

Wireless Exploitation

Lecture II

Instructor: C. Pu (Ph.D., Assistant Professor)

puc@marshall.edu



Ethical Wireless Hacking

- A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range.
- The devices in a wireless network have the freedom to be in motion, but be in connection with the network and share data with other devices in the network.
- One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.

Ethical Wireless Hacking

- Wireless networks are widely used and it is quite easy to set them up.
- They use IEEE 802.11 standards.
- A wireless router is the most important device in a wireless network that connects the users with the Internet.

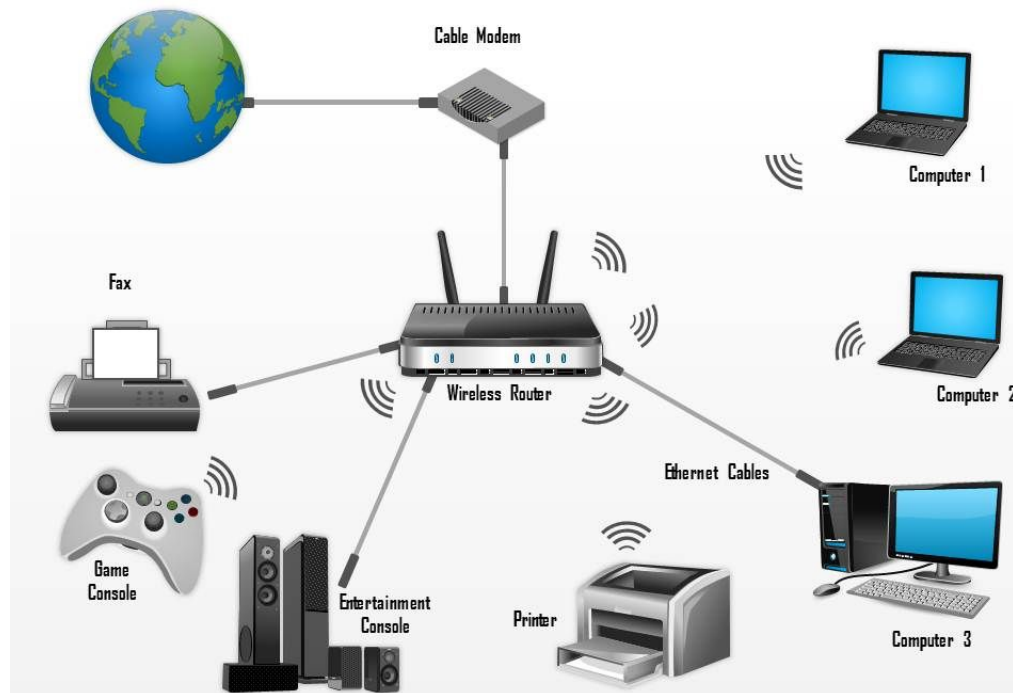


A Wireless Router

Ethical Wireless Hacking

- In a wireless network, we have Access Points which are extensions of wireless ranges that behave as logical switches.

Home Wireless Network Diagram





Ethical Wireless Hacking

- Although wireless networks offer great flexibility, they have their security problems.
- A hacker can sniff the network packets without having to be in the same building where the network is located.
- As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location.
- Most attackers use network sniffing to find the SSID and hack a wireless network.
- When wireless cards are converted in sniffing modes, they are called monitor mode.



CommView for WiFi

- CommView for WiFi is a tool for monitoring wireless 802.11 a/b/g/n/ac/ax networks.
- To use this product, you must have a compatible wireless adapter.
- To enable the monitoring features of your wireless adapter, you will need to use a special driver that comes with this product

CommView for WiFi

- Go to <https://www.tamos.com/download/main/ca.php>

The screenshot shows the Tamosoft website's download page for CommView for WiFi. The page features a navigation menu at the top with links for Home, Products, Purchase, Download, Support, Partners, Contact, and About Us. A featured offer section highlights a 'super bundle' for site surveys and spectrum analysis. Below this, there is a 'Download CommView for WiFi' button and a list of compatible adapters. The adapters are categorized into 802.11ax (Wi-Fi 6) and 802.11ac. The 802.11ax section includes Intel AX200, AX201 and Killer Wi-Fi 6 AX1650x, AX1650s. The 802.11ac section includes Alfa Networks AWUS1900 and AWUS036ACM. A 'Live Support' button is visible on the right side of the page.

