

CWNP


CWSP

PW0-200 PW0-200 PW0-200 PW0-200 PW0-200 PW0-200 PW0-200

PRINTABLES

PRINTABLE PRACTICE QUESTIONS

QUESTIONS, ANSWERS, AND
DETAILED EXPLANATIONS IN AN
EASY-TO-USE PRINTABLE FORMAT

 LearnSmart™

Chapter 1

Wireless LAN Discovery

1. You are performing a penetration test on a WLAN. Which of the following tools may be used in the process of network discovery? Choose all that apply.

- A. Kismet
- B. Netstumbler
- C. Aircrack-ng
- D. ASLEAP

[Find the Answer](#) p. 58

2. An attacker is wardriving in order to locate WLANs that are open and provide Internet access. She detects 11 WLANs at a specific location and needs to determine which WLANs will provide open access and Internet connectivity. She performs the following steps: 1) Look at the list of WLANs to see if any are listed as unsecured. 2) Connect to the WLAN that is listed as unsecured with the greatest signal strength. Did she meet her objective of locating an open WLAN that provides Internet access and why? Select the best answer.

- A. Yes. Because she was able to identify and connect to an unsecured WLAN.
- B. Yes. Because an unsecured WLAN always provides Internet access.
- C. No. Because she does not have the appropriate WEP key.
- D. No. Because she has connected to the WLAN, but she has not determined if Internet access is available.

[Find the Answer](#) p. 58



3. The Windows XP and later Windows operating systems have a built-in wireless networking client that may be used for WLAN discovery. What is the name of this wireless networking client? Select the best answer.
- A. Wireless Zero Configuration
 - B. Wireless Auto Configuration
 - C. WiFi Locater
 - D. Wireless LAN Supplicant

[Find the Answer](#) p. 58

4. Mary is a help desk employee in XYZ Corporation. She receives a call from an individual who refers to himself as Jim and says that he is from the network administration group. He says that he needs Mary to walk through the configuration of a wireless laptop with him so that he can verify that the help desk has the appropriately documented steps. Rather than reading the steps to her, he asks her to recite the steps to him. If this is an attack, what kind of attack method is being employed? Select the best answer.
- A. Dumpster Diving
 - B. Shoulder surfing
 - C. Social Engineering
 - D. Port Scanning

[Find the Answer](#) p. 58

5. An attacker is using OmniPeek Personal in order to view the WLAN traffic in a small business. The traffic is unencrypted and the attacker is filtering for the keywords of username and password. What kind of information gathering attack is this? Select the best answer.
- A. Social Engineering
 - B. Eavesdropping
 - C. Port Scanning
 - D. Hijacking

[Find the Answer](#) p. 58



Answers: Chapter 1

1. A, B	Review Question p. 2	Detailed Explanation p. 68
2. D	Review Question p. 2	Detailed Explanation p. 68
3. A	Review Question p. 3	Detailed Explanation p. 68
4. C	Review Question p. 3	Detailed Explanation p. 69
5. B	Review Question p. 3	Detailed Explanation p. 69
6. C	Review Question p. 4	Detailed Explanation p. 70
7. B, C	Review Question p. 4	Detailed Explanation p. 70
8. A	Review Question p. 5	Detailed Explanation p. 71
9. A	Review Question p. 5	Detailed Explanation p. 71
10. A	Review Question p. 6	Detailed Explanation p. 72



Explanations: Chapter 1

1. [Review Question](#) p. 2

Answers: A, B

Explanation A. Correct. Kismet is capable of locating WLANs that are implemented with IEEE standard technology. Kismet is mostly used on Linux systems.

Explanation B. Correct. Netstumbler is used on Windows systems to locate WLANs using IEEE standard technology.

Explanation C. Incorrect. Aircrack-ng is a tool used to sniff and then crack WEP keys on WLANs in order to penetrate them. If you are using Aircrack-ng, the network discovery phase of the attack is complete and you are now in the network attack phase.

Explanation D. Incorrect. ASLEAP is used to attack the Lightweight EAP authentication solution by Cisco. If you are using ASLEAP, the network discovery phase of the attack is complete and you are now in the network attack phase.

