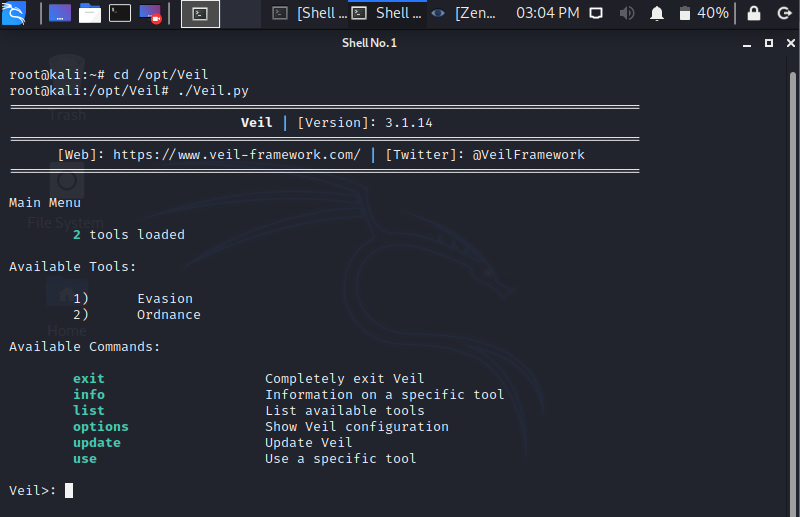
Once Veil-Framework installed, we are going to look at its commands.

Run Veil Using commands

# cd /opt/Veil

# ./Veil.py

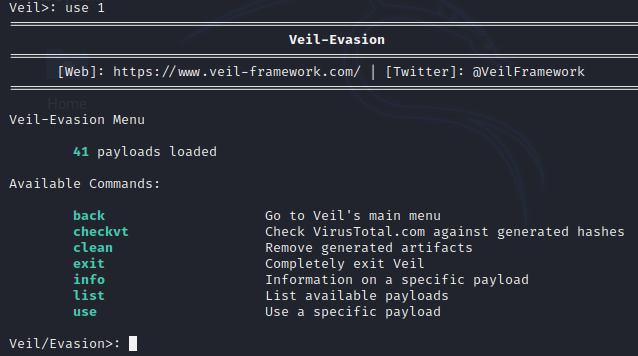


The **exit** allow us to exit the program, **info** is used to provide us the information about a specific tool, **list** is used to list the available tools, **update** is used to update Veil, **use** is used to enable the use of any tool.

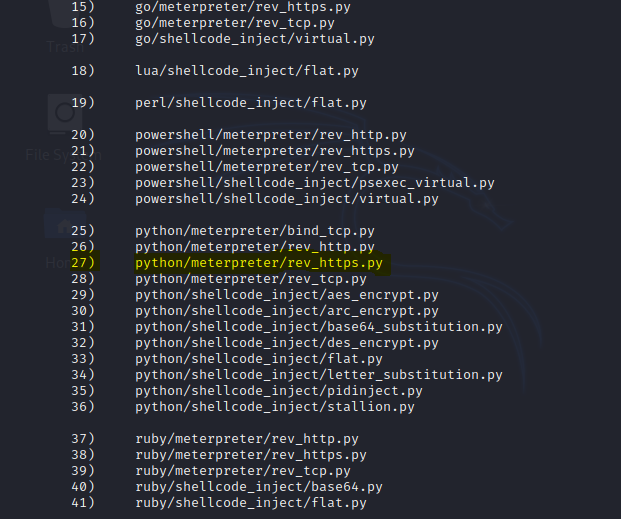
There are two types of tools that are used in the Veil

1. Evasion : This tool is used to generate an undetectable backdoor.
2. Ordnance : This tool is used to generate the payloads used by Evasion. This is more of a secondary tool.

The payload is a part of the code, that does what we want it to. In this case, it gives us a reverse connection, downloads and executes something on a target computer. Now we are using the **use** command to enable the use of any tool. We want to run Evasion, so we are going to run **use 1** command. When Veil-Evasion has loaded, we should see something similar to the following command:



Veil gives a **list** of commands that can run on this tool. In the following screenshot, There are each payload is divided into three parts, and highlighted payload we will be using which are **27) python/meterpreter/rev\_https.py**:



The first part of the payload's name is the programming language in which the payload will be wrapped. In the preceding screenshot, we can see the language used include CS, Python, GO, C, PowerShell, and Ruby. In this example, we are going to use the **go** language.

The second part of the payload is the type of payload. In other words, the type of code that is going to be executed on the target network. In this example, we are going to use **Meterpreter**, which is a payload designed by Metasploit. Metasploit is a huge framework, and sometimes it is used for hacking. Meterpreter runs in memory, so it is difficult to detect, and it does not leave a large footprint. With Meterpreter, we can gain full access over a target computer. It allows us to navigate through the filesystem, install or download files, and much more.

The third part of the payload's name is the method that's going to be used to establish its connection. In our example, that is **rev\_https**. Where **rev** stands for reverse, and **https** is the protocol that will be used to establish the connection. In the preceding screenshot, there are a few examples of **rev\_tcp**, which creates a reverse TCP connection.

A reverse connection is where the target machine connects to the attacker's machine via a backdoor. This method bypass antivirus programs, because the connection is not directed at the target computer, but rather at the attacker instead. In our example, we are going to use a port 80 or 8080, that many websites use, so that the connection will appear as a harmless website connection.

