🔷

Hacking Tools Blue Team

- Este curso se hará con los recursos que nos dan en un fichero zip

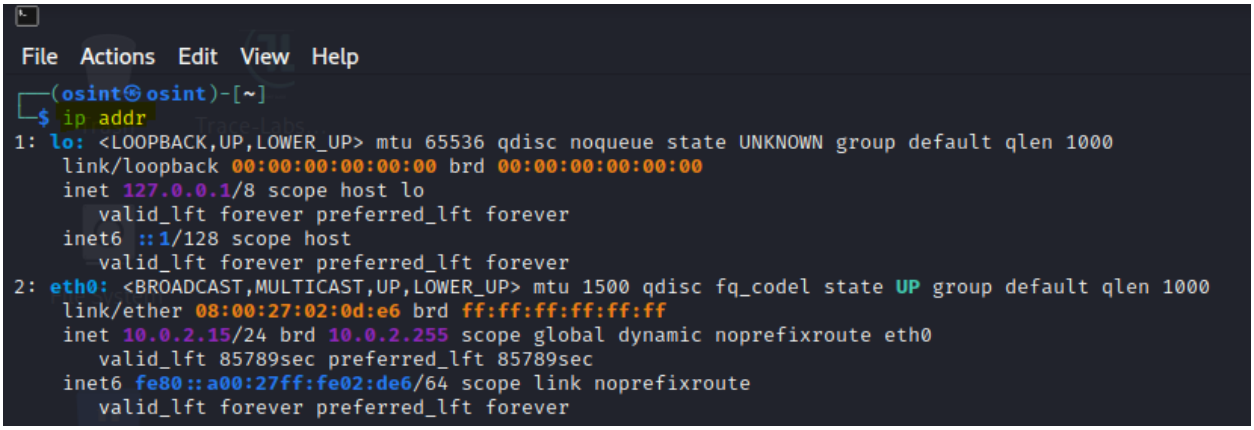
En el primer apartado veremos como se modifican los grupos y usuario de linux (doy por hecho que esta información ya se conoce)

Por si no sabeis de esta información dejo este link: https://santi-gf.github.io/usuarios-grupos/

Accesos remotos

Para esto necesitaremos otra máquina virtual para hacer conexiones

Primero miraremos cual es nuestra ip:



En nuestra máquina que tiene el servicio ssh checkeamos su estado:

```
service ssh status
```

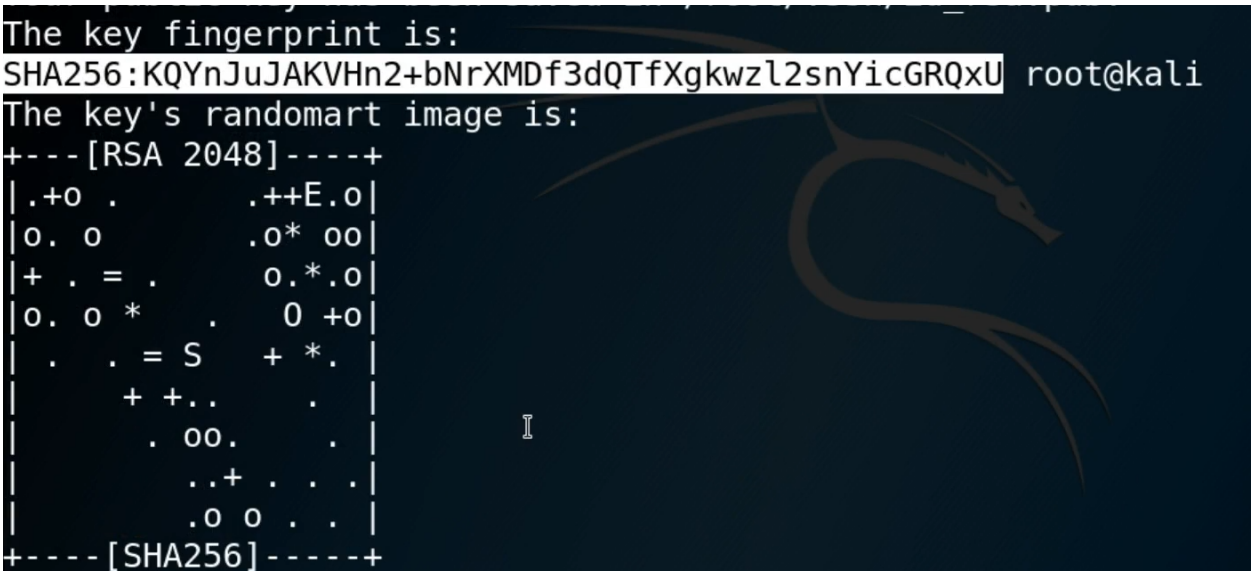
- Ahora si quisieramos conectarnos a una máquina usariamos:

```
ssh nombre@ip
```

y la password que nos pida posteriormente.