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale (higher is better)
Intel AX200, AX201	2.4 GHz/5 GHz	Integrated	Windows 10	Recommended See tech. notes	Not rated
Killer Wi-Fi 6 AX1650x, AX1650s	2.4 GHz/5 GHz	Integrated	Windows 10	Recommended See tech. notes	Not rated

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale (higher is better)
Alfa Networks AWUS1900, AWUS036ACM	2.4 GHz/5 GHz	USB	Windows 8 or higher	Recommended See tech. notes	5

CommView for WiFi

■ Click “Download CommView for WiFi”

The screenshot shows the TamoSoft website's download page for CommView for WiFi. The page includes a navigation menu, a featured offer section, and a list of compatible wireless adapters. A red box highlights the 'Download CommView for WiFi' button.

Download CommView for WiFi

CommView for WiFi is a tool for monitoring wireless 802.11 a/b/g/n/ac/ax networks. To use this product, you must have a compatible wireless adapter. To enable the monitoring features of your wireless adapter, you will need to use a special driver that comes with this product.

Alternatively, you may want to consider using the standard, non-wireless CommView edition that will allow you to capture your own inbound and outbound wireless network packets, without capturing the traffic generated by other wireless stations.

If your card is not on the list, please click [here](#) for the technical information, or take advantage of our special offer and get a compatible adapter free of charge!

[Download CommView for WiFi](#)

The following adapters have been tested and are compatible with CommView for WiFi:

802.11ax (Wi-Fi 6) Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale (higher is better)
Intel AX200, AX201	2.4 GHz/5 GHz	Integrated	Windows 10	Recommended See tech. notes	Not rated
Killer Wi-Fi 6 AX1650e, AX1650h, AX1650s	2.4 GHz/5 GHz	Integrated	Windows 10	Recommended See tech. notes	Not rated

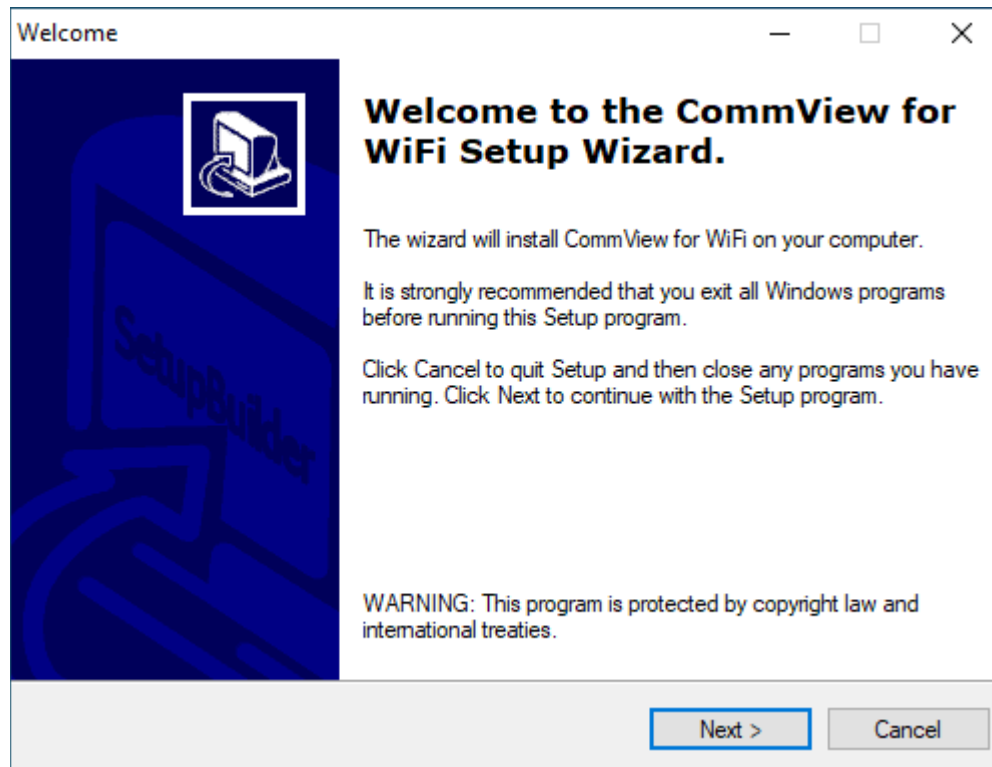
802.11ac Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale (higher is better)
Alfa Networks AWUS1900, AWUS036ACM	2.4 GHz/5 GHz	USB	Windows 8 or higher	Recommended See tech. notes	5



