CTF101 Machine

🕵️ CTF101 Walkthrough | My Cybersecurity Learning Journey

Challenge Overview:-

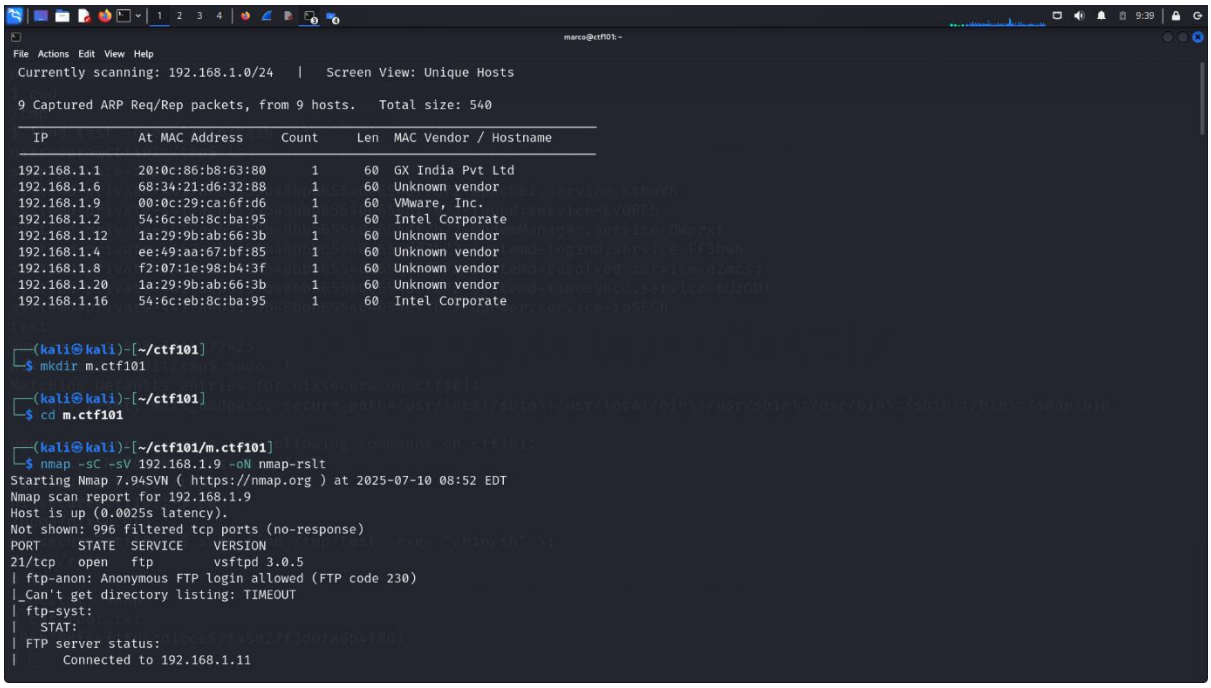
CTF101 is an entry-level Capture The Flag challenge designed to strengthen fundamental cybersecurity skills like reconnaissance, enumeration, exploitation, and privilege escalation. It's a great starting point for beginners stepping into the world of penetration testing.

