

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] "Forgot" your WiFi password? Here's a fix](#)

ra1d - January 28, 2017, 6:03 am

How to extract passwords from WiFi's you've connected to on Windows

Open up CMD or Windows PowerShell with Administration permissions.

#step1

We want to list the wireless networks that the computer has connected to.

We can do that by going into netsh, type netsh in the terminal.

Then type the following

Code wlan show profiles

#step2

Now we want to export the profile that we are interested in.

NOTE: If the WiFi name contains spaces then make sure to write the profile name in quotation marks.

Code wlan export profile %ProfileName% folder=c:\sampleDirectory

Now you when you've exported the profile you will see that the password is encrypted if you open it in a text editor.

Let's fix this by adding key=clear to the end of that command.

So it will look like this:

Code wlan export profile %ProfileName% folder=c:\sampleDirectory key=clear

#step3

Use the following command to import the profile on new computers.

Code wlan add profile filename="%PathAndFileName%" user=all

#step4

You've now acquired the password to your WiFi, it will be located inside the .xml file that is exported.

It can be found under <keyMaterial>passwordHere</keyMaterial>

Save your wireless network profiles and setup your new computer in no time with a quick Batch script, or whatever you decide to write a script in.

Very useful for IT technicians, operations, etc...

Simple but very neat to have.

Also it doesn't work for all WiFi's, some have different authentication methods.

s?hane - January 28, 2017, 6:06 am

Thanks for the tutorial, gonna try it now. :)

TopKekeroni - January 28, 2017, 6:07 am

Very useful tutorial, thanks for sharing this with us!

Phil - January 28, 2017, 6:15 am

Very simple and easy to follow, can be very useful for many purposes.

Spoiler ([Click to View](#))

ra1d - January 28, 2017, 6:37 am

(Jan 28, 2017 07:15 AM)DehPhil Wrote: [\[CITE\]](#) Very simple and easy to follow, can be very useful for many purposes.

Spoiler ([Click to View](#))

It definitely can be useful for a lot of things.
Glad you liked it.

Lufasu - January 29, 2017, 2:31 am

Amazing tutorial ra1d :D now i can do cool stuff

Craze* - January 29, 2017, 2:49 am

So my neighbour was RATED by me one month ago and now i will find his WiFi pass and have for a long time free wifi

Thanks :D

DroidX - January 29, 2017, 3:19 am

Thanks man? Nice tutorial

ra1d - February 1, 2017, 3:40 pm

Glad to hear you peeps enjoyed this tutorial.

I'll be releasing some more PowerShell tutorials soon. :-)

HackRain - February 2, 2017, 3:41 pm

-Added to sticky.

Tested and working on win10 enterprise.

Stendoh - February 2, 2017, 3:43 pm

wow I must be too stupid to do this tbh

?eptic - February 2, 2017, 3:45 pm

Another HQ thread from rai1d. I'm sure a lot of people will benefit from this tutorial.

ra1d - February 4, 2017, 2:45 am

Thanks for the feedback.

Do not hesitate to contact me if you have a question or want something explained.

TheMockingBird - February 4, 2017, 2:49 am

Hmmm well very nice tutorial. ?

But can't we access to the password in plain text trough the network card status --> wireless properties --> security and then show password ? :(

ra1d - February 4, 2017, 2:52 am

(Feb 4, 2017 03:49 AM)TheMockingBird Wrote: [\[CITE\]](#) Hmmmm well very nice tutorial. ?

But can't we access to the password in plain text trough the network card status --> wireless properties --> security and then show password ? :(

This allows for IT technicians, penetration testers and likewise to write scripts that can automate the process.

Also in case you're using a shared computer for example at a library, you will see all the WiFi profiles.

There's a lot of uses, those are only some of them.

HackYouBitch16 - February 5, 2017, 10:38 am

tried and it worked, Thanks for the tutorial.

x4binode - February 6, 2017, 1:59 pm

Thanks for the tutorial, HQ post!

GZUZ - February 7, 2017, 2:41 pm

Would it make sense if my neighbor forgot his wifi and and I talk to him (SE) so I get connected for a short amount of time to his wifi with my Laptop and do the things explained above once I am back @home?

Also it does work on Windows 64 Bit, right?

Lante - February 7, 2017, 2:49 pm

(Feb 4, 2017 03:52 AM)ra1d Wrote: [\[CITE\]](#) This allows for IT technicians, penetration testers and likewise to write scripts that can automate the process.

Also in case you're using a shared computer for example at a library, you will see all the WiFi profiles.

There's a lot of uses, those are only some of them.

