

Ethical hacking and penetration testing

HOME

LOCALBITCOINS

How to increase TX-Power of Wi-Fi adapters in Kali Linux in 2021

The default TX-Power of wireless is set to 20 dBm but you can increase it with a little trick to 30 dBm but let me warn you first that it might be illegal in your country, so use it at your own risk. Moreover some models will not support these settings or wireless chip may state that it "can" transmit with higher power, but the device's manufacturer probably did not place the appropriate heat sink in order to accomplish this.

In different countries, legislation and technical standards varies, including in relation to Wi-Fi. In some countries it is not allowed to use the frequencies of some Wi-Fi channels (for example, channels 12, 13 and 14 can not be used in the USA). In most countries, a Wi-Fi signal power limit of 20.0 dBm is set. But there are countries in which there is a limitation of 30.0 dBm. You can take advantage of this loophole (make your wireless thinks it is located in a country where 30.0 dBm is allowed) and raise its TX Power to a value of 30.0 dBm.

Regulatory domains (or "regdomain") is the country in which this device is supposed to work. There is also an accompanying database, in which are prescribed the permitted frequencies and the allowed power.

The algorithm is:

- set the system-wide setting of the regulatory domain to the value, that matches to a country where the power is allowed to be 30.0 dBm;
- set the increased power for the wireless adapter.

In theory, the described method should work for many wireless cards, but in practice there are the following limitations:

- the physical inability of an adapter to operate at capacities greater than 20.0 dBm (for example, the wireless interface initially shows a power of 15.0 dBm while 20.0 dBm is allowed. In this case it is impossible to raise the power above 15.0 dBm, even to 20.0 dBm);
- driver features, for example, some drivers ignore system settings. This is not an insoluble problem, but each model needs its own approach.

To check capabilities of your wireless adapter issue the command:

```
1 | sudo iw list
```

For example, the following frequencies and power are allowed for the US:

```
* 2412 MHz [1] (30.0 dBm)
* 2417 MHz [2] (30.0 dBm)
* 2422 MHz [3] (30.0 dBm)
* 2427 MHz [4] (30.0 dBm)
* 2432 MHz [5] (30.0 dBm)
* 2437 MHz [6] (30.0 dBm)
* 2442 MHz [7] (30.0 dBm)
* 2447 MHz [8] (30.0 dBm)
* 2452 MHz [9] (30.0 dBm)
* 2457 MHz [10] (30.0 dBm)
* 2462 MHz [11] (30.0 dBm)
* 2467 MHz [12] (disabled)
* 2472 MHz [13] (disabled)
* 2484 MHz [14] (disabled)
```

SUBSCRIBE
ARTICLE

Email*

SUBMIT

JOIN US IN TE

Telegram notificatio
articles on M
t.me/miloserdov

ALSO RECOM

SEARCH

ENHANCED BY Google

CATEGOR

- Anonymity, data e anti-forensics
- Exploitation
- Hardware
- Improving security
- Information Gather
- IT Forensics
- Kali Linux
- Maintaining Access
- Online books
- Password Attacks
- Reverse Engineerin
- Sniffing & Spoofing
- Web Applications
- Website news
- Wireless Attacks
- Work Environment



```
* 5180 MHz [36] (23.0 dBm)
* 5190 MHz [38] (23.0 dBm)
* 5200 MHz [40] (23.0 dBm)
* 5220 MHz [44] (23.0 dBm)
* 5230 MHz [46] (23.0 dBm)
* 5240 MHz [48] (23.0 dBm)
* 5260 MHz [52] (23.0 dBm) (radar detection)
* 5270 MHz [54] (23.0 dBm) (radar detection)
* 5280 MHz [56] (23.0 dBm) (radar detection)
* 5300 MHz [60] (23.0 dBm) (radar detection)
* 5310 MHz [62] (23.0 dBm) (radar detection)
* 5320 MHz [64] (23.0 dBm) (radar detection)
* 5500 MHz [100] (23.0 dBm) (radar detection)
* 5510 MHz [102] (23.0 dBm) (radar detection)
* 5520 MHz [104] (23.0 dBm) (radar detection)
* 5540 MHz [108] (23.0 dBm) (radar detection)
* 5550 MHz [110] (23.0 dBm) (radar detection)
* 5560 MHz [112] (23.0 dBm) (radar detection)
* 5580 MHz [116] (23.0 dBm) (radar detection)
* 5590 MHz [118] (23.0 dBm) (radar detection)
* 5600 MHz [120] (23.0 dBm) (radar detection)
* 5620 MHz [124] (23.0 dBm) (radar detection)
* 5630 MHz [126] (23.0 dBm) (radar detection)
* 5640 MHz [128] (23.0 dBm) (radar detection)
* 5660 MHz [132] (23.0 dBm) (radar detection)
* 5670 MHz [134] (23.0 dBm) (radar detection)
* 5680 MHz [136] (23.0 dBm) (radar detection)
* 5700 MHz [140] (23.0 dBm) (radar detection)
* 5745 MHz [149] (30.0 dBm)
* 5755 MHz [151] (30.0 dBm)
* 5765 MHz [153] (30.0 dBm)
* 5785 MHz [157] (30.0 dBm)
* 5795 MHz [159] (30.0 dBm)
* 5805 MHz [161] (30.0 dBm)
* 5825 MHz [165] (30.0 dBm)
* 5835 MHz [167] (disabled)
* 5845 MHz [169] (disabled)
* 5855 MHz [171] (disabled)
* 5865 MHz [173] (disabled)
```

