Exam Code: PW0-200

Exam Name: Certified Wireless Security professional (CWSP)

Vendor: CWNP

Version: DEMO

Part: A

1: What policies would prevent peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?
A.Require managed personal firewall software on each laptop.
B.Require secure applications such as POP3/S, HTTPS, and SSH2.
C.Require VPN software for connectivity to the corporate network.
D.Require WPA2-Enterprise as the minimal WLAN security solution.
E.Require Port Address Translation (PAT) on each laptop.
F.Require a managed wireless endpoint security agent on each laptop.
Correct Answers: A B C F

2: Given: You have a laptop computer with an integrated Wi-Fi compliant MiniPCI card.
What statements describe the limited effectiveness of locating rogue access points using WLAN discovery software such as NetStumbler, Kismet, or MacStumbler?
A.Discovery tools like those listed cannot determine the authorization status of an access point.
B.A laptop computer can only be in one location at a time.
C.Discovery tools like those listed cannot determine if an access point is attached to a wired network.
D.Rogue access points using non-IEEE 802.11 frequency bands or unpopular modulations are not detected.
E.When data encryption in use, access points cannot be detected using discovery tools like those listed.
Correct Answers: A B C D

3: What happens in a bit flipping attack against an IEEE 802.11 device?
A.An attacker captures an encrypted frame, modifies the ciphertext, modifies the ICV to hide the change to the ciphertext, and then transmits the frame to appear as if it is from the original source.
B.An attacker uses a non-linear Message Integrity Check (MIC) on his computer to form a wireless crossover connection with the target computer.
C.An attacker injects data into a wireless transmission that results in a memory access exception at the target system for the purpose of breaching security.
D.An attacker sends each frame with the first bit alternating between 0 and 1, causing the target computer to disable encryption synchronization.
E.An attacker captures an encrypted authentication frame, and then executes a cracking algorithm against each 0 and 1 in the frame. After the frame is cracked, it is used to authenticate the attacker's computer.
Correct Answers: A

4: Given: ABC Company has a WLAN controller with three access points, 15 client devices, and uses WPA2-Personal for WLAN security.
What statement about ABC Company's WLAN security is true?
A.Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt data traffic.

B.Traffic injection attacks are possible because the transmitter lacks frame numbering.

C.An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt broadcast traffic.

D.An authorized WLAN user with a protocol analyzer can decode data frames of other authorized users if he captures that user's 4-Way Handshake.

E.Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

Correct Answers: D

5: What WIPS parameter is configured to generate notifications?

