

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Kali Veil-Evasion Exploiting + Antivirus Evasion](#)

Floppy - December 20, 2016, 12:18 pm

[TUTORIAL] Kali Veil-Evasion Exploiting + Antivirus Evasion

This tutorial will teach you to create an Trojan for a victims computer to gain access to all their files, Watch their webcam, Take screenshots, Use their command prompt, Keylog and much more.

This tutorial is written in an way so a noob with the most basic understanding of computers can use it.

(Works fine in Live OS)

(Don't think it works in Virtual Machine)

I'M NOT RESPONSIBLE FOR ANY ACTIONS DONE BY PEOPLE INSPIRED BY THIS TUTORIAL IN ANY WAY.

I'm verry new to this Forum and it seems like a nice community so i thought i'd get a good start in it by writing this tutorial.

I wanted to include pictures but i'm apparently required to write 50 posts before i can do that ?.

For this tutorial i'm gonna be using Kali (OS), Veil-Evasion (For payload encoding), Armitage (As listener and Exploiting kit)

INSTALLS: (Gonna assume you use Kali2)

To install Veil-Evasion simply open terminal in Kali and use these commands:

```
apt-get install update
```

```
apt-get install veil-evasion
```

```
veil-evasion (This will start the installation process)
```

early in the installation it might ask if it can restart some applications just hit yes.

It will also install Python and Ruby versions. Just spam next (You don't need to change any settings)

Armitage is installed by deffault in Kali Linux but to get it to work use these commands:

```
msfdb init (Only first time)
```

```
/etc/init.d/postgresql start (Might have to use each time you boot Kali)
```

After veil-evasion install is done it should launch automatically if not type "veil-evasion" without qoutes in terminal.

Veil-Evasion:

Type "list" To view all available payloads (Files the victim computers start to inithiate the attack)

Personally i recommend python/meterpreter/rev_tcp which works great but recently has been

picked up by antivirus software in rare occasions. or powershell/meterpreter/rev_tcp which doesn't get picked up by antivirus as easy however might crash powershell in rare occasions.

Select the Payload you want to use by writing "use [Payload number]".

Now we have to select some settings for the payload.

To change the settings we use the following: "set [Setting] [Value]".

We have to change the "LHOST" setting to your IP adress. If you're gonna hack locally then use your private IP which can be found by typing "ifconfig" in terminal (192.168.x.x, 10.x.x.x or 172.16.x.x). If you're gonna hack someone outside your LAN then use your public IP. (go to whatsmyip.org)(Attacking outside your LAN might require PORT-FORWARDING).

If you're using the Python payload you might wanna change "ARCHITECTURE" to 64, sense 64bit has become standard these days.

The rest should be fine left to default.

You can view updated info about your Payload settings by simply typing "info"

Once you have the settings you want type "generate" and it will ask you to name your payload. This can be anything.

If it asks how you would like to create the payload just stick to the default option.

Once it says "Press any key to return to the main menu" You can close the window.

Your file should be located in /var/lib/veil-evasion/output/source/filename.bat if powershell or /var/lib/veil-evasion/output/compiled/filename.exe if python.

Armitage:

Open armitage and click "connect" without changing any of the options.

If it asks to start Metasploit hit "Yes"

Once you're in the Armitage GUI select "Armitage" in the top left corner and select Listeners, Reverse.

Change "Port" to 4444 and "Type" to meterpreter then start listener.

Now you have to get the file we created in Veil-Evasion to the victims computer and start it on the victims computer. This, I won't be covering however some suggestions would be Email, Facebook chat, Skype and so on. If what you're using won't let you send the file because of its file extension you can bypass this by simply adding to .zip or .rar archive.

If done correctly the victims computer should appear in red with some lighting on it.

Now you can simply rightclick on it. Select "Meterpreter1" and go to "Explore". Here you can view your victims entire file system, Take screenshots to see what they're doing, Take/view photo from webcam and Keylog.

If you instead go to the "Interact" menu and "Meterpreter shell" you have lots of options. Type "help" for a list of the things you can do. Some examples would be downloading their files and streaming their webcam.

Once you're done you can simply write "kill -s" in the meterpreter shell to terminate the connection.

If you have suggestions for other Kali related tutorials I would be happy to write em. ?

Freshnuts - December 20, 2016, 12:59 pm

Awesome, man. Thanks for the contribution and welcome to the forums.

This is pretty cool. I use steghide for myself then crypt it with another module, but

I'll be trying this out on the weekend. Thanks

Not Your Average Orange - December 20, 2016, 1:34 pm

Awesome post, but I'd recommend adding color to it or format it so it's easier to read.

Flopppy - December 20, 2016, 1:49 pm

(Dec 20, 2016 02:34 PM)hkessel1 Wrote: [\[CITE\]](#) Awesome post, but I'd recommend adding color to it or format it so it's easier to read.

Did some changes, Hope it's better now.

blakken - December 20, 2016, 3:36 pm

Thanks for the tutorial. It looks nice and it is very well put. I will be toying around with this later. =)

DoxProxy - January 4, 2017, 5:09 pm

Good tutorial, however, I tried this and e-mail detected as a threat and when I tried on my own virtual machine, windows defender detected threat.

Maxs - January 4, 2017, 11:13 pm

Good tutorial, however, I tried this and e-mail detected as a threat and when I tried on my own virtual machine, windows defender detected threat.

semendaemon - January 5, 2017, 12:34 am

Quote:This tutorial is written in an way so a noob with the most basic understanding of computers can use it.

Why is this good?

Freddy Kru?ger - January 5, 2017, 12:42 am

Pretty good tut man, thanks a lot.

Flopppy - January 5, 2017, 5:24 am

(Jan 4, 2017 06:09 PM)firepaw100 Wrote: [\[CITE\]](#) Good tutorial, however, I tried this and e-mail detected as a threat and when I tried on my own virtual machine, windows defender detected threat.

Strange. I tested both of the ones i recommended with AVG and Windows Defender and the only detection was from windows defender and Python reverse_TCP.

Feel free to play around with the other payloads

(Jan 5, 2017 01:34 AM)semendaemon Wrote: [\[CITE\]](#) Why is this good?

Because noobs gotta start somewhere

JackRed - February 2, 2017, 11:23 am

I saw the incomplete Udemy (warez disallowed) course about veil framework. You tut was better! Thanky for sharing! ?

Last_viking - February 6, 2017, 11:28 am

thanks man good tut
help full

camarazon100 - February 8, 2017, 10:00 am

Good tutorial, however, I tried this and e-mail detected as a threat and when I tried on my own virtual machine..