CommView for WiFi

- Install CommView for WiFi
 - Follow all default settings





CommView for WiFi

- Install WiFi adapter driver

Driver Installation

DRIVER INSTALLATION GUIDE

CommView for WiFi is a tool for monitoring wireless 802.11 networks. You **must** have a compatible wireless adapter to use this product. In order to enable the monitoring features of your wireless adapter, you will need to use the special drivers that come with this product.

When CommView for WiFi is not running, your adapter will be able to connect and communicate with other wireless hosts or access points, as it normally does. When CommView for WiFi is running, your adapter will be put in passive, promiscuous monitoring mode with no connectivity.

The following supported, compatible adapters have been found on your computer:

- None

The following adapters that have not been tested, but that may be compatible, have been found on your computer:

- None

Please make a selection from the following options and click "Next":

I want to install the driver for my compatible adapter.

I want to test my untested adapter that may be compatible.

I have a compatible adapter, but I have not plugged it in yet. Tell me what to do after I plug in the compatible adapter.

Next >

For your reference, you can find the complete list of supported, compatible adapters by visiting the following page:

<https://www.tamos.com/products/commwifi/adapterlist.php>

CommView for WiFi **may** support other adapters. If your adapter is not listed above, please refer to the online [FAQ](#) for up-to-date information.

