CSCI-476 Final Test

Gunnar Holwerda

May 6, 2015

Table of Contents

Executive Summary

1.1 Executive Summary

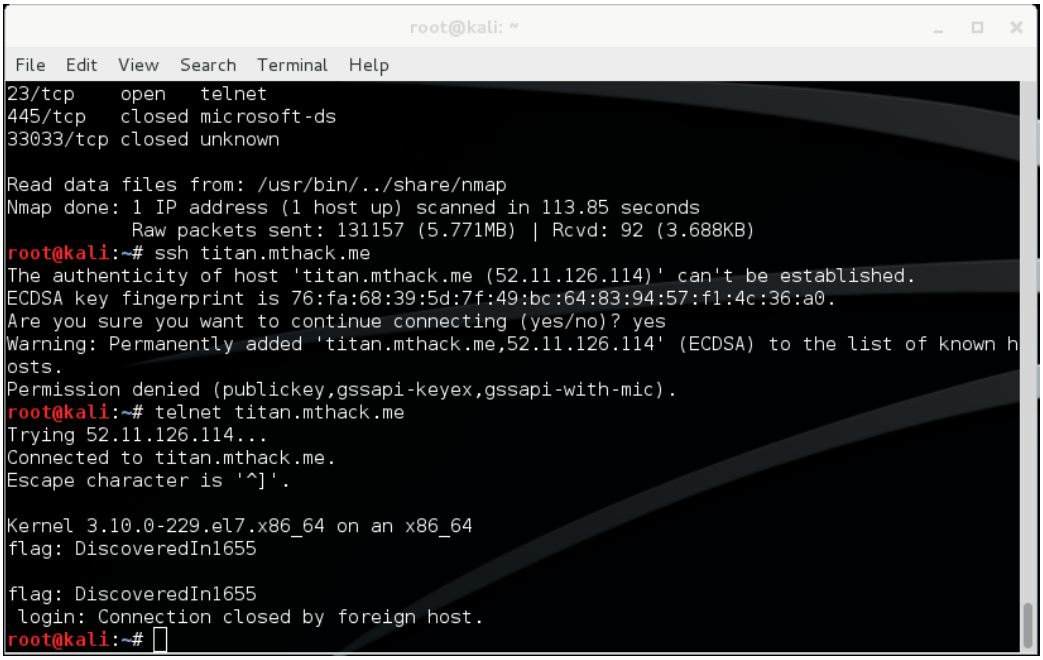
Round 1

2.1 DiscoveredIn1655

When starting out I was given the information that the members of mhk had been discussing RFC2100. This RFC mentions a few names, so I began using the names mentioned as subdomains of mthack.me and quickly found titan.mthack.me. I ran nmap on the host to see what ports were open...

```
$ nmap -sS -p1-65535 titan.mthack.me -v -T4
```

The nmap returned that port 22 and 23 were open. I attempted to ssh, but found that a public key was needed. Next I used telnet to connect to port 23 and was presented with my first flag "DiscoveredIn1655".

