California State University, Sacramento

Lab 3-Pentesting

Elliot Turner

Professor Dr. Jun Dai

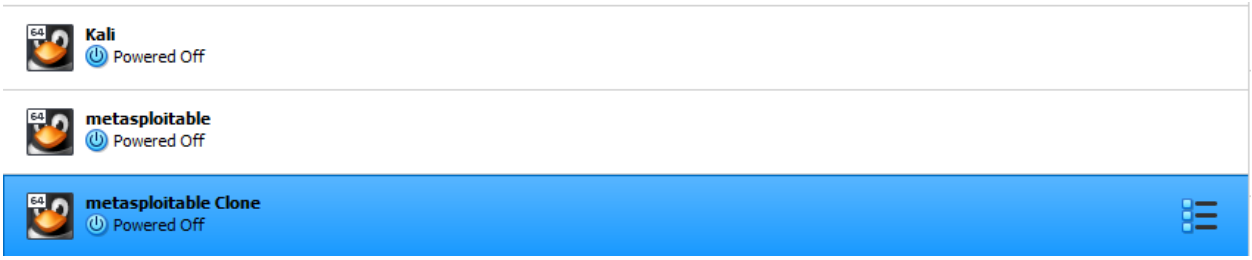
CSC 154

June 26, 2022

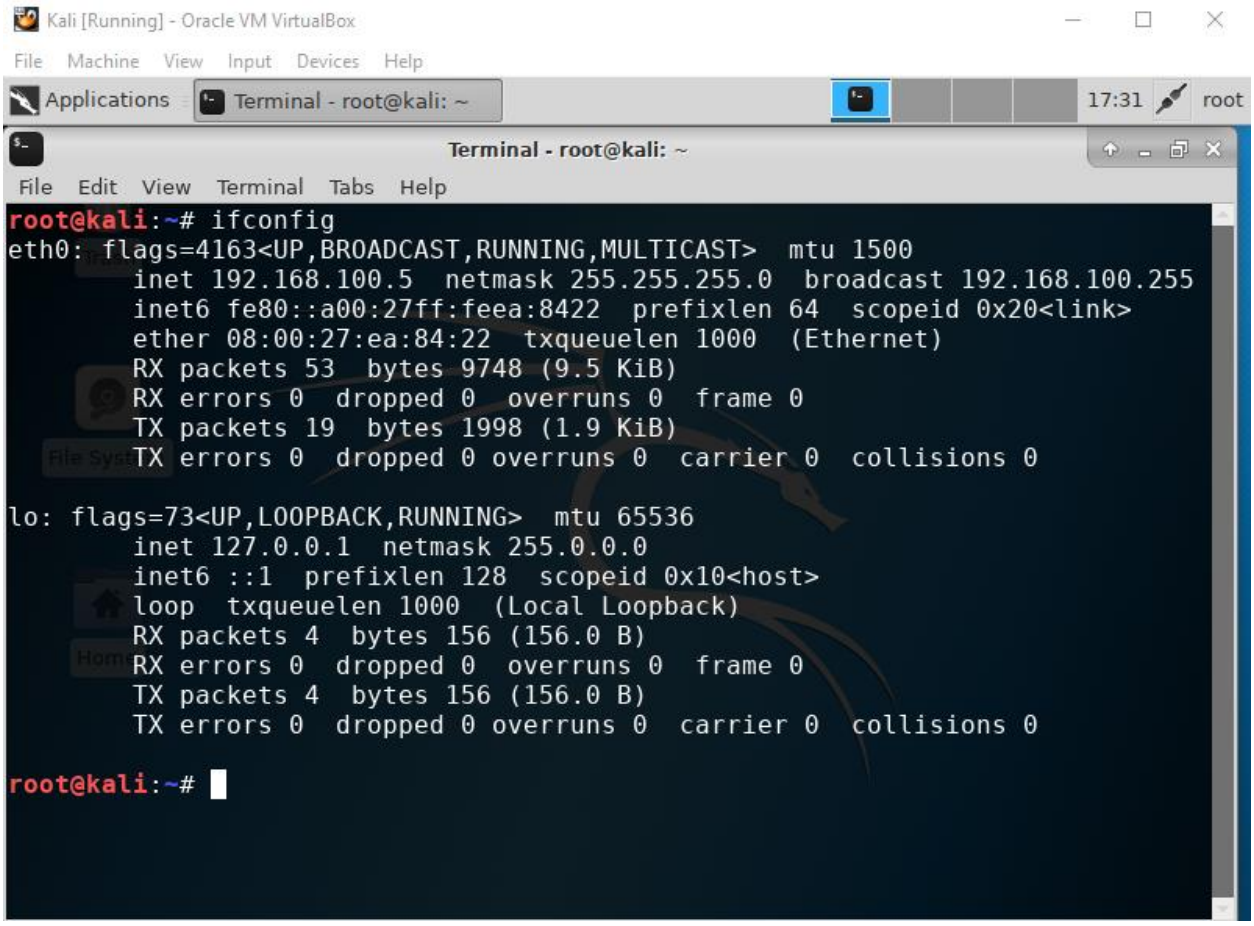
Introduction to Attack

Using a Kali virtual machine, launch a Hail Mary (penetration test) attack towards Metasploitable machines.