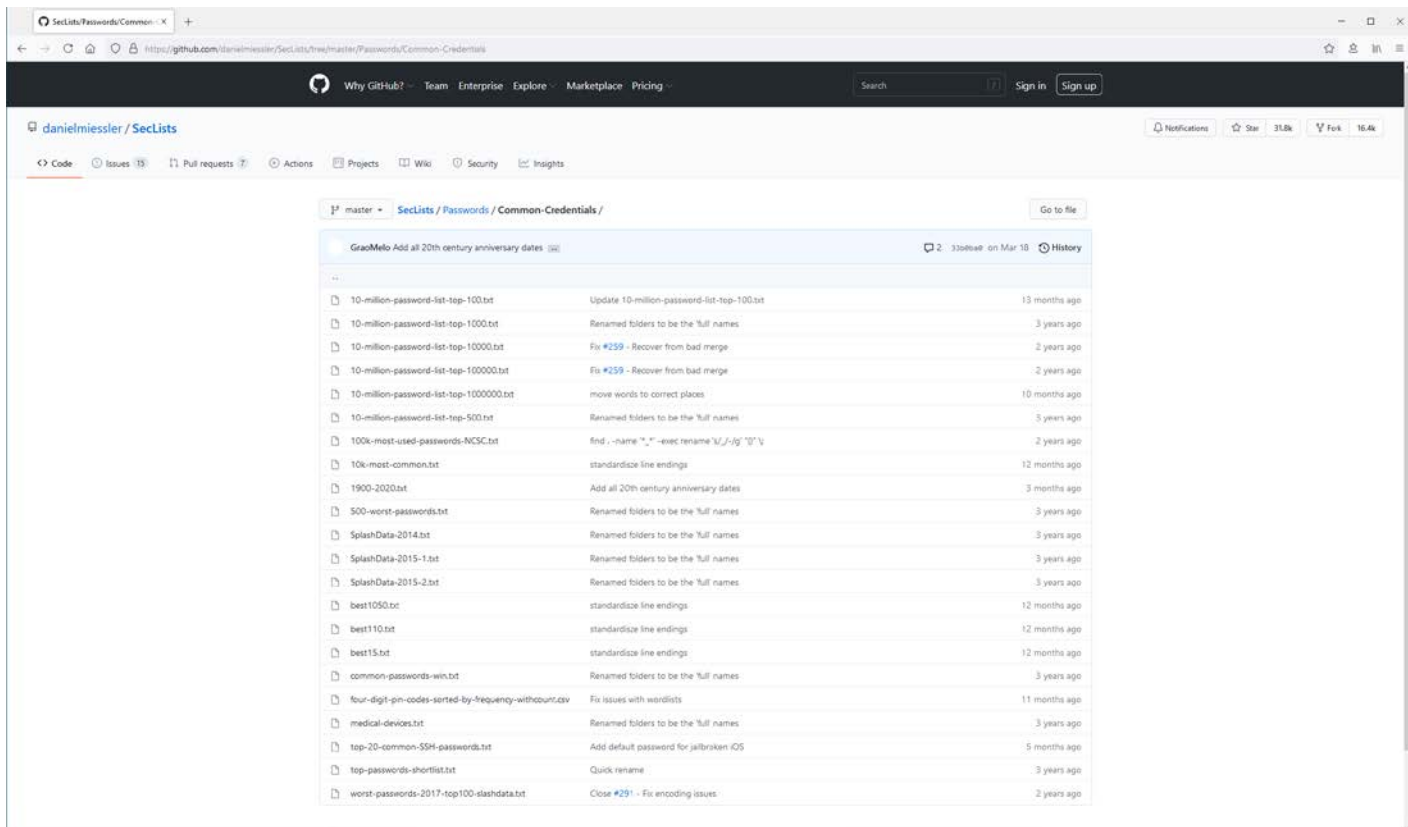


CommView for WiFi

- Capture handshake packets for Aircrack-ng to crack WiFi password
 - Watch <https://www.youtube.com/watch?v=2BffQsIDh48>
 - Sometimes, you will see 3-way handshake packets. It also works.
 - Export “Wireshark/Tcpdump Format” with the file name wpa.full
- There are some chances that handshake packets will not be captured.
 - In that case, you will need to continue until handshake packets are captured.

Password Files

- Go to Common-Credentials, download one password file, and save it on Desktop



The screenshot shows a web browser displaying the GitHub repository page for 'SecLists/Passwords/Common-Credentials' by danielmiessler. The page is viewed on the 'master' branch. The repository contains a list of files and folders, including various password lists and scripts. The files listed include:

