

How I Hacked My Windows 10 Local Account In 30 Seconds



Marcus Fernström · [Follow](#)

4 min read · Mar 2, 2020



Listen



Share

... More

I'm about to show you exactly how I hacked into my Windows 10 laptop. The whole thing takes about thirty seconds after booting up.

I wasn't planning on writing this article, but when the opportunity presented itself I figured I should do a little write-up showing just *why* it's a bad idea to use a local Windows 10 account.

The opportunity, in this case, was that I forgot the Admin password for one of my Windows 10 laptops.

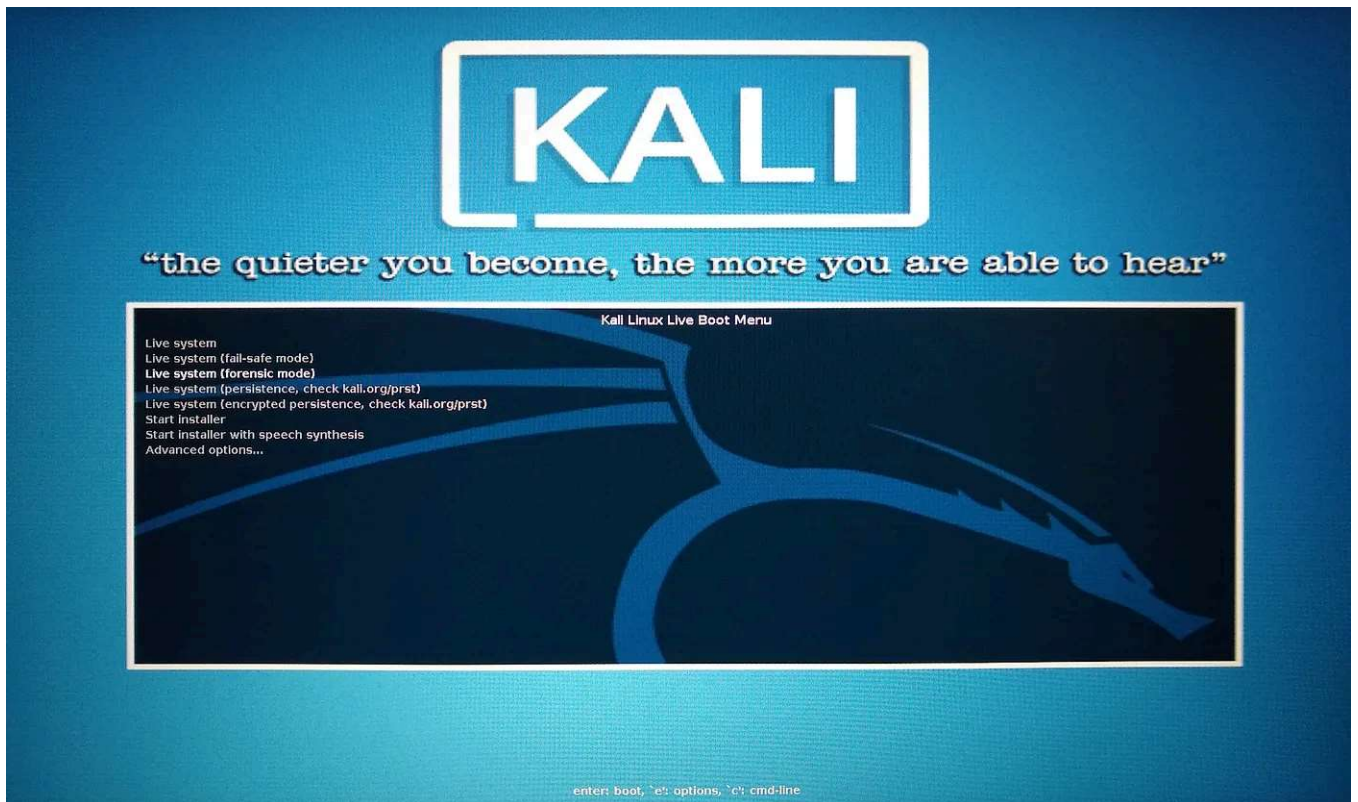
Luckily this is my gaming laptop, which is set up with a local account and without drive encryption.