A.Mobile unit density violations

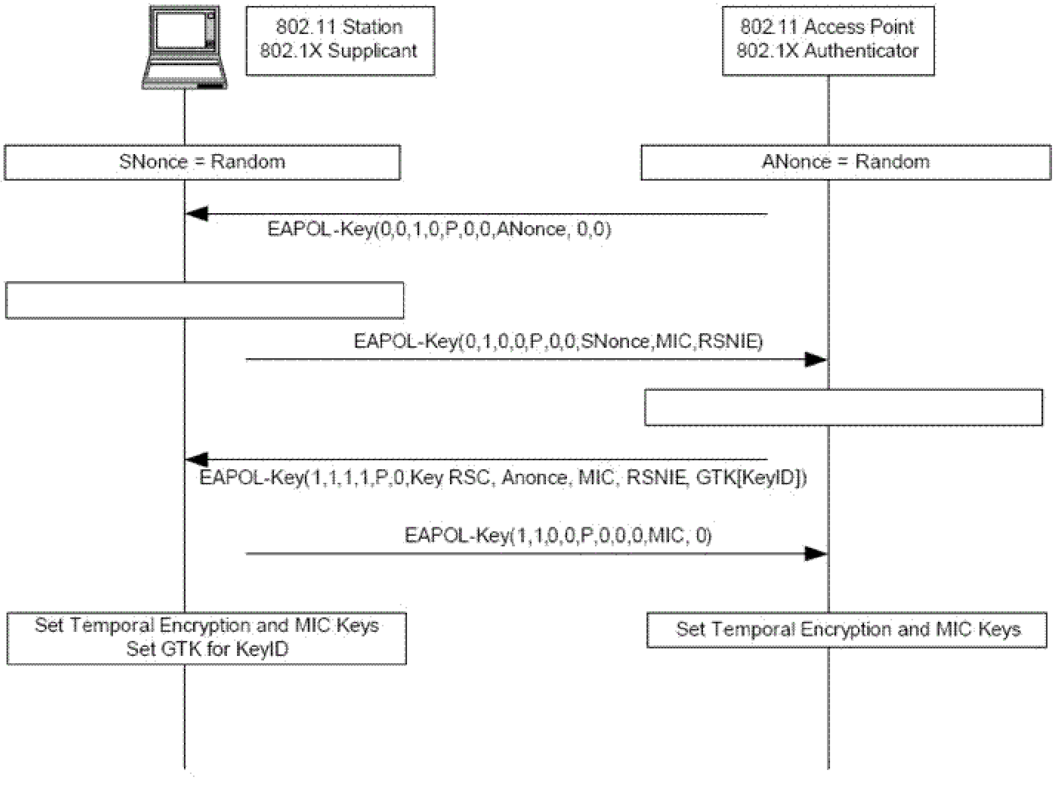
B.Admission control status

C.Sensor sensitivity levels

D.Policy threshold values

Correct Answers: D

6: In this diagram illustrating an example of the IEEE 802.11 standard's 4-Way Handshake, what is the purpose of the ANonce and SNonce?


802.11 Station
802.1X Supplicant
802.11 Access Point
802.1X Authenticator
SNonce = Random
ANonce = Random
EAPOL-Key(0,0,1,0,P,0,0,ANonce, 0,0)
EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,RSNIE)
EAPOL-Key(1,1,1,1,P,0,Key RSC, Anonce, MIC, RSNIE, GTK[KeyID])
EAPOL-Key(1,1,0,0,P,0,0,0,MIC, 0)
Set Temporal Encryption and MIC Keys
Set GTK for KeyID
Set Temporal Encryption and MIC Keys

A.They are used to pad Message 1 and Message 2 so there is no empty space in the frame.

B.The IEEE 802.11 standard requires that all cryptographic frames contain a nonce for security purposes.

C.They are added together and used as the GMK, from which the GTK is derived.

D.They are values used in the derivation of the Pairwise Transient Key.

Correct Answers: D

7: Given: John Smith often works from home and wireless hotspots rather than commuting to the office. His laptop connects to the office network over IEEE 802.11 WLANs.

To safeguard his data, what wireless security policy items should be implemented?

A.Use an IPSec VPN for remote connectivity

B.Use an HTTPS captive portal for authentication at hotspots

C.Use personal firewall software on his laptop

D.Use a protocol analyzer on his laptop to monitor for risks

E.Use 802.1X/PEAPv0 to connect to the corporate office network

Correct Answers: A C

8: Given: A network security auditor is assessing an IEEE 802.11 network's exposure to security holes.

What task would save the most time if performed before the audit?

A.Identify the IP subnet information for each network segment.

B.Identify the manufacturer of the wireless intrusion prevention system.

C.Identify the skill level of the wireless network security administrator(s).

D.Identify the manufacturer of the wireless infrastructure hardware.

E.Identify the wireless security solution(s) currently in use.

Correct Answers: E

9: Given: ABC Corporation is selecting a security solution for their new WLAN, and a PPTP VPN is their first consideration because it is included with both server and desktop operating systems. While the 128-bit encryption of Microsoft's MPPE is considered strong enough to adhere to corporate security policy, the company is worried about security holes in MS-CHAPv2 authentication.

As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication in a PPTP VPN?

A.MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.

B.MS-CHAPv2 is subject to offline dictionary attacks.

C.MS-CHAPv2 is only secure when combined with WEP.

D.MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.

E.MS-CHAPv2 uses anonymous Diffie-Hellman authentication, and is therefore secure.

F.MS-CHAPv2 can be replaced with EAP-TLS as the authentication mechanism for PPTP.

