CompTIA® PenTest+ Cert Guide
Chapter 1 Introduction to Ethical Hacking and Penetration Testing

1) Which of these describes a scenario in which the tester starts with credentials but not full documentation of the network infrastructure?
A) Black-box test
B) White-box test
C) Gray-box test
D) Blue-box test
Answer: C

2) Which of the following would an ethical hacker *not* participate in?
A) Unauthorized access
B) Responsible disclosure
C) Documentation
D) Black-box testing
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) What type of attack encrypts user files until the victim pays a fee?
A) Ransomware
B) Denial of Service attack
C) Hacktivism
D) Shoulder surfing
Answer: A

6) IoT devices are most susceptible to being used for what type of attack?
A) Ransomware
B) DDoS
C) Man-in-the-Middle
D) Social engineering
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) Web application tests
B) Network infrastructure tests
C) Wireless network tests
D) Physical facility tests
Answer: A

9) What type of tests would be most important to conduct to find out whether the client's WAPs are properly secured?
A) Web application tests
B) Network infrastructure tests
C) Wireless network tests
D) Physical facility tests
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 firewalls, routers, and switches on a LAN?
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) Which testing methodology pertains to the specific needs of credit card processing systems?
A) PTES
B) PCI DSS
C) Penetration Testing Framework
D) OSSTMM
Answer: B

15) Which testing methodology focuses on the hands-on aspects of penetration testing and provides links to many tools in an HTML format?
A) PTES
B) PCI DSS
C) Penetration Testing Framework
D) OSSTMM
Answer: C

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) Social engineering
B) WPA
C) Open network
D) Virtual environment
Answer: D

19) Which type of hacker has consent to attempt to access the target?
A) Penetration tester
B) Hacktivist
C) Nonethical hacker
D) Insider threat
Answer: A

20) Russia's interference with the 2016 United States elections was an example of which type of attack?
A) Insider threat
B) State sponsored
C) Hacktivist
D) Organized crime
Answer: B