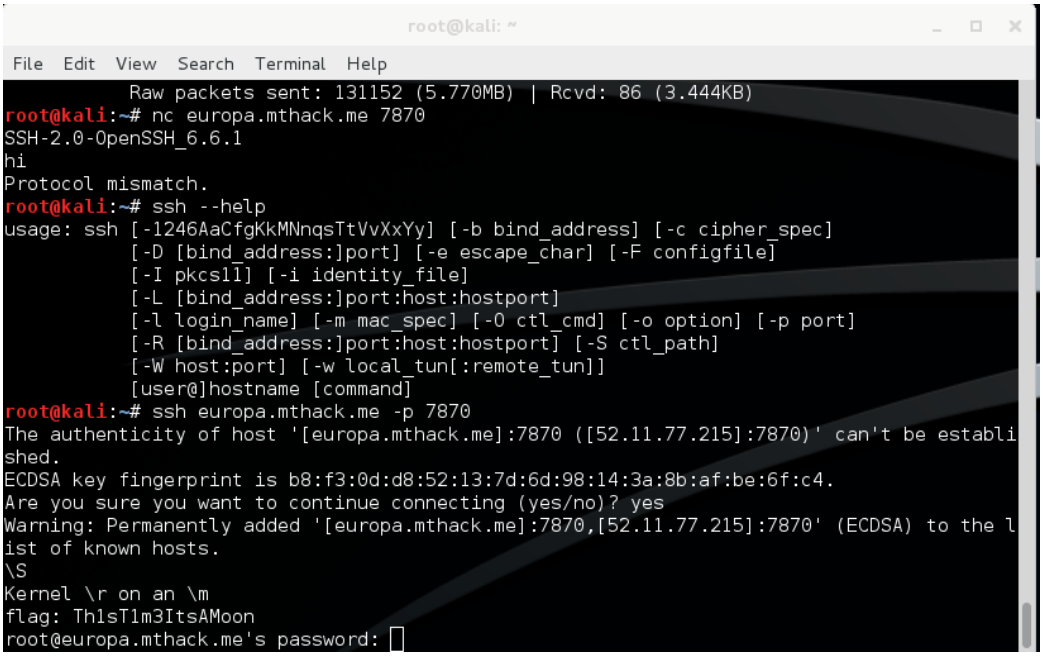


2.2 Th1sT1m3ItsAMoon

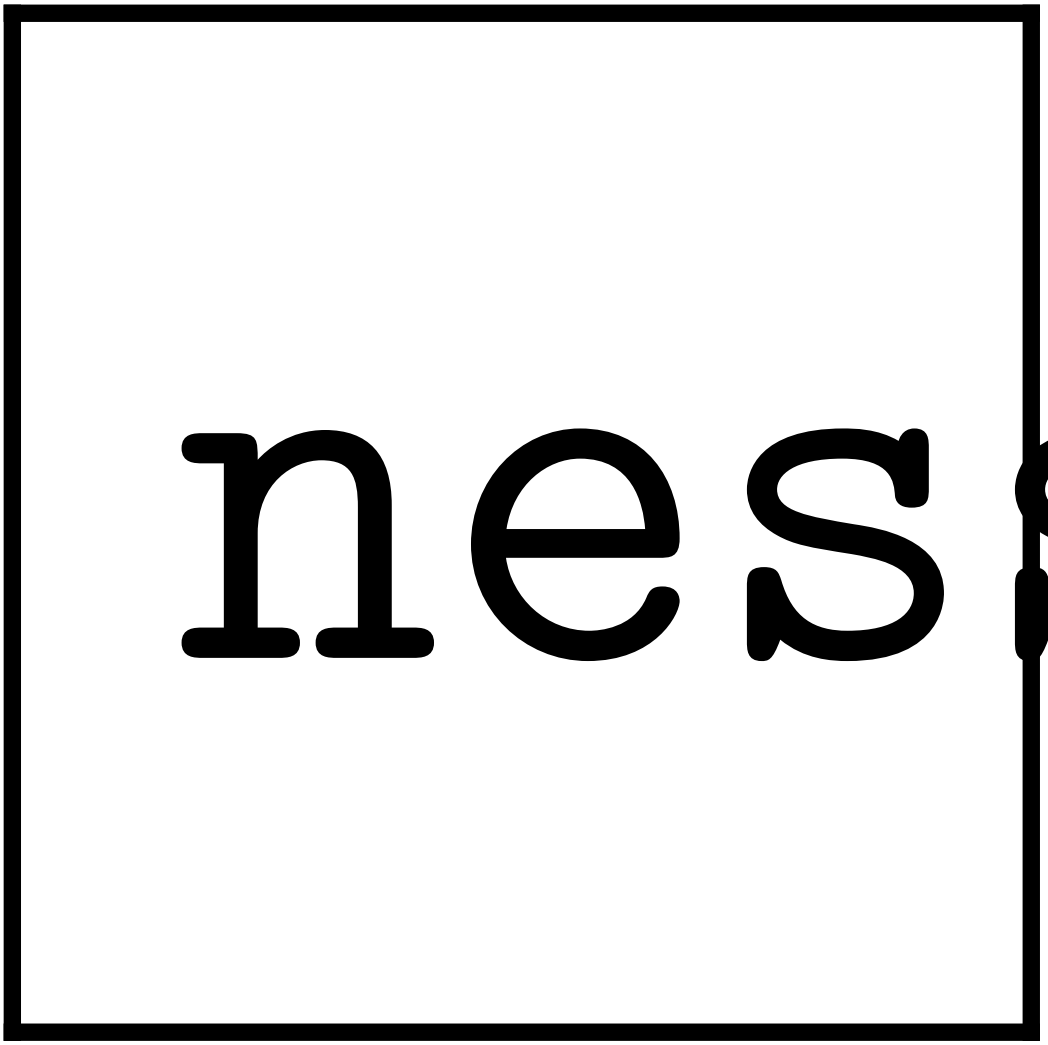
In addition to titan.mthack.me, I was able to find the europa.mthack.me subdomain. After an nmap on europa I saw that port 7870 was open. There was no information about this port, so I used NetCat to connect to it, it returned "SSH-2.0-OpenSSH_6.6.1". After seeing this I knew that I should use SSH to connect to europa.mthack.me on this port.

```
$ ssh europa.mthack.me -p 7870
```