You can examine the full current database in plain text [here](#).

Countries where allowed channels 1 through 13 on 30.0 dBm power are (for instance):

- BZ
- GY
- NZ
- VE

Note that for channels at 5 GHz they have different values (different list of allowed frequencies and powers).

Next, I'll show the power increasing of [Alfa AWUS052NH](#) in Kali Linux. The old guides tell to install additional packages, but currently this is not necessary. Everything you need is already available in Kali Linux!

To find out which region is currently configured, run the command:

```
1 | sudo iw reg get
```

RECENT P

- Active Directory guide, from ins configuration to se Part 6: Activ configuration tools
- Analysis of a Linux Bash
- How to find and re from Linux
- How to find the fas and BlackArch mirr
- How to install d Mediatek MT7921 MT7961 in Linux

RECENT COM

- Adam Fyfe on F Greenbone Management (GV OpenVAS) on Kali L
- Airbadone on How for Wi-Fi for a RTL8814AU ch AWUS1900)
- Andrea on How Greenbone Management (GV OpenVAS) on Kali L
- Ivan Lombardi on Greenbone Management (GV OpenVAS) on Kali L
- Alex on How to inc of Wi-Fi adapters i 2021

NEW PENET TESTING T

- Metadata Cleaner Source: New Penet Tools | Published on
- mat2 Source: New Penet Tools | Published on
- TrID Source: New Penet Tools | Published on

- Detect It Easy 

```

root@miloserdov: ~
File Edit View Search Terminal Help
root@miloserdov:~# sudo iw reg get
global
country 00: DFS-UNSET
(2402 - 2472 @ 40), (N/A, 20), (N/A)
(2457 - 2482 @ 20), (N/A, 20), (N/A), AUTO-BW, NO-IR
(2474 - 2494 @ 20), (N/A, 20), (N/A), NO-OFDM, NO-IR
(5170 - 5250 @ 80), (N/A, 20), (N/A), AUTO-BW, NO-IR
(5250 - 5330 @ 80), (N/A, 20), (0 ms), DFS, AUTO-BW, NO-IR
(5490 - 5730 @ 160), (N/A, 20), (0 ms), DFS, NO-IR
(5735 - 5835 @ 80), (N/A, 20), (N/A), NO-IR
(57240 - 63720 @ 2160), (N/A, 0), (N/A)

root@miloserdov:~#

```

The string **country 00** indicates that I have not set any value and the default settings was applied.

Now set the regulatory domains to BZ:

```
1 | sudo iw reg set BZ
```

To insure the setting was applied run the command:

```
1 | sudo iw reg get
```

```

root@miloserdov: ~
File Edit View Search Terminal Help
root@miloserdov:~# sudo iw reg set BZ
root@miloserdov:~# sudo iw reg get
global
country BZ: DFS-JP
(2402 - 2482 @ 40), (N/A, 30), (N/A)
(5735 - 5835 @ 80), (N/A, 30), (N/A)

root@miloserdov:~#

```

At the same time, you can look at the new features with the command:

```
1 | sudo iw list
```

```

* 2412 MHz [1] (30.0 dBm)
* 2417 MHz [2] (30.0 dBm)
* 2422 MHz [3] (30.0 dBm)
* 2427 MHz [4] (30.0 dBm)
* 2432 MHz [5] (30.0 dBm)
* 2437 MHz [6] (30.0 dBm)
* 2442 MHz [7] (30.0 dBm)
* 2447 MHz [8] (30.0 dBm)
* 2452 MHz [9] (30.0 dBm)
* 2457 MHz [10] (30.0 dBm)
* 2462 MHz [11] (30.0 dBm)
* 2467 MHz [12] (30.0 dBm)
* 2472 MHz [13] (30.0 dBm)
* 2484 MHz [14] (disabled)