Now set LHOST, LPORT and generate payload:

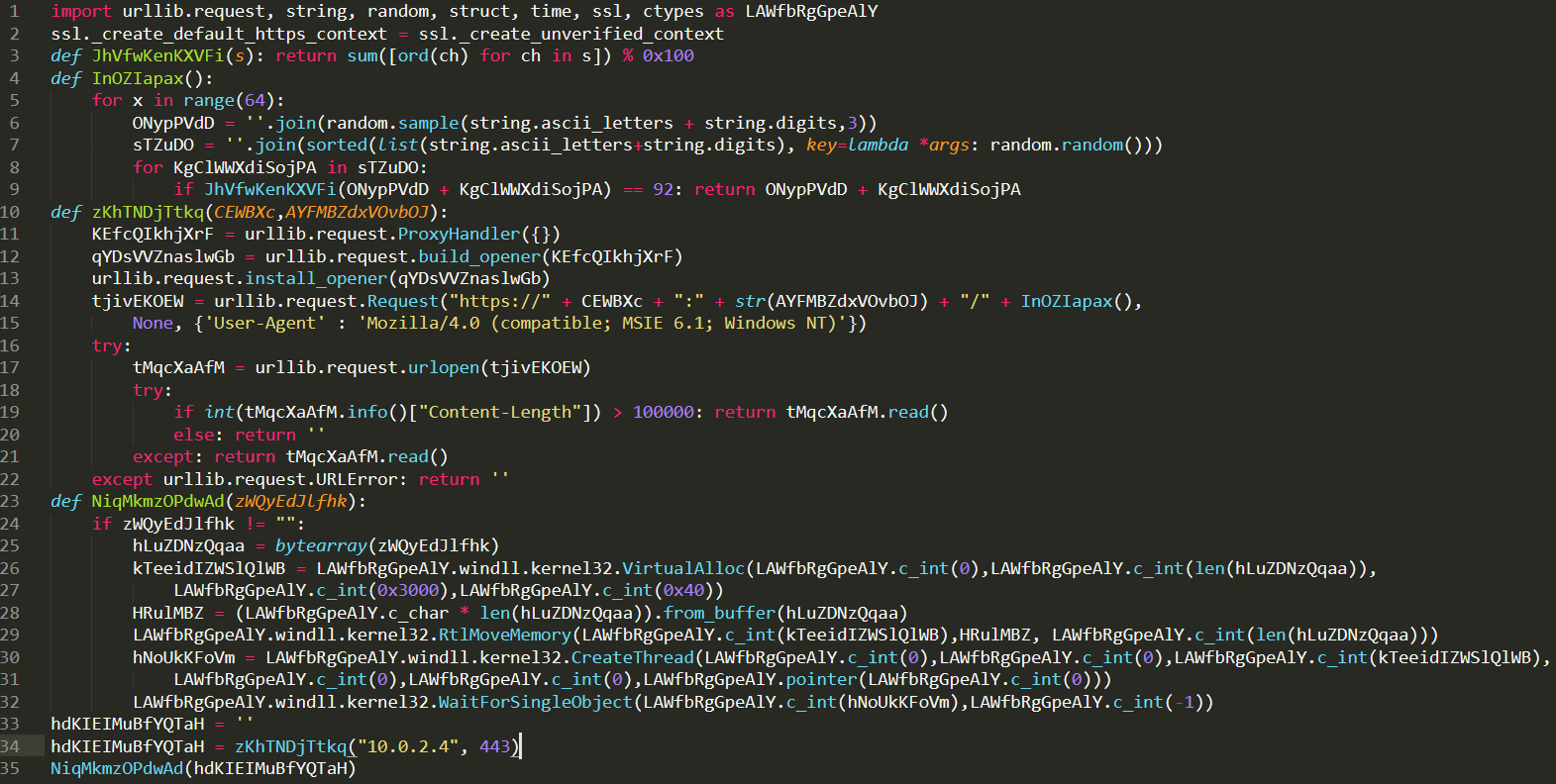


Set file name:



Generated Executable written to: /var/lib/veil/output/compiled/trojanfile.exe

Source Code of executable file:



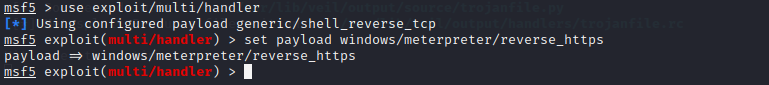
**Listening for connection:**

The backdoor which created uses a reverse payload. To work the reverse payload, a port need to open in our Kali machine so that the target machine can connect to it. When created the backdoor, port set to 447, so port 447 needed to open on Kali machine. In this example, the name of chosen payload is **windows/meterpreter/rev\_https**.

To listen for an incoming connection Metasploit Framework used. To run msfconsole use command:

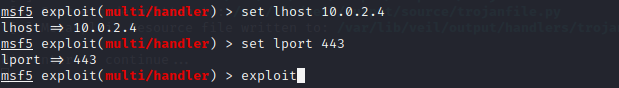


To listen incoming connections a module in Metasploit Framework used. Use following command to launch that module and set PAYLOAD:



Now set the LHOST and LPORT to the IP address of our Kali machine using the following command:

And then execute exploit command:



Server started for listening connections. When user execute .exe file in target Windows Machine, Kali Machine will show connection form target computer.

After you get the successful connection, you can see a check system info by using command :

meterpreter**>** sysinfo

If there is any error occurred:

1. **Check LHOST and LPORT again. LHOST and LPORT must be in multi/handler as we set while we create payload.**
2. **Check “set payload command” again.**

If windows defender detect trojan file:

**Then try different language to generate payload and repeat all steps again and again until you get undetectable payload.**

**Tip: One thing you should remember that while running command :**

**$ msfconsole**

**You must not be in the root directory.**

**That’s all for now!!**