Exam Report: 13.1.15 Practice Questions

Date: 5/21/2020 9:01:52 am
Time Spent: 1:48

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 33%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following best describes a wireless access point?

- A device used to connect two or more computers without using any pre-existing infrastructure, such as a router.
- A device that repeats the wireless signal from your router to expand its coverage.
- A device that forwards IP packets between your wireless subnet and any other subnet.
- A networking hardware device that allows other Wi-Fi devices to connect to a wired network.

Explanation

A wireless access point is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

A range extender is a device that repeats the wireless signal from your router to expand its coverage.

An ad-hoc wireless network is a wireless connection that connects to a computer directly without having to connect to a Wi-Fi access point or router.

A wireless router forwards IP packets between your wireless subnet and any other subnet. Typically, wireless routers are used in residences and small businesses, where all users can be supported by one combined AP and router. Wireless APs are used in larger businesses and venues, where many APs are required to provide service.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_ACCESS_POINTS_01_EH1]

Question 2: Incorrect

You work for a very small company that has 12 employees. You have been asked to configure wireless access for them. Knowing that you have a very limited budget to work with, which of the following technologies should you use?

- A software-based access point.
- A software-based range extender
- A hardware-based access point.
- ~~A hardware-based range extender.~~

Explanation

To connect your wireless computers to the network, you will want to install an access point. Since you are working with a limited budget, using a software-based access point will give your employees wireless access for the lowest cost.

A hardware-based access point would work, but would typically cost more than a software-based access point.

Range extenders are not required, as your company is so small. In addition, range extenders only extend the coverage area, but do not connect your wireless access points to the network.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_ACCESS_POINTS_02_EH1]

Question 3: Incorrect

You are configuring several wireless access points for your network. Knowing that each access point will have a service set identifier (SSID), you want to ensure that it is configured correctly. Which of the following SSID statements are true?

- The SSID and the name of the access point are the same thing.
- ~~The SSID can be hidden, making it less vulnerable to attack.~~
- The SSID is a unique name, separate from the access point name.
- The SSID name adds security, but is optional in most cases.

Explanation

Although the name (or host name) of an access point can be the same as the SSID, most wireless routers let you assign a unique SSID which users or customers see when connecting the network. Although an SSID is necessary for a secure network, on its own, it doesn't do much to make a network more secure. For example, SSIDs are sent in a packet in plain text. A hacker can easily capture the packet and find the SSID using a sniffing tool, such as Wireshark and tcpdump.

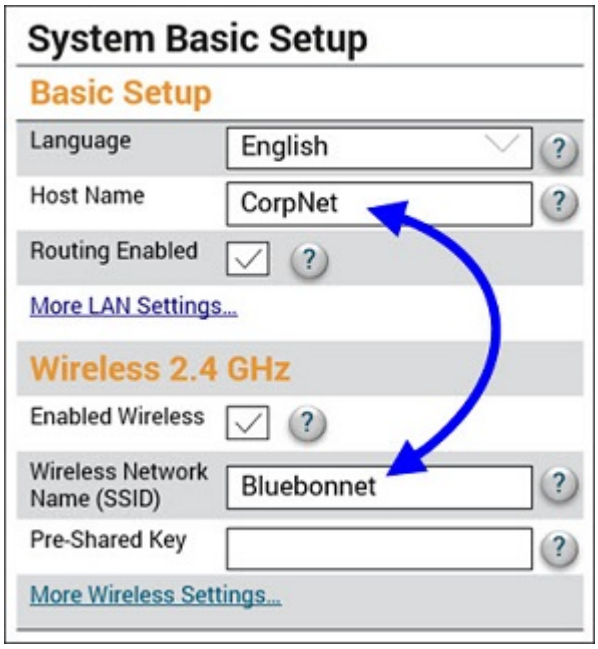
Some network administrators turn off SSID broadcasting in an attempt to hide a network, but many experts say that this can actually make a wireless LAN more vulnerable to attack. This is due to the fact that once hidden, your laptop or mobile device is going to start pinging over the air to try and find your router, telling anybody with a network scanner that you've got a hidden network at your house or job.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_SERVICE_SET_IDENTIFIERS_01_EH1]

Question 4: Incorrect

You are configuring a wireless access point and are presented with the image shown below. Which of the following is the most correct statement regarding the access point's configuration?