- Crear una clave para entrar siempre que queramos

```
ssh-keygen -t rsa
```



Ahora lanzaremos:

```
ssh-copy-id-i /root/.ssh/id_rsa.pub nombre@ip
```

y le metemos la password.

Metasploit

Usaremos el siguiente código para instalar la herramienta:

```
sudo apt install metasploit-framework
```

Ahora con msfconsole lanzaremos la consola de metasploit

Con -show exploits podremos saber que exploits tiene el framework

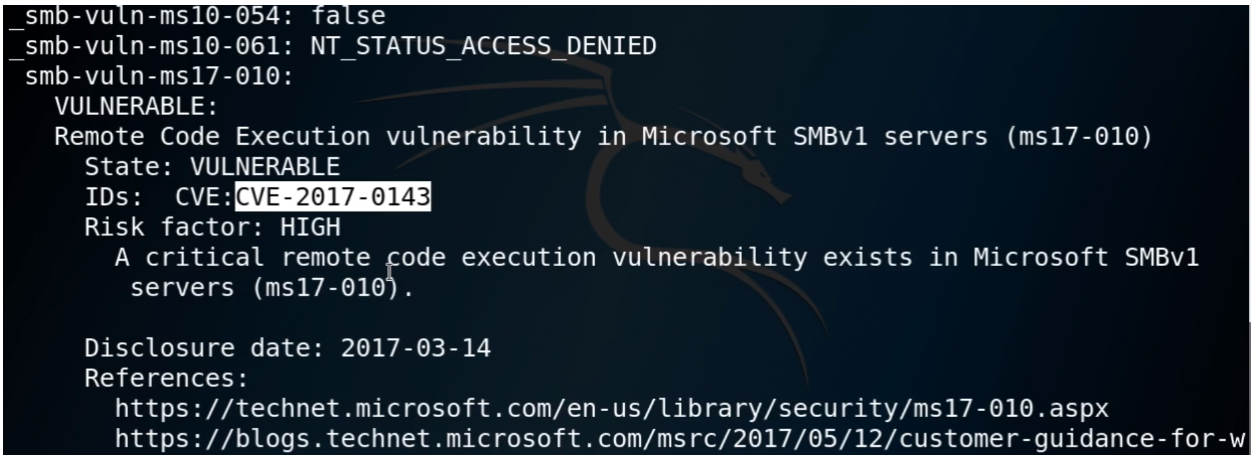
Por aquí podremos ir usando uno o otro para los objetivos que tengamos en el momento

Ahora vamos a atacar una máquina de windows server:

Con el siguiente comando podremos sacar que puertos tiene un host

```
nmap --script vuln "ip"
```

Este es un ejemplo conseguido sobre un máquina Microsoft Server 2008:

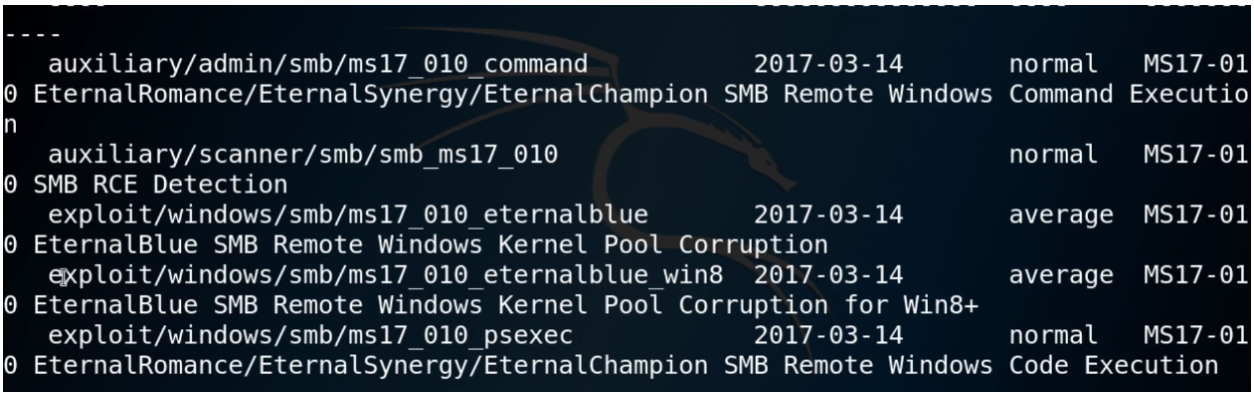


Es una vulnerabilidad registrada en el CVE con el id subrayado

Ahora buscaremos esa vulnerabilidad:

```
search CVE-2017-0143
```

Resultado, una lista de exploits usables:



Por ejemplo, usaremos:

```
use exploit/windows/smb/ms17_010_psexec
```

Este nos dará una serire de parámetros para usar, indicando qué pasará cuando los usemos.

