

Forum:[Hack Forums](#)

Thread: [How could an outside hacker gain remote access to our PC given our security setup??](#)

Zebra41567 - February 27, 2022, 10:03 pm

Our single PC is in a data centre in a co-location "locked" rack so no person has physical access to my PC except for myself which means no person can insert a USB stick into the PC and still my sensitive files that way. Via our Cisco hardware firewall, which is in the same rack in the data centre, all inbound ports and outbound ports are closed except for port 5001 which needs to remain open so as our PC can communicate with our forex broker's trading server. Also, all inbound and outbound traffic has been blocked except for outbound and inbound traffic between my PC and the forex broker's server. I was thinking that we do not need to apply Windows 10 Pro OS security updates as there are no windows services (or windows programs) "listening" on any ports (all these ports have been closed via our firewall) and therefore it would be impossible for an outside hacker to gain remote access to our PC via exploiting any vulnerabilities in any windows services, windows programs or the windows OS itself, does this make sense and is this logic correct, please let me know where I'm making a mistake here? Also, the only program that is allowed to connect to the internet is my trading platform application/software (which is not an open-source program/code and there are no publicly known vulnerabilities in this trading platform software as well) and the internet connection between my PC and the broker's server is an "established connection" via port 5001 (as opposed to my trading platform program "listening" on port 5001 which is not the case). Given this additional information, if someone knew my PC's IP address (maybe someone who works in the data centre could find out this info or someone who works at my forex broker could find out my IP address too) could they hack into my PC and steal my sensitive files and if so what method could they use to do this? Also, given my system setup listed above, do we need to download and apply windows 10 "security" updates given that there are no windows services or windows program listening on any open ports, as all of these ports have been closed via our Cisco firewall? So, in summary I have 2 questions (a) Is it possible that an outside hacker could steal our sensitive files on our PC and if so, what method could they use to do this? And (b) If we don't apply windows 10 "security" updates to our PC given that there are no windows services or programs listening on any open ports could this failure to apply windows patches allow an outside hacker to gain remote access to our machine and if how would he or she do this?

ice_c00l - February 28, 2022, 2:21 pm

Good description, just a quick read through, You say Cisco firewalls, are they cisco firepowers? Are they upto date, most have web frontend that use legacy libraries.

You have mentioned the firewall is blocking all ports but have you checked with nmap? There are a few command to evade firewalls and IDS.

Is your server vlanned off from the other servers in the data centre? Could someone compromise a relative server and pivot onto yours? Is the switch your server hangs off upto date? Say to prevent arp spoofing or vlan hopping, cisco-torch attempts.

As regards to Windows updates that is upto you and risk is factored. A fully updated system makes it much harder to get onto but if it's in an isolated environment with old patches then same thing. How would you get updates, direct from Microsoft or do you have in-house WSUS (thinking of MITM attacks)?

It's an established connection to the broker server but with what account? Does it have full access

on this account, can it be compromised? What software are you using to connect is it vulnerable?

It's specialist broker software but have you checked if you can escalate privilege (if there's a standard account on your system) to check for unquoted service paths and reg entries. (Something like powerup/winpeas/jaws etc).

Would it be possible for someone to use a hak5 Lan turtle on your server?