

Forum:[Hack Forums](#)

Thread: [Obtaining WiFi Passwords](#)

hea1th - July 29, 2025, 12:28 pm

Firstly im not sure if this is the right sub-forum if im wrong ill delete the post and move it to the correct one

I want to learn how wifi password cracking is done for personal reasons i see alot of people use linux when hacking/cracking not sure if this is a requirement however i currently run Win11 i can change if needed pointers to guides or programs that can help me do this on win11 would be appreciated

DeathPenalty666 - July 29, 2025, 12:42 pm

(Jul 29, 2025 12:28 PM)hea1th Wrote: [\[CITE\]](#) Firstly im not sure if this is the right sub-forum if im wrong ill delete the post and move it to the correct one

I want to learn how wifi password cracking is done for personal reasons i see alot of people use linux when hacking/cracking not sure if this is a requirement however i currently run Win11 i can change if needed pointers to guides or programs that can help me do this on win11 would be appreciated

First you will need a usb wifi adaptor with packet injection and monitoring to achieve this. this specific kind of adaptor wil allow to send the request and capture que handshake, leaving you at the end with a psk the password. There is different kind of method

Wi-Fi Attacks

Major Wi-fi attacks are done by setting up a rogue Access Point.

Evil Twin attack:

Here the attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

Wi-Fi Attacks | Ethical Hacking

Wi-Fi Attacks

Major Wi-fi attacks are done by setting up a rogue Access Point.

Evil Twin attack:

Here the attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

Jamming Signals:

An attacker can disrupt the network connection by jamming the signal, there are functioning tools for this purpose also called as creating noise.

Misconfiguration Attacks:

If a router is set up using the default configuration, weak credentials, weak encryption algorithms, then the attacker can easily break into the network.

Honey spot Attack:

An attacker can set up fake access points/hotspots with the same SSID as that of a public wi-fi AP; thus, he can set traps for the users who connect to these AP's.

Unauthorised/Ad-Hoc connection attacks:

An attacker can enable an AD-HOC connection in a user's system utilizing Trojan, malware, or if an employee is already using an AD-HOC connection to share the internet with peers. The attacker can compromise the connection operating in AD-HOC mode since this mode does not provide stronger encryption to the connection.

Methodology:

An attacker has to find out the wireless devices through methods like war-walking, warchalking, war-driving. There are tools like NetStumbler, Kismet to find out wireless access points and capture the traffic.

Once he captures the traffic of that connection, he has to analyse the traffic using protocol analysers to identify the authentication method used, SSID, and connected devices and how to compromise the connection.

Depending upon the protocol used for encryption, he has to follow different tools/methods to break into the network and gain access to the unauthorised network.

there is always a possibility that you CANT hack it. If your router is up to date, properly config and use Strong password you can have some hard time.

most used tools are wifite wifite2 airchack

??????????? - July 29, 2025, 12:51 pm

(Jul 29, 2025 12:28 PM)hea1th Wrote: [\[CITE\]](#) Firstly im not sure if this is the right sub-forum if im wrong ill delete the post and move it to the correct one

I want to learn how wifi password cracking is done for personal reasons i see alot of people use linux when hacking/cracking not sure if this is a requirement however i currently run Win11 i can change if needed pointers to guides or programs that can help me do this on win11 would be appreciated

For reliable WPA/WPA2 cracking you'll almost always use Linux (e.g., Kali Live USB) because most Wi-Fi chipsets only support monitor mode and packet injection under Linux, but you can do it on Windows 11 if you plug in a compatible USB adapter (like an Atheros AR9271) and install the Aircrack-ng suite plus Hashcat for GPU-accelerated cracking. The basic workflow is: enable monitor mode, capture the 4-way handshake with airodump-ng (or Wifite to automate), then run aircrack-ng or hashcat against your capture with a wordlist. Check out the official Aircrack-ng docs and the "Wi-Fi Hacking with Aircrack-ng" guide on Null Byte for step-by-step instructions, and always only test networks you own or have explicit permission to assess.

hea1th - July 29, 2025, 1:25 pm

(Jul 29, 2025 12:51 PM)??????? Wrote: [\[CITE\]](#) For reliable WPA/WPA2 cracking you'll almost always use Linux (e.g., Kali Live USB) because most Wi-Fi chipsets only support monitor mode and packet injection under Linux, but you can do it on Windows 11 if you plug in a compatible USB adapter (like an Atheros AR9271) and install the Aircrack-ng suite plus Hashcat for GPU-accelerated cracking. The basic workflow is: enable monitor mode, capture the 4-way handshake with airodump-ng (or Wifite to automate), then run aircrack-ng or hashcat against your

capture with a wordlist. Check out the official Aircrack-ng docs and the “Wi-Fi Hacking with Aircrack-ng” guide on Null Byte for step-by-step instructions, and always only test networks you own or have explicit permission to assess.