En el caso de una máquina Linux server pues el procedimiento es igual

Este tipo de ataques nos ayudarán a conseguir diferentes objetivos como, mandar un pantallazo azul, tirar el servidor o incluso entrar en el sistema operativo de la máquina atacada, pudiendo así robar toda la información que queramos.

Librerias Python

Con python instalado en nuestro sistema, ejecutaremos la siguiente linea para instala python WhoIs:

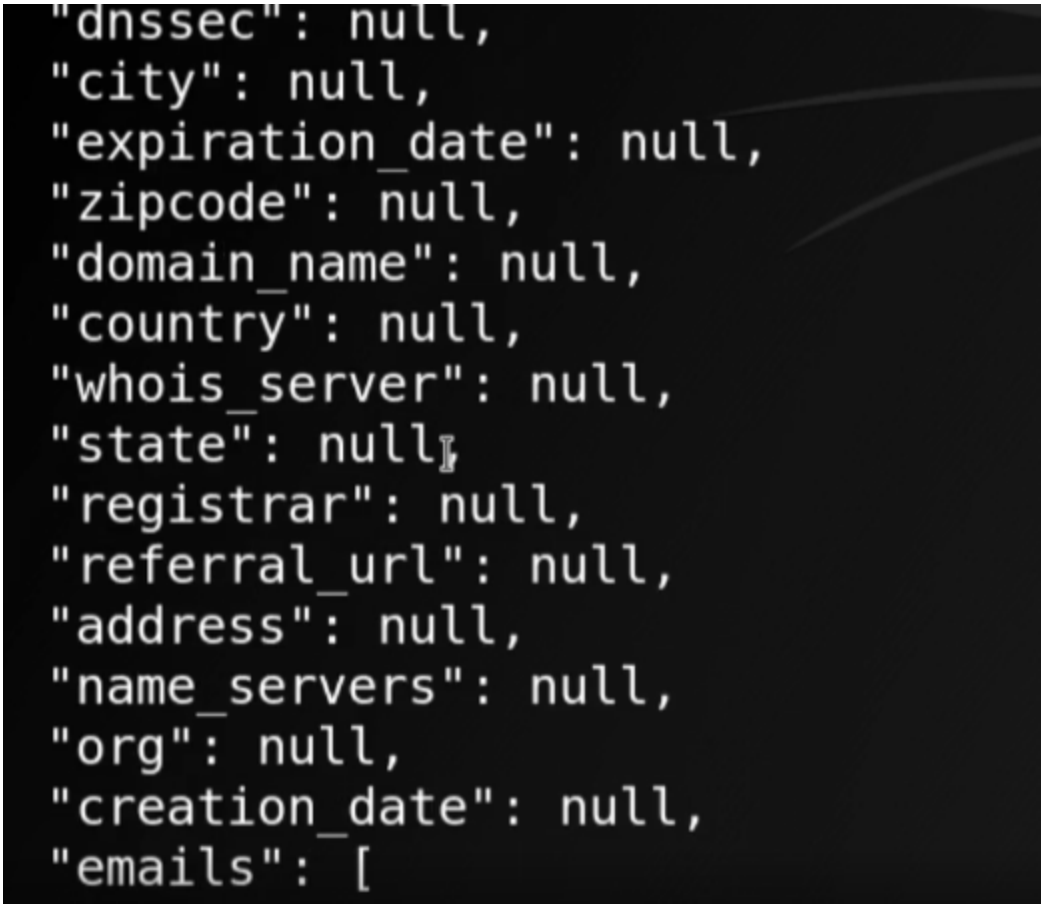
```
sudo apt install python3-whois
```

Con el comando “python” podremos iniciar un entorno python3

Usamos:

```
import whois
w = whois.whois('openwebinars.net')
```

```
print("w")
```



Consiguermos mucha información de cualquiera página web

Librerias

Scapy: Nos ayudará a rastrear una dirección ip de muchas maneras, podremos detectar los puertos abiertos e incluso los filtrados. También nos servirá para trackear paquetes al igual que wireshark, pero la ventaja que tienes es que también es capaz de enviarlos, por lo tanto se podría inyectar código malicioso en uno de estos paquetes.

Beautifulsoup: Será una herramienta capaz de analizar un documento html y a través de estos, obtener mucha información.