

Forum: [Hack Forums](#)

Thread: [question: Hidden VNC/RDP metasploit/empire](#)

macpromo - April 17, 2019, 5:54 am

is there any module or tool for kali/metasploit/empire powershell as HVNC or HRDP?

Asdethprime - April 18, 2019, 5:11 am

This is interesting.

Looking around on github this is the closest I can find.

<https://github.com/#/CreateDesktop>

This is new to me ; the whole idea of system programming but while many parameters seems pretty straight forward.

Once the hidden desktop is created what code u run is up to you.

Fair warning system programming need admin access.

Looked through the code a bit closely it's actually just 1 single function call to create this hidden desktop (or a new desktop)

CreateDesktopA() function defines in Windows.h header file.

This is very useful ; I am pretty surprised I don't see this brought up on hackforum.

Keen to find out what are u trying to you VNC for ? Banking Trojan ?

CyberStrike - April 18, 2019, 8:18 am

(Apr 17, 2019 05:54 AM)macpromo Wrote: [\[CITE\]](#) is there any module or tool for kali/metasploit/empire powershell as HVNC or HRDP?

You are missing a HUGE point of how and what RDP/VNC is generally used for in a real pentest by skilled operators, being it's for lateral movement to gain further privileges. You are less efficient in a GUI than in a CLI, that is why administrators use CLI's. The fall of a handful of machines should be enough to have an entire network fall. Even in Windows there is rarely something you can do in a GUI which can't be done in a CLI.

macpromo - April 19, 2019, 9:43 am

(Apr 18, 2019 08:18 AM)CyberStrike Wrote: [\[CITE\]](#) You are missing a HUGE point of how and what RDP/VNC is generally used for in a real pentest by skilled operators, being it's for lateral movement to gain further privileges. You are less efficient in a GUI than in a CLI, that is why administrators use CLI's. The fall of a handful of machines should be enough to have an entire network fall. Even in Windows there is rarely something you can do in a GUI which can't be done in a CLI.

Hidden RDP is not simple RDP or VNC

.eXe - April 19, 2019, 3:32 pm

(Apr 18, 2019 08:18 AM)CyberStrike Wrote: [\[CITE\]](#) You are missing a HUGE point of how and what RDP/VNC is generally used for in a real pentest by skilled operators, being it's for lateral movement to gain further privileges. You are less efficient in a GUI than in a CLI, that is why administrators use CLI's. The fall of a handful of machines should be enough to have an entire network fall. Even in Windows there is rarely something you can do in a GUI which can't be done in a CLI.

In addition to this, most of what you do in the Windows GUI (Exchange Admin Center, for example), just pretty much runs the PowerShell equivalent anyway.

CyberStrike - April 21, 2019, 3:36 pm

(Apr 19, 2019 09:43 AM)macpromo Wrote: [\[CITE\]](#) Hidden RDP is not simple RDP or VNC

Yes I know this, and there is no "good" reason to include something which is not going to be used. I have used one version of Metasploit since about 2005 including professionally at work I have not once needed a hidden whatever. In fact the only time I deal with RDP is just for the reasons I mentioned above. I have never had a coworker say "Hey we need to build a hidden RDP or VNC it'd make work so much easier".

(Apr 19, 2019 03:32 PM)eXe Wrote: [\[CITE\]](#) In addition to this, most of what you do in the Windows GUI (Exchange Admin Center, for example), just pretty much runs the PowerShell equivalent anyway.

Exactly! There is really nothing you can do in GUI which in CLI it can't be done. MSFT did this because generally minus Server Manager there is no GUI on the average install it's a core install, and the client machines also can be administered using a CLI. People who don't have experience with actual administration less engagements in a mature environment won't know this much.

Faith Connors - April 21, 2019, 3:38 pm

(Apr 21, 2019 03:36 PM)CyberStrike Wrote: [\[CITE\]](#) Exactly! There is really nothing you can do in GUI which in CLI it can't be done.

i beg to differ that you can make your environment look pretty and actually usable by people :)

CyberStrike - April 22, 2019, 6:01 am

(Apr 21, 2019 03:38 PM)Faith Connors Wrote: [\[CITE\]](#) i beg to differ that you can make your environment look pretty and actually usable by people :)

Faith, I am talking administration of like 300 machines perhaps more are you planning to RDP or VNC into all of them to push out a new config? Hope not because in 15 minutes you can use psession and be done. If you are talking about users then yes they need a GUI that is normal.

aerohacker - September 27, 2019, 4:00 pm

(Apr 18, 2019 08:18 AM)CyberStrike Wrote: [\[CITE\]](#) You are missing a HUGE point of how and what RDP/VNC is generally used for in a real pentest by skilled operators, being it's for lateral movement to gain further privileges. You are less efficient in a GUI than in a CLI, that is why administrators use CLI's. The fall of a handful of machines should be enough to have an entire network fall. Even in Windows there is rarely something you can do in a GUI which can't be done in a CLI.

There's a way to control the GUI of Operating Systems like Linux, MacOS, BSD and Solaris in hidden mode like Hidden RDP or Hidden VNC on Windows?

Something like Hidden RDP, Hidden VNC, Hidden Teamviewer or Hidden AnyDesk to another Operating Systems?

CyberStrike - September 28, 2019, 3:50 pm

(Sep 27, 2019 04:00 PM)aerohacker Wrote: [\[CITE\]](#) There's a way to control the GUI of Operating Systems like Linux, MacOS, BSD and Solaris in hidden mode like Hidden RDP or Hidden VNC on Windows?

Something like Hidden RDP, Hidden VNC, Hidden Teamviewer or Hidden AnyDesk to another Operating Systems?

Everyone wants hidden rdp or VNC the hell do you need it for? You cannot use a cli? Like I say what can you do in a cli other than interacting say with a 3rd party AV or use their browser to navigate resources which that machine might have access to that you cannot do in a CLI? I am being serious you want to dump passwords? Great mimikatz has no gui, want to get interweb passwords from chrome great go download their SQLite db and the json file to decrypt.

I will say it and just lay it out there, on OSX, Linux, BSD, Solaris and Windows if you need a VNC/RDP to do everything what will you do when you hit a Windows Server (generally a "Core" install) or a *NIX server with no gui? Install a gui?