After adding europa to my known_hosts I was presented with my second flag "Th1sT1m3ItsAMoon".


root@kali: ~
File Edit View Search Terminal Help
Raw packets sent: 131152 (5.770MB) | Rcvd: 86 (3.444KB)
root@kali:~# nc europa.mthack.me 7870
SSH-2.0-OpenSSH_6.6.1
hi
Protocol mismatch.
root@kali:~# ssh --help
usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
[-D [bind_address:]port] [-e escape_char] [-F configfile]
[-I pkcs11] [-i identity_file]
[-L [bind_address:]port:host:hostport]
[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
[-R [bind_address:]port:host:hostport] [-S ctl_path]
[-W host:port] [-w local_tun[:remote_tun]]
[user@]hostname [command]
root@kali:~# ssh europa.mthack.me -p 7870
The authenticity of host '[europa.mthack.me]:7870 ([52.11.77.215]:7870)' can't be establi
shed.
ECDSA key fingerprint is b8:f3:0d:d8:52:13:7d:6d:98:14:3a:8b:af:be:6f:c4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[europa.mthack.me]:7870,[52.11.77.215]:7870' (ECDSA) to the l
ist of known hosts.
\S
Kernel \r on an \m
flag: Th1sT1m3ItsAMoon
root@europa.mthack.me's password:

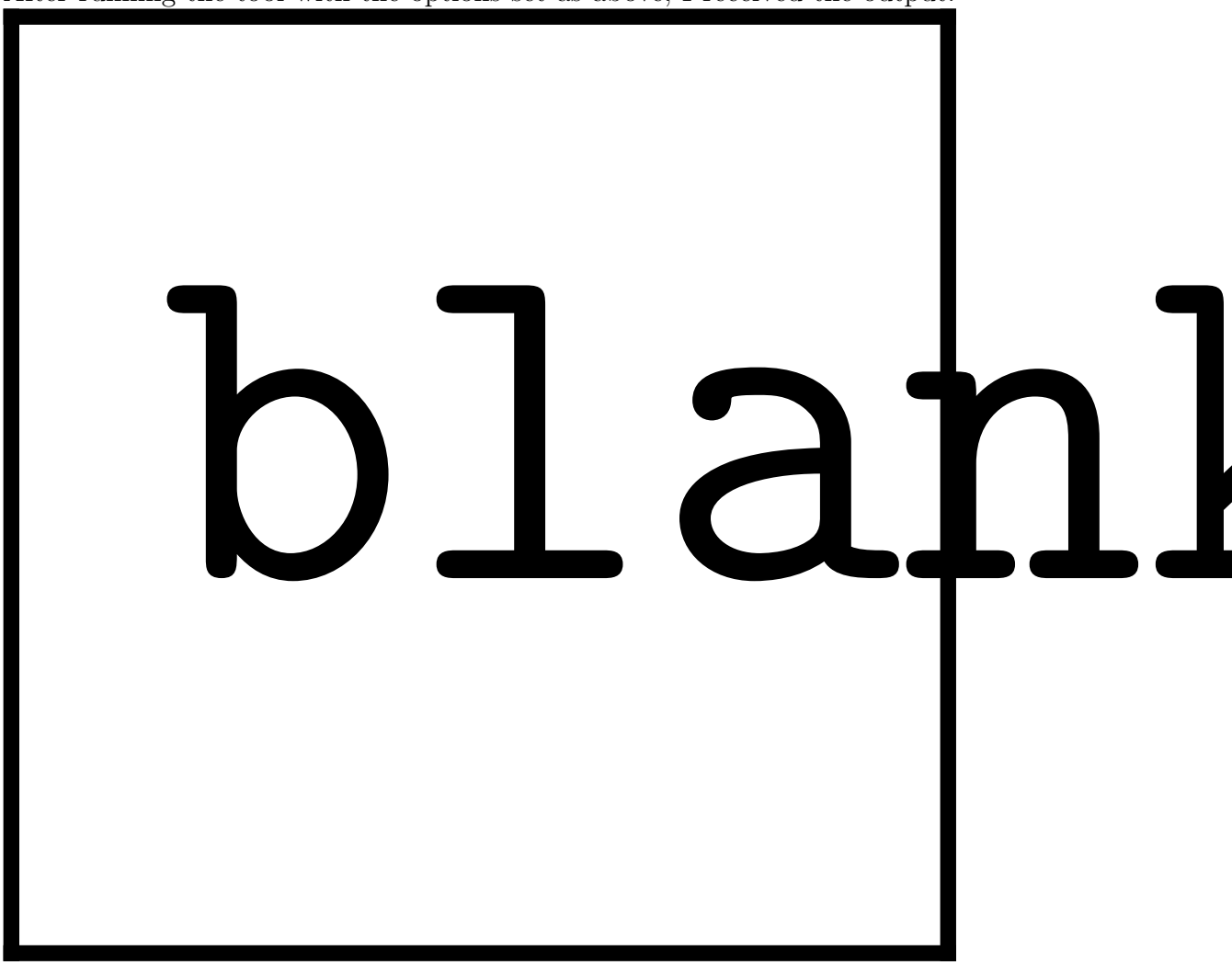
2.3 Round 2



The Nessus scan of the virtual machine returned many errors, but since I was interested in attacking the MySQL service I started to check if there were any errors associated with it. I was able to find a vulnerability associated with MySQL of "MySQL Unpassworded Account Check".
After finding this vulnerability I decided that it was time to load up msfconsole and start to try to exploit it. After searching for MySQL I was able to find a tool called "mysql_login". I decided to try it out as I figured I would try to login to the MySQL service using a blank password like Nessus suggested there was.

```
> use auxiliary/scanner/mysql/mysql_login
> info
> set RHOSTS 192.168.2.12
> set BLANK_PASSWORDS true
> exploit
```

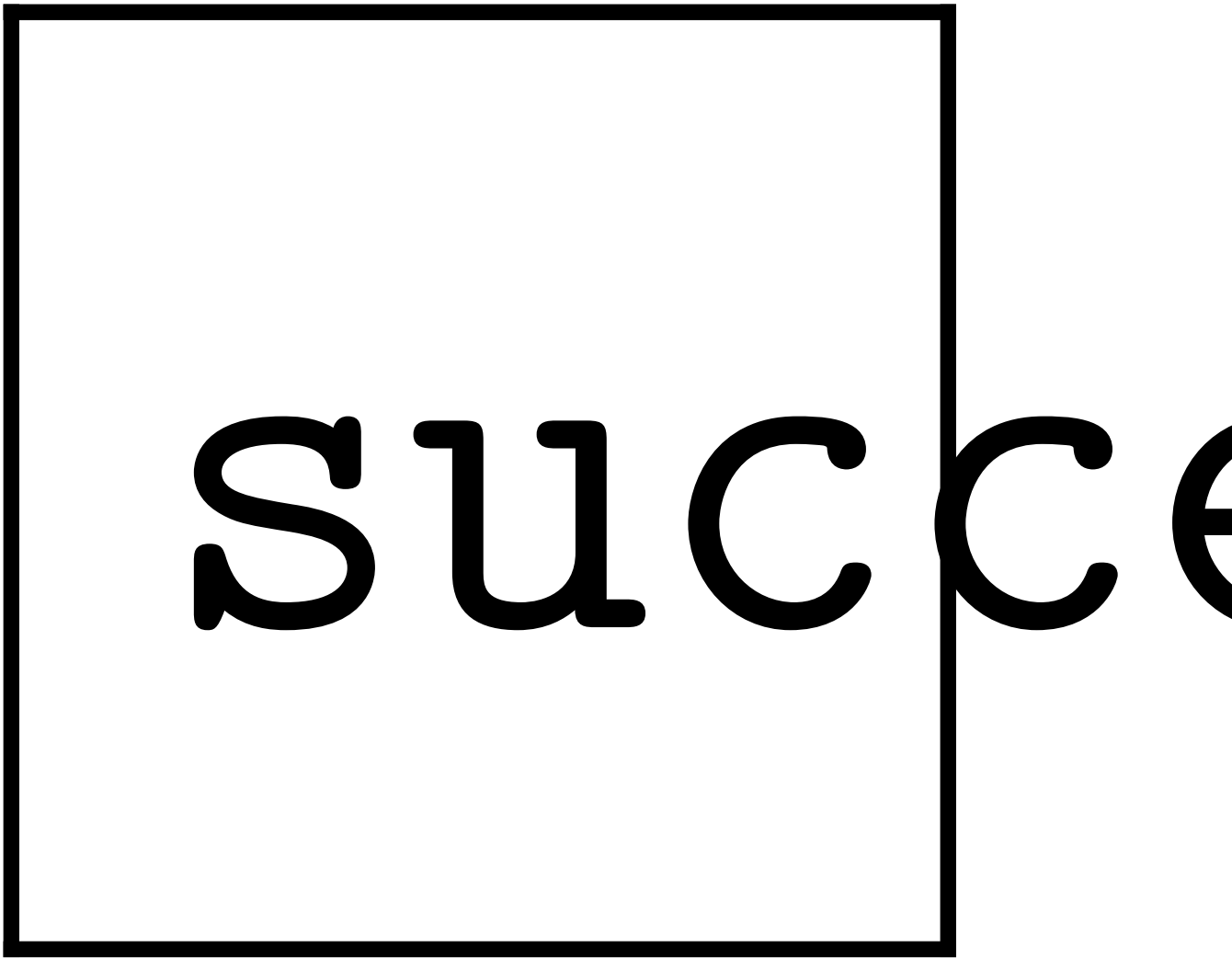
After running the tool with the options set as above, I received the output:



I was confused at first as I had thought that Nessus had said the password was blank. Then I remembered that I had forgotten to set a username, so I set the username to root and ran it again:

```
> set USERNAME root
```

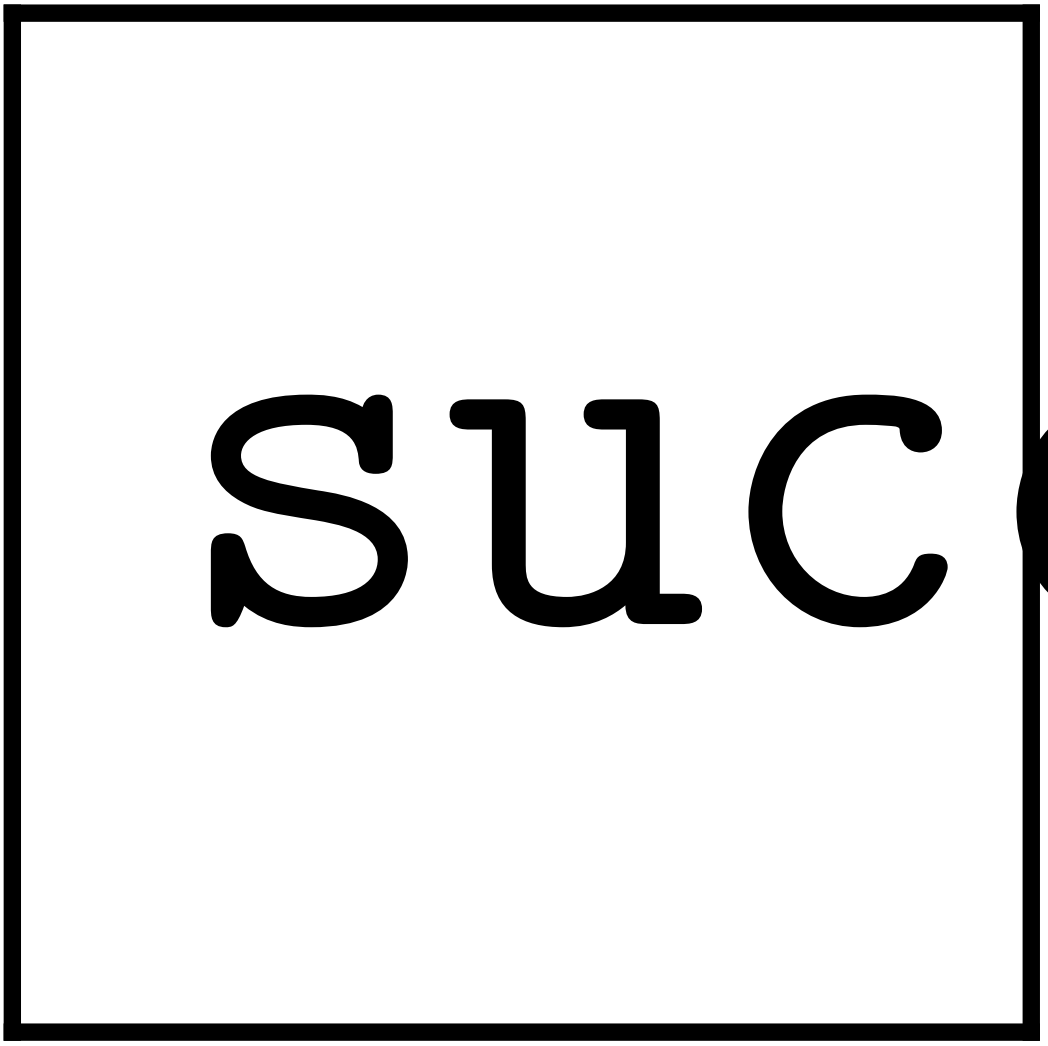
```
> exploit
```



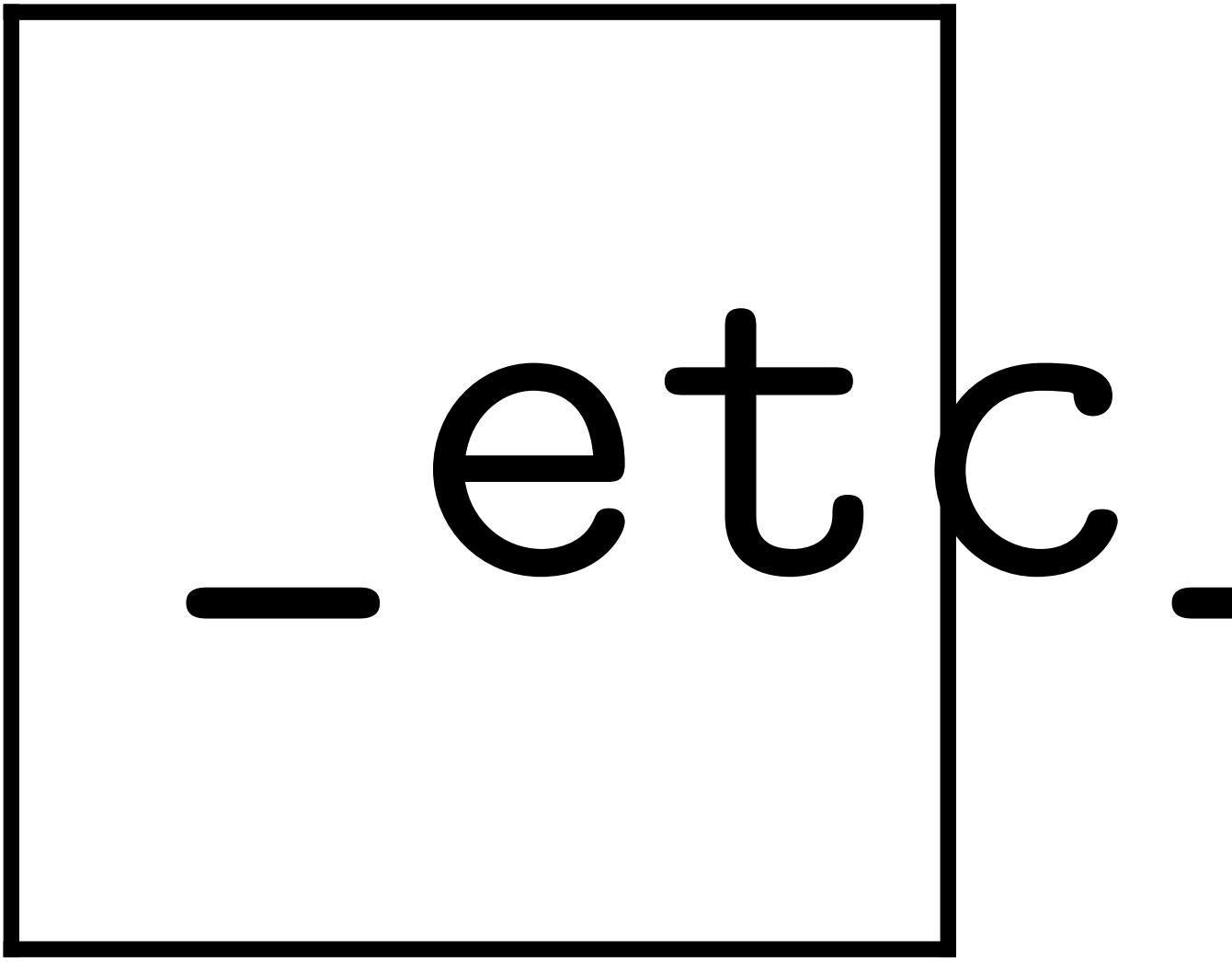
2.4 Round 3

I now have the username and password to the MySQL service. I decided to attempt to log into the service remotely through my machine to see what I could do from there:

```
# mysql -h 192.168.2.12 -u root -p
```



I ran a “show grants;” to find out how much power the user I now controlled has. Turns out I had access to everything in MySQL! What if I tried to open the “/etc/passwd” file?

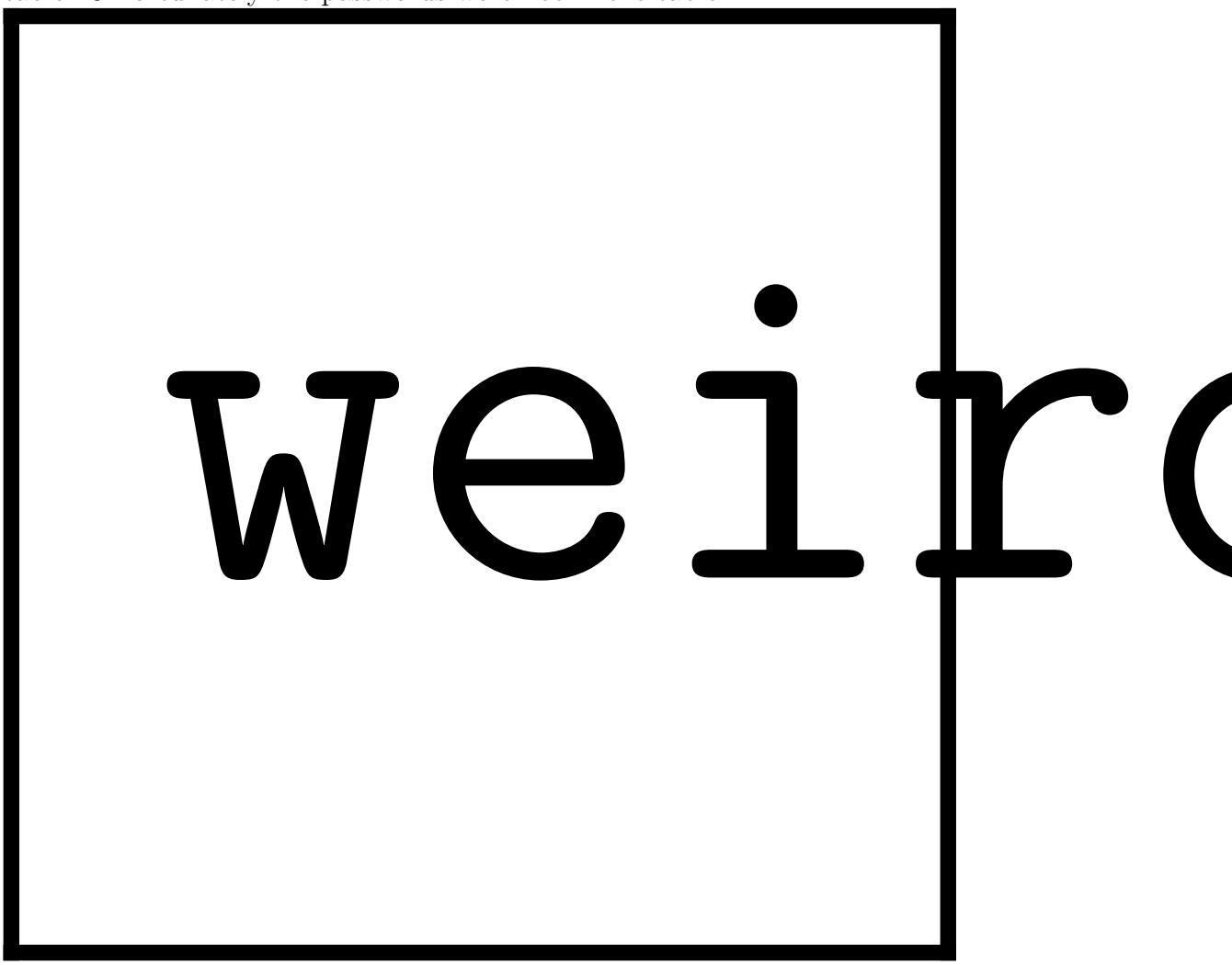


I was able to get the file, so now I have a list of users and what group they belong to on the system. I attempted to get the "/etc/shadow" file, but was rejected. So this still leaves me with no ability to get into a shell. Now I decided that I would try to investigate the datbases contained within the system to see if there was any information contained within in them that could help me out.

```
> show databases;
> use mysql;
> Select *;
> show tables;
```

```
> select * from user;
> select User from user;
> select User, Password from user;
```

When I selected everything from the user table, I got a very messy printout of the table (see screenshot below). I was able to determine that the table contained a username and password, so I selected both of those from the table. Unfortunately the passwords were not in the table.



