

## Challenge 04 – WPA / WPA2 PSK Attack

David Murillo Santiago  
Professor Pugh  
IS-3513  
5 November 2023

### INTRODUCTION

---

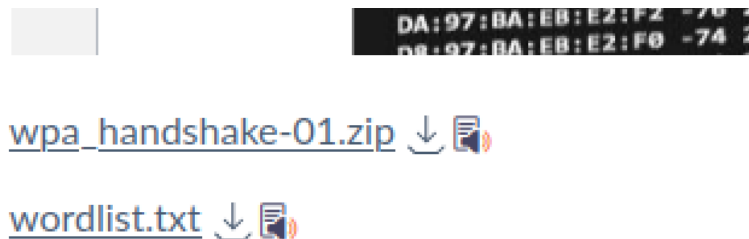
In this challenge, I will engage in a practical exercise involving a WPA or WPA2 Pre-Shared Key (PSK) attack using aircrack-ng within a Kali Linux Virtual Machine (VM).

### PROCESS

---

#### Step 1: Download the required files.

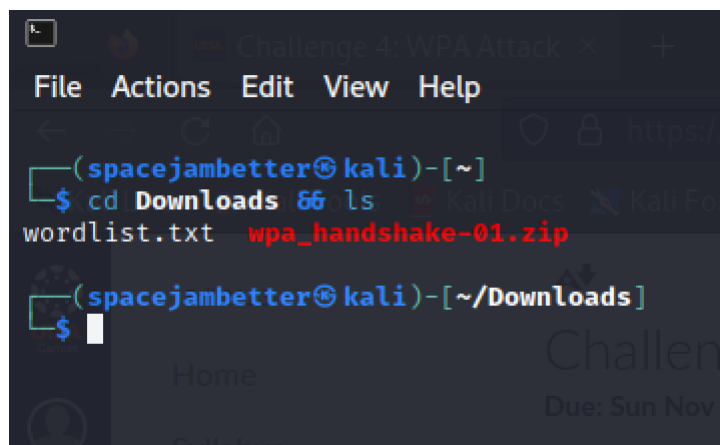
To begin, I downloaded the following files from canvas:



#### Choose a submission type

---

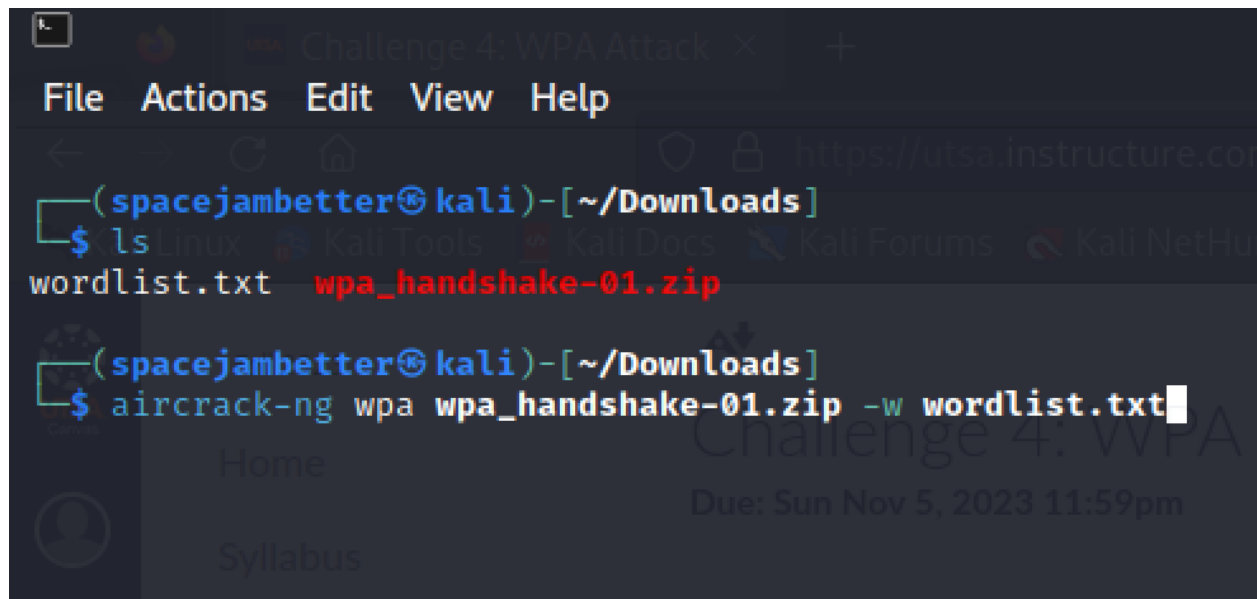
I downloaded wpa\_handshakw-01.zip and wordlist.txt.