```

To view the name of the wireless interface and its current status, use the command:

```
1 | sudo iw dev
```

Next, increase the power (replace wlan0 with the actual name of your wireless interface):

```

1 | sudo ip link set wlan0 down
2 | sudo iw dev wlan0 set txpower fixed 30mBm
3 | # sudo iw wlan0 set monitor control # if monitor mode needed
4 | sudo ip link set wlan0 up

```

Checking:

```
1 | sudo iw dev
```

Source: New Penetration
Tools | Published on

■ Binwalk
Source: New Penetration
Tools | Published on

■ Spraykatz
Source: New Penetration
Tools | Published on

```
mial@HackWare:~$ sudo iw dev
phy#0
    Interface wlan0
        ifindex 3
        wdev 0x1
        addr 00:c0:ca:90:0d:9f
        type managed
        txpower 0.00 dBm
mial@HackWare:~$ sudo ip link set wlan0 down
mial@HackWare:~$ sudo iw dev wlan0 set txpower fixed 30mBm
mial@HackWare:~$ sudo ip link set wlan0 up
mial@HackWare:~$ sudo iw dev
phy#0
    Interface wlan0
        ifindex 3
        wdev 0x1
        addr 00:c0:ca:90:0d:9f
        type managed
        txpower 30.00 dBm
mial@HackWare:~$
```

The line **txpower 30.00 dBm** indicates that we have succeeded.

How to increase TX-Power of Alfa AWUS036NHA

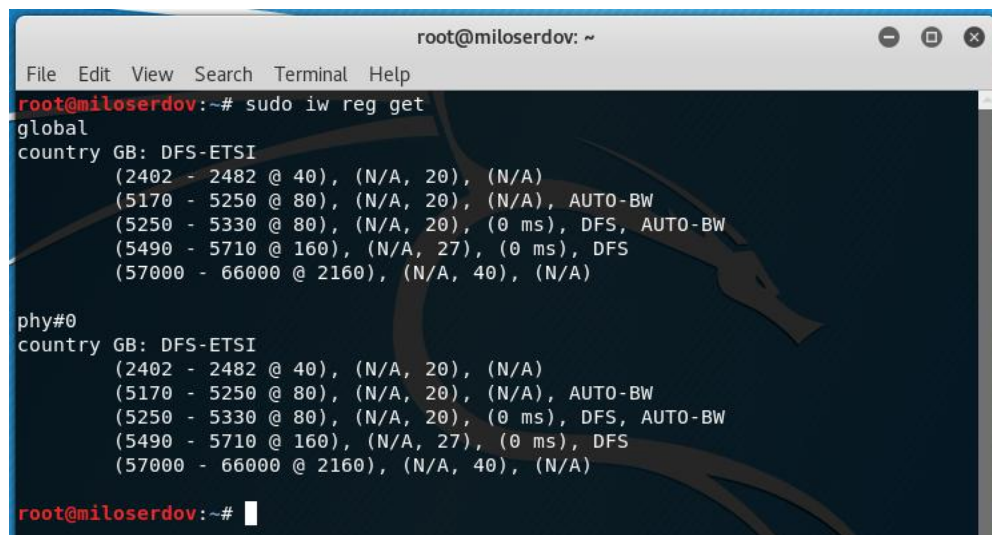
The above commands have no effect for [AWUS036NHA](#). The driver of this adapter ignores regulatory domain value.

If you have Alfa AWUS036NHA or any other that ignores settings of regulatory domain, this is no reason to give up.

We are able to change database of the world regulatory domain.

