



# 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:

```
File Actions Edit View Help
(osint@osint)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:02:0d:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 85789sec preferred_lft 85789sec
    inet6 fe80::a00:27ff:fe02:de6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

En nuestra máquina que tiene el servicio ssh chequeamos 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
```

```
The key fingerprint is:
SHA256:KQYnJuJAKVHn2+bNrXMDf3dQTfXgkwzl2snYicGRQxU root@kali
The key's randomart image is:
+---[RSA 2048]---+
|. +o .      .++E.o|
|o. o      .o* oo|
|+ . = .      o.*.o|
|o. o *      0 +o|
| . . = S    + *.|
|      + +..   .|
|      . oo.   .|
|      ..+ . . .|
|      .o o . .|
+-----[SHA256]-----+
```

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:

```
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
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 SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-w
```

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:

----									
0	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	MS17-01	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution				
0	auxiliary/scanner/smb/smb_ms17_010		normal	MS17-01	SMB RCE Detection				
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	MS17-01	EternalBlue SMB Remote Windows Kernel Pool Corruption				
0	exploit/windows/smb/ms17_010_eternalblue_win8	2017-03-14	average	MS17-01	EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+				
0	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	MS17-01	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution				

Por ejemplo, usaremos:

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

Este nos dará una serie 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.

## Librerías Python

Con python instalado en nuestro sistema, ejecutaremos la siguiente línea para instalar 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")
```

```
"dnssec": null,  
"city": null,  
"expiration_date": null,  
"zipcode": null,  
"domain_name": null,  
"country": null,  
"whois_server": null,  
"state": null,  
"registrar": null,  
"referral_url": null,  
"address": null,  
"name_servers": null,  
"org": null,  
"creation_date": null,  
"emails": [
```

Consiguermos mucha información de cualquiera página web

## Librerías

**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.