

CompTIA PenTest PT0 002 Cert Guide 2nd edition
Santos Test Bank

SKU: 9780137566174-TEST-BANK

Chapter 1 Introduction to Ethical Hacking and Penetration Testing

1) Which of these describes a scenario in which the tester is provided credentials but not full documentation of the network infrastructure?

- A) Unknown-environment test
- B) Known-environment test
- C) Partially known environment test
- D) Unspecified environment test

Answer: C

2) Which of the following would an ethical hacker *not* participate in?

- A) Unauthorized access
- B) Responsible disclosure
- C) Documentation
- D) Unknown-environment test

Answer: A

3) Which of these attack types involves tricking the user into disclosing information or taking action?

- A) DDoS
- B) Ransomware
- C) Social engineering
- D) Botnet

Answer: C

4) What type of attacker is most likely to be motivated purely by financial profit?

- A) Hacktivist
- B) Nation-state
- C) Insider threat
- D) Organized crime

Answer: D

5) Cyber war and cyber espionage are two terms that best fit into this category:

- A) State-sponsored attackers
- B) Hacktivists
- C) Insider threats
- D) Organized crime

Answer: A

6) Which of the following frameworks is a collection of different matrices of tactics, techniques, and subtechniques?

- A) WSTG
- B) MITRE ATT&CK
- C) NIST
- D) OSSTMM

Answer: B

7) What type of attacker steals sensitive data and then reveals it to the public in order to embarrass the target?

- A) Kidnapper
- B) Nation state
- C) Organized crime
- D) Hacktivist

Answer: D

8) What type of tests would be most important to conduct to find out whether hackers could use the Internet to compromise your client's online ordering system?

- A) Application-based tests
- B) Network infrastructure tests
- C) Penetration testing in the cloud
- D) Physical facility tests

Answer: A

9) What is the first phase of the Penetration Testing Execution Standard testing methodology?

- A) Intelligence gathering
- B) Vulnerability analysis
- C) Pre-engagement interactions
- D) Threat modeling

Answer: C

10) What type of tests would be most important to conduct to find out whether unauthorized people can reach the company's server rooms?

- A) Web application tests
- B) Network infrastructure tests
- C) Wireless network tests
- D) Physical facility tests

Answer: D

11) What type of tests would be most important to conduct to find out whether there are any poorly secured switches, firewalls, routers, and supporting resources?

- A) Web application tests
- B) Network infrastructure tests
- C) Wireless network tests
- D) Physical facility tests

Answer: B

12) Which testing methodology involves seven phases, including pre-engagement interactions, intelligence gathering, threat modeling, and vulnerability analysis?

- A) PTES
- B) PCI DSS
- C) Penetration Testing Framework
- D) OSSTMM

Answer: A

13) Which testing methodology has key sections including Operational Security Metrics, Trust Analysis, Work Flow, and Human Security Testing?

- A) PTES
- B) PCI DSS
- C) Penetration Testing Framework
- D) OSSTMM

Answer: D

14) In this type of test, the tester would normally be provided things like network diagrams, IP addresses, configurations, and a set of user credentials:

- A) Unknown-environment test
- B) Known-environment test
- C) Partially known environment test
- D) Black-box test

Answer: B

15) ISSAF covers which of the following phases?

- A) Information gathering
- B) Network mapping
- C) Vulnerability identification
- D) All of the above

Answer: D

16) What document created by the National Institute of Standards and Technology provides organizations with guidelines on planning and conducting information security testing?

- A) Special Publication (SP) 800-115
- B) General Publication (GP) 2006-110
- C) Special Publication (SP) 2018-01
- D) International Publication (IP) 2016-330

Answer: A

17) Which of these is *not* a requirement for a typical penetration testing environment?

- A) Closed network
- B) Virtualized computing environment
- C) Sign-in credentials for the systems to be tested
- D) Practice targets

Answer: C

18) Which of these can help protect the client in the event that you break something during a test?

- A) Health monitoring
- B) WPA
- C) Open network
- D) Virtualized computing environment

Answer: D

19) Which type of hacker has consent to attempt to access the target?

- A) Penetration tester
- B) Hactivist
- C) Nonethical hacker
- D) Insider threat

Answer: A

20) Which of the following is the first phase of ISSAF?

- A) Threat modeling
- B) Network mapping
- C) Intelligence gathering
- D) Information gathering

Answer: D