First let's check which country your wireless card is made for:

```
1 | sudo iw reg get
```



```
root@miloserdov: ~
File Edit View Search Terminal Help
root@miloserdov:~# sudo iw reg get
global
country GB: DFS-ETSI
(2402 - 2482 @ 40), (N/A, 20), (N/A)
(5170 - 5250 @ 80), (N/A, 20), (N/A), AUTO-BW
(5250 - 5330 @ 80), (N/A, 20), (0 ms), DFS, AUTO-BW
(5490 - 5710 @ 160), (N/A, 27), (0 ms), DFS
(57000 - 66000 @ 2160), (N/A, 40), (N/A)

phy#0
country GB: DFS-ETSI
(2402 - 2482 @ 40), (N/A, 20), (N/A)
(5170 - 5250 @ 80), (N/A, 20), (N/A), AUTO-BW
(5250 - 5330 @ 80), (N/A, 20), (0 ms), DFS, AUTO-BW
(5490 - 5710 @ 160), (N/A, 27), (0 ms), DFS
(57000 - 66000 @ 2160), (N/A, 40), (N/A)

root@miloserdov:~#
```

In my case, the **country GB** line indicates that the adaptor was produced for the country that is named **GB** in the database.

My method differs from other tutorials, where the **wireless-regdb** and **crda** packages are manually installed. These packages should already be installed on your system (in Kali Linux is the default). The only thing we do is replace the database file.

The latest versions of Kali Linux do not have the **crda** package installed, let's install it:

```
1 | sudo apt install crda
```

Install the dependency required to compile the database:

```
1 | sudo apt install python3-m2crypto
```

We clone the source files:

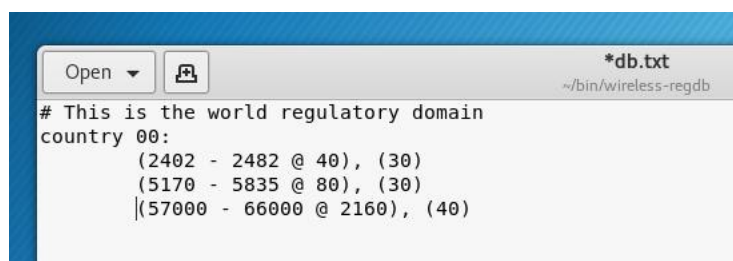
```
1 | git clone git://git.kernel.org/pub/scm/linux/kernel/git/sforshee/wireless-regdb/
2 | cd wireless-regdb/
```

Now we need to edit the database file:

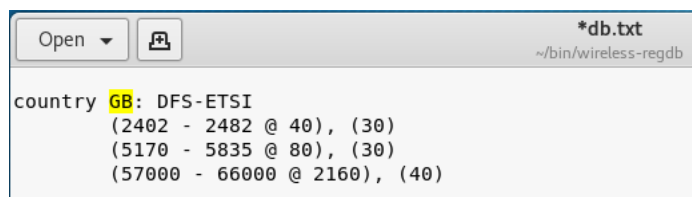
```
1 | gedit db.txt
```

In the file, find the **country 00** line and replace line after it with something like that (correct it up to you):

```
1 | (2402 - 2482 @ 40), (30)
2 | (5170 - 5835 @ 80), (30)
3 | (57000 - 66000 @ 2160), (40)
```



Now I find and change the lines according to the country wireless made for, for me it is **GB** (you may have a different country – it depends on your adapters, you can see this value with the **sudo iw reg get** command):



Save and close the file.

Patch files for using Python3

```
1 | sed -i 's/#!/usr/bin/env python/#!/usr/bin/env python3/' *.py
```

Execute the command:

```
1 | make
```

As a result, a binary file of the database (**regulatory.bin**) was created from the text file. We will use it to replace the file with the same name in the system.

Delete the original database file:

```
1 | sudo rm /lib/crda/regulatory.bin
```

We copy our modified database:

```
1 | sudo cp regulatory.bin /lib/crda/regulatory.bin
```

Once again for the new DB format, which is also used:

```
1 | sudo rm /usr/lib/firmware/regulatory.db
2 | sudo cp regulatory.db /usr/lib/firmware/regulatory.db
```

We copy the required public key (the database file is signed with a specially generated key for our user):