File Name	Commit Message	Time Ago
10-million-password-list-top-100.txt	Update 10-million-password-list-top-100.txt	13 months ago
10-million-password-list-top-1000.txt	Renamed folders to be the full names	3 years ago
10-million-password-list-top-10000.txt	Fix #259 - Recover from bad merge	2 years ago
10-million-password-list-top-100000.txt	Fix #259 - Recover from bad merge	2 years ago
10-million-password-list-top-1000000.txt	move words to correct places	10 months ago
10-million-password-list-top-500.txt	Renamed folders to be the full names	3 years ago
100k-most-used-passwords-NCSC.txt	find -name "*" -exec rename 's/./[0-9]'	2 years ago
10k-most-common.txt	standardize line endings	12 months ago
1900-2020.txt	Add all 20th century anniversary dates	3 months ago
500-worst-passwords.txt	Renamed folders to be the full names	3 years ago
SplashData-2014.txt	Renamed folders to be the full names	3 years ago
SplashData-2015-1.txt	Renamed folders to be the full names	3 years ago
SplashData-2015-2.txt	Renamed folders to be the full names	3 years ago
best1050.txt	standardize line endings	12 months ago
best110.txt	standardize line endings	12 months ago
best15.txt	standardize line endings	12 months ago
common-passwords-win.txt	Renamed folders to be the full names	3 years ago
four-digit-pin-codes-sorted-by-frequency-without.csv	Fix issues with wardlists	11 months ago
medical-devices.txt	Renamed folders to be the full names	3 years ago
top-20-common-SSH-passwords.txt	Add default password for jailbroken iOS	5 months ago
top-passwords-shortlist.txt	Quick rename	3 years ago
worst-passwords-2017-top100-slashdata.txt	Close #291 - Fix encoding issues	2 years ago



Ethical Wireless Hacking: Aircrack-ng

- Aircrack-ng is a complete suite of tools to assess WiFi network security.
- It focuses on different areas of WiFi security:
 - Monitoring: Packet capture and export of data to text files for further processing by third party tools
 - Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
 - Testing: Checking WiFi cards and driver capabilities (capture and injection)
 - Cracking: WEP and WPA PSK (WPA 1 and 2)

Ethical Wireless Hacking: Aircrack-ng

- Go to <https://www.aircrack-ng.org/>



[Home](#)
[Forum](#)
[Wiki](#)
[GitHub](#)
[Blog](#)
[IRC](#)

Documentation

[Getting started](#)
[Installation](#)
[Compatibility](#)
[Screenshots](#)
[In movies](#)
[Main Docs](#)

Misc

[Support](#)
[Resources](#)
[Contribute](#)
[Contact](#)
[License](#)
[Code of Conduct](#)

Download



- [Aircrack-ng 1.6](#)
 - [Sources](#)
 - [Windows](#)
- [Changelog](#)

[More downloads...](#)

Fresh news

Aircrack-ng 1.6 25 Jan 20

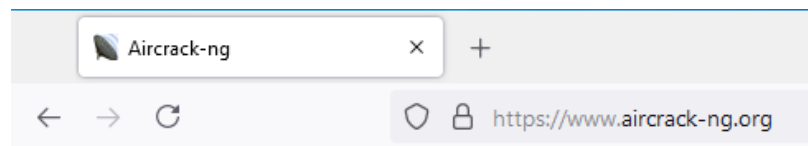
This release brings a ton of improvements. Along with bug fixes and improvements for a lot of tools, we have huge improvements under the hood thanks to code cleanup, deduplication, and reorganization of the source code. We also improved our buildbot, and added integration tests.

The most notable changes are in Airodump-ng, it now sees WPA3 and OWE. Its rates now takes into account 802.11n/ac and aren't limited to 54Mbit anymore. It has PMKID detection, and some basic UTF-8 among other things.



Ethical Wireless Hacking: Aircrack-ng

- Click “Windows” download option



[Home](#)
[Forum](#)
[Wiki](#)
[GitHub](#)
[Blog](#)
[IRC](#)

Documentation

[Getting started](#)
[Installation](#)
[Compatibility](#)
[Screenshots](#)
[In movies](#)
[Main Docs](#)