- The Host Name is what the users see in the list of available networks when they connect to the

access point.

- The Host Name and Wireless Network Name cannot be identical.
- ~~The Host Name provides additional security for the access point.~~
- The Wireless Network Name (SSID) is the name users see when they connect to the access point.

Explanation

The Host Name is the name users see when they try to connect to an access point.

The Wireless Network Name (SSID) is a unique name separate from the name users see when they connect to the wireless access point.

The name of an access point can be the same as the SSID. However, most wireless routers assign a unique SSID separate from the name users see when connecting the network.

A SSID is necessary for a secure network, while the Host Name provides no security benefits.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_SERVICE_SET_IDENTIFIERS_02_EH1]

Question 5: Incorrect

Which of the following types of wireless antenna is shown?

- Parabolic
- ~~Dipole~~
- Helical
- Yagi

Explanation

The antenna shown is a Yagi antenna, a special type of high-gain directional antenna.

A Parabolic antenna is a high-gain antenna that uses a curved surface.

A Dipole antenna is a straight electrical conductor measuring 1/2 wavelength from end to end that is connected to a radio-frequency feed line at the center.

A Helical antenna is an antenna consisting of one or more conducting wires wound into a helix.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_ANTENNA_TYPES_01_EH1]

Question 6: Correct

Which of the following types of wireless antenna is shown in the image?

- Dipole
- Helical
- Parabolic
- Yagi

Explanation

The antenna shown is a parabolic antenna, which is a high-gain antenna that uses a curved surface.

A yagi antenna is a special type of high-gain directional antenna.

A dipole antenna is a straight electrical conductor measuring 1/2 wavelength from end to end that is connected to a radio-frequency feed line at the center.

A Helical antenna is an antenna consisting of one or more conducting wires wound into a helix.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_ANTENNA_TYPES_02_EH1]

Question 7: Incorrect

Which of the following best describes a wireless hotspot?

- A physical location where people may obtain free internet access using Wi-Fi.
- A device used to create a Peer-to-Peer network.
- A networking hardware device that allows other Wi-Fi devices to connect to a wired network.
- ~~A device that repeats the wireless signal from your router to expand its coverage.~~

Explanation

A hotspot lets you connect an internet-capable device to the internet through a wireless, portable device, such as a phone. Hotspots often use third, fourth, and fifth generation (3G, 4G, and 5G) technology to provide this type of connection. Although personal phones are often used as hotspots, many businesses, such as airports and coffee shops, provide hotspots for their customers.

A wireless access point (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network. The WAP usually connects to a router as a standalone device via a wired network, but it can also be an integral component of the router itself.

An ad-hoc wireless network is where you set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router.

Range extenders only extend the coverage area, but do not connect your wireless access points to the network.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_CONNECTION_TYPES_01_EH1]

Question 8: Incorrect

You are a cybersecurity specialist. ACME, Inc. has hired you to install and configure their wireless network. As part of your installation, you have decided to use Wi-Fi Protected Access 2 (WPA2) security on all of your wireless access points. You want to ensure that the highest level of security is used. Which of the following encryption protocols should you use to provide the highest level of security?

- TKIP
- PSK
- CCMP
- ~~WEP~~

Explanation

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) provides the highest level of security. CCMP also provides data integrity and authentication and is an improvement over TKIP because it has a larger block size for encryptions and a larger key size. CCMP also has stronger algorithms. Using CCMP in conjunction with AES ensures a higher level of security than TKIP and RC4.

Wired Equivalent Privacy (WEP) is the original encryption protection mechanism developed for wireless networks and is less secure than CCMP.

Temporal Key Integrity Protocol (TKIP) encryption algorithm is an older encryption mechanism used to protect wireless communications. It has been replaced by CCMP and is considered obsolete.

