Vendor: CWNP

Exam Code: PW0-204

Exam Name: Certified Wireless Security Professional (CWSP)

Version: DEMO
1. Which of the following protocols is used to provide on-demand authentication within an ongoing data transmission?
   A. LEAP
   B. EAP
   C. PPTP
   D. CHAP
   Answer: D

2. Which of the following is a common Windows authentication protocol used by the IEEE 802.1X security standard?
   A. TACACS
   B. LDAP
   C. RADIUS
   D. SSL/TLS
   Answer: C

3. Which of the following authentication processes are specified by the IEEE 802.11 standards? Each correct answer represents a complete solution. Choose all that apply.
   A. Open System authentication
   B. RADIUS
   C. Shared Key authentication
   D. EAP
   Answer: AC

4. Which of the following methods are capable of operating in wireless networks? Each correct answer represents a complete solution. Choose all that apply.
   A. EAP-TLS
   B. LEAP
   C. PEAP
   D. EAP-TTLS
   Answer: BAD

5. John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?
   A. Rainbow attack
   B. DoS attack
   C. Replay attack
   D. ARP spoofing
   Answer: B

6. Which of the following protocols uses a program layer located between the Internet’s Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers?
   A. TFTP
B. HTTPS  
C. SCP  
D. SSL  
Answer: D

7. You have been hired to perform a penetration test on a client's network. You want to see if remote connections are susceptible to eavesdropping or perhaps session hijacking. Which network tool would be most helpful to you?  
A. Vulnerability analyzer  
B. Port scanner  
C. Performance analyzer.  
D. Protocol analyzer  
Answer: D

8. Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?  
A. Remote Authentication Dial-In User Service (RADIUS)  
B. IEEE 802.1x  
C. Wired Equivalent Privacy (WEP)  
D. Wi-Fi Protected Access 2 (WPA2)  
Answer: B

9. Which of the following will you recommend for providing security?  
A. HTTP  
B. VPN  
C. SSL  
D. S/MIME  
Answer: C

10. Which of the following tools is John using to crack the wireless encryption keys?  
A. Kismet  
B. AirSnort  
C. Cain  
D. PsPasswd  
Answer: B

11. Which of the following tools is John using to crack the wireless encryption keys?  
A. Kismet  
B. AirSnort  
C. Cain  
D. PsPasswd  
Answer: B
12. Which of the following are the important components of the IEEE 802.1X architecture? Each correct answer represents a complete solution. Choose all that apply.
   A. Authenticator server
   B. Extensible Authentication Protocol (EAP)
   C. Supplicant
   D. Authenticator
   Answer: CAD

13. You work as a System Administrator for Tech Perfect Inc. The company has a wireless LAN network. You want to implement a tool in the company's network, which monitors the radio spectrum used by the wireless LAN network, and immediately alerts you whenever a rogue access point is detected in the network. Which of the following tools will you use?
   A. Firewall
   B. WIPS
   C. MFP
   D. NAT
   Answer: B

14. Which of the following methods can be used to detect a rogue access point in order to enhance the security of the network? Each correct answer represents a complete solution. Choose all that apply.
   A. Install WIPS
   B. Hide the SSID of all AP
   C. Check in the managed AP list
   D. Use of wireless sniffing tools
   Answer: ADC

15. Which of the following works as a protocol for providing secure communications between wireless clients and wireless access points?
   A. Virtual Private Network
   B. Firewall
   C. Packet filtering
   D. Robust Secure Network
   Answer: D

16. Which of the following is a type of security management for computers and networks in order to identify security breaches?
   A. EAP
   B. IPS
   C. IDS
   D. ASA
   Answer: C
17. Which of the following types of attacks cannot be prevented by a firewall? Each correct answer represents a complete solution. Choose all that apply.
A. Shoulder surfing attack
B. Ping flood attack
C. URL obfuscation attack
D. Phishing attack
**Answer:** CDA

18. Which of the following protocols uses public-key cryptography to authenticate the remote computer?
A. SSL
B. Telnet
C. SCP
D. SSH
**Answer:** D

19. Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer? Each correct answer represents a complete solution. Choose two.
A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
B. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.
C. Attacker can use the Ping Flood DoS attack if WZC is used.
D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.
**Answer:** AB

20. Which of the following is a part of computer network that is used to prevent unauthorized Internet users from accessing private networks connected to the Internet?
A. Protocol analyzer
B. Wired Equivalent Privacy
C. Intrusion detection system
D. Firewall
**Answer:** D