

Forum:[Hack Forums](#)

Thread: [Howto hack/kill the CMOS password using cmospwd](#)

ub€rh4x0r - February 18, 2010, 3:49 pm

This tut will learn you how to hack or kill the CMOS (BIOS) password using a simple program called cmospwd-5.0

NOTICE: I AM NOT RESPONSIBLE FOR ANY KIND OF DATA LOSS OR ANY DAMAGE YOU CAUSE THROUGH USING THIS PORGAMS AND/OR THIS GUIDE!?

FOR EDUCATIONAL AND SECURITY PURPOSES ONLY!

The program you'll need can be found under:

<http://www.cgsecurity.org/wiki/CmosPwd>

Here is also the direct download link to the binaries:

Windows/DOS:

<http://www.cgsecurity.org/cmospwd-5.0.zip>

Linux:

<http://www.cgsecurity.org/cmospwd-5.0.tar.bz2>

How to use cmospwd:

For Windows/DOS users:

IMPORTANT: Windows users need to install the including [i]ioperm driver so they can get direct access to the CMOS[/i]

To install the ioperm driver you need first to extract the archive to e.g. C:\ and the open cmd.

In the directory where the cmospwdbinary is located there also is a prodam called ioperm which you use to install the driver with.

To install it just simply type ioperm -i (make sure you run it as admin).

Now you'll be able to run cmospwd without any problems.

Just type cmospwd and some possible password hacks will show for different BIOSes.

But the most easy way to get rid of the password is just to run cmospwd /k.

After you done that you'll notice that everything gets very laggy but that just normal because you killed the CMOS ?

Just restart the computer and the you will get a warning that the BIOS has been reset, just enter BIOS and check the settings, save and reboot.

Now the CMOS password has been reset.

#?

godsp33d - February 18, 2010, 5:05 pm

iv never done anything in cmos...ever

but isnt their a battery on the motherboard you can pull out for 2 mins or so and it resets that?
(the battery im talking about keeps the time even when the pc is poweered off)

im probaly wrong however

edit: http://www.dewassoc.com/support/bios/bios_password.htm

Option #1: Mechanically Removing the Password

Most motherboards manufactured over the last decade or more use a battery to sustain the dynamic Bios/CMOS settings for the motherboards PROM chip. These dynamic settings are those manually set by either the computers manufacturer or you, the user. There are two ways to erase these dynamic settings, by either resetting a jumper on the motherboard itself (referred to as a "clear CMOS" jumper), or by physically remove the power from the computer (disconnecting the power plug) and then removing a battery (used to maintain power to the PROM chip that contains the Bios/CMOS information) from the motherboard.

still a clean guide though

nnkvnu - February 18, 2010, 5:28 pm

How can you go into command line before you can crack cmos password later?

just a thought, try the battery approach.

Any suggestion for laptops?

phoenixphreak - February 18, 2010, 5:51 pm

if you have an acer laptop this likely will not work ! I was given an acer aspire to get round the security on it ,and took the job on just thinking that there was a windows password on it ,I was wrong and it had a cmos and win password. Caused all sorts of problems ,mainly the fact that I couldnt change the boot order to reinstall windows from a cd as a last resort ,or boot my password recovery software.

easy way around this although daunting sounding,is to remove the hard disk,remove the memory sticks and put a flat screwdriver over the 2 jumper circuits ,start the laptop ,switch it off,then reinstall hard disk and memory and the pass is gone completely .

this took a whole 5 mins to do :)

the old battery trick ,removing it for a few mins then replacing ,or putting the laptop in the freezer,or any other silly ideas do not work anymore.

ub€rh4x0r - February 19, 2010, 3:41 am

(Feb 18, 2010 06:05 PM)godsp33d Wrote: [\[CITE\]](#) iv never done anything in cmos...ever

but isnt their a battery on the motherboard you can pull out for 2 mins or so and it resets that?
(the battery im talking about keeps the time even when the pc is powered off)

im probaly wrong however

edit: http://www.dewassoc.com/support/bios/bios_password.htm

Option #1: Mechanically Removing the Password

Most motherboards manufactured over the last decade or more use a battery to sustain the dynamic Bios/CMOS settings for the motherboards PROM chip. These dynamic settings are those manually set by either the computers manufacturer or you, the user. There are two ways to erase these dynamic settings, by either resetting a jumper on the motherboard itself (referred to as a "clear CMOS" jumper), or by physically remove the power from the computer (disconnecting the power plug) and then removing a battery (used to maintain power to the PROM chip that contains the Bios/CMOS information) from the motherboard.

still a clean guide though

This program is used for those who don't have access to the battery or the motherboard at all e.g. if the computer is locked in some sort of cage ?

And for those who are to lazy to open it up ?

(Feb 18, 2010 06:51 PM)phoenixphreak Wrote: [\[CITE\]](#) if you have an acer laptop this likely will not work ! I was given an acer aspire to get round the security on it ,and took the job on just thinking that there was a windows password on it ,I was wrong and it had a cmos and win password. Caused all sorts of problems ,mainly the fact that I couldnt change the boot order to reinstall windows from a cd as a last resort ,or boot my password recovery software.

easy way around this although daunting sounding,is to remove the hard disk,remove the memory sticks and put a flat screwdriver over the 2 jumper circuits ,start the laptop ,switch it off,then reinstall hard disk and memory and the pass is gone completely .

this took a whole 5 mins to do :)

the old battery trick ,removing it for a few mins then replacing ,or putting the laptop in the freezer,or any other silly ideas do not work anymore.

Yes laptops CMOS (and especially Acer laptop CMSOSes) are hard to hack because either they are protected or either the password are stored in the EEPROM on the motherboard.

The Readme says just simply:

Quote:DO NOT KILL THE CMOS ON LAPTOPS!

?

So I don't recommend you to kill your CMOS on you laptop, your doing it at your won risk!

cmospwd is used for desktop computers, but if anyone still tries to kill the CMOS on their laptops they can post what happened ?

#

#

?

:D - February 19, 2010, 6:50 am

Might do it on mine. Prolly not though, seeing as it is an acer.

ub€rh4x0r - February 22, 2010, 3:28 am

(Feb 19, 2010 07:50 AM)shadowdeem Wrote: [\[CITE\]](#) Might do it on mine. Prolly not though, seeing as it is an acer.

Try to kill it and see whats happening ?

The worst that can happen is that your BIOS get corrupt ?

Chapa7 - September 3, 2016, 10:03 pm

updated Hiren's didn't support for laptop Bios like InsydeH20 to bruteforce .. while using cmospwd , i realize it corrupting my old laptop bios , later i find any useful things that run it smooth , but for other Insyde bios ... so can we flash that old things to make sure its works back ? i wonder Hiren and Pankaj will updateing their tools for laptop so i can make my works done !

giggetto94 - September 9, 2016, 11:39 am

Amazing thread and great tutorial thanks for sharing!