Both of those points, *local account* and *lack of drive encryption*, are key to this particular method.

We'll exploit the local account by booting into a Kali flash drive and clearing the Admin password on the Windows machine. You can't do that with a Microsoft network account or if the drive is encrypted.

Let's go

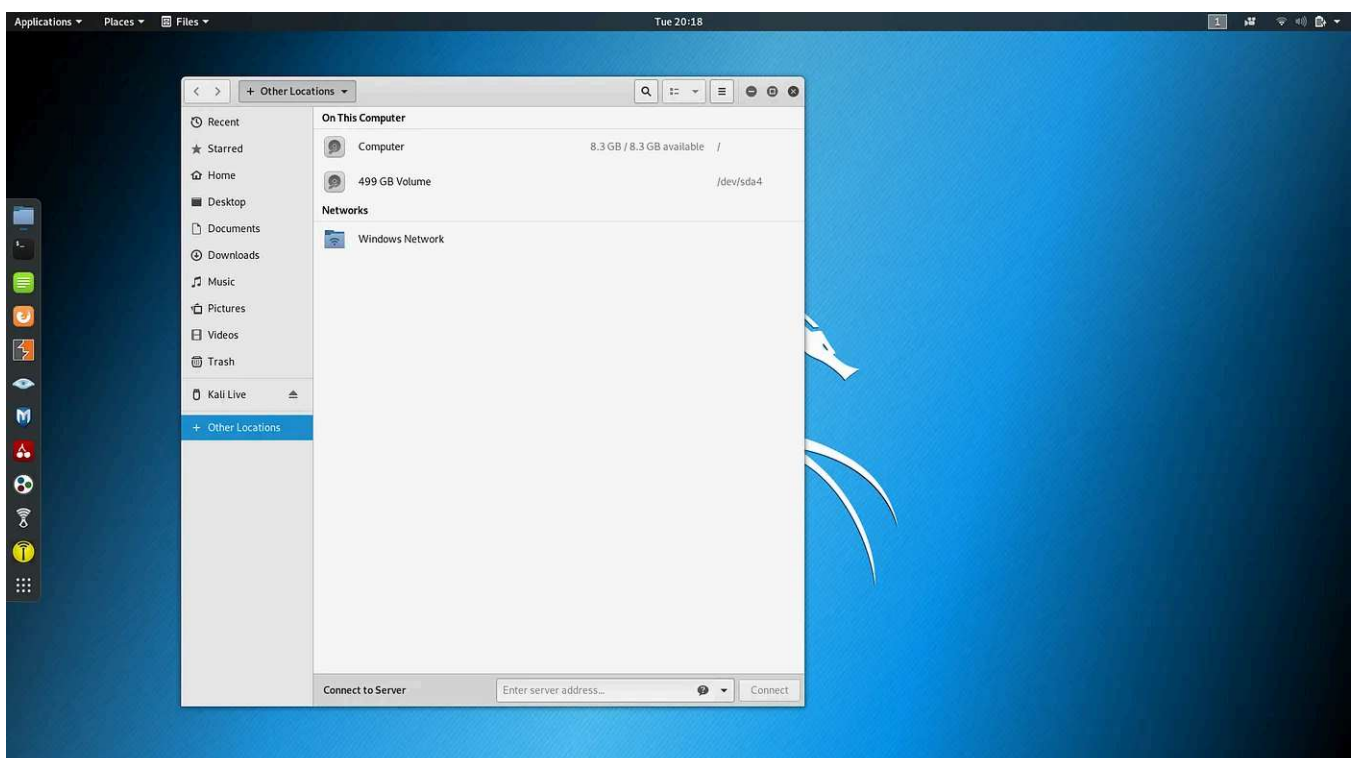
Booting up the Kali flash drive we get this menu