Correct Answers: B D F

10: Given: ABC Company's ERP WLAN has worked perfectly for the last 6 months. One morning, none of the company's 10 users can connect to the company's only access point. When the administrator logs into the access point, there are hundreds of users associated using Open System authentication.

What is the problem?

A.The AP has been the victim of an RF DoS attack.

B.The AP has experienced an AP spoofing attack from a rogue AP.

C.The AP firmware has been corrupted and is erroneously reporting the number of users.

D.The AP has experienced an association flood attack.

Correct Answers: D

11: During 802.1X/LEAP authentication, what authentication credential is passed using clear text across the wireless medium?

A.Password

B.x.509 certificate

C.Username

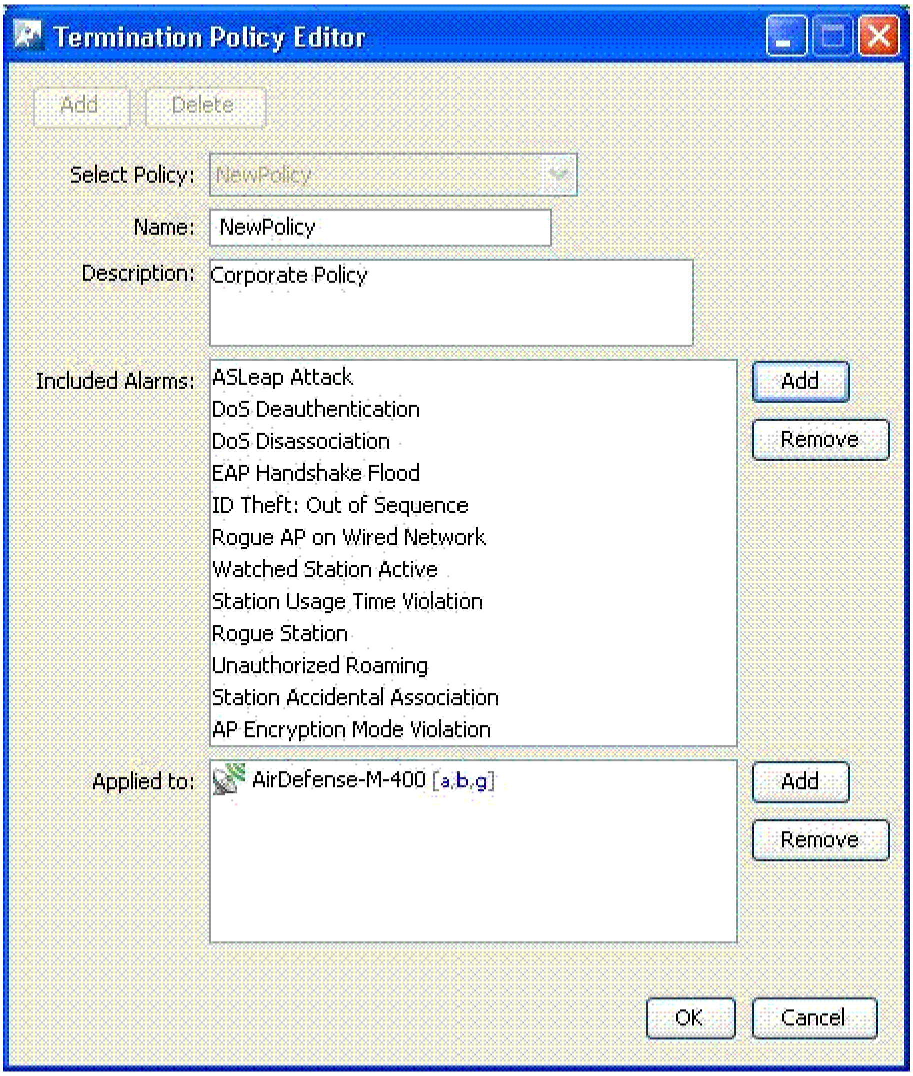
D.PAC

E.Shared secret

Correct Answers: C

12: Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 network. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS for connectivity to all Marketing department APs before it was given to him yesterday. The WIPS termination policy is shown in the exhibit.