Luckily no one has to re-invent the wheel, a batch script extracting saved WiFi passwords exists and works just fine over here:

<http://lallouslab.net/2016/05/14/wifirevealscript-a-script-to-reveal-all-the-saved-wifi-passwords-in-windows-7-and-above/>

source code [\(Click to View\)](#)

Code @echo off

```
::  
:: (c) Elias Bachaalany <lallousz-x86@yahoo.com>  
:: Batchography: The Art of Batch Files Programming  
::
```

```
setlocal enabledelayedexpansion
```

```
:main
```

```
    title WiFiPasswordReveal v1.0 (c) lallouslab.net - The Batchography book
```

```
    echo.
```

```
    echo Reveal all saved WiFi passwords Batch file script v1.0 (c) lallouslab.net
```

```
    echo.
```

```
    echo Inspired by the book "Batchography: The Art of Batch Files Programming"
```

echo.

:: Get all the profiles

call :get-profiles r

:: For each profile, try to get the password

:main-next-profile

for /f "tokens=1* delims=," %%a in ("%r%") do (

call :get-profile-key "%%a" key

if "!key!" NEQ "" (

echo WiFi: [%%a] Password: [!key!]

)

set r=%%b

)

if "%r%" NEQ "" goto main-next-profile

echo.

pause

goto :eof

::

:: Get the WiFi key of a given profile

:get-profile-key <1=profile-name> <2=out-profile-key>

setlocal

set result=

FOR /F "usebackq tokens=2 delims=:" %%a in (

`netsh wlan show profile name^="%%~1" key^=clear ^| findstr /C:"Key Content") DO (

set result=%%a

set result=!result:~1!

)

(

endlocal

set %2=%result%

)

goto :eof

::

:: Get all network profiles (comma separated) into the result result-variable

:get-profiles <1=result-variable>

setlocal

set result=

FOR /F "usebackq tokens=2 delims=:" %%a in (

`netsh wlan show profiles ^| findstr /C:"All User Profile") DO (

set val=%%a

set val=!val:~1!

```
    set result=%!val!,!result!  
  )  
  (  
    endlocal  
    set %1=%result:~0,-1%  
  )  
  
goto :eof
```

Might be interesting to add to the OP for whoever is looking for a run&profit .bat file.

Infinity™ - February 10, 2017, 7:35 pm

Very useful tutorial. Great share mate, It works on my windows 10 . Additional, Lante's shared working also.

arefinsharif - February 11, 2017, 11:57 pm

I need more screenshot how do you it.

oziadovicomareo - February 12, 2017, 7:47 am

hey brothers

Do u think that this method is effecient
please answer me

ShadeMilcaras - February 12, 2017, 2:02 pm

Would it be possible to write the commands on a single bat file, so it works fast and sneaky? Thx
haha

lebouskii - February 12, 2017, 7:47 pm

(Jan 29, 2017 03:49 AM)Craze* Wrote: [\[CITE\]](#) So my neighbour was RATED by me one month ago
and now i will find his WiFi pass and have for a long time free wifi

Thanks :D
how did you give him it ?

arvinzx20 - February 13, 2017, 3:16 am

Let me try this method if this is working in my laptop.thanks

lusr - February 13, 2017, 4:35 am

(Jan 28, 2017 07:03 AM)ra1d Wrote: [\[CITE\]](#) method.
Hey! Thanks for sharing!

I knew how to see password of WiFi's you've connected to on Windows, but it was different and (I think) very simple:

Go to "Network Manager", right-click on a saved wifi Network, select "Wireless Properties", select "Security" and check the box for "show characters" (you need Admin permission, like in your method).

Is there any additional benefit to do your method?

Thanks again.

ra1d - February 13, 2017, 6:25 am

(Feb 13, 2017 05:35 AM)gabr Wrote: [\[CITE\]](#) Hey! Thanks for sharing!

I knew how to see password of WiFi's you've connected to on Windows, but it was different and (I think) very simple:

Go to "Network Manager", right-click on a saved wifi Network, select "Wireless Properties", select "Security" and check the box for "show characters" (you need Admin permission, like in your method).

Is there any additional benefit to do your method?

Thanks again.

This method allows you to get the WiFi passwords from all users on the PC.

Siktah - February 22, 2017, 2:50 am

Finally got a use for this. Worked well.

For the Win8 machine it was:

1. Open CMD with Admin privledges
2. Type Code netsh
3. Type Code wlan show profiles
4. Type Code wlan export profile "wifiprofilenamehere" folder=C:\folderyouchoose key=clear
(Where C:\ is the drive of your USB stick if you are exporting externally)

Netflix076 - March 3, 2017, 8:04 am

thanks man this really helped I was almost calling my provider but not need anymore

Hydraxus - March 3, 2017, 6:52 pm

Oh boy, ra1d sharing all these tips and tricks. Was a nice read, this is written very well. Cheers my dude!

zask - March 23, 2017, 7:43 pm

This is how I did it ;)

Luckily I didn't have to recode because I made this script before you even created this thread.
Completely automated just in case anyone needs it.
No errors either

```
Code @echo off
for /f "tokens=4 delims=: " %%A in ('netsh wlan show profiles') do (
for /f "tokens=2,* delims=: " %%B in ('netsh wlan show profiles "%%A" key^=clear ^| find /i "Key
Content" ') do set "pw=%%C"
)
echo "%pw%"
pause
```

alwayslate - March 24, 2017, 1:28 pm

Interesting. I also tried it with my ISP's EAP account, it allocates 2mb to anyone with the same ISP's account so you can use other peoples routers as a kind of guest mode when visiting them.