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

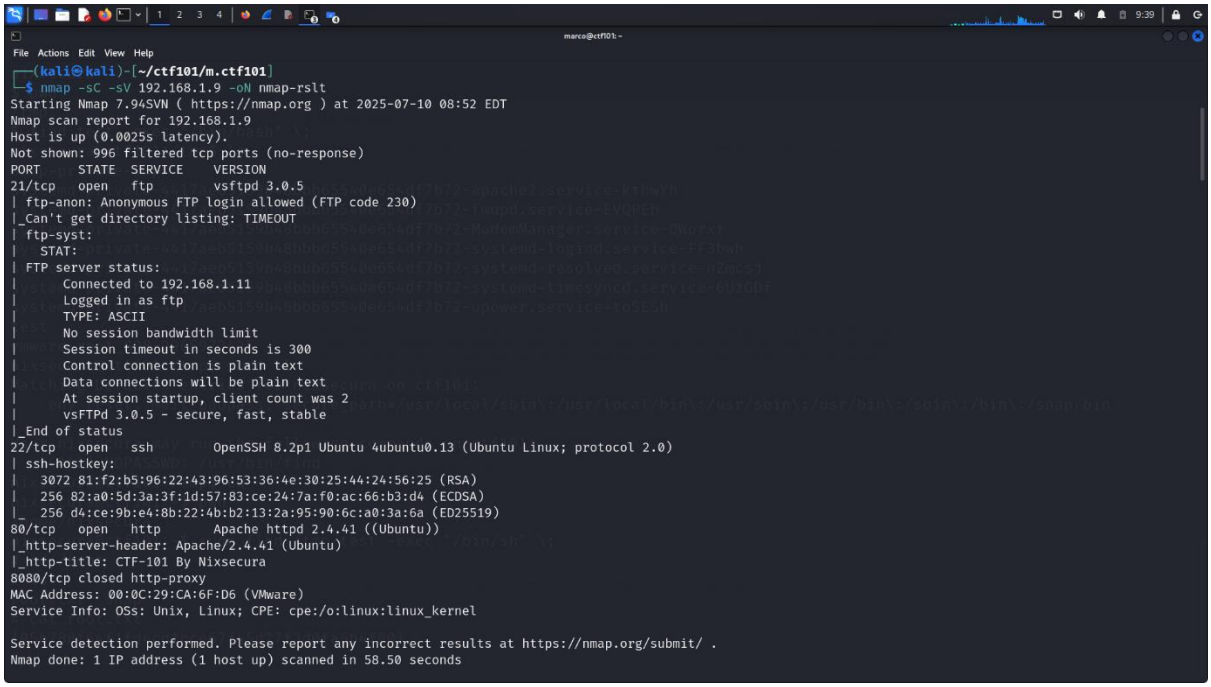
It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.



Step-2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing.
It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.



Step-3:-

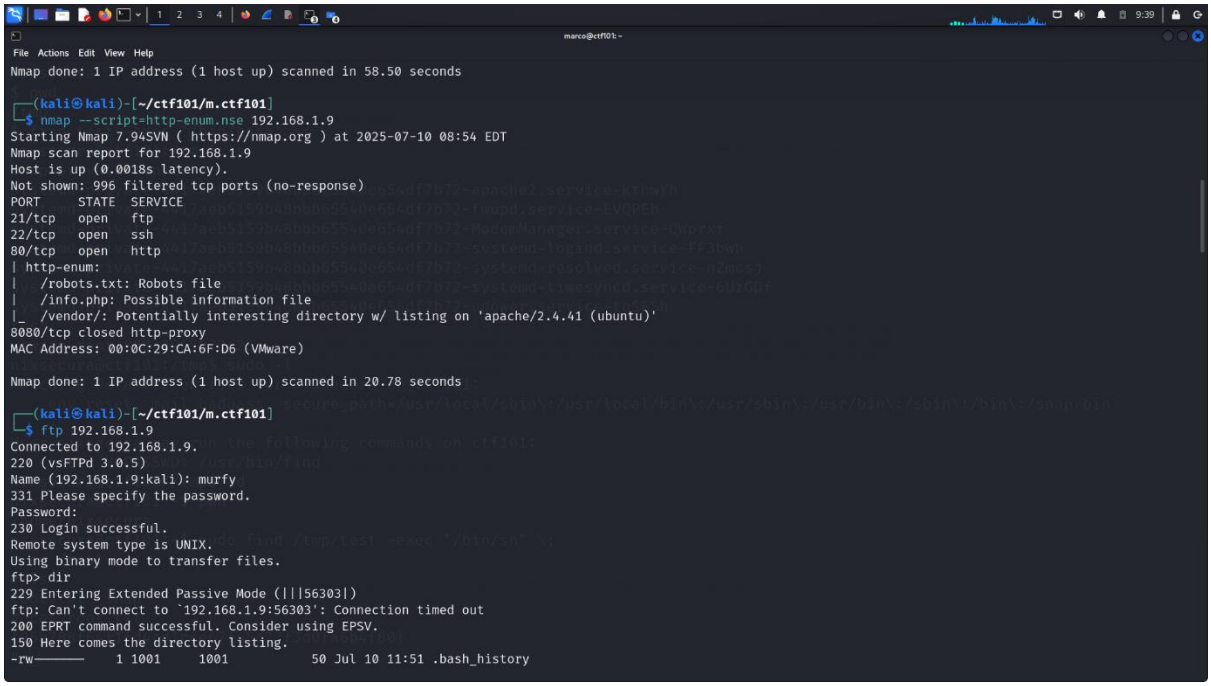
- **`nmap`** → The network scanning tool.
- **`--script=http-enum.nse`** → Runs the **Nmap Scripting Engine (NSE)** script named `http-enum.nse`.
- **`<target>`** → The IP address, domain, or hostname of the system you're scanning.

