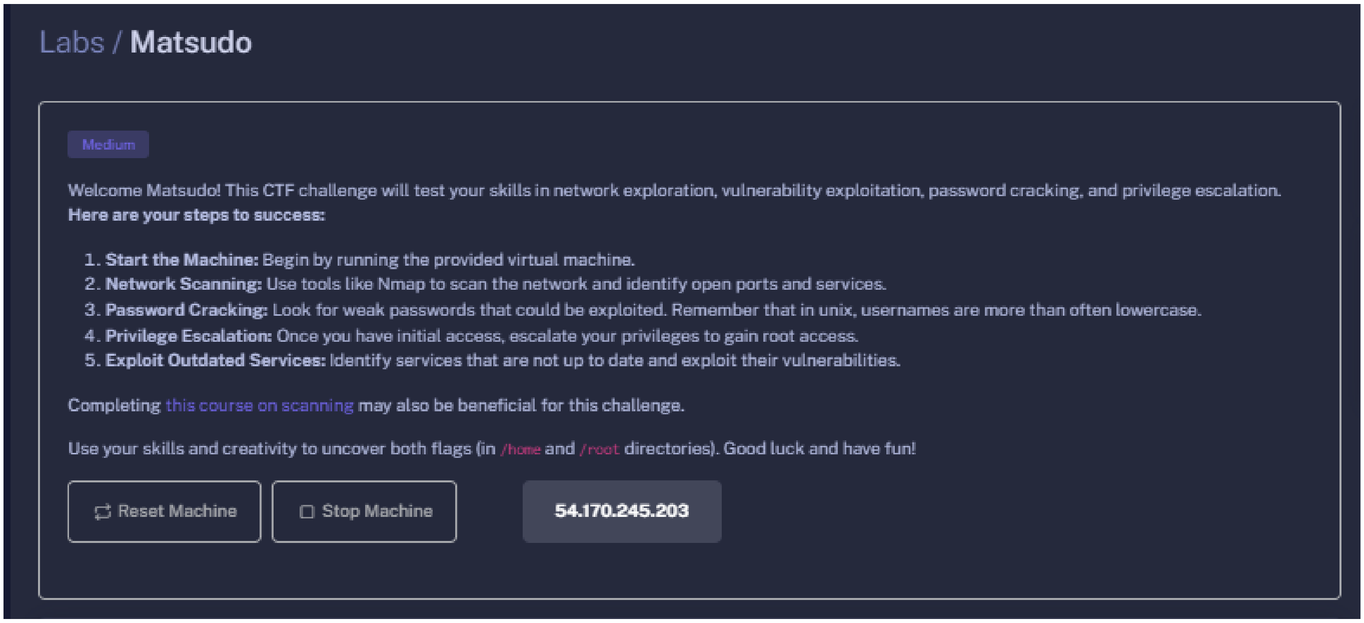


Labs / **Matsudo**

Medium

Welcome Matsudo! This CTF challenge will test your skills in network exploration, vulnerability exploitation, password cracking, and privilege escalation.
Here are your steps to success:

1. **Start the Machine:** Begin by running the provided virtual machine.
2. **Network Scanning:** Use tools like Nmap to scan the network and identify open ports and services.
3. **Password Cracking:** Look for weak passwords that could be exploited. Remember that in unix, usernames are more than often lowercase.
4. **Privilege Escalation:** Once you have initial access, escalate your privileges to gain root access.
5. **Exploit Outdated Services:** Identify services that are not up to date and exploit their vulnerabilities.

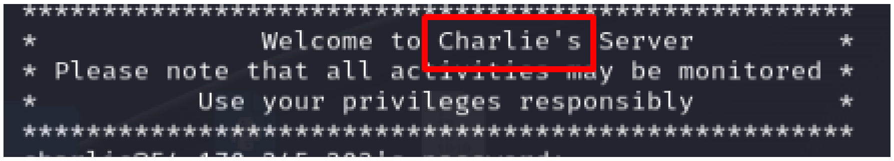
Completing this course on scanning may also be beneficial for this challenge.

Use your skills and creativity to uncover both flags (in `/home` and `/root` directories). Good luck and have fun!

if you try to connect to the ssh server

```
ssh $ip
```

you will get the username

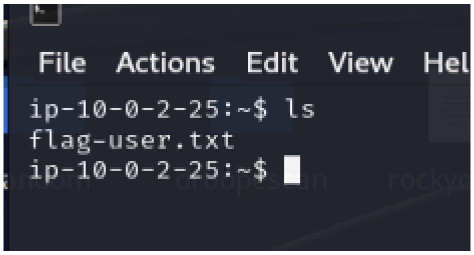


```
*****************************************************
*              Welcome to Charlie's Server          *
* Please note that all activities may be monitored *
*          Use your privileges responsibly          *
*****************************************************
```

and for link usernames should be lowercase so "charlie"

well nice we found the username we need the password now

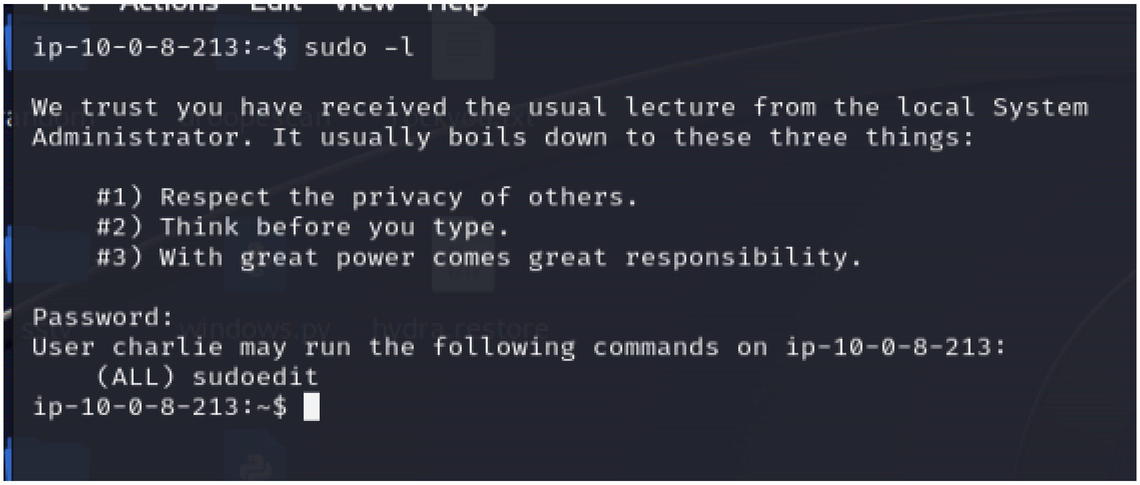
running a brute force attack gave us the password and got flag-user.txt



```
ip-10-0-2-25:~$ ls
flag-user.txt
ip-10-0-2-25:~$ 
```

then we need to do privilege escalate

doing `sudo -l` will give us the permissions that we have as charlie user



```
ip-10-0-8-213:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
User charlie may run the following commands on ip-10-0-8-213:
    (ALL) sudoedit
ip-10-0-8-213:~$ 
```

amazing we got access to `sudoedit` which is dangerous to have a non-root user
so now we can do `sudo sudoedit /root/flag-root.txt` and you will get the root flag :)