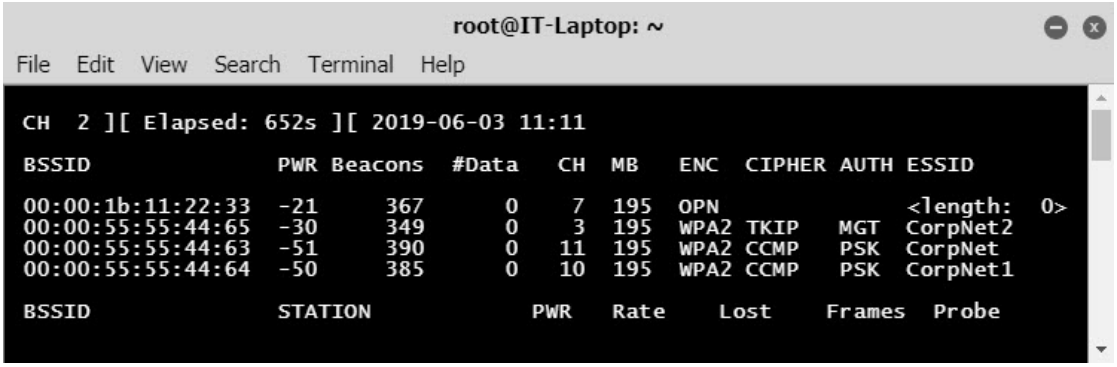
Pre-Shared Key (PSK) authentication was designed for home users without an enterprise authentication server and is a subset of CCMP. Most corporate networks should be configured to use Extensible Authentication Protocol (EAP) instead of PSK.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WI-FI_PROTECTED_ACCESS_01_EH1]

Question 9: Correct

You are a cybersecurity consultant. The company hiring you suspects that employees are connecting to a rogue access point (AP). You need to find the name of the hidden rogue AP so it can be deauthorized. Which of the following commands would help you locate the rouge access point from the wlp1s0 interface and produce the results shown?



- **aircrack-ng start wlp1s0**
- **airodump-ng wlp1s0mon**
- **airocrack-ng wlp1s0mon**
- **airmon-ng start wlp1s0**

Explanation

The command **airodump-ng wlp1s0mon** is used to display access points. From the output, you see that there is one access point currently being shown as length: 0. As you let this program run, the next time a person attaches to this access point, the name of the hidden/rogue point will be captured and displayed.

The command **airmon-ng start wlp1s0** is used to place the interface into monitor or promiscuous mode.

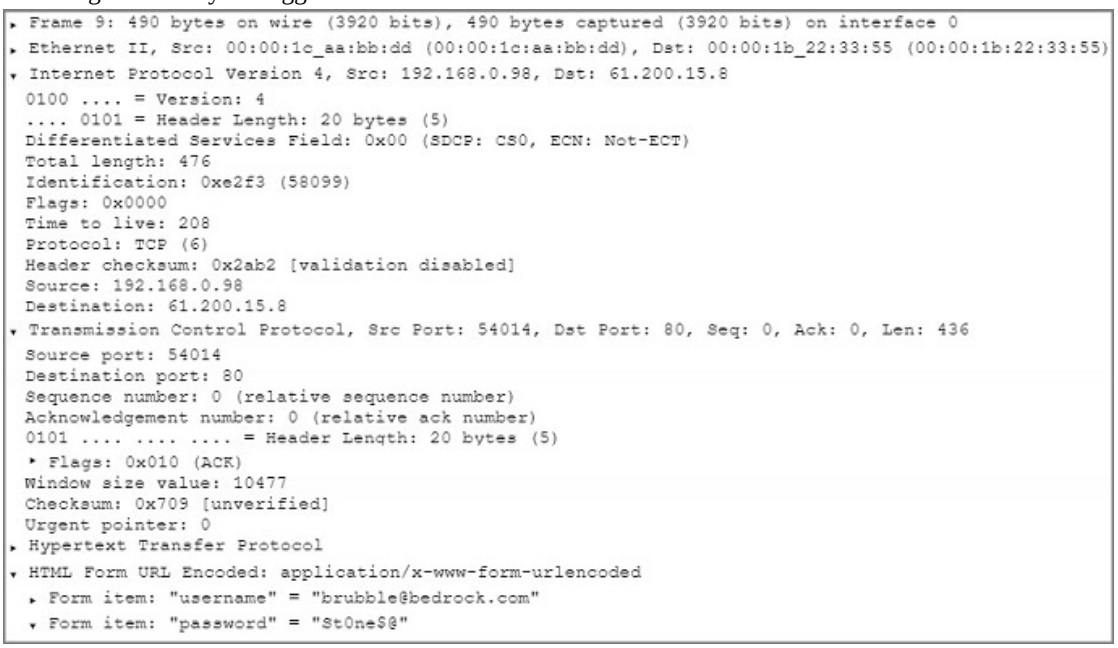
Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and an analysis tool for 802.11 wireless LANs. Airodump-ng is a subset of Aircrack.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_DISCOVER_HIDDEN_AP_01_EH1]

Question 10: Incorrect

You are the cybersecurity specialist for your company and have been hired to perform a penetration test. You have been using Wireshark to capture and analyze packets. Knowing that HTTP POST data can sometimes be easy prey for hackers, you have used the http.request.method==POST Wireshark filter. The results of that filter are shown in the image. After analyzing the captured information, which of the following would be your biggest concern?



- ~~Port 54014 has not been secured.~~
- Clear text passwords are shown.
- The checksum is unverified.
- Checksum validation has been disabled.

Explanation

The biggest concern for the captured packet would be that the username and password are being transmitted in clear text.

For HTTP POST packets, port 54014 is a common port, and the fact that the checksum was not validated is not a major concern.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_HTTP_POST_PACKETS_01_EH1]

Question 11: Correct

Which of the following best describes a rogue access point attack?

- A hacker getting a user or client to unintentionally connect to their access point instead of the legitimate point the user intended to use.
- A hacker advertising an access point using an extremely strong signal for malicious purposes.
- A hacker installing an unauthorized access point within a company.
- A hacker taking advantage of an access point that has not implemented the basic techniques to protect the network.

Explanation

A rogue access point is an unauthorized access point that has been set up in a company. These access points are sometimes set up by employees to bypass the existing limitation of the company's authorized access points. They can also be installed by a hacker who has gained physical access to the building.

A hacker taking advantage of an access point that has not implemented the basic techniques to protect the network is known as an access point misconfiguration attack.

A hacker getting a user or client to unintentionally connect to their access point instead of to the legitimate one the user intended to connect with is a client misassociation attack.

A hacker that adversities an access point using an extremely strong signal for malicious purposes is executing a promiscuous client attack. Since most users are looking for the strongest signal, when a promiscuous client's is offered, it is almost irresistible. Being blinded by the great connection being offered, they often forget to consider the fact that they may be opening themselves up to an attacker's clutches.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_ATTACK_TYPES_01_EH1]

Question 12: Incorrect

Which of the following best describes the purpose of the wireless attack type known as wardriving?

- To trick a user into using the hacker's access point.
- To find information that will help breach a victim's wireless network.
- To block a company's authorized wireless communications using radio noise or signals.
- ~~To capture user's critical information, such as passwords or bank account numbers.~~

Explanation

Wardriving, or war driving, is when a hacker drives around in their car and uses a laptop or smartphone to search for wireless networks they can then attempt to break into.

Although wardriving may eventually lead to the ability to capture a person's password or bank account numbers, this information cannot be gleaned until wardriving is used to discover the wireless networks.

The process of blocking a company's authorized wireless communications using radio noise or signals is called jamming.

Tricking a user into using the hacker's access point is called client misassociation.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_ATTACK_TYPES_02_EH1]

Question 13: Correct

You have just discovered that a hacker is trying to penetrate your network using MAC spoofing. Which of the following best describes MAC spoofing?

- The process of sending many Ethernet frames, each containing different source MAC addresses, to a switch.
- Driving around in a car and searching for wireless networks that allow MAC addresses to be captured.
- Changing a hacker's network card to match a legitimate address being used on a network.
- Configuring a network card to run in promiscuous mode, allowing MAC addresses to be captured.

Explanation

MAC spoofing is changing a network interface card's (NIC's) media access control (MAC) address to a different MAC address in an attempt to impersonate another computer or disguise the source of the transmission.

MAC flooding is the process of sending many Ethernet frames, each containing different source MAC addresses, to a switch.

Running a network card in promiscuous or monitor mode allows a user to use a sniffing tool to capture all packets transmitted over the network, which, of course, includes capturing MAC addresses, but is not considered MAC spoofing.

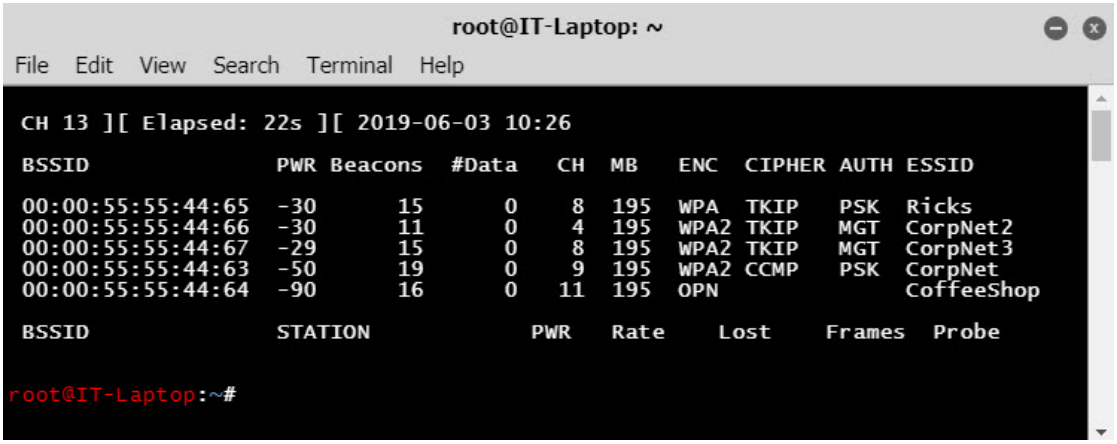
Wardriving is when a hacker drives around in their car and uses a smartphone or laptop to search for wireless networks they can then attempt to break into. Although wardriving is defined as using a car for this purpose, any means of transportation can be used, such as biking, walking, and jogging. These are then referred to as warbiking, warwalking, and warjogging.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WIRELESS_ATTACK_TYPES_03_EH1]

Question 14: Incorrect

From your Kali Linux computer, you have used a terminal and the airodump-ng command to scan for wireless access points. From the results shown, which of the following is most likely a rogue access point?



- CorpNet3
- ~~Ricks~~
- CoffeeShop
- CorpNet2

Explanation

According to the output, the power rating (PWR) of the CoffeeShop access point is very high compared to the other access points and is, therefore, most likely the rogue access point.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_ROGUE_WIRELESS_AP_EH1]

Question 15: Incorrect

The ACME company has decided to implement wireless technology to help improve the productivity of their employees. As the cybersecurity specialist for this company, you have the responsibility of seeing that the wireless network is as secure as possible. Which of the following best describes one of the first countermeasures that should be used to ensure wireless security?

- ~~Ensure that passphrases are used for WPA and WPA2 encryption.~~
- Actively perform radio frequency (RF) scanning to monitor the RF spectrum for rogue access points.
- Perform a pre-penetration test.
-

Use a Wi-Fi predictive planning tool to determine where to place your access points.

Explanation

Proper planning and implementation of the wireless network from the beginning will help make it more difficult for hackers to have any effect on your network after it's been installed. Therefore, one of the first countermeasures is to take advantage of Wi-Fi predictive planning tools, such as iBwave Design, AirMagnet Planner, and TamoGraph Site Survey.

After properly planning the implementation of the wireless network and installing and configuring access points, it is important to properly use passphrases to further protect against WPA/WPA2 cracking.

Penetration testing is the process of running several different types of tests to ensure that the wireless network is secure. Trying to perform a penetration test prior to planning and installing a wireless network has no benefit.

While scanning for rogue access points is always a wise step to take, your first concern is to ensure that the new wireless network is installed securely.

References

TestOut Ethical Hacker Pro - 13.1 Wi-Fi
[e_wifi_eh1.exam.xml Q_WI-FI_PREDICTIVE_PLANNING_&_TOOLS_EH1]