What are some possible reasons that Joe cannot connect to the network?



Select Policy: NewPolicy

Name: NewPolicy

Description: Corporate Policy

Included Alarms:
ASLeap Attack
DoS Deauthentication
DoS Disassociation
EAP Handshake Flood
ID Theft: Out of Sequence
Rogue AP on Wired Network
Watched Station Active
Station Usage Time Violation
Rogue Station
Unauthorized Roaming
Station Accidental Association
AP Encryption Mode Violation

Applied to: AirDefense-M-400 [a,b,g]

A.Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio because of its updated chipset, drivers, and client utilities.

B.Joe's integrated 802.11 radio is sending too many Probe Request and EAPoL Start frames due to a corrupted driver.

C.Joe's radio card has associated to an access point belonging to a neighboring 802.11 WLAN because it was configured to connect to any wireless network.

D.An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.

E.Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.

F.Joe changed the system time on his computer, and the WIPS is detecting this as a usage time violation.

Correct Answers: A C

13: What four tools are required to hijack a wireless station (at Layer 2 and Layer 3) from the authorized wireless network onto the unauthorized wireless network? (Select two answers that together specify the four necessary tools)

A.Access point software and a narrowband RF jamming device

B.A high-gain Yagi antenna and terminal emulation software

C.A wireless workgroup bridge and a spectrum analyzer

D.A wireless PC card and DHCP server software

E.MAC spoofing software and data flooding software

Correct Answers: A D

14: Given: ABC Company is planning to implement IPSec VPN technology using the Encapsulating Security Payload (ESP) protocol to secure their wireless connections. You are hired as a security consultant to discuss the security strength of this solution.

What statement about this WLAN security implementation is true?

A.ESP can only use 3DES encryption which causes high latency on half-duplex networks.

B.Wireless clients should be configured for NAT transparency so encrypted frames can traverse gateways.

C.ESP uses public key cryptography, which is incompatible with the 802.11 protocol.

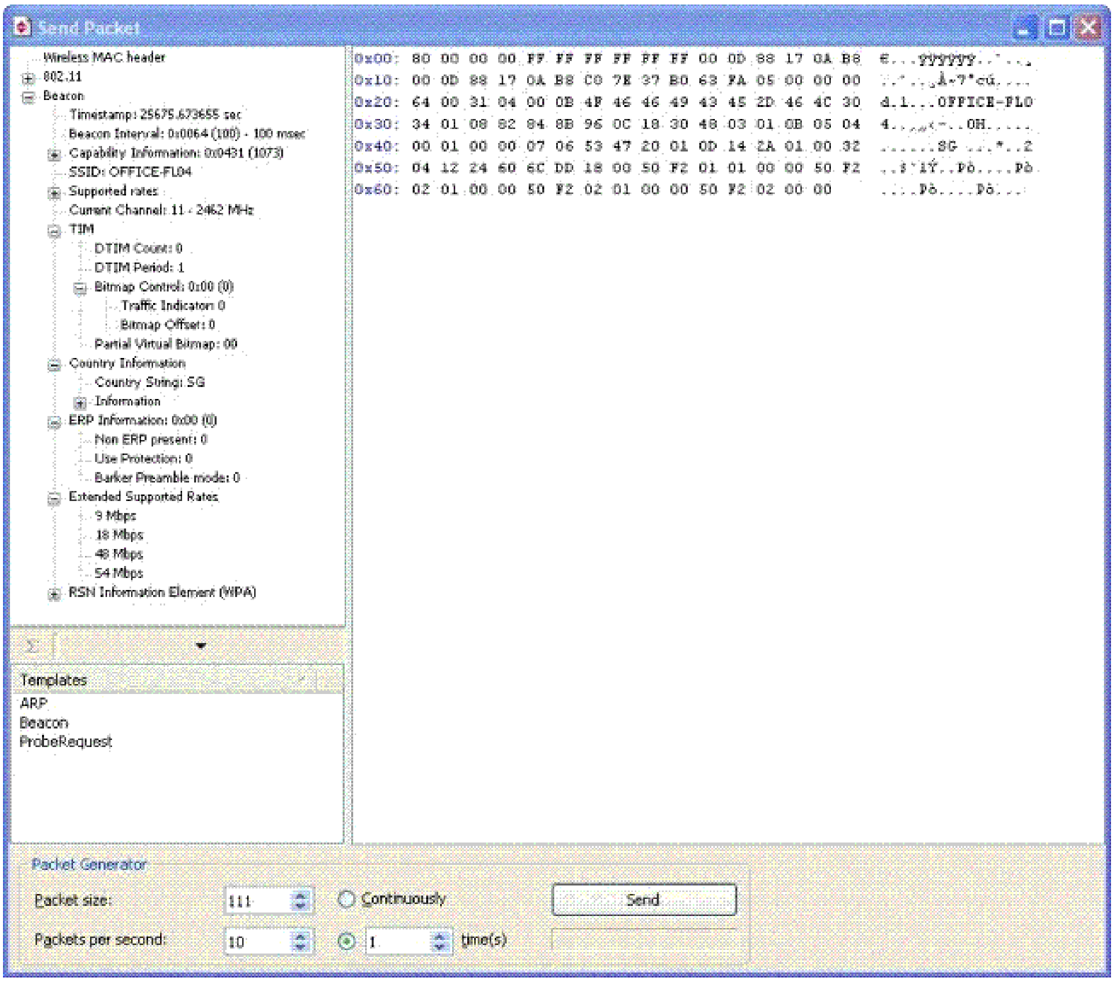
D.The ESP protocol encrypts the entire original frame if implemented in tunnel mode.