- It's an **NSE script** included with Nmap.

- Purpose: **Enumerate common web application directories and files** on a web server.

- Similar to what **DirBuster / Gobuster / Dirsearch** do.

- It relies on a **dictionary file of common paths** and makes HTTP requests to check if those directories or files exist.

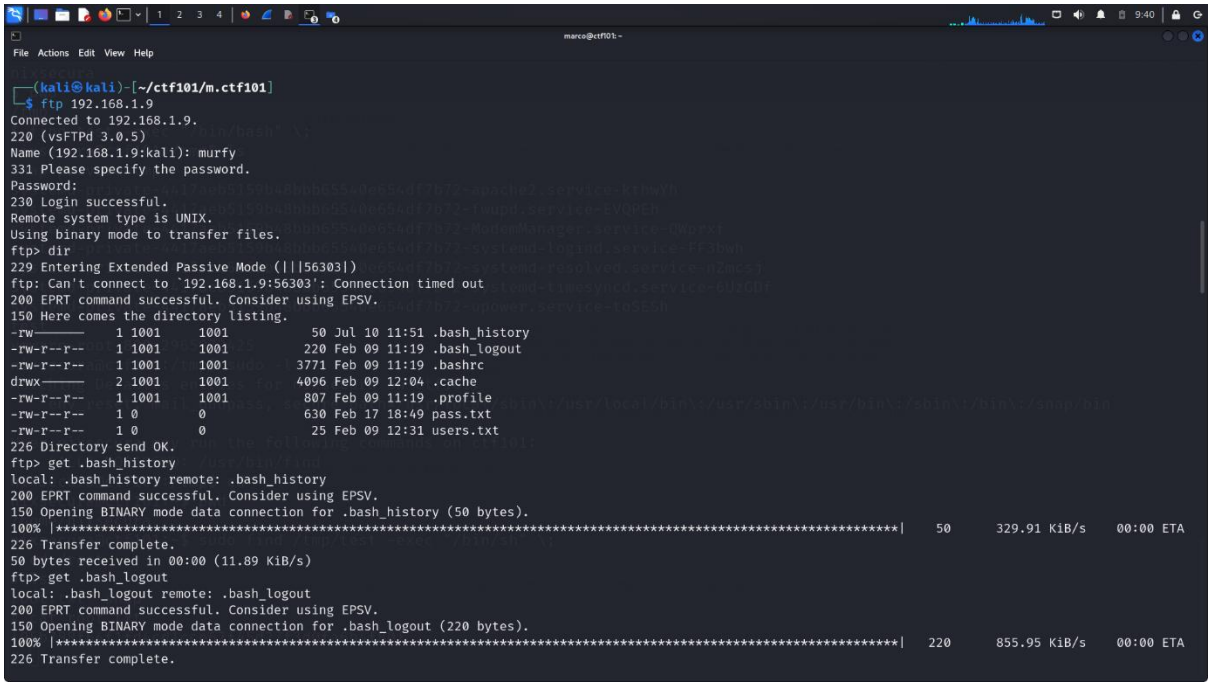


Step-4:-

FTP (**File Transfer Protocol**) is a standard network protocol used to transfer files between a client and a server over a TCP/IP network (like the Internet).
It usually runs on **port 21** (control connection) and sometimes **port 20** (data connection).

You can use the **ftp command** in Linux/Windows to connect to an FTP server, upload, download, and manage files.

