

Forum:[Hack Forums](#)

Thread: [Windows Reverse TCP shell](#)

esfomeado - February 7, 2018, 1:16 pm

Hello,

I'm exploiting a buffer overflow vulnerability although I'm having a strange problem with my shellcode.

I'm using the payload "windows/shell/reverse_tcp" from metasploit and I'm able to successfully receive a connection from the victim machine although the "cmd.exe" isn't executed on the victim machine. I'm only able to "chat" with the victim.

Anyone has any idea why the cmd.exe isn't opening?

Thanks

I'm retarded...

windows/shell_reverse_tcp is the correct one.

spector117 - February 13, 2018, 3:19 am

(Feb 7, 2018 02:16 PM)esfomeado Wrote: [\[CITE\]](#) Hello,

I'm exploiting a buffer overflow vulnerability although I'm having a strange problem with my shellcode.

I'm using the payload "windows/shell/reverse_tcp" from metasploit and I'm able to successfully receive a connection from the victim machine although the "cmd.exe" isn't executed on the victim machine. I'm only able to "chat" with the victim.

Anyone has any idea why the cmd.exe isn't opening?

Thanks

I'm retarded...

windows/shell_reverse_tcp is the correct one.

Haha I was just gonna say that until you posted that! Working on OSCP?