

Forum: [Hack Forums](#)

Thread: [\[Notorious\] Hack almost any Windows Machine \[Tutorial\]](#)

Leroy Jethro Gibbs - April 27, 2017, 10:37 pm

This is going to be a bit short and to the point. I've been using this method for probably the last 7 or 8 years.

Requirements: Another computer running Windows

Physical access to the target machine.

1 USB Flash Drive with at least 4GB of storage.

An internet connection.

Alright. Go ahead and do the following step by step:

Download <https://unetbootin.github.io/>

Run it and select Ubuntu

Have it install to your Flash drive (Backup anything ahead of time that's on the flash drive).

After it's finished, boot to it on the Windows machine you got.

Select the Live option for testing etc.

Open the file manager on Ubuntu.

Go to the Windows drive then to this path: Windows/System32/

Find Utilman.exe and rename it to Utilman.exe.bak

Copy CMD and rename the copy to Utilman.exe

Restart and boot back into Windows

Hit the accessibility tools button on the login screen.

Type in the box that pops up Code net user Administrator /active:yes then press enter.

Type in the box again Code net user Administrator * then press enter.

Enter a password then press enter. I suggest Code P@ssw0rd as it will get past most requirements. Repeat the password and press enter again.

Exit the black box.

Attempt to login as Code Administrator using the password you set.

You now have administrative access over the computer. If you stole the shit, you can now wipe it out or go looking for someones porn. Enjoy the newly accessed machine.

This works on Windows XP (I believe) all the way up to Windows 10. Why does it work so well? Because linux (ubuntu) doesn't give a fuck about Windows permissions. Enjoy your hacking!

EXTRA: If you end up getting a machine with a locked BIOS, try the following website with master BIOS codes. Doesn't have all of them but a decent amount of them.

<https://bios-pw.org/>

Vobz - April 28, 2017, 4:28 am

Very nice thread, Pretty HQ too

Korvo - April 28, 2017, 4:37 am

Great tutorial man. I'm sure this will be very helpful to many people. I've myself used a similar process before. Sometimes I'll go to yard sales/pawn shops and buy cheap computers, they'll have a password on them..However this will work perfectly to fix that issue. Thanks for the share bro!

Cylow - April 28, 2017, 4:37 am

Seems like a really good tutorial, thank you!

Leroy Jethro Gibbs - April 28, 2017, 10:16 am

(Apr 28, 2017 04:28 AM)Vobz Wrote: [\[CITE\]](#) Very nice thread, Pretty HQ too
Thanks for the kind words sir!

(Apr 28, 2017 04:37 AM)Røbbøt Wrote: [\[CITE\]](#) Great tutorial man. I'm sure this will be very helpful to many people. I've myself used a similar process before. Sometimes I'll go to yard sales/pawn shops and buy cheap computers, they'll have a password on them..However this will work perfectly to fix that issue. Thanks for the share bro!

I have another method I can use as well involving Trinity Rescue Kit. I just didn't post that one because this one has less steps and places to go wrong. As for the computers at pawnshops, I get my laptops for about \$25 each time I go. I find the laptops they got locked out of and fix them. Either resell or keep them.

(Apr 28, 2017 04:37 AM)Cylow Wrote: [\[CITE\]](#) Seems like a really good tutorial, thank you!
No thank you. For those kind words sir!

M9Bayonet - April 28, 2017, 3:10 pm

Vouch, used it to get into 3 different laptops. Thanks!

Leroy Jethro Gibbs - April 28, 2017, 9:07 pm

(Apr 28, 2017 03:10 PM)M9Bayonet Wrote: [\[CITE\]](#) Vouch, used it to get into 3 different laptops.
Thanks!

No problem man. I'll hit you up tomorrow about that thing you were PMing me about.

TheChi?f - April 28, 2017, 9:47 pm

Quite informative and easy-to-follow instructions. Thank you for contributing to the community.

ZuGgY - April 28, 2017, 9:55 pm

Thanks for sharing. Might actually test this out soon.

Cheers.

Leroy Jethro Gibbs - April 28, 2017, 11:07 pm

(Apr 28, 2017 09:47 PM)TheChi?f Wrote: [\[CITE\]](#) Quite informative and easy-to-follow instructions. Thank you for contributing to the community.

Not a problem at all man. Trying to put out some Notorious content! lol

juiceman2020 - April 28, 2017, 11:09 pm

thanks for this man i actually found this really useful because i am trying to do something similar to this :)

PrivateDonut - April 28, 2017, 11:25 pm

Pretty interesting, thanks for posting this tutorial. ?

Leroy Jethro Gibbs - April 29, 2017, 10:16 am

(Apr 28, 2017 11:25 PM)PrivateDonut Wrote: [\[CITE\]](#) Pretty interesting, thanks for posting this tutorial. ?

Not a problem man. Hopefully it can help you someday.

OnePlus6 - April 29, 2017, 10:18 am

Cheers mate, learn something every day.

Dr. Gonzo - April 29, 2017, 10:39 am

Great tutorial for those with physical access. Sometimes this is really all you need to get a solid foothold into a network.

Leroy Jethro Gibbs - April 29, 2017, 10:41 am

(Apr 29, 2017 10:39 AM)Veridian Wrote: [\[CITE\]](#) Great tutorial for those with physical access. Sometimes this is really all you need to get a solid foothold into a network.

Lmao. I used this exact tutorial in high school to hack a Windows XP laptop and get the WiFi password. Ended up giving it to 3 people that in return gave it to over 450 people lmao. And there was only 350 students and faculty. So yes, a quick way to get into the network indeed.

nicksaban1 - April 29, 2017, 10:50 am

Use WinPE for Windows 8, 10, Server 2008 and 2012. If you can get your machine to restart into troubleshooting, and you can get into x:/ cli, then do as you said in original post. There is really no need for running linux, or booting linux.

Exe2Aut - April 29, 2017, 10:53 am

Which is why you lock your BIOS to protect against this. Haven't seen a machine without BIOS password for a long time.

Leroy Jethro Gibbs - April 29, 2017, 10:58 am

(Apr 29, 2017 10:50 AM)Nick Saban Wrote: [\[CITE\]](#) Use WinPE for Windows 8, 10, Server 2008 and 2012. If you can get your machine to restart into troubleshooting, and you can get into x:/ cli, then do as you said in original post. There is really no need for running linux, or booting linux.

You also need the password to access it.

(Apr 29, 2017 10:53 AM)Exe2Aut Wrote: [\[CITE\]](#) Which is why you lock your BIOS to protect against this. Haven't seen a machine without BIOS password for a long time.
I provided a website to help bypass that.

p1rat3sc0d3 - April 29, 2017, 11:57 am

Thanks For Sharing

I Will Try It Soon

Rangers. - April 29, 2017, 3:00 pm

Used to try this when I was a kid :P