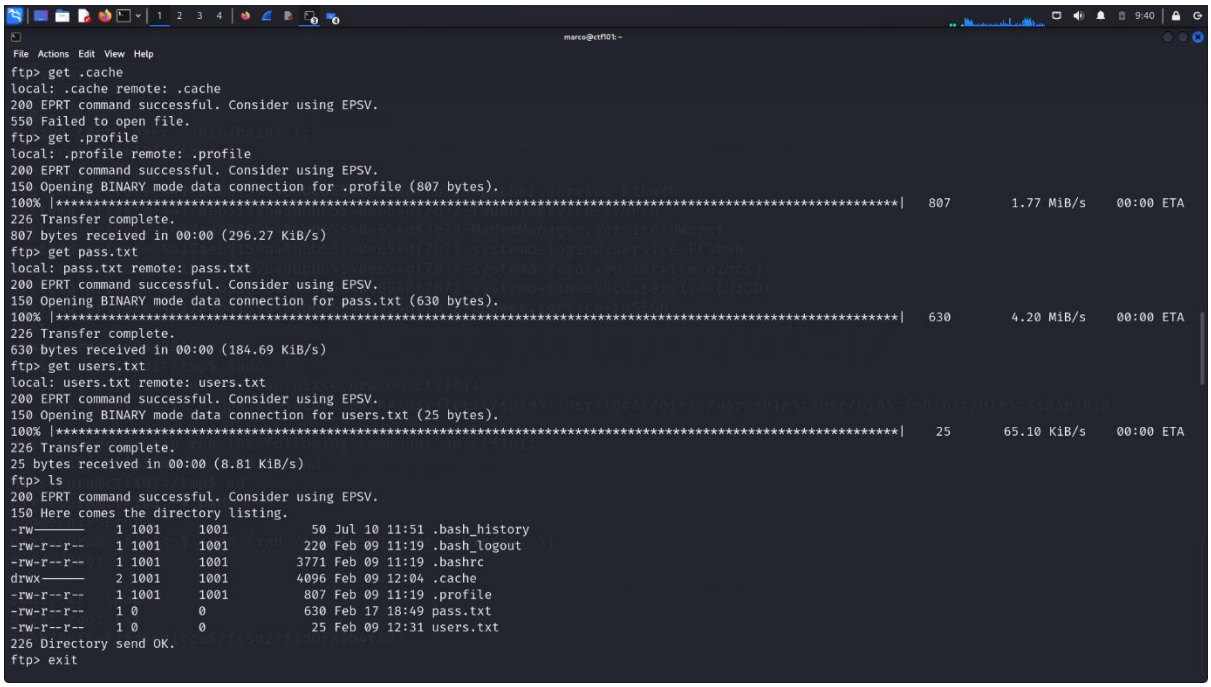
1. **Client initiates a connection** to an FTP server.
2. Authentication happens (using a **username and password**, or anonymously).
3. Files can then be **uploaded, downloaded, renamed, deleted, or listed**.
4. Communication uses **two channels**:
    - **Control Channel (Port 21):** For commands (e.g., login, list files).
    - **Data Channel (Port 20 by default):** For transferring the actual file contents.



In these step of we can get two files that is :-

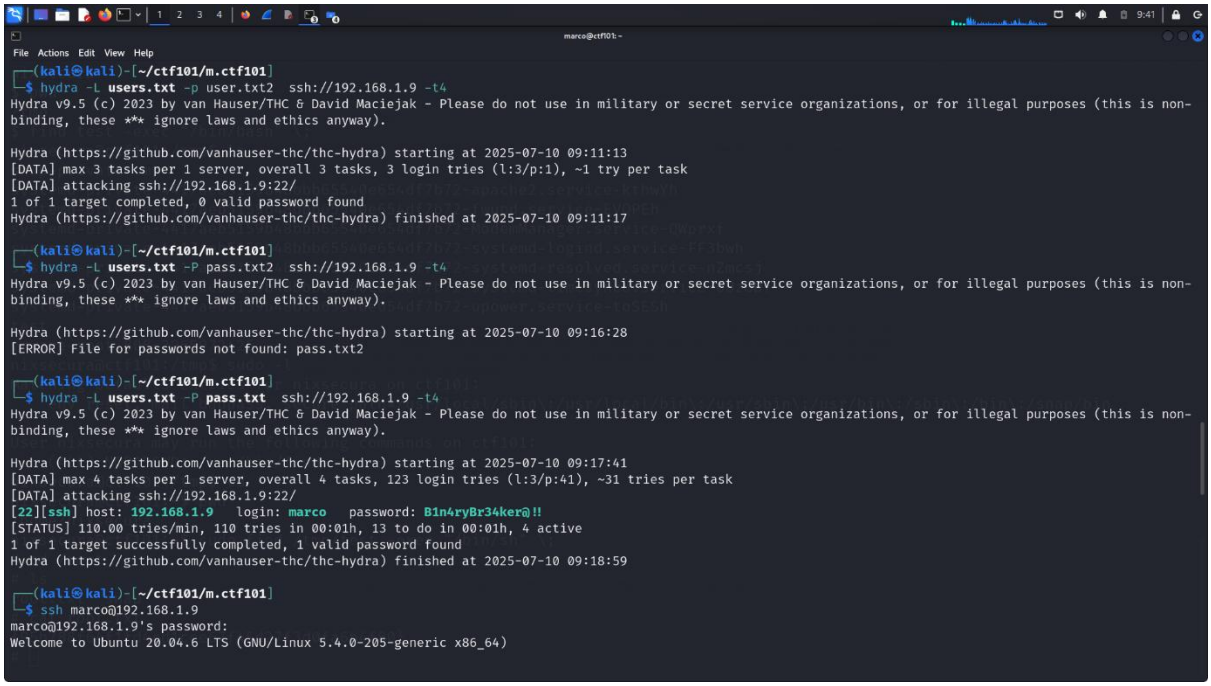
Pass.txt

User.txt



Step-5:-

Hydra (also called **THC-Hydra**) is a **popular password-cracking tool** used in penetration testing for performing **brute force attacks** on login services like SSH, FTP, HTTP, RDP, MySQL, Telnet, and many more.

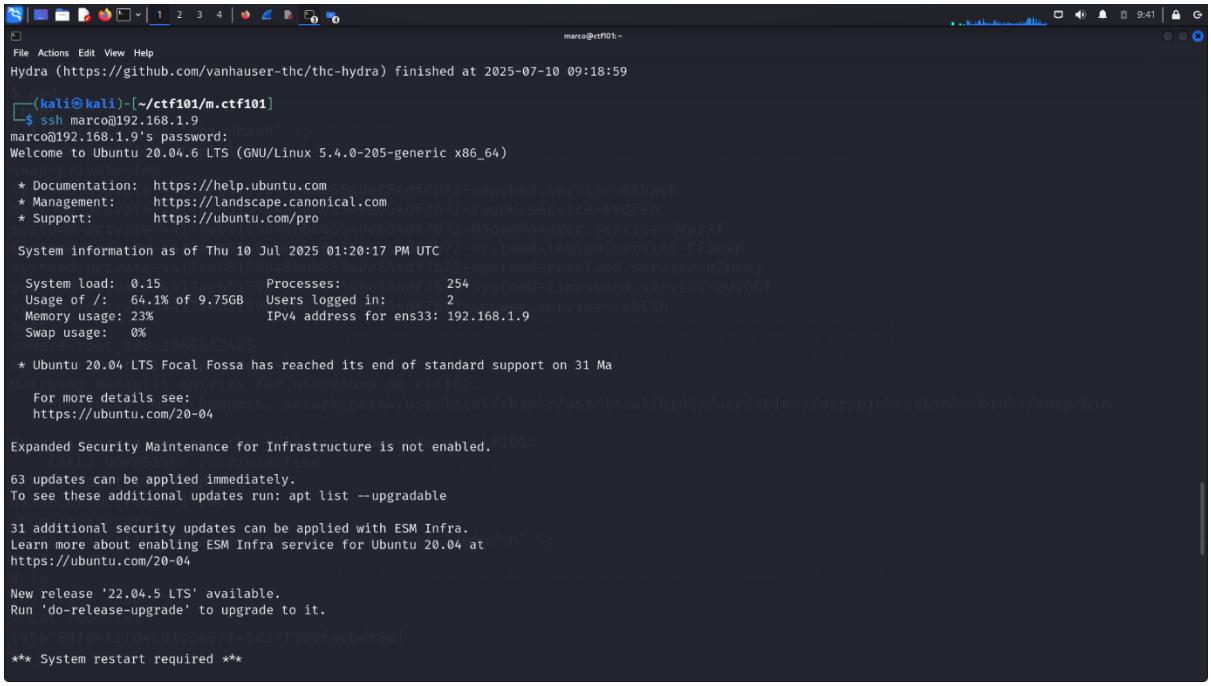


Step-6:-

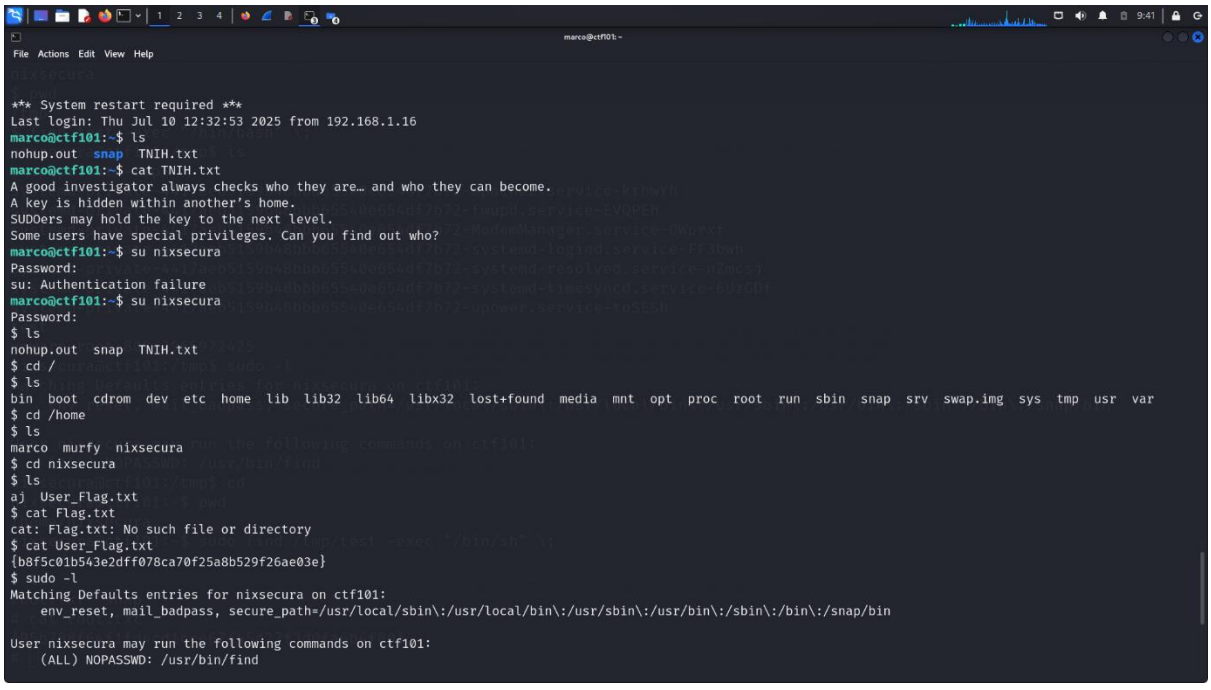
SSH (**Secure Shell**) is a **network protocol** that allows secure communication between two computers over an insecure network. It is commonly used for:

- Remote login to servers
- Secure file transfer (SCP, SFTP)
- Tunneling and port forwarding
- Running commands remotely

It replaces older, insecure protocols like **Telnet, rlogin, and FTP**, which send data in plaintext.