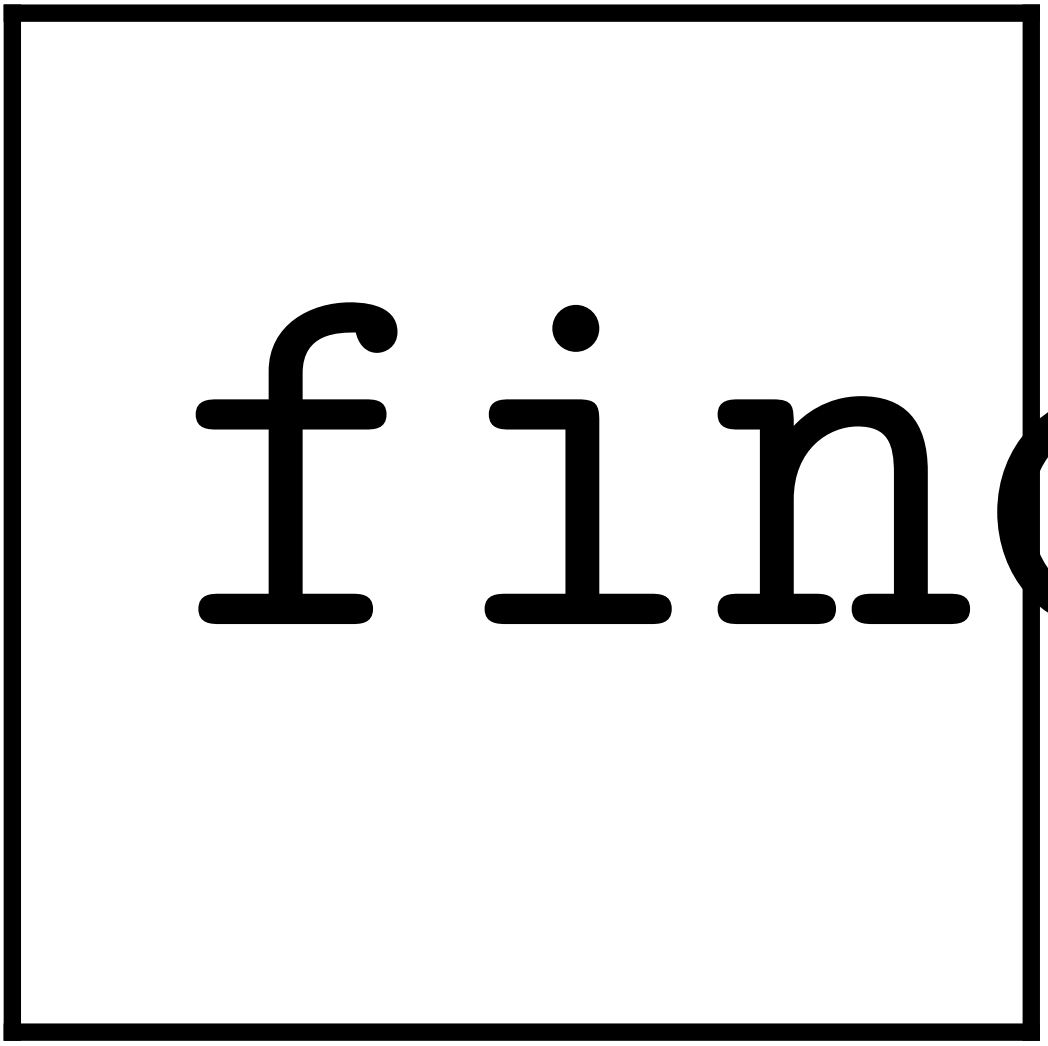
I then attempted to try to use the mysql_hashdump tool from msfconsole, unfortunately it was unable to provide me with anything. Next I decided to see if there were any known exploits for the current MySQL version that

was running on the system. That search turned up nothing as well. I went into MySQL again and grabbed the print out of the "/etc/passwd" file from before to use it as a user list to try to brute force an SSH account.

2.5 Round 4

I determined that I was going to try to brute force an SSH account using the users from the "/etc/passwd" file I was able to print out from MySQL. AFter waiting for a long time as Hydra attempted to test multiple passwords for the large user list, I decided to just focus on one user. I picked the user "user" and decided to try to brute force it using the namelist.txt wordlist from "/usr/share/wordlists/metasploit/" built into Kali.

```
# hydra ssh://192.168.2.12 -l user -P /usr/share/wordlists/metasploit/namelist.txt
```



I was able to successfully find the password for “user” and thus login to an SSH account with shell access.

Summary

Biography