

Forum:[Hack Forums](#)

Thread: [\[TuT\] Hacking Windows XP Administrator Password \[SCHOOL HACKS\] \[NOOB FRIENDLY\]](#)

Dan Smith - August 23, 2013, 2:06 pm

Edit: reading back on this now (feb 2017), this is pretty cringey. I'm going to leave it the way it was though, as a memory to my first tutorial, IIRC. I don't know how this was grave dug but I don't really care either. Cheers.

Hello fellow HF members,

Ever wanted administrator access to your school's computers? Well, me too. I found out how and today I'm going to write an in-depth tutorial about it.

DISCLAIMER: This is for educational purposes only. I won't be in any way responsible for how you use this information. Think for yourself and think of the consequences if you get caught. Also, don't be a dick and format C:...

Requirements:

A school computer where no one is looking over your shoulder (preferably out of sight of a security camera).

2 USB sticks, one with another OS (I used Backtrack Linux) installed.

The ability to think for yourself and see what you're actually doing.

Most schools (or companies, for that matter) still use Windows XP. About 35% of computers still has XP, and when talking about companies, that number is even higher. Schools usually don't have sufficient funds to hire security experts or even professional system/network administrators, that's why the computer engineering teacher usually handles that. He may be a teacher, but he's still (most of the times) not a professional system admin or security guy.

So, let's get into it, I'm first going to explain broadly what we will be doing:

First, we're going to look how we can access the computer's file system and how the security is configured. If we found a way to access it, we're going to copy the files which store the user accounts and encrypted passwords to our USB drive. When that's done, we'll go home and crack the hashes using Ophcrack and rainbow tables.

First part - Acquiring the files

So, there are a few possibilities here. I can not look at your school's computers right now and see what's possible and what's not. I'm going to talk about a few things you can try. Start with the first one, and if that doesn't work, move on to the next. And so forth.

1. Open explorer and see if you can access the C: drive. If not, move on to the next step. If you can, check if you can access C:\WINDOWS\system32\config. If not, move on. If it's possible, try to copy the files 'SAM' and 'system' onto one of your USB drives. You can skip the rest of this part and go home to crack.

2. Can't access C:\WINDOWS\system32\config through explorer or can't copy the files? Try the

command screen: Open cmd.exe, type the following (in this order, hit ENTER after every command):

Code cd\

C: (if you're not already there)

cd WINDOWS

cd system32

cd config

If you're getting an error trying any of these commands, move on to the next step. If you didn't and successfully managed to get into the folder, type this:

Code copy SAM <letter of your USB drive>\<folder you want it in>

copy system <letter of your USB drive>\<folder you want it in>

Let's say my USB's letter is E: and my folder is \hacks\school, I would have to type:

Code copy SAM E:\hacks\school

copy system E:\hacks\school

If this worked, move on to the next part.
If it didn't, try the next step.

3. We can't get access through Windows itself? Okay, well, let's use another OS then. I used Backtrack to do this, but any OS installed on your USB drive should work, as long as there is an explorer on it.

Plug in both USB sticks. Turn off the computer (if it's not off already) and try to get into the boot menu. Usually, there is this text on the first screen you see when booting, it should look something like this:

[img]<http://pad1.whstatic.com/images/thumb/3/32/Flash-the-Laptop-Bios-Step-1.jpg/550px-Flash-the-Laptop-Bios-Step-1.jpg>[img]

Please mind that it's different for almost every computer!

You're looking for something like 'Boot Menu' or 'Change Boot Order', and you want to hit the designated key. You can boot to read first, then boot a second time to hit the key. It won't run away. But if the text is not there, it might be hidden or disabled. To find out, just hit all the Fkeys while booting. If nothing happens, they're disabled and you have to do it the difficult way... Move on to the next step, if this is the case.

Now that you got into the boot menu, find your USB drive and boot from there. (Assuming you installed your OS on there correctly) Start your OS up and open explorer. Find the C:\WINDOWS\system32\config folder and copy 'SAM' and 'system' to your second USB drive. This is the way I did it myself, move on to the next part.

4. If you can't get into the boot menu, but you can get into the setup, you can try to find the option to enable boot menu. If you can't get into any of those, you'd have to open the computer, disconnect the hard drive, and maybe it'll ask you where to boot from. Again, I've got no idea about the room your schools computers are in. If you're with 30 other students in the room, this might not be a good idea...

My knowledge about the boot menu and BIOS setup stops here. If you were unable to access it, use Google and maybe you can find something for the specific computers your school uses.

Second Part - Cracking

So, we acquired the files with the encrypted password hash in them, all we need to do now is crack it. We're going to use a program called Ophcrack. This program in combination with rainbow tables cracks hashes extremely fast. First, we're going to use a small table. If that doesn't work, we're going to use a larger one, which includes special characters.