Do you have some sort of video on yt for this or have I gotta walk in blind

???????????? - July 29, 2025, 1:36 pm

(Jul 29, 2025 01:25 PM)hea1th Wrote: [\[CITE\]](#) Do you have some sort of video on yt for this or have I gotta walk in blind

I do not use yt. You need to do your own research.

hea1th - July 29, 2025, 1:44 pm

(Jul 29, 2025 01:36 PM)??????? Wrote: [\[CITE\]](#) I do not use yt. You need to do your own research. sound mate will do thanks for the info

DramaKing - July 29, 2025, 2:24 pm

(Jul 29, 2025 12:28 PM)hea1th Wrote: [\[CITE\]](#) Firstly im not sure if this is the right sub-forum if im wrong ill delete the post and move it to the correct one

I want to learn how wifi password cracking is done for personal reasons i see alot of people use linux when hacking/cracking not sure if this is a requirement however i currently run Win11 i can change if needed pointers to guides or programs that can help me do this on win11 would be appreciated

Microsoft Network Monitor is a non-hacking tool and could technically capture the needed frames and be combined with a web tool to get a hashfile, but you'd be making it way more difficult on yourself. You could be capturing for hours. Just putting a WiFi adapter in monitor mode is problematic. It's a lost cause.

(Jul 29, 2025 01:25 PM)hea1th Wrote: [\[CITE\]](#) Do you have some sort of video on yt for this or have I gotta walk in blind

David Bombal used to do tutorials on little else. He made so many that he would rehash old materials. Hearing him say "Don't use weak passwords" got annoying.

(Jul 29, 2025 12:51 PM)??????? Wrote: [\[CITE\]](#) For reliable WPA/WPA2 cracking you'll almost always use Linux (e.g., Kali Live USB) because most Wi-Fi chipsets only support monitor mode and packet injection under Linux, but you can do it on Windows 11 if you plug in a compatible USB adapter (like an Atheros AR9271) and install the Aircrack-ng suite plus Hashcat for GPU-accelerated cracking. The basic workflow is: enable monitor mode, capture the 4-way handshake with airodump-ng (or Wifite to automate), then run aircrack-ng or hashcat against your capture with a wordlist. Check out the official Aircrack-ng docs and the “Wi-Fi Hacking with Aircrack-ng” guide on Null Byte for step-by-step instructions, and always only test networks you own or have explicit permission to assess.

Aircrack-ng actually does support Windows. I'll be. It won't be the same, of course.

Lastly, you need a high-end GPU. There will hardly be a network using 'spiderman' as a password.

Chrome - July 31, 2025, 4:45 am

(Jul 29, 2025 12:42 PM)arlalala01 Wrote: [\[CITE\]](#) First you will need a usb wifi adaptor with packet injection and monitoring to achieve this. this specific kind of adaptor wil allow to send the request and capture que handshake, leaving you at the end with a psk the password. There is different kind of method

Wi-Fi Attacks

Major Wi-fi attacks are done by setting up a rogue Access Point.

Evil Twin attack:

Here the attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

Wi-Fi Attacks | Ethical Hacking

Wi-Fi Attacks

Major Wi-fi attacks are done by setting up a rogue Access Point.

Evil Twin attack:

Here the attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

Jamming Signals:

An attacker can disrupt the network connection by jamming the signal, there are functioning tools for this purpose also called as creating noise.

Misconfiguration Attacks:

If a router is set up using the default configuration, weak credentials, weak encryption algorithms, then the attacker can easily break into the network.

Honey spot Attack:

An attacker can set up fake access points/hotspots with the same SSID as that of a public wi-fi AP; thus, he can set traps for the users who connect to these AP's.

Unauthorised/Ad-Hoc connection attacks:

An attacker can enable an AD-HOC connection in a user's system utilizing Trojan, malware, or if an employee is already using an AD-HOC connection to share the internet with peers. The attacker can compromise the connection operating in AD-HOC mode since this mode does not provide stronger encryption to the connection.

Methodology:

An attacker has to find out the wireless devices through methods like war-walking, warchalking, war-driving. There are tools like NetStumbler, Kismet to find out wireless access points and capture the traffic.

Once he captures the traffic of that connection, he has to analyse the traffic using protocol analysers to identify the authentication method used, SSID, and connected devices and how to compromise the connection.

Depending upon the protocol used for encryption, he has to follow different tools/methods to break into the network and gain access to the unauthorised network.

there is always a possibility that you CANT hack it. If your router is up to date, properly config and use Strong password you can have some hard time.

most used tools are wifite wifite2 airchack

Looks promising, might do some testing on this.