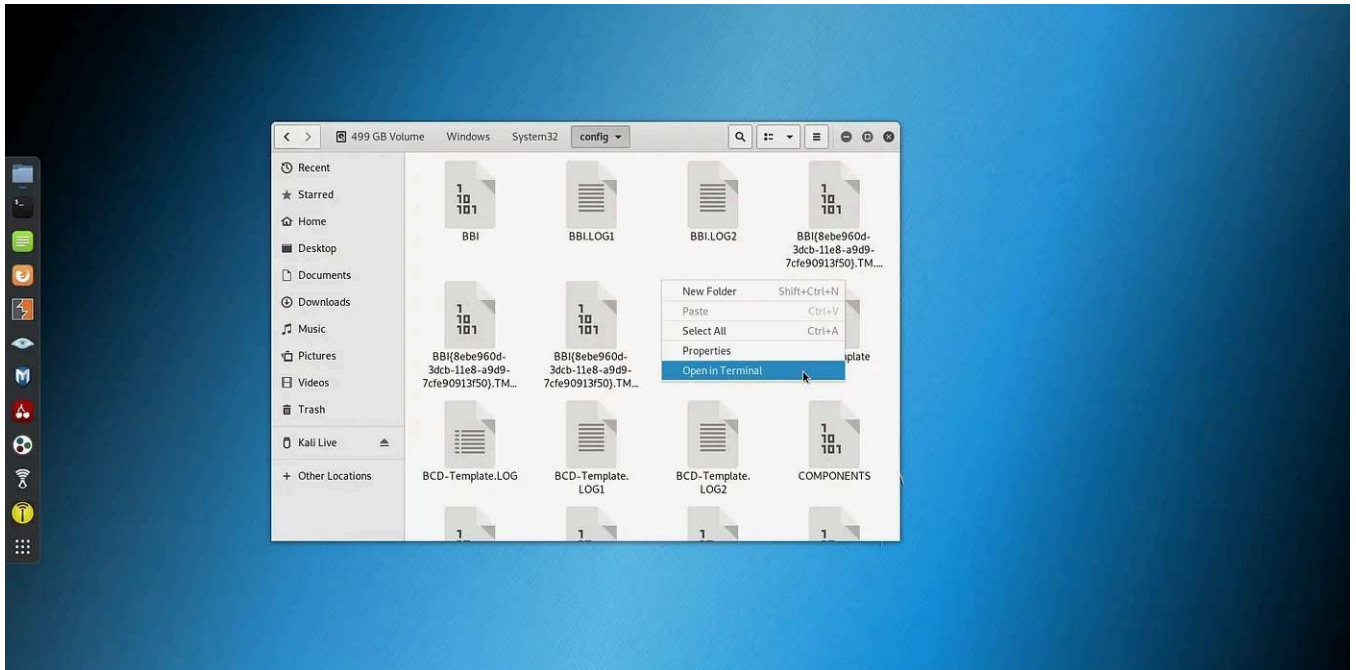
We don't want to interact with the system more than necessary, so choose Live System (forensic mode) from the menu and hit Enter.

Once booted, click on the blue folder icon in the Favorites menu on the left side and select "Other Locations" in the menu.

