

# Forum:[Hack Forums](#)

Thread: [Bruteforce ssh](#)

**Booga991** - January 5, 2026, 3:24 pm

Anyone know how to bruteforce a password to a pc using ssh on windows, im running the command "ssh administrator@iphere" and i try to guess the password but i fail, anyone know how to bruteforce it? Port 22 is open

**Terry A. Davis** - January 5, 2026, 3:26 pm

You will be there a long time.

Also, Administrator is Windows, root is Linux, check your target OS.

Do you know anything about the remote service to work out what wordlists might work better?

**Booga991** - January 5, 2026, 3:30 pm

i know nothing about the person im trying to hack and i know hes using windows 10

**Terry A. Davis** - January 5, 2026, 3:39 pm

(Jan 5, 2026 04:30 PM)Booga991 Wrote: [\[CITE\]](#) i know nothing about the person im trying to hack and i know hes using windows 10

Despite Port 22 being open, how sure are you that he is actually using a SSH Server? Do you get banners back?

Look into word lists, maybe something like Medusa could do the job?

**MadScientist** - January 5, 2026, 4:07 pm

hydra and rockyou.txt wordlist is your best bet but very unlikely to succeed Especially if good configuration that limits attempts and sets cooldown times on failed attempts / blocks An IP address after a certain amount of tries. On top of that a good configuration will prevent root or administrator logins Directly so you would need to know the username.

**Booga991** - January 5, 2026, 4:11 pm

(Jan 5, 2026 04:39 PM)Terry A. Davis Wrote: [\[CITE\]](#) Despite Port 22 being open, how sure are you that he is actually using a SSH Server? Do you get banners back?

Look into word lists, maybe something like Medusa could do the job?

I know almost nothing about ssh, learnt about it like a week ago

**Terry A. Davis** - January 5, 2026, 4:13 pm

(Jan 5, 2026 05:11 PM)Booga991 Wrote: [\[CITE\]](#) I know almost nothing about ssh, learnt about it like a week ago

Then my friend, you have got a long road ahead of you, and I do not think you will get anywhere quick.

Windows disables the Administrator account by default and needs to be turned on, and even then has no password, and if OpenSSH from MS is anything like their Terminal Service client then it will not allow password less logins which means the target will have not only had to turn on the account which most people do not do, and also set a password for it.

Then, I am not sure what the stance of users allowed ssh login, so if that is disallowed, you're also out of luck.

Finally, you will then need to find a tool you can leave running brute forcing, like I said, maybe Medusa, though I am not super familiar with Windows SSH.

**Booga991** - January 5, 2026, 4:17 pm

(Jan 5, 2026 05:13 PM)Terry A. Davis Wrote: [\[CITE\]](#) Then my friend, you have got a long road ahead of you, and I do not think you will get anywhere quick.

Windows disables the Administrator account by default and needs to be turned on, and even then has no password, and if OpenSSH from MS is anything like their Terminal Service client then it will not allow password less logins which means the target will have not only had to turn on the account which most people do not do, and also set a password for it.

Then, I am not sure what the stance of users allowed ssh login, so if that is disallowed, you're also out of luck.

Finally, you will then need to find a tool you can leave running brute forcing, like I said, maybe Medusa, though I am not super familiar with Windows SSH.

I learnt about it a bit more and i am 90% sure theres an ssh server running on the ip, also i know the person is familiar with havking and databases so probably has administrator on and uses it

**Terry A. Davis** - January 5, 2026, 4:19 pm

(Jan 5, 2026 05:17 PM)Booga991 Wrote: [\[CITE\]](#) I learnt about it a bit more and i am 90% sure theres an ssh server running on the ip, also i know the person is familiar with havking and databases so probably has administrator on and uses it

You are wrong.

Anyone who knows anything about anyhting will not use the Administrator account as their daily account, anyone who does and thinks they're a hacker is ... fucking retarded.

You are ready then, you've validated that the port is open, you've said you're getting connects approved.

Now look into Medusa, see if it is going to do what you want it to do, find good wordlists, and then. Wait. Seriously, you can not speed it up past throwing more hardware at it which I don't think you want to do.

**Booga991** - January 5, 2026, 4:24 pm

(Jan 5, 2026 05:19 PM)Terry A. Davis Wrote: [\[CITE\]](#) You are wrong.

Anyone who knows anything about anyhting will not use the Administrator account as their daily account, anyone who does and thinks they're a hacker is ... fucking retarded.

You are ready then, you've validated that the port is open, you've said you're getting connects approved.

Now look into Medusa, see if it is going to do what you want it to do, find good wordlists, and then. Wait. Seriously, you can not speed it up past throwing more hardware at it which I don't think you want to do.

Thanks for the information, also i thought that they might use administrator because i think you get access to more commands on cmd

Terry A. Davis - January 5, 2026, 4:35 pm

(Jan 5, 2026 05:24 PM)Booga991 Wrote: [CITE](#) Thanks for the information, also i thought that they might use administrator because i think you get access to more commands on cmd  
You seem like you want to learn, so I will give you some knowledge to take with you.

The User Administrator is different than your User, your user is what you make during the Out of Box Experience (OOBE), Windows by default will add this user to the Group Administrator that allows you execution of commands with a higher privilege level, by design applications / commands / whatever will launch with your standard privilege level, this is "You" since Windows is Multi-Users, different Users can have different permissions, but we'll save ACLs for a later post.

If you right click something and say Run as Administrator, you will get a UAC prompt asking if you wish to run it by default, Yes/No appear, which is a quick way to tell you're in the Administrators group, as it's asking for confirmation, sometimes enterprise policies will ask you to enter a password, but typically if you get asked for a password you are being asked for elevation, which means you are not in the Administrators group.

You do not need to enable the Administrator User to run things as them, as you can be part of the group and get the "same" permissions, without trawling through secpol and other areas of Security Windows, I do not believe being the Administrator user grants you anything extra special, if anything, I imagine it locks a few more settings down in some areas due to it being a known user making attacks on it more likely, similar to how they let you rename the Guest user, and how it doesn't actually exist anymore on Windows.

It might be dry, boring, and well out of scope for what you want to learn, but I suggest reading Windows Internals, a lot is out of depth for this, but Windows is a very complex system with how it handles users.

Bonus points.

When you copy something from a network drive, to a protected folder when asked to provide admin consent and you say yes, then get told the source file doesn't exist, it is because the admin consent does not have the network drive mapped as that is done using a different login token, though Windows call them something different I can't remember.