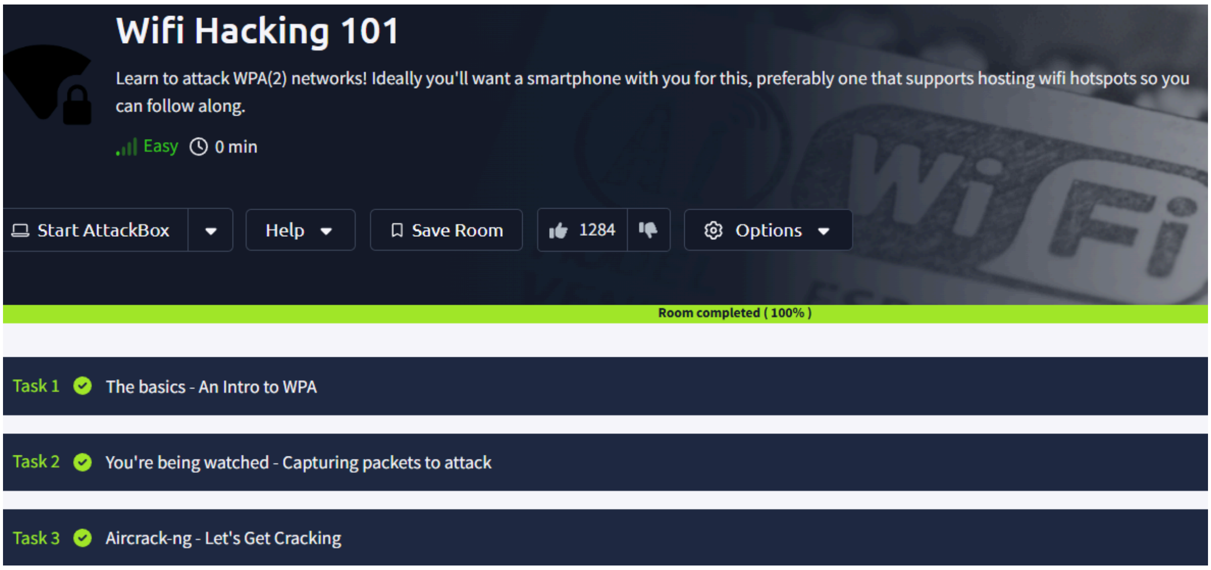
Wifi Attack

TrackHackMe Exercise



Wifi Hacking 101

Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.

Task 1 ✓ The basics - An Intro to WPA

Task 2 ✓ You're being watched - Capturing packets to attack

Task 3 ✓ Aircrack-ng - Let's Get Cracking

Minimum Length of a WPA2 Password

The minimum length for a WPA2 password (also known as a **pre-shared key** or **PSK**) is **8 characters**. WPA2 passwords can range from 8 to 63 characters in length.

4 Possible Attacks on Wi-Fi Networks

Here are four common types of attacks that can be used to compromise Wi-Fi networks:

1. **Brute-Force Attack**:
   - **Description**: In a brute-force attack, the attacker attempts to guess the password by systematically trying every possible combination of characters until the correct one is found. While this can be time-consuming, it's feasible if the password is weak or short.
   - **Prevention**: Use a long and complex password with a mix of upper and lower case letters, numbers, and special characters.
2. **Dictionary Attack**:
   - **Description**: Similar to a brute-force attack, a dictionary attack involves trying a list of pre-defined passwords or passphrases, usually derived from commonly used words or phrases. It's faster than a brute-force attack but relies on the password being something predictable or common.
   - **Prevention**: Avoid using common words, phrases, or simple combinations in your password.
3. **Evil Twin Attack**:
   - **Description**: In an evil twin attack, an attacker sets up a rogue Wi-Fi access point that mimics a legitimate one. Users may unknowingly connect to this fake network, allowing the attacker to intercept their data or credentials.
   - **Prevention**: Always verify the SSID of the network before connecting, and use VPNs for added security.
4. **Deauthentication Attack**:

  - **Description**: A deauthentication attack forces devices on a Wi-Fi network to disconnect by sending deauthentication frames. When the devices attempt to reconnect, the attacker can capture the WPA2 handshake, which can then be used to crack the password using brute-force or dictionary attacks.
  - **Prevention**: Use WPA3 if available, as it includes protections against this type of attack. Additionally, using strong, complex passwords makes it more difficult for attackers to crack the WPA2 handshake.

Sources:

"Computer Security: Principles and Practice" by William Stallings and Lawrie Brown.

Standards documentation such as IEEE 802.11i.

Security websites e.g OWASP, SANS Institute, or specific cybersecurity blogs and forums.