Proof of download of the aforementioned files.

## Step 2: Run Aircrack-ng

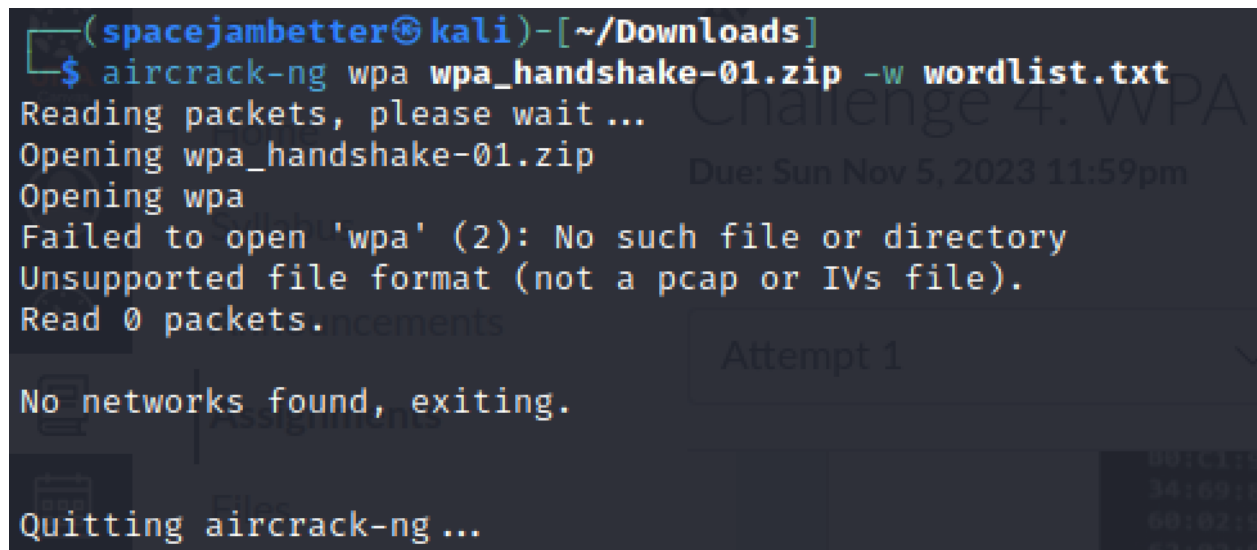
Next, I began the aircrack-ng attack by entering the following:

A terminal window with a dark background. The prompt is `(spacejambetter@kali)-[~/Downloads]`. The user has entered `$ ls` and the output is `wordlist.txt wpa_handshake-01.zip`. The user then enters `$ aircrack-ng wpa wpa_handshake-01.zip -w wordlist.txt` and the cursor is at the end of the command.

```
(spacejambetter@kali)-[~/Downloads]
$ ls
wordlist.txt  wpa_handshake-01.zip

(spacejambetter@kali)-[~/Downloads]
$ aircrack-ng wpa wpa_handshake-01.zip -w wordlist.txt
```

I entered "aircrack-ng wpa wpa\_handshake-01.zip -w wordlist.txt."

A terminal window showing the output of the aircrack-ng command. The prompt is `(spacejambetter@kali)-[~/Downloads]`. The output is:  
`$ aircrack-ng wpa wpa_handshake-01.zip -w wordlist.txt`  
`Reading packets, please wait ...`  
`Opening wpa_handshake-01.zip`  
`Opening wpa`  
`Failed to open 'wpa' (2): No such file or directory`  
`Unsupported file format (not a pcap or IVs file).`  
`Read 0 packets.`  
`No networks found, exiting.`  
`Quitting aircrack-ng ...`

```
(spacejambetter@kali)-[~/Downloads]
$ aircrack-ng wpa wpa_handshake-01.zip -w wordlist.txt
Reading packets, please wait ...
Opening wpa_handshake-01.zip
Opening wpa
Failed to open 'wpa' (2): No such file or directory
Unsupported file format (not a pcap or IVs file).
Read 0 packets.
No networks found, exiting.
Quitting aircrack-ng ...
```

That time the command did not work.

```
(spacejambetter@kali)-[~/Downloads]
$ ls
wordlist.txt  wpa_handshake-01.zip

(spacejambetter@kali)-[~/Downloads]
$ unzip wpa_handshake-01.zip
Archive:  wpa_handshake-01.zip
  inflating: wpa_handshake-01.cap

(spacejambetter@kali)-[~/Downloads]
$ ls
wordlist.txt  wpa_handshake-01.cap  wpa_handshake-01.zip

(spacejambetter@kali)-[~/Downloads]
$
```