Ophcrack for Backtrack 5R3 can be found under: Applications > Backtrack > Privilege Escalation > Password Attacks > Offline Attacks > Ophcrack-GUI

Ophcrack for Windows can be downloaded here: <http://ophcrack.sourceforge.net/>

The small rainbow table can be downloaded here (703 MB):

http://downloads.sourceforge.net/ophcrack/tables_xp_free_fast.zip

The large rainbow table can be downloaded here (7.5 GB):

<https://sourceforge.net/projects/ophcrack/files/tables/XP%20special/>

Start by opening Ophcrack and click 'Load'. Then click 'Encrypted SAM'. Now, you're going to select the FOLDER that contains the SAM and system files. It will now display all accounts on the computer where you got the SAM file from. For the sake of speed, we're going to remove all the accounts except for the admin account. (Not necessary, but will increase speed)

Next, we're going to install our rainbow table. Click on the 'Tables' menu and select either 'XP free small' or 'XP special', depending on the one you're using. Now hit 'Install' and select the FOLDER containing the rainbow table. Hit OK.

We're all set to try and crack the password. Hit the 'Crack' button to commence cracking. Depending on your computer's specs, the cracking should be done in a few minutes. Used the small table but didn't crack the password? Download and install the larger table. It takes a bit longer but it'll get the job done on 99% of school passwords. Still not able to crack it? You can try downloading bigger tables, but they can be very large and take very long to go through. It's probably not worth it.

Cracked it? Nice! Now, if you're lucky, the admin password on the machines is the same as the network admin's account. This was the case at my school, so I was able to access their entire network.

Thanks for reading my first actual tutorial on this site. I hope the lulz will be big and the trolls will have laughs. Have a nice day. ?

Any suggestions/corrections? Please post below and I'll look into it!

Manas95 - August 24, 2013, 12:46 am

Great and detailed tutorial. I will attempt this later, thanks for the share :D

Dan Smith - August 25, 2013, 2:31 am

(Aug 24, 2013 12:46 AM)Manas95 Wrote: [\[CITE\]](#) Great and detailed tutorial. I will attempt this later, thanks for the share :D

Glad you liked it. Have fun with it! ?

King Xerxes - August 25, 2013, 3:23 am

Awesome tutorial! Good job bro, keep it up! :D

ramonhackpro - August 25, 2013, 6:15 am

damn, the best hacking admin account tut i have seen! nice work bro will try it

Dan Smith - August 25, 2013, 12:34 pm

Loving the positive feedback! Thanks everyone!

Hopsin - August 25, 2013, 12:44 pm

Thanks for sharing. You can use some colors to make it look better :)

Fmerchau - August 25, 2013, 8:01 pm

Thanks for the Tut man, so much to know so little time... :)

espinosi - August 26, 2013, 2:28 am

Thanks for sharing. Is very easy to do!! Thank you very much!!

Murphys_lawless - August 26, 2013, 2:35 am

I liked it, knew this all already but it was a good Tut none the less!

PS. I like things with pictures.

stordy007 - August 26, 2013, 2:43 am

cool let me try that out..hope it works out great..thanks in advanced

Dan Smith - August 26, 2013, 6:03 am

(Aug 25, 2013 12:44 PM)Hopsin Wrote: [\[CITE\]](#) Thanks for sharing. You can use some colors to make it look better :)

Done! It makes it a lot easier and cleaner to read!

zetustiger - August 26, 2013, 7:40 am

Awesome tutorial very nice. Thanks OP

justsomeguy008 - August 26, 2013, 2:02 pm

good tutorial thanks didn't know this could be done

Dan Smith - September 2, 2013, 7:39 am

Thanks for the feedback! Have fun at school :)

taylor333 - September 2, 2013, 11:43 am

Great tut OP. the girl on Murphys_lawless pic is so cute :D

pisangelat80 - July 9, 2014, 9:11 pm

Dear Element115,

Good day to you.

I've question, Is this applicable for Win7?Win8?

raindrophk9 - July 12, 2014, 12:20 pm

wow this is interesting. will comes in handy for sure

tsmcy - July 12, 2014, 2:38 pm

Good tutorial. Thx for posting... ;)

TAOofHacking - January 10, 2017, 11:28 am

Thanks a lot, very detailed. Access was denied when trying to configure the cd. Don't have a USB with me today but will try copying the SAM and system tmrw.

CFour - January 10, 2017, 2:43 pm

Thank you for the thread nice post.

private.member - February 13, 2017, 8:48 am

Thanks for the Tut man, so much to know so little time... :)

Hopsin - February 13, 2017, 9:03 am

(Feb 13, 2017 09:48 AM)private.member Wrote: [CITE](#) Thanks for the Tut man, so much to know so little time... :)

If your little time is used correctly, you can have some powerful knowledge at your hands overall. Just saying and also this thread is 3 years old, nonetheless have a nice day. ?

CheeseCakez - February 13, 2017, 6:44 pm

Sounds really cool and I would love to try it, but I'm pretty new and it's slightly confusing to me. Regardless thanks for the share

Husnain5678 - February 15, 2017, 9:45 am

Nice share will test out with certain machines ;).

Dan Smith - February 17, 2017, 6:05 am

Lmao guys who tf dug this up? I wrote this almost 3 years ago.

Glad it's still useful though!