Nothing too interesting came out of it as far as I could see but it does make me wonder if you could access the main ISP account or router while connected with an EAP account.

zask - March 25, 2017, 11:05 am

(Mar 24, 2017 01:28 PM)alwayslate Wrote: [\[CITE\]](#) Interesting. I also tried it with my ISP's EAP

account, it allocates 2mb to anyone with the same ISP's account so you can use other peoples routers as a kind of guest mode when visiting them.

Nothing too interesting came out of it as far as I could see but it does make me wonder if you could access the main ISP account or router while connected with an EAP account.

Mhm, you should make it then.

lobo30 - March 26, 2017, 6:06 am

'wlan' is not recognized as an internal or external command??

zask - March 26, 2017, 11:58 am

(Mar 26, 2017 06:06 AM)lobo30 Wrote: [\[CITE\]](#) 'wlan' is not recognized as an internal or external command??

Its an issue with your computer, not the code. Possibility a problem with one of your drivers. You should google up the issue, ask on stack overflow. It also could be because the netsh wlan command isnt supported on your computer, could be many possibilities, but I don't think it will take long to resolve the issue.

Press the windows key + R at the same time, when the run dialog box appears type Cmd in it. When the black box appears type this in it.

Netsh wlan show profiles

If it still says the same error, its definitely a issue with the computer not the code.

h600600s - April 16, 2017, 9:23 pm

we can also just do netsh wlan show profile wifiname key=clear. It is good as well.

h600600s - April 18, 2017, 3:54 pm

we can also just do netsh wlan show profile wifiname key=clear. It is good as well.

SeanBanks98 - June 1, 2017, 2:48 am

Very useful thank you. Saved me a lot of time.

Knzaaks - June 2, 2017, 1:19 am

It's funny, I was just trying to do that yesterday.

Thank you !

Siciliano - June 2, 2017, 1:30 am

Thanks for the tutorial OP, If you have free time you can make a tutorial how to change a password on the wi-fi, would be very helpful! Thanks again. ?

Mad76e - June 4, 2017, 11:14 am

Or simply

You need to be admin to see the WPA key tho

Also easy to do

ra1d - June 4, 2017, 1:28 pm

(Jun 4, 2017 11:14 AM)Smnfz Wrote: [\[CITE\]](#) Or simply

You need to be admin to see the WPA key tho

Also easy to do

The method in OP drops all saved wifi passwords on the machine.

Pretty sure anyone with a brain knows the method you showed.

reignQ - June 4, 2017, 2:06 pm

(Jan 28, 2017 07:03 AM)ra1d Wrote: [\[CITE\]](#) How to extract passwords from WiFi's you've connected to on Windows

Open up CMD or Windows PowerShell with Administration permissions.

#step1

We want to list the wireless networks that the computer has connected to.

We can do that by going into netsh, type netsh in the terminal.

Then type the following

Code wlan show profiles

#step2

Now we want to export the profile that we are interested in.

NOTE: If the WiFi name contains spaces then make sure to write the profile name in quotation marks.

Code wlan export profile %ProfileName% folder=c:\sampleDirectory

Now you when you've exported the profile you will see that the password is encrypted if you open it in a text editor.

Let's fix this by adding key=clear to the end of that command.

So it will look like this:

Code wlan export profile %ProfileName% folder=c:\sampleDirectory key=clear

#step3

Use the following command to import the profile on new computers.

Code wlan add profile filename="%PathAndFileName%" user=all

#step4

You've now acquired the password to your WiFi, it will be located inside the .xml file that is exported.

It can be found under <keyMaterial>passwordHere</keyMaterial>

Save your wireless network profiles and setup your new computer in no time with a quick Batch script, or whatever you decide to write a script in.

Very useful for IT technicians, operations, etc...

Simple but very neat to have.

Also it doesn't work for all WiFi's, some have different authentication methods.

Thanks for the tutorial! I'll be sure to use this later down the road!

Dotexe - June 4, 2017, 2:10 pm

Thank you ra1d, useful information ^^

H4RP4L - June 20, 2017, 2:03 am

Very useful tutorial, thanks for sharing this with us!

ExDeeMan - June 22, 2017, 3:26 pm

That was a great tutorial. I hope I have the instance to use it when everyone in the house forgets the wifi password for a guest, haha.

kareem123 - March 3, 2025, 6:38 am

Thank you. this is useful [warn]

lalala-blip - March 30, 2025, 3:49 am

fgnaHmhfgzdafshgdaeganbsgaseaasn frtgnhfrwgnd