitigation:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 3

A penetration tester would like to leverage a CSRF vulnerability to gather sensitive details from an application\\'s end users. Which of the following tools should the tester use for this task?

A. Browser Exploitation Framework

B. Maltego

C. Metasploit

D. theHarvester

Correct Answer: A

Cross-Site Request Forgery (CSRF) vulnerabilities can be leveraged to trick authenticated users into performing unwanted actions on a web application. The right tool for this task would help in exploiting web-based vulnerabilities, particularly

those related to web browsers and interactions.

Browser Exploitation Framework (BeEF) (Answer: A):

Maltego (Option B):

Metasploit (Option C):

theHarvester (Option D):

Conclusion: The Browser Exploitation Framework (BeEF) is the most suitable tool for leveraging a CSRF vulnerability to gather sensitive details from an application\\'s end users. It is specifically designed for browser-based exploitation, making

it the best choice for this task.

QUESTION 4

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:

QUESTION 5

A penetration tester gains access to a host but does not have access to any type of shell. Which of the following is the best way for the tester to further enumerate the host and the environment in which it resides?

A. ProxyChains

B. Netcat

C. PowerShell ISE

D. Process IDs

Correct Answer: B

If a penetration tester gains access to a host but does not have a shell, the best tool for further enumeration is Netcat. Here\\'s why:

Netcat:

Comparison with Other Tools:

Netcat\\'s ability to perform multiple network-related tasks without needing a shell makes it the best choice for further enumeration.