

Forum:[Hack Forums](#)

Thread: [Installing Auto-Remote Backdoor physically in a Computer with Linux?](#)

minkche - October 20, 2017, 3:55 am

hei guys,

So lets say i have physical access to the victims computer. I will now access the harddrive with kali linux and drop a backdoor payload in some folder.

When the victim boots up the computer, i would expect a connection in my meterpreter session.

So it's this possible?

Is there a way to create that kind of backdoor? This is bugging me now for quite some time...

Looking forward to your suggestions :)

cheers,

minkche

OK GUYS,

thats funny, i just found a solution haha :D

you will need to start the computer with a kali live usb. Then you go to the following directory: "programdata/Microsoft/Windows/Start Menu/Programs/Startup".

This is the autorun file in windows. Every file in it will be autorun at a restart of the computer.

So now you can drop any file like your payload in it. The next time the user restarts the PC, your Payload will be run and your connection is made, without the victim even touching the exe or whatever you drop there.

All you need is physical access to the victims PC... Thats pretty unexpected for me, thats actually just too easy... My testings were on windows 7 and windows 10!

have a nice day,

minkche

CyberStrike - October 21, 2017, 12:36 am

If you want to avoid AV you can put in the startup a reverse cmd to your machine with no extra payload. Which would make it a bit difficult in IR since there is no payload per say. And if you have redirects setup then target will have nothing to work with.