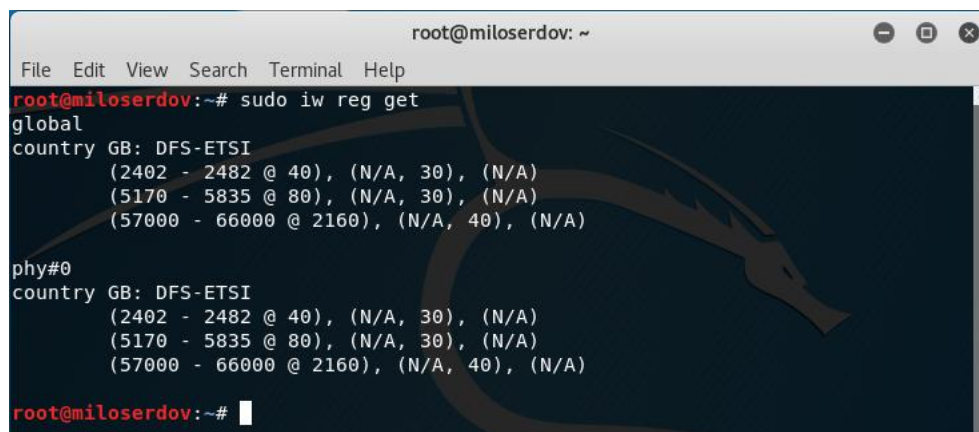
```
1 | sudo cp $USER.key.pub.pem /lib/crda/pubkeys/
2 | sudo cp $USER.x509.pem /usr/lib/crda/pubkeys/
```

Restart your computer.

Now do not use **sudo iw reg set BZ**.

Let us check:

```
1 | sudo iw reg get
```



```

root@miloserdov: ~
File Edit View Search Terminal Help
root@miloserdov:~# sudo iw reg get
global
country GB: DFS-ETSI
(2402 - 2482 @ 40), (N/A, 30), (N/A)
(5170 - 5835 @ 80), (N/A, 30), (N/A)
(57000 - 66000 @ 2160), (N/A, 40), (N/A)

phy#0
country GB: DFS-ETSI
(2402 - 2482 @ 40), (N/A, 30), (N/A)
(5170 - 5835 @ 80), (N/A, 30), (N/A)
(57000 - 66000 @ 2160), (N/A, 40), (N/A)

root@miloserdov:~#

```

Strings

```
1 | country GB: DFS-ETSI
2 | (2402 - 2482 @ 40), (N/A, 30), (N/A)
```

mean we are able increasing the power to 30 dBm.

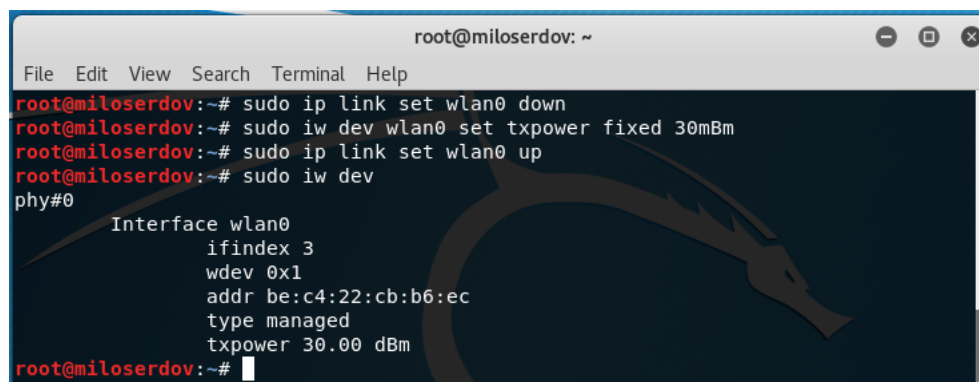
We try:

```

1 | sudo ip link set wlan0 down
2 | sudo iw dev wlan0 set txpower fixed 30mBm
3 | # sudo iw wlan0 set monitor control # if monitor mode needed
4 | sudo ip link set wlan0 up

```

Result:



```

root@miloserdov: ~
File Edit View Search Terminal Help
root@miloserdov:~# sudo ip link set wlan0 down
root@miloserdov:~# sudo iw dev wlan0 set txpower fixed 30mBm
root@miloserdov:~# sudo ip link set wlan0 up
root@miloserdov:~# sudo iw dev
phy#0
Interface wlan0
ifindex 3
wdev 0x1
addr be:c4:22:cb:b6:ec
type managed
txpower 30.00 dBm

root@miloserdov:~#

```

After we patched the database, there is no longer any need to change the value of the regulatory domains for any wireless interface!

Conclusion

Increasing TX power of the Wi-Fi adapter is undeniably useful only for Wi-Fi jamming, as well as for deauthentication attacks. In all other attacks, increasing TX power would not matter. Since power affects how loudly your Wi-Fi adapter is "talking", but does not increase its sensitivity (how well it 'hears' others).

Changing value of regulatory domains lets to unlock some channels that might not be available in your country.

If you want to return everything to its original state, then run the following commands:

```

1 | sudo apt purge wireless-regdb crda
2 | sudo apt install wireless-regdb

```

Related articles: