CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 10

Testing Wireless Networks

Objectives

- Given a scenario, research attack vectors and perform network attacks.
- Explain use cases of the following tools during the phases of a penetration test.

Lesson 10

Topic 10A

Discover Wireless Attacks

Securing Wireless Transmissions

- Wireless transmissions are sent through the air using a radio wave and are not protected by a bounded media, such as a cable.
  - Any human or device within range and direction of the signal will be able to intercept that signal
- Because of this, wireless networking technology is at a greater risk of compromise from several types of attacks.
- A malicious actor might be able to obtain your information, such as credit card numbers or login credentials, by using traffic sniffing.

Encrypt Data Transmissions

- Over the years, the predominant encryption standard, Wi-Fi Protected Access (WPA), has been used to secure data
- Over time it has evolved and improved:
  - **WPA2** is an improvement of WPA and replaced RC4 and TKIP with Counter Mode CBC-MAC Protocol (CCMP) using AES.
  - **WPA3** includes advanced features to secure wireless transmissions and is considered the most secure option

Eavesdropping Communications

- By sniffing traffic, you may be able to eavesdrop on communications between a client and an AP.
  - This is more likely possible in public, open Wi-Fi networks that don't incorporate encryption.
- Encrypted data will make your eavesdropping more difficult, however certain information is transmitted in cleartext
  - A client's MAC address, which can be used in a spoofing attack.

Deauthenticating Clients

- A deauthentication (deauth) attack will boot a victim from an AP and force them to reauthenticate.
  - Once booted, the victim will generate the required traffic needed for the malicious actor to capture the handshake.
- Used in several attacks:
  - Denial of service, evil twin, replay, and cracking attacks.
- Tools use to perform deauthentication include *airodump-ng* to sniff the handshake and *aireplay-ng* to deauthenticate all clients

Jamming a Signal

- Jamming disrupts a Wi-Fi signal by broadcasting on the same frequency as the target WAP, which blocks the signals
- Physical jamming devices can send disruptive signals to several wireless devices in a targeted area and trigger a DoS
- To launch a jamming attack, a malicious actor can either use a physical device or software jammer.
  - *Wi-Fi jammer* is a Python script that can jam the signals of all WAPs in an area.

Cracking WPA

- Most Wi-Fi networks today use WPA/WPA2 to provide a more robust method of preventing an attack.
- To crack a password, the team can try the following:
  - Attempt a dictionary attack
  - Launch a key reinstallation (KRACK) attack

Accessing the WPS PIN

- A malicious actor may be able to access a WPS device by using either a physical attack or brute force the PIN.
  - A physical attack takes advantage of the “push to connect” feature found on many routers.
- Another method is to determine the PIN number of the WPS device, using an online or offline brute force attack.
  - A malicious actor can launch an online attack using a tool called Reaver, which is included in Kali Linux.

Review Activity: Discover Wireless Attacks

- Discuss why wireless transmissions are especially vulnerable
- Ways used to encrypt data transmissions
- Explain how a deauth attack works
- Outline why someone would want to jam a Wi Fi signal
- Discuss ways to crack a WPA password or WPS PIN

Lesson 10

Topic 10B

Explore Wireless Tools

Attacking the WLAN

- Common plan of attack moves through the following phases:
  1. Begin by scanning across all channels looking for networks in range.
  2. Grade and sort the networks by signal strength (strongest to weakest).
  3. Gather information, and specifically assess any obvious vulnerabilities.
- Ensure that the capture device is equipped with the required tools and any companion software is installed as well.
  - The wireless card must support monitor mode and packet injection.
- The team will need to select an appropriate antenna.

Monitoring with Aircrack-ng

- A suite of utilities tools designed to test wireless network security
- The principal tools in the suite are as follows:
  - **Airmon-ng**—will enable and disable monitor mode on a wireless interface.
  - **Airodump-ng**—provides the ability to capture 802.11 frames to identify the BSSID of the WAP along with the MAC address of a victim client device.
  - **Aireplay-ng**—Inject frames to perform an attack to obtain the authentication credentials for WAP (generally performed using a deauth attack).

Discovering Kismet

- Kismet primarily works on Linux and OSX on most Wi-Fi and Bluetooth interfaces
  - Can capture packets and act as a wireless IDS.
- Once up and running, Kismet will search for wireless networks and identify what device is transmitting the traffic.
  - If any handshake packets are captured, Kismet will preserve them to attempt to crack the password later.
- In addition to specialized adapters, it can also capture traffic when using software defined radio (SDR) devices.

Assessing the WLAN with Wifite2

- Wifite2 is a wireless auditing tool you can use to assess the WLAN.
  - Once launched, you can begin a site survey and identify and display any active targets, along with and hidden access points.
  - Identify if the network advertises WPS and the type of encryption used
  - Can launch a variety of attacks to retrieve the password of a WAP
- If you select a group of targets, Wifite2 will proceed to attempt to capture handshakes and then attack the easiest targets first.
  - Once done it will then move to more challenging targets.

Exploring Bluetooth Enabled Devices

- Because Bluetooth uses a different method to transmit a signal, the team will need to use specialized tools launch an attack.
- Spooftooph is a tool used to spoof or clone a Bluetooth device
- Once spoofed, it will blend into the background and hide in plain sight whenever someone scans for Bluetooth devices.
  - Some devices are paired with interesting or essential hardware devices
  - When blending in, you can observe the interaction between devices.

Auditing with Fern

- Fern is a Python-based program used to test wireless networks and can recover WEP/ WPS/WPA/ keys using a variety of methods:
  - Bruteforce, dictionary, session hijacking, replay, and on-path attacks.
- Prior to using Fern, you'll need to make sure you have all essential dependencies such as:
  - Python, Aircrack-NG and Macchanger
- Fern is a commercial product; however, there is a free version as well that offers limited functionality and is part of Kali Linux

Unearthing the Power of EAPHammer

- EAPHammer is a toolkit with a wide range of features.
  - Provides several options that the team can use to launch an attack on a WPA2-Enterprise 802.11a or 802.11n network in an easy-to-use platform.
- Once you have all essential dependencies, you can plan an attack:
  - Launch a karma attack using an evil twin to trick someone into joining a bogus network.
  - Steal RADIUS credentials such as WPA-EAP and WPA2-EAP authentication
  - Conceal or cloak an SSID and perform captive portal attacks to capture AD credentials.

Testing the Wi-Fi with MDK4

- MDK4 is a powerful Linux based tool that features. It supports 2.4 to 5GHz and has nine attack modules, that include:
  - **Mode b:** create the appearance of many wireless networks
  - **Mode a**: authentication DoS with the intent of overwhelming an AP
  - **Mode p:** probes AP for SSID and bruteforce any hidden SSIDs
  - **Mode d**: sends a deauth to disconnect and disassociate all clients from an AP
  - **Mode w:** will provoke an IDS/IPS confusion attack

Review Activity: Explore Wireless Tools

- List steps to take prior to launching an attack on the WLAN
- Review the tools in the Aircrack-ng suite of tools
- Explain some of the features of Kismet
- Discuss how the team can use Wifite2 during the PenTest
- Outline some of the testing options when using Fern
- Describe how EAPHammer can be used to launch an attack
- Summarize some of the modules in MDK4

Lab Activity

Assisted Lab: Monitoring with Aircrack-ng

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

Lesson 10

Summary