I realized that I forgot to unzip the downloaded file and therefore I could not use an aircrack-ng because I did not have the required capture file.

```
(spacejambetter@kali)-[~/Downloads]
$ aircrack-ng wpa wpa_handshake-01.cap -w wordlist.txt
```

Next, I entered the aircrack-ng command to initiate the key recovery attack.

```
Aircrack-ng 1.7
[00:00:05] 9676/10000 keys tested (2113.87 k/s)

Time left: 0 seconds 96.76%

KEY FOUND! [ password123 ]

Master Key   : 2C 0F 9F 60 F3 68 7B 2B 17 D6 F2 70 C0 A2 45 59
              47 6C 2B FE C8 8A 35 F0 99 4F 43 8F 3E BF 0C 05

Transient Key : E2 8B EC 01 2D 10 BC D9 4C 17 1C 61 89 24 48 FB
                1E 91 D4 0B 3E 83 80 CA C0 30 8D 8C 31 FA C3 22
                E6 DF E6 33 9B B0 FE 4B B8 F9 C0 E6 48 25 54 C2
                72 C3 E0 DE 6F 98 F5 E5 B4 1C 52 BA 87 8E DA 15

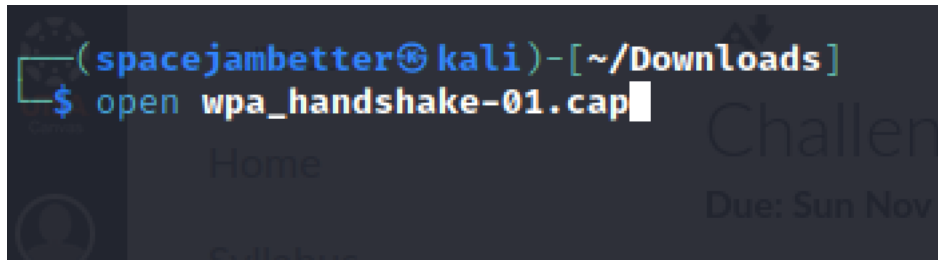
EAPOL HMAC   : 32 2A 43 B6 AC 16 46 CE EF 8E 94 07 9C 3A D3 FC

(spacejambetter@kali)-[~/Downloads]
$
```

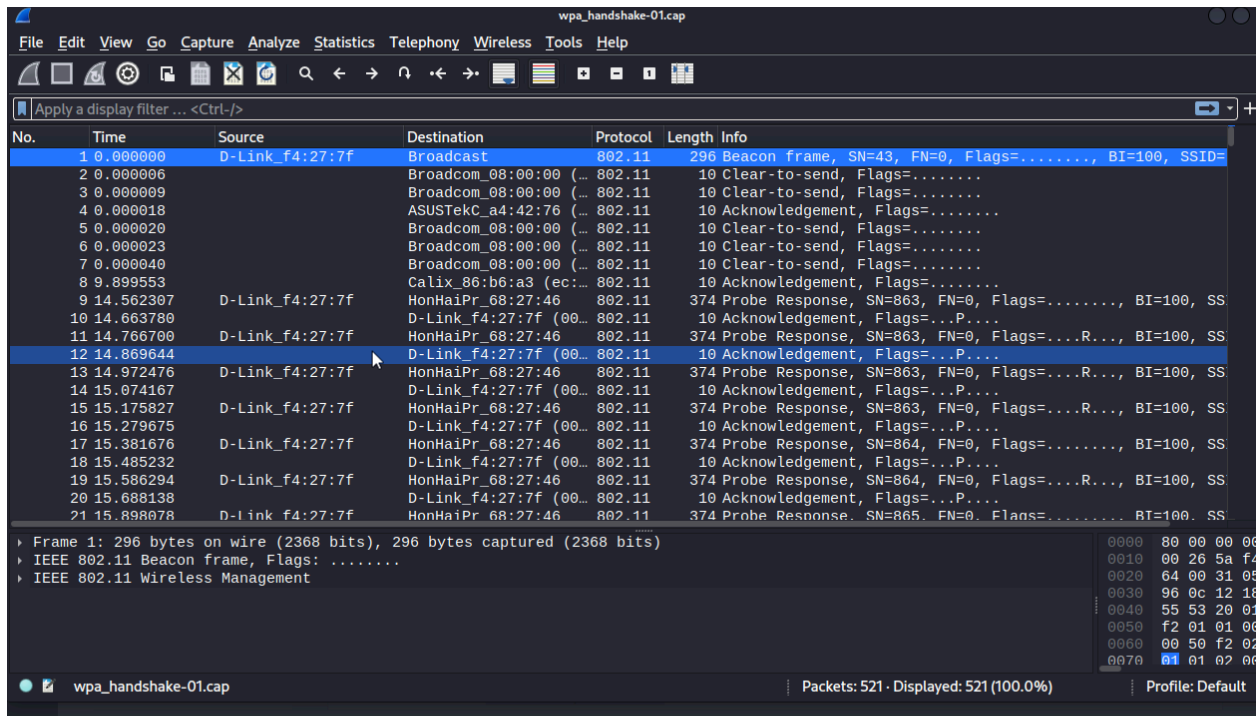
The key value was 'password123' was shown in the screenshot.