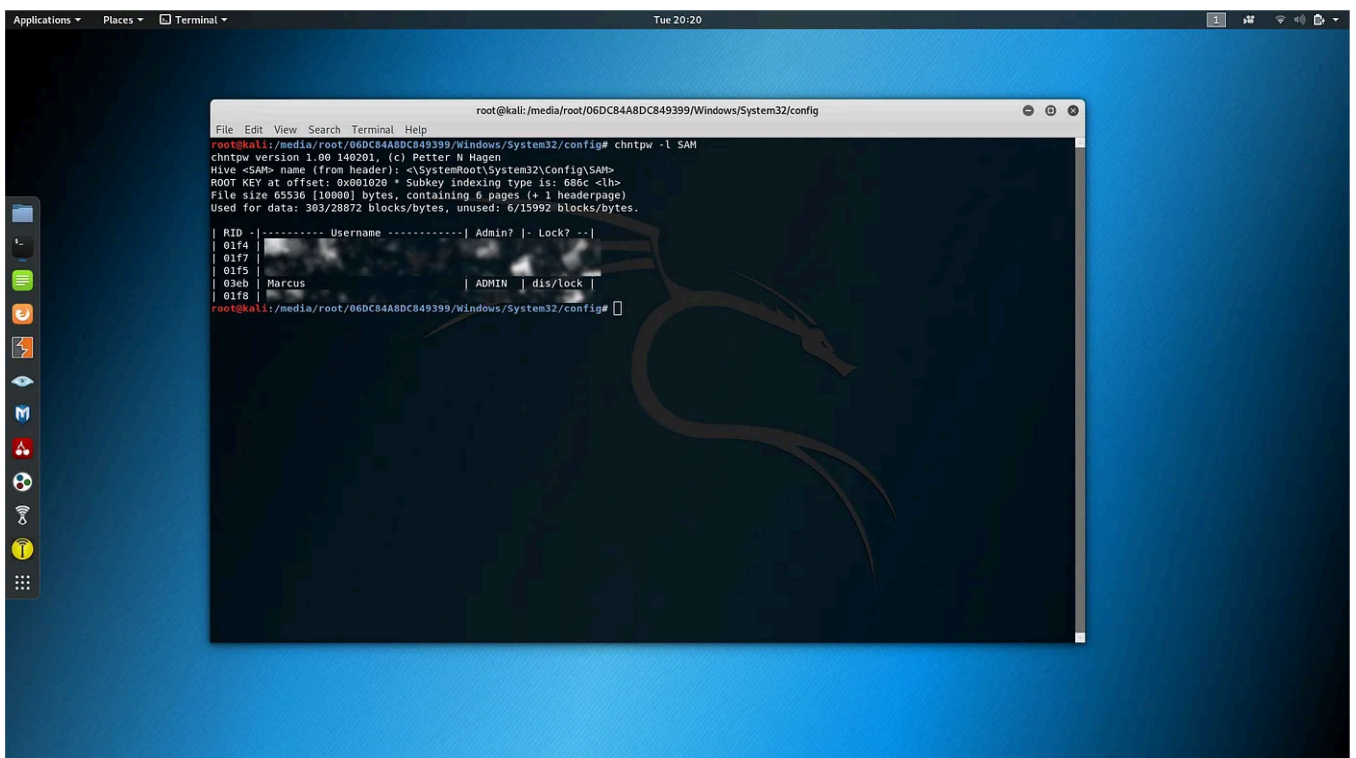
Here I see the 500gb laptop drive, just double click it to mount and start browsing it.



You need to run the terminal commands inside a particular folder on the Windows drive, so head over to `/Windows/System32/config/` right-click and open in Terminal