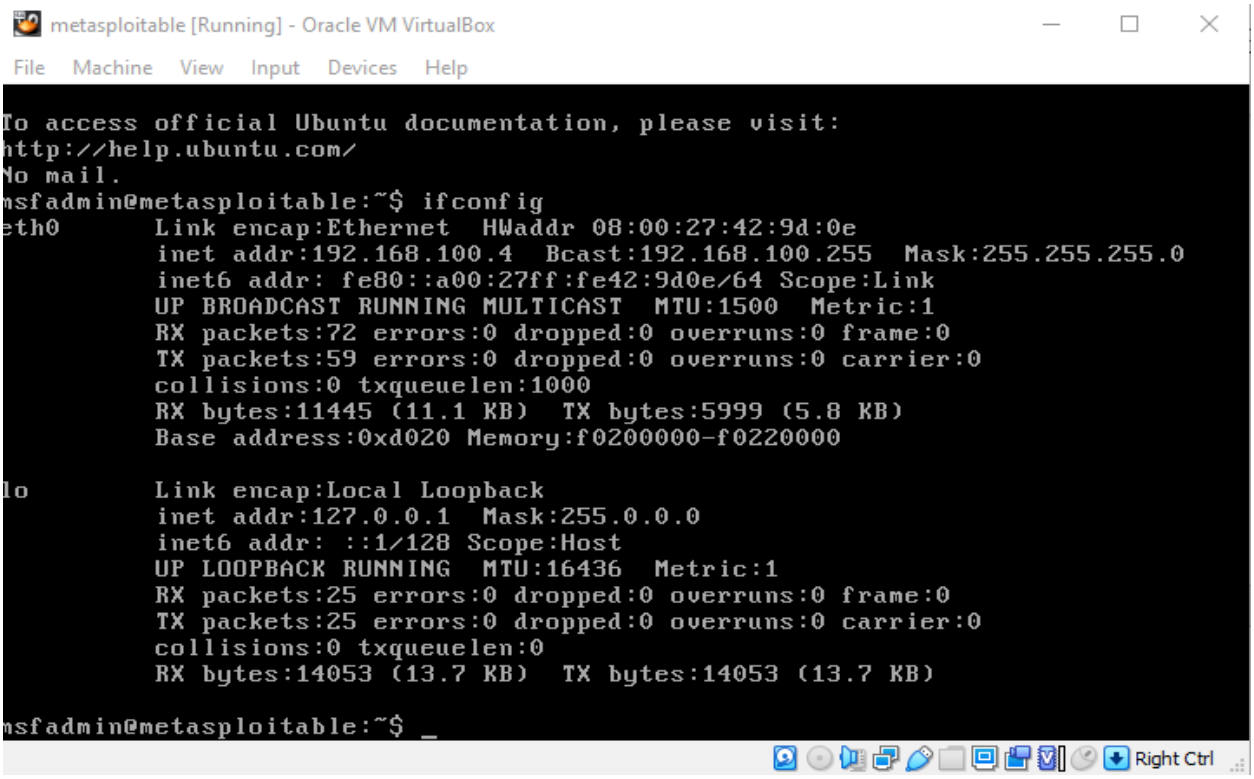
Commands and Screenshots



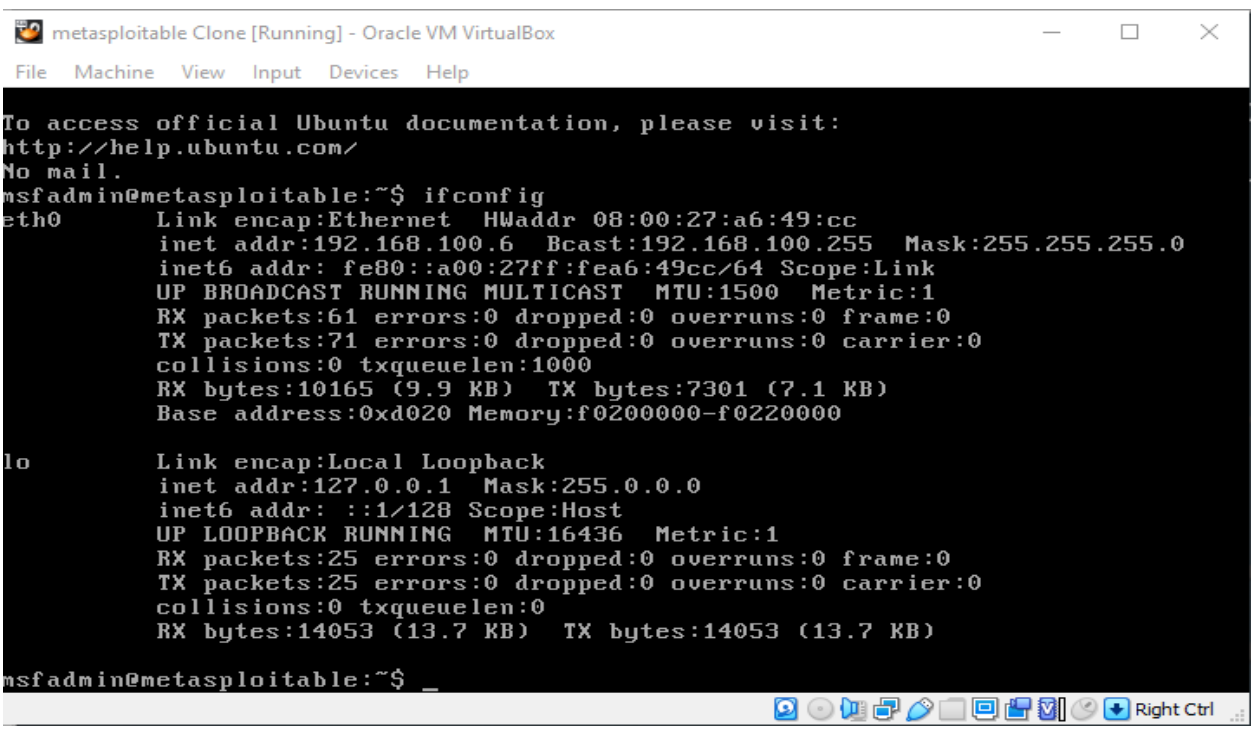
- **Virtual machines for testing.**



- `ifconfig` **to determine inet on kali virtual machine.**



- **ifconfig to determine inet on metasploitable virtual machine.**



- **ifconfig to determine inet on metasploitable clone virtual machine.**

```
root@kali:~# ping 192.168.100.6
PING 192.168.100.6 (192.168.100.6) 56(84) bytes of data.
64 bytes from 192.168.100.6: icmp_seq=1 ttl=64 time=0.833 ms
64 bytes from 192.168.100.6: icmp_seq=2 ttl=64 time=0.941 ms
^C
--- 192.168.100.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.833/0.887/0.941/0.054 ms
root@kali:~# ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data.
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=0.593 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.910 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=0.984 ms
^C
--- 192.168.100.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.593/0.829/0.984/0.169 ms
root@kali:~#
```