### Step 3: Wireshark

Next, I opened the capture file on Wireshark.

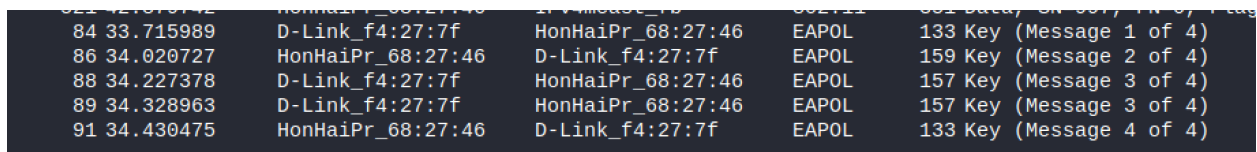


I used the open command to open the file.



Screenshot of the file open on Wireshark.

Next, I clicked on 'protocol' pane to sort the protocol order to have 802.11 packets on the top and EAPOL on the bottom.



On Wireshark I was able to find the 4-way handshake. The 4 way-handshake secures an encrypts connections between Wi-Fi clients and Wi-Fi access points. The EAPOL protocol is a common 4-way handshake protocol.

## Questions:

### What is the difference between WPA and WPA2?

WPA and WPA2 are security protocols designed to secure wireless networks. Both adhere to the IEEE 802.11i standards; however, WPA2 offers more robust security measures compared to WPA. WPA uses a TKIP encryption, a form of encryption which dynamically changes keys for each data packet, enhancing

the security of wireless communications. On the other hand, WPA2 uses AES encryption and a 4-way handshake, providing a higher level of security by employing strong encryption and a secure key exchange process to protect wireless communications from modern security threats.

**Did this exercise make you think about how a WiFi router should be configured?**

This exercise has revealed to me the different forms of Wi-Fi security. Originally, if your Wi-Fi router was configured to use WEP security, you would be highly vulnerable to hacking techniques such as a man in the middle attack. This is because WEP relies on static encryption keys, meaning the keys are unchanging. Based on this lab and the research I conducted, I found that WPA2 is the safest choice for securing a network, as it incorporates dynamic encryption keys, strong encryption methods like AES, and a robust 4-way handshake, providing a higher level of security and resistance against modern hacking techniques.

**What could you do to make your WiFi router more secure (IP address, router admin login credentials, network password, disabling services)?**

One thing you could do to enhance the security of your Wi-Fi router is change the default IP. For most routers, when you purchase them, it is common for them to come with a default IP address which facilitates the initial setup of the network. After the network is set up, if you leave the default IP, attackers can easily locate and access your router's login page. Additionally, disabling UPnP (Universal Plug and Play) on your WiFi router significantly enhances security by preventing automatic port access, thus reducing the risk of unauthorized devices or applications compromising your network. Updating the router's admin login credentials is another good step to prevent unauthorized access. Finally, you should use WPA2 as the security protocol for your Wi-Fi network because it provides stronger encryption and security compared to WPA. By implementing all the mentioned methods, you will significantly boost your router's security.

---

## LIMITATIONS/CONCLUSION

In this challenge I learned about WPA and WPA2, and how the protocols are used to secure the Wi-Fi connections.

---

## REFERENCES

Brother UK: 'WPA vs WPA2: What's the Differences' <https://www.brother.co.uk/business-solutions/insights-hub/resources/managed-print-services/wpa-vs-wpa2#:~:text=WPA2%20was%20created%20to%20be,all%20verified%20Wi%2DFi%20hardware.>

I used this link to understand the differences between WPA and WPA2.

FLAMINGO Project: 'How does WPA and WPA2 work?' [https://www.youtube.com/watch?v=-Q\\_WXeEf8Fw](https://www.youtube.com/watch?v=-Q_WXeEf8Fw)

I used this website to better understand the history of WEP, WPA, and WPA2 and how they work.

CSO: 'How to secure your router and home network' <https://www.csoonline.com/article/556941/how-to-secure-your-router-and-home-network.html>

I used this article to learn about different ways I could protect a Wi-Fi router.

Resmo: 'What is UPnP? -Why It's Still a Security Risk-' <https://www.resmo.com/blog/what-is-upnp#:~:text=Unauthorized%20Access%3A%20UPnP%20may%20allow,data%2C%20or%20perform%20malicious%20actions>.

I used this article to learn about Universal Plug and Play and why it's a security risk.