WiFi Password Hacking

Ryan Scott

Grand Canyon University  
Information Security II

Prof. Christine Bakke

**Part 1: Hack a Router**

**Intercepting WiFi Traffic with Monitor Mode**

Using a wireless network adapter's monitor mode, you can capture and analyze all wireless network traffic within your adapter's range. Regardless of the packet's source or destination, the wireless adapter listens to all wireless traffic in monitor mode, (Stantzouris, n.d.). The intercepting of WiFi traffic is essential for analyzing networks, detecting intrusions, and hacking, all related to security.

In the demonstration, the goal of the aerodump-ng command was to capture packets from the target WiFi network. This command was used to scan for nearby WiFi networks and to capture information such as MAC addresses, signal strength, and channel information, (Stantzouris, n.d.). After identifying the target network, aerodump-ng was used to extract data packets transmitted over the network.

**How Deauthentication Attacks Work**

During a deauthentication Attack, the target device receives deauthentication packets, causing it to disconnect from the wireless network. Once the client device reconnects to the network, the attacker can capture various authentication packets, including login credentials, (Stantzouris, n.d.).

**How Big Are Password Dictionaries**

In the real world, attackers usually use password dictionaries that are considerably larger than the one shown in the video. Several million passwords can be stored in these dictionaries, including common passwords, words, and combinations of letters, numbers, and symbols, (CodeVerd, 2017). Attackers may also use specialized dictionaries that are tailored to the target organization or individual, such as lists of popular sports teams, music bands, or movie characters.

**How Deauth Leads to a Password Capture**

Deauthentication attacks can result in password capture by causing client devices to disconnect from a wireless network and then reconnect, sending authentication packets containing login credentials to the network. By capturing these packets, the attacker will be able to extract the login credentials and use them in order to gain access to the network, (CodeVerd, 2017).

**What is a Wifi “Handshake”**

WiFi handshakes refer to the process used by client devices and WiFi access points to establish secure connections. When a client device requests access to the access point, the access point responds with a series of packets that include information about the network as well as a cryptographic key as part of the “handshake” process, (CodeVerd, 2017). After encrypting the key with its own private key, the client device sends a packet to the access point which can be decrypted with its own private key. As a result, a secure connection can be established between the client device and the access point, enabling the client to access the network, (CodeVerd, 2017).

**How Does “aircrack-ng” Work?**

The “aircrack-ng” command is used to crack the password of a captured WiFi handshake. The command takes two parameters: the name of the captured handshake file and the name of the password dictionary file.

The command itself uses either a brute-force attack or a dictionary attack to try different combinations of passwords until it finds the correct one, (CodeVerd, 2017). A captured handshake file is compared with each password in the dictionary file, attempting to decrypt the encrypted key in the handshake with each password. Once the decrypted key matches the key in the handshake, the password is considered compromised, (CodeVerd, 2017).

However, the “aircrack-ng” command can take a long time to crack a password, depending on the complexity of the password and the size of the given password dictionary, (CodeVerd, 2017). In the video, a relatively simple password was used, so the program was able to crack it quickly. In real-world scenarios, it may take much longer to crack a more complex password.

**Part 2: Phreaked Out**

**False Network IDs**

Users are tricked into connecting to false network IDs by false wireless network names. Using names similar to legitimate access points that the user has previously connected to, attackers can create fake wireless access points, (Motherboard, 2014). As soon as the user connects to the fake access point, the attacker is able to intercept the user's data and steal sensitive information such as login credentials, credit card numbers, and personal details.

**Man-in-the-Middle**

When an attacker intercepts communication between two devices and impersonates each of them, a man-in-the-middle attack (MITM) occurs. As a type of phone security attack, a MITM attack involves intercepting communications between the phone and wireless network and relaying them to the attacker, allowing the attacker to eavesdrop on and manipulate the conversation between the two parties, (Motherboard, 2014). An attacker may be able to steal sensitive information or inject malicious code into a communication as a result.

**Snoopy**

Wireless network hacking tools such as Snoopy are used to scan for nearby devices in search of wireless networks to collect their metadata, (Motherboard, 2014). In addition to collecting information about the device's name and type, this tool can also collect information about the wireless networks to which the device has previously connected. As a result of this information, attackers can create false network IDs that mimic previously connected networks, increasing the likelihood that the user will be connected to the attacker's fake network, (Motherboard, 2014).

**Drone Control SkyJack**

As a result of exploiting weaknesses in drone communication protocols, Drone Control SkyJack can be used to compromise drone security. The tool is used to scan for nearby drones, and by injecting code into the communication between drones and the user's phone, the tool takes control of them, (Motherboard, 2014). An attacker may be able to take control of the drone, capture sensitive audio or video, or even crash it as a result of this.

# References

CodeVerd. (2017, June 9). *Hacking wifi Passwords (wpa/wpa2) - Ethical Hacking for absolute beginners - Episode #10* [Video]. YouTube. <https://www.youtube.com/watch?v=tgZ5KwrSouo>

Motherboard. (2014, June 5). *All The Ways To Hack Your Phone: Phreaked Out (Episode 3)* [Video]. YouTube. <https://www.youtube.com/watch?v=dysnKiXUlRU>

Stantzouris, T. (n.d.). *Deauthentication attack using Kali Linux*. <https://duthcode.com/Blog/blogPostContent.php?post=deauthentication-attack-using-kali-linux-18>