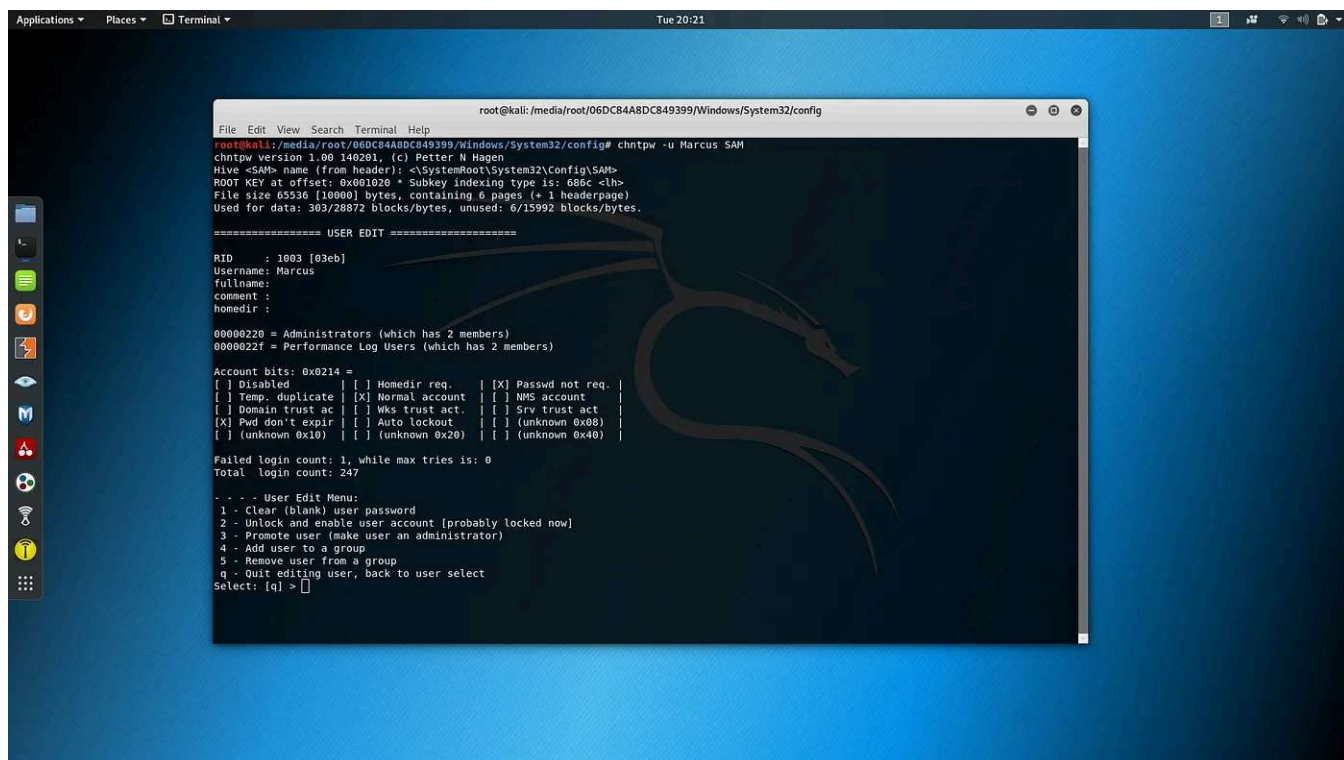
Before you can reset an account you need to know its name, so list them out with the command `chntpw -l SAM`



Let's go ahead and reset the password for `Marcus`, which is an ADMIN account.

Type `chntpw -u Marcus SAM` to get the interactive prompt.

Choose 2 to “Unlock and Enable” the account, and then pick 1 to remove the current password.



```
root@kali:/media/root/06DC84A8DC849399/Windows/System32/config# chntpw -u Marcus SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 688c <lh>
File size 65536 [10000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 303/28872 blocks/bytes, unused: 6/15992 blocks/bytes.

===== USER EDIT =====

RID      : 1003 [03eb]
Username: Marcus
Fullname:
comment :
homedir  :

00000220 = Administrators (which has 2 members)
0000022f = Performance Log Users (which has 2 members)

Account bits: 0x0214 =
[ ] Disabled          [ ] Homedir req.    [X] Pswd not req. |
[ ] Temp. duplicate  [X] Normal account  [ ] NMS account   |
[ ] Domain trust ac  [ ] Wks trust act.  [ ] Srv trust act  |
[X] Pwd don't expir  [ ] Auto logout   [ ] (unknown 0x08) |
[ ] (unknown 0x10)  [ ] (unknown 0x20)  [ ] (unknown 0x40) |

Failed login count: 1, while max tries is: 0
Total login count: 247

-- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account (probably locked now)
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 2

-- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account (probably locked now)
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
```

That's it, we're done!

I rebooted the laptop, logged into the Administrator account with no password, and could once again play Neverwinter!



[Open in app](#)



 Search



That's the How-To-Exploit-Local-Account side of things, and as you can see it's fast and very easy. But what can you do to protect yourself?

It's actually really easy to protect yourself if you know how.