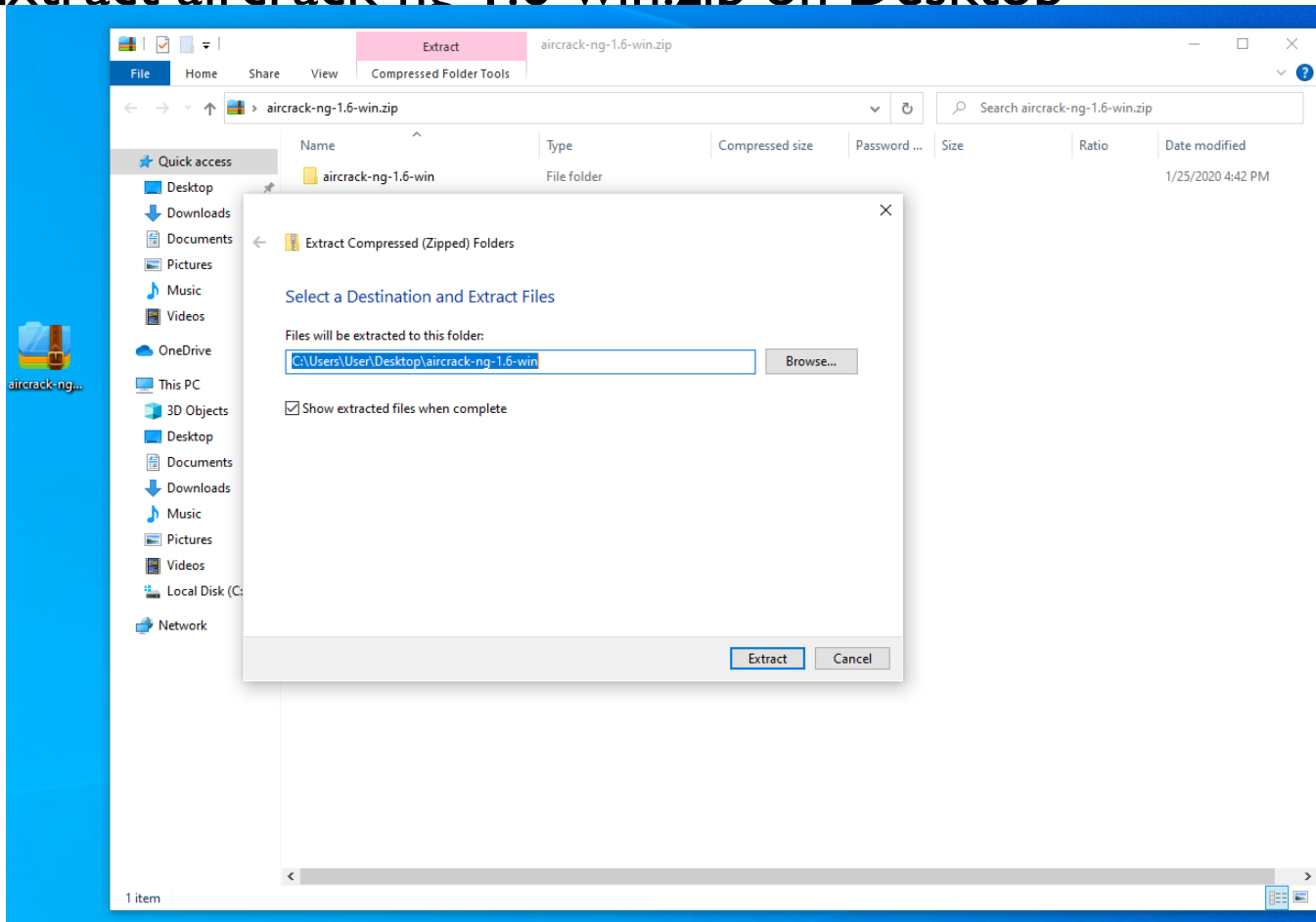
Download



- [Aircrack-ng 1.6](#)
 - [Sources](#)
 - [Windows](#)
- [Changelog](#)