E.When using ESP as a VPN solution, the implementation must incorporate SSH2 tunneling as well.

Correct Answers: D

15: Given: The illustrated WLAN software tool can transmit customized 802.11 frames.

What are two uses for such a tool?



```
Wireless MAC header
802.11
Beacon
    Timestamp: 25675.673655 sec
    Beacon Interval: 0x0064 (100) - 100 msec
    Capability Information: 0x0431 (1073)
    SSID: OFFICE-FL04
    Supported rates
    Current Channel: 11 - 2462 MHz
    TIM
        DTIM Count: 0
        DTIM Period: 1
        Bitmap Control: 0x00 (0)
            Traffic Indicator: 0
            Bitmap Offset: 0
        Partial Virtual Bitmap: 00
    Country Information
        Country String: SG
        Information
    ERP Information: 0x00 (0)
        Non ERP present: 0
        Use Protection: 0
        Barker Preamble mode: 0
    Extended Supported Rates
        9 Mbps
        18 Mbps
        48 Mbps
        54 Mbps
    RSN Information Element (WPA)
```

```
0x00: 80 00 00 00 FF FF FF FF FF FF 00 0D 88 17 0A B8   €...ÿÿÿÿÿÿ..ˆ...¸
0x10: 00 0D 88 17 0A B8 C0 7E 37 B0 63 FA 05 00 00 00   ..ˆ...¸À~7°cú....
0x20: 64 00 31 04 00 0B 4F 46 46 49 43 45 2D 46 4C 30   d.1...OFFICE-FL0
0x30: 34 01 08 82 84 8B 96 0C 18 30 48 03 01 0B 05 04   4..‚„‹–..0H.....
0x40: 00 01 00 00 07 06 53 47 20 01 0D 14 2A 01 00 32   ......SG ...*..2
0x50: 04 12 24 60 6C DD 18 00 50 F2 01 01 00 00 50 F2   ..$`lÝ..Pò....Pò
0x60: 02 01 00 00 50 F2 02 01 00 00 50 F2 02 00 00      ....Pò....Pò...
```

Templates

ARP

Beacon

ProbeRequest

Packet Generator

Packet size: 111

Packets per second: 10

○ Continuously

● 1 time(s)

A.EAPoL flood attacks against access points

B.Auditing the performance features of a WIPS

C.Testing Role-Based Access Control features of a WLAN controller

D.NAV/duration attacks against all stations in a BSA

E.Altering physical layer frame headers for frame injection attacks

F.Changing a frame's WEP ICV while it is in transit

Correct Answers: A D