Use a Microsoft network account

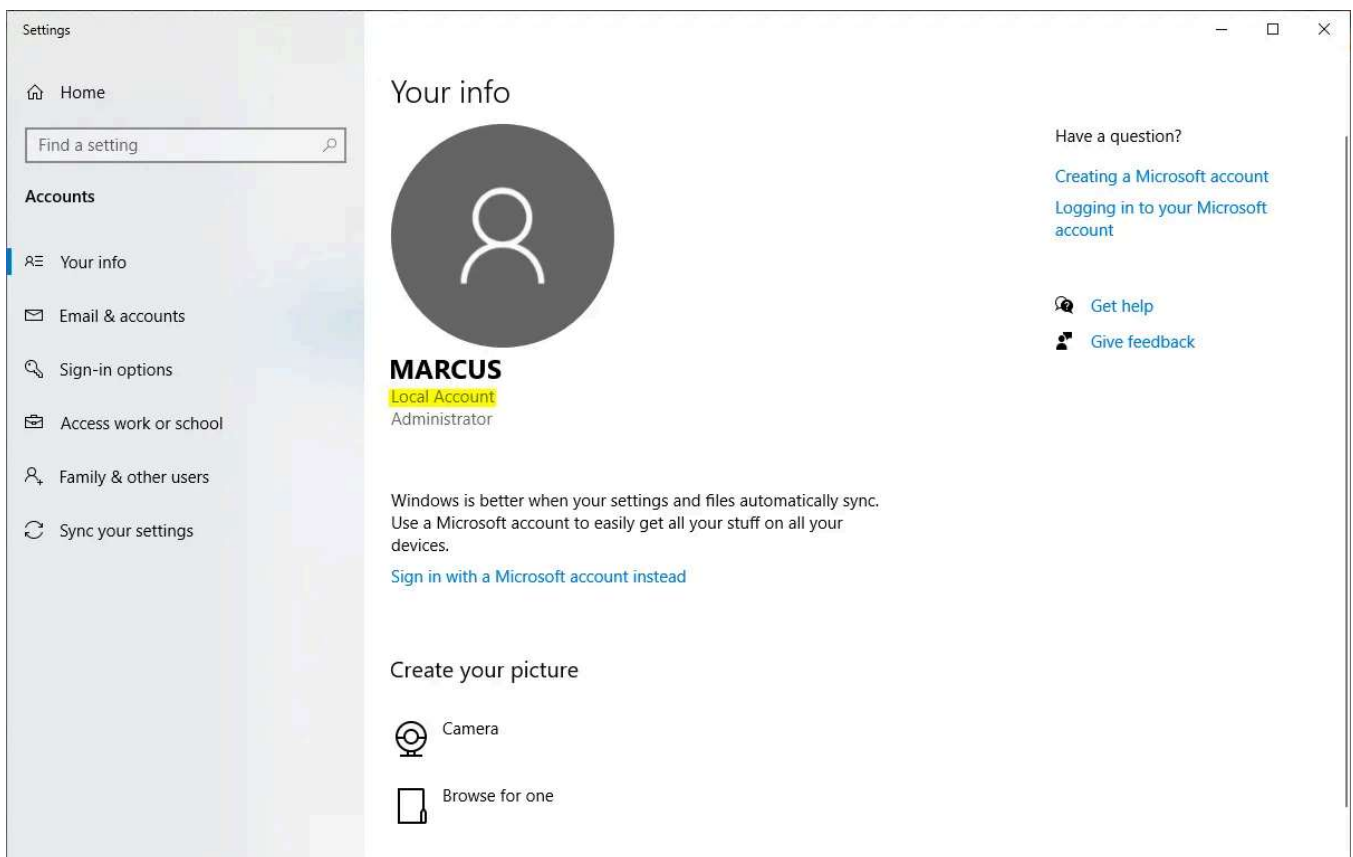
If the account had been a Microsoft network account I wouldn't have been able to do any of this.

While it does mean you rely on internet access and an account hosted by Microsoft, it's a simple solution and something I recommend for most users.

If you're not sure if you have a local account or not, here's a quick way to check.

Press the Windows key and type Account, you'll see an option for "Manage your account", click that to see info about your account.

Under the image, you'll see "Local Account" if it is, or an email address if you're already using a Microsoft network account.



It's easy to set up an account and use it to log into your computer: [link](#)

Turn on drive encryption

Drive encryption means that just because someone can access the drive itself, that doesn't mean they can actually access the data on it, because it's encrypted.

Two easy-to-use solutions are [Windows Device Encryption](#) and [VeraCrypt](#).

There's information on the websites for how to set up and use them.

Security

Hacking

Windows 10

Kali Linux

Encryption



Follow