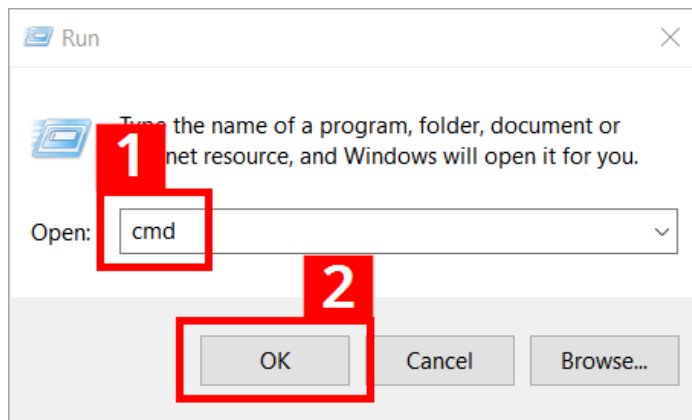
Ethical Wireless Hacking: Aircrack-ng

- Extract aircrack-ng-1.6-win.zip on Desktop



Ethical Wireless Hacking: Aircrack-ng

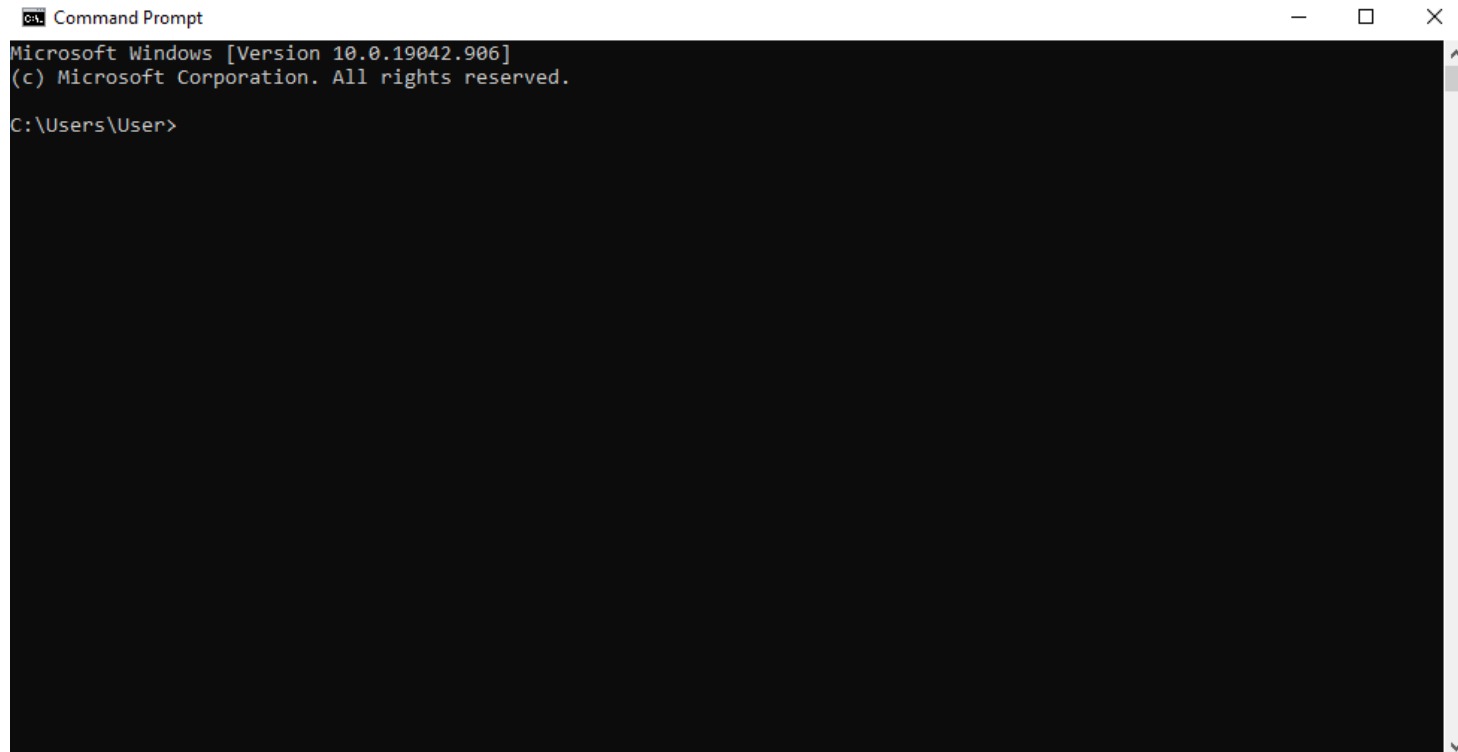
- Press the key combination [Windows] + [R]
- Enter “cmd” into the entry field (1)
- Press the “OK” button (2)