PrepLogic Question: [11340-100](#)

2. [Review Question](#) p. 2

Answers: D

Explanation A. Incorrect. She has not verified that this WLAN provides Internet access.

Explanation B. Incorrect. An unsecured WLAN provides access to the WLAN in an insecure fashion, but this WLAN may not provide any connectivity to the Internet.

Explanation C. Incorrect. Since she located a WLAN that is insecure, a WEP key or other authentication credential will not be required.

Explanation D. Correct. Her ultimate goal was to gain access to the Internet and this has not been accomplished with the steps provided.

PrepLogic Question: [11340-101](#)

3. [Review Question](#) p. 3

Answers: A

Explanation A. Correct. WZC is used to detect and connect to wireless networks in Windows XP systems by default; however, you may install a wireless client that is used



in place of the WZC client.

Explanation B. Incorrect. There is no such client in Windows XP systems. Wireless auto configuration is the phrase Microsoft uses to refer to the actions of Wireless Zero Configuration. WZC exists as a wireless client, wireless auto configuration does not.

Explanation C. Incorrect. There is no such client in Windows XP systems by default.

Explanation D. Incorrect. The phrase wireless LAN or WLAN supplicant is a generic phrase used to reference any wireless client software.

PrepLogic Question: [11340-102](#)

4. [Review Question](#) p. 3

Answers: C

Explanation A. Incorrect. Dumpster diving refers to the process of sifting through the trash that an organization or individual discards in order to discover information that can be used in an attack.

Explanation B. Incorrect. Shoulder surfing refers to an attack that involves looking at the computer screen of a valid user when the valid user is unaware that he is being observed. This is performed in order to gather information such as logon IDs and passwords.

Explanation C. Correct. Social Engineering refers to the process of manipulating another person into revealing information that he or she should not reveal. It usually involves psychological tactics and can only be protected against through training and retraining.

Explanation D. Incorrect. Port scanning is a technical attack that investigates TCP ports in order to discover running services and protocols on a target machine. This information is then used to launch a computerized attack.

PrepLogic Question: [11340-103](#)

5. [Review Question](#) p. 3

Answers: B

Explanation A. Incorrect. Social Engineering refers to the process of manipulating another person into revealing information that he or she should not reveal. It usually involves psychological tactics and can only be protected against through training and retraining.



Explanation B. Correct. The attacker is not cracking encryption keys or authentication algorithms and is simply monitoring the traffic. This is known as eavesdropping.

Explanation C. Incorrect. Port scanning is a technical attack that investigates TCP ports in order to discover running services and protocols on a target machine. This information is then used to launch a computerized attack.

Explanation D. Incorrect. Session hijacking refers to an attack where the attacker either takes over the client's association with an AP or the attacker impersonates the AP with which a client has an association.

PrepLogic Question: [11340-104](#)

6. [Review Question](#) p. 4

Answers: C

Explanation A. Incorrect. Standard omni-directional antennas would be much less obvious as they would look more like a satellite radio antenna or a standard radio antenna.

Explanation B. Incorrect. Since satellite signals are on a different frequency than WLAN signals, a different antenna would be required.

Explanation C. Correct. The highly directional antenna will have higher gain and this improves both reception and transmission distance.

Explanation D. Incorrect. An antenna that looks like a satellite dish is likely a highly directional or semi-directional antenna and this would prevent the attacker from jamming WLANs in one or more directions.

PrepLogic Question: [11340-105](#)

7. [Review Question](#) p. 4

Answers: B, C

Explanation A. Incorrect. While the spectrum analyzer is small and will not be as noticeable as a laptop computer, it will only report on spectrum activity and cannot report on the specific configuration requirements of the WLANs.

Explanation B. Correct. A handheld PC or PDA will attract the least attention and can detect the WLANs and whether they are implementing security or not.

Explanation C. Incorrect. This would attract far too much attention. Once the attacker locates an insecure WLAN with his PDA, he may choose to park close to the WLAN in

