**WiFi Password Hacking**

Austin Johns

ITT-306

20 March 2021

Professor Kris Peters

**Part 1: Hack a Router**

After viewing “Perform Deauthentication Attack with Kali Linux Ethical Hacking for Absolute Beginners – Episode #9,” answer the following questions:

1. Explain what monitor mode is on a network card and why it is necessary to intercept WiFi traffic. In the demonstration, describe the goal of the aerodump-ng command and what it did during the demo.
   1. In the Kali Linux example from the video, monitor mode helps to monitor all internet traffic that’s received from a wireless network interface. By intercepting and monitoring all internet traffic from an internet source, the wireless card can make a record of all of the packets that are received from the internet without the filtering of other software. This is useful because the software allows for the monitoring of data without any further processing. As a network security monitor, this would be useful. In this software, aerodump-ng is used to capture the pure format that they are sent. It also shows all access points of the packet to help with sourcing.
2. Explain the strategy of a “Deauthentication Attack” and how it works to capture login credentials.
   1. When a client wants to disconnect form a network, the deauthentication frame is sent to the network. In this situation, the hacker sends a faked MAC address of the original client that they are trying to hack as a deauth frame. The network receives this and the network connection for the actual client is dropped. Then, the aerodump-ng program is run to complete the deauth attack. By monitoring the packet count, the deauth can be verified.

After viewing “Hacking WiFi Passwords (wpa/wpa2) - Ethical Hacking for Absolute Beginners - Episode #10,” answer the following questions:

1. The first part of the video uses the utility “Crunch” to create a short password dictionary. In the real world, what kind of password dictionary would be used?
   1. In the real world, a useful password dictionary that would be used would be one that is local on the device. A password dictionary is usually securely stored on the local computer for memorized connections.
2. The hacking process uses the deauth method as shown in the previous video. How does a deauth lead to a password capture?
   1. A deauth leads to a password capture by comparing known knowledge with a connection handshake. This handshake communicates information between the device and the network to create a secure connection.
3. Explain what a “handshake” is in WiFi terminology.
   1. A handshake creates information that is temporarily and locally stored on the device that comes from the network. The handshake creates some files that are designed to help the computer communicate with the network.
4. The final step in the hacking process is using “aircrack-ng” with two parameters. Explain how the command is able to identify a password.
   1. Using aircrack-ng, the command can identify a passkey by referencing previous knowledge about the password with the connection handshake. The command identifies the password by analyzing packet files with the previous knowledge to make comparative similarities between both. This comparison identifies the password in a format that the hacker can use.

**Part 2: Phreaked Out**

After viewing the “All the Ways to Hack Your Phone: Phreaked Out (Episode 3),” explain the following terms and the process used to compromise phone security:

1. False network IDs
   1. A false network ID is a malicious network that is created by a hacker to take advantage of past connections of a mobile device. By creating a false network ID that a smartphone has connected to in the past, the smartphone will automatically connect to it without the user’s permission. This is useful to the hacker because the phone will automatically start sending information through the false network. After all, the device has connected to it as it’s a primary internet connection.
2. Man-in-the-Middle
   1. By using a false network ID, the hacker that is controlling the false network now has full control between the device and the internet. For example, the device user can try to log into an account on the internet, but now the “Man in the middle” or the false network ID owner can receive all information from this login.
3. Snoopy
   1. Snoopy is a tracking data interception and profiling network. It can detect mobile devices and intercept data that will be sent to an outside network. A mobile phone can connect to snoopy without the user’s notice, and the hacker can track people through this hack because, on a drone, the network is mobilized. Potentially, the hacker can determine where a user lives through the GPS connection through the drone.
4. Drone Control SkyJack
   1. Skyjacking is a hacking method using a false network ID that is designed to take over the control of drones. Through multiple links between networks, a drone can connect to another drone to overtake control. One drone is designed by a hacker to take over control of another drone, and the drone now has no communication with the unsecured connection between the drone and the mobile device.