Ethical Wireless Hacking: Aircrack-ng

- After doing so, the cmd.exe will open with the following screen:



```
Command Prompt
Microsoft Windows [Version 10.0.19042.906]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>
```

Ethical Wireless Hacking: Aircrack-ng

- To start the program file (aircrack-ng), you also need to switch to the storage location.
- Type
- `cd Desktop\aircrack-ng-1.6-win\bin`

```
cmd Select Command Prompt
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>cd Desktop\aircrack-ng-1.6-win\bin
C:\Users\User\Desktop\aircrack-ng-1.6-win\bin>
```

Ethical Wireless Hacking: Aircrack-ng

- To start the program file (aircrack-ng), you also need to switch to the storage location.
- Type
-

```
Command Prompt
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>cd Desktop\aircrack-ng-1.6-win\bin

C:\Users\User\Desktop\aircrack-ng-1.6-win\bin>aircrack-ng -w C:\Users\User\Desktop\500-worst-passwords.txt C:\Users\User\Desktop\wpa.full.cap
```

aircrack-ng command

password file

Captured
handshake packets

Ethical Wireless Hacking: Aircrack-ng

- If CommView for WiFi captured packets from multiple networks, you will need to specify the target network by entering the index number.

```
Opening test1.pcap please wait...
Read 192 packets.

# BSSID          ESSID          Encryption
1 00:0D:58:EF:88:09 tmpAP          No data - WEP or WPA
2 00:0D:58:EF:88:0A Vodafone      No data - WEP or WPA
3 00:0D:58:EF:88:0B veles3        No data - WEP or WPA
4 14:CC:20:C1:CB:2C Lekonora      No data - WEP or WPA
5 24:A4:3C:FE:22:36 Intertelecom_FREE No data - WEP or WPA
6 28:10:7B:94:BB:29 ogogo         WPA (0 handshake, with PMKID)
7 F4:EC:38:A6:2F:EA TPLIN         WPA (0 handshake)
8 F8:1A:67:E5:05:62 Smile)       WPA (1 handshake)

Index number of target network ? █
```

- E.g., if the target network is named “Smile)”, you will enter 8 and press [Enter]

Ethical Wireless Hacking: Aircrack-ng

- Cracking begins...
- Now all you have to do is wait till you see (KEY Found (your key is here 😊)).

```
ca. Command Prompt - aircrack-ng -w C:\Users\User\Desktop\500-worst-passwords.txt C:\Users\User\Desktop'

                                Aircrack-ng 1.6

[00:00:06] 65/499 keys tested (10.01 k/s)

Time left: 43 seconds                                13.03%

                                Current passphrase: daniel

Master Key      : FE 37 1F 89 FC BF D1 E4 B6 02 43 9F 79 F1 03 C1
                  42 06 A4 36 34 F5 61 FE 1E FA 45 63 F0 5A 89 12

Transient Key   : 18 9C C1 E0 33 54 2E 3F 41 40 2D 73 32 BF 85 52
                  42 5F 6E E7 EB 2B 2D 36 D1 E1 DD 73 BF D7 F2 8B
                  DE C9 E2 F6 26 D4 5E 03 35 66 97 D3 0B 5B 6D 7A
                  F9 3A F9 AE 90 F7 E5 54 FB 2F 9E 3F 0B E2 F9 12

EAPOL HMAC     : 02 15 91 04 AC 4B 87 B6 AA E0 12 35 72 2D 55 EC
```