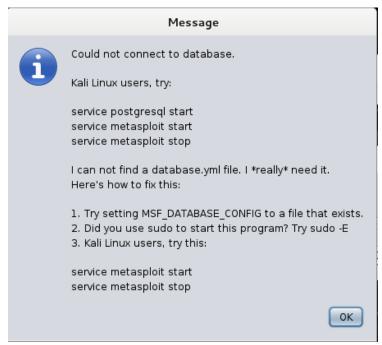
## Lab 3 Pentesting Lab Report



1) Here is an error message after trying to run armitage. I had to go back to an earlier version of Kali because the version we used for lab 2 just refused to work for a future step. More on that later.

```
File Edit View Search Terminal Help

Creating metasploit database 'msf3'...
insserv: warning: current start runlevel(s) (empty) of script `metasploit' overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `metasploit' overrides LSB defaults (0 1 6).

[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit worker: worker.

root@kali:~# service metasploit stop
[ ok ] Stopping Metasploit worker: worker.

[ ok ] Stopping Metasploit worker: worker.

[ ok ] Stopping Metasploit rpc server: prosvc.

root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.

root@kali:~# armitage
[*] Starting msfrpcd for you.

[*] MSGRPC starting on 127.0.0.1:55553 (NO SSL):Msg...

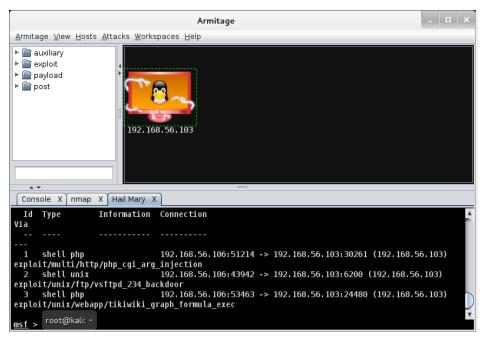
NOTICE: CREATE TABLE will create implicit sequence "hosts_id_seq" for serial column "hosts.id"

NOTICE: CREATE TABLE will create implicit sequence "clients_id_seq" for serial column "clients.id"

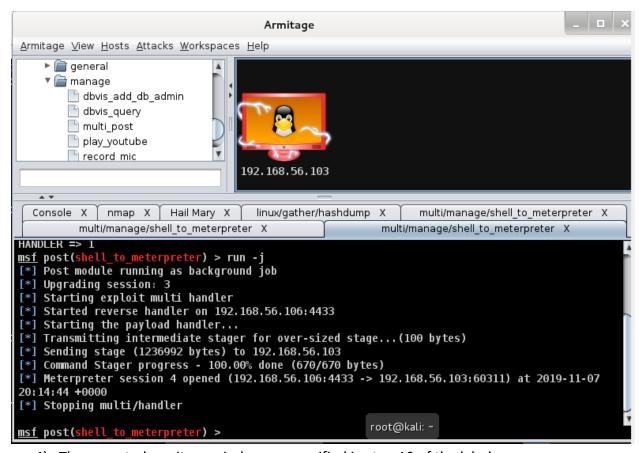
NOTICE: CREATE TABLE will create implicit sequence "clients_id_seq" for serial column "clients.id"

NOTICE: CREATE TABLE / PRIMARY KEY will create implicit index "clients_pkey" for recompose Arming Armi
```

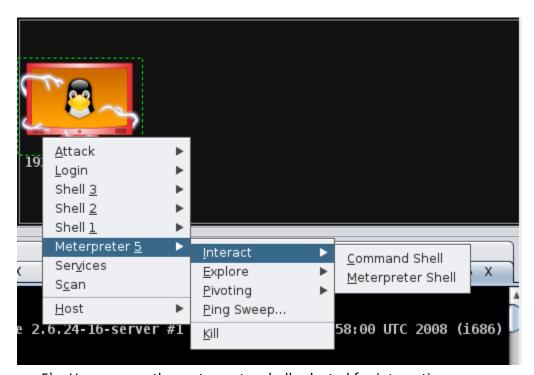
2) This is me running the fix suggested in the above error message. It ends up working.



3) Here we see the armitage window after doing the nmap scan as well as the hail mary attack on the metasploitable IP address. This was the step that I was stuck on when using the Kali virtual machine used in lab 2. I looked up some things and the research suggests that msf5 was what screwed everything over. The regular msf shell as seen in the above screenshot appears to be working fine.



4) The expected armitage window, as specified in step 10 of the lab doc.



5) Here we see the meterpreter shell selected for interaction

- 6) List of all commands used in order of screenshots below
  - a. Sysinfo
  - b. Getwd
  - c. Getlwd
  - d. Ipconfig (2 parts)
  - e. Getuid
  - f. Route

meterpreter > sysinfo

Computer : metasploitable

OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 (1686)

Architecture : i686 Meterpreter : x86/linux

meterpreter > getwd
/var/www/tikiwiki

meterpreter > getlwd
/usr/share/armitage
meterpreter >

## <u>meterpreter</u> > ipconfig

Interface 1

Name : lo

Hardware MAC : 00:00:00:00:00:00

MTU : 16436

Flags : UP LOOPBACK RUNNING

IPv4 Address : 127.0.0.1 IPv4 Netmask : 255.0.0.0

IPv6 Address : ::1

IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff

## Interface 2

\_\_\_\_\_

Name : eth0

Hardware MAC: 08:00:27:22:a4:c5

MTU : 1500

Flags : UP BROADCAST RUNNING MULTICAST

IPv4 Address : 192.168.56.103 IPv4 Netmask : 255.255.255.0

IPv6 Address : fe80::a00:27ff:fe22:a4c5
IPv6 Netmask : ffff:ffff:ffff:

<u>meterpreter</u> >

<u>meterpreter</u> > getuid

Server username: uid=33, gid=33, euid=33, egid=33, suid=33, sgid=33

<u>meterpreter</u> >

<u>meterpreter</u> >