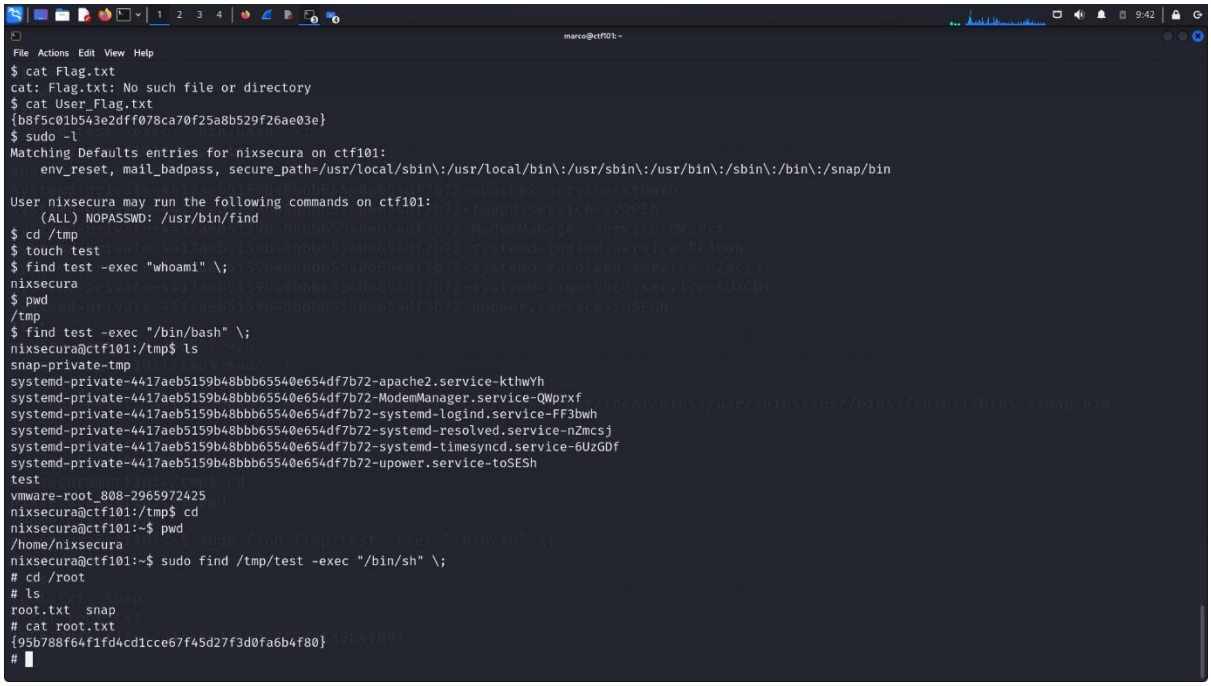


In the 6th step, we get 1st flag we can capture



Step-7:-

In the last step, we can get the last flag in this CTF machine.


marco@ctf101: ~
File Actions Edit View Help
$ cat Flag.txt
cat: Flag.txt: No such file or directory
$ cat User_Flag.txt
{b8f5c01b543e2dff078ca70f25a8b529f26ae03e}
$ sudo -l
Matching Defaults entries for nixsecura on ctf101:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User nixsecura may run the following commands on ctf101:
(ALL) NOPASSWD: /usr/bin/find
$ cd /tmp
$ touch test
$ find test -exec "whoami" \;
nixsecura
$ pwd
/tmp
$ find test -exec "/bin/bash" \;
nixsecura@ctf101:/tmp$ ls
snap-private-tmp
systemd-private-4417aeb5159b48bbb65540e654df7b72-apache2.service-kthwYh
systemd-private-4417aeb5159b48bbb65540e654df7b72-ModemManager.service-QWprxf
systemd-private-4417aeb5159b48bbb65540e654df7b72-systemd-logind.service-FF3bwh
systemd-private-4417aeb5159b48bbb65540e654df7b72-systemd-resolved.service-nZmcsj
systemd-private-4417aeb5159b48bbb65540e654df7b72-systemd-timesyncd.service-6UzGDf
systemd-private-4417aeb5159b48bbb65540e654df7b72-upower.service-toSESh
test
vmware-root_808-2965972425
nixsecura@ctf101:/tmp$ cd
nixsecura@ctf101:~$ pwd
/home/nixsecura
nixsecura@ctf101:~$ sudo find /tmp/test -exec "/bin/sh" \;
cd /root
ls
root.txt snap
cat root.txt
{95b788f64f1fd4cd1cce67f45d27f3d0fa6b4f80}
#