- **ping metasploitable machines to make sure they are talking**

```
metasploitable [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11445 (11.1 KB)  TX bytes:5999 (5.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14053 (13.7 KB)  TX bytes:14053 (13.7 KB)

msfadmin@metasploitable:~$ ping 192.168.100.5
PING 192.168.100.5 (192.168.100.5) 56(84) bytes of data.
64 bytes from 192.168.100.5: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 192.168.100.5: icmp_seq=2 ttl=64 time=0.884 ms

--- 192.168.100.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.342/0.613/0.884/0.271 ms
msfadmin@metasploitable:~$
```

- **ping kali machine to make sure they are talking.**

metasploitable Clone [Running] - Oracle VM VirtualBox

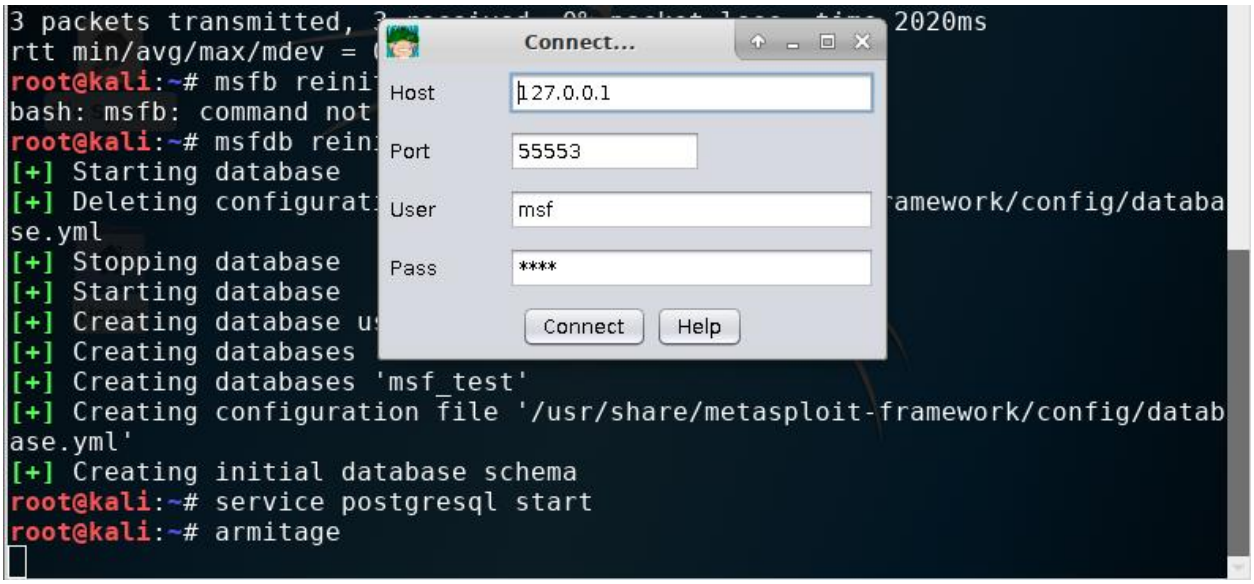
File Machine View Input Devices Help

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10165 (9.9 KB)  TX bytes:7301 (7.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14053 (13.7 KB)  TX bytes:14053 (13.7 KB)

msfadmin@metasploitable:~$ ping 192.168.100.5
PING 192.168.100.5 (192.168.100.5) 56(84) bytes of data.
64 bytes from 192.168.100.5: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from 192.168.100.5: icmp_seq=2 ttl=64 time=0.977 ms

--- 192.168.100.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.387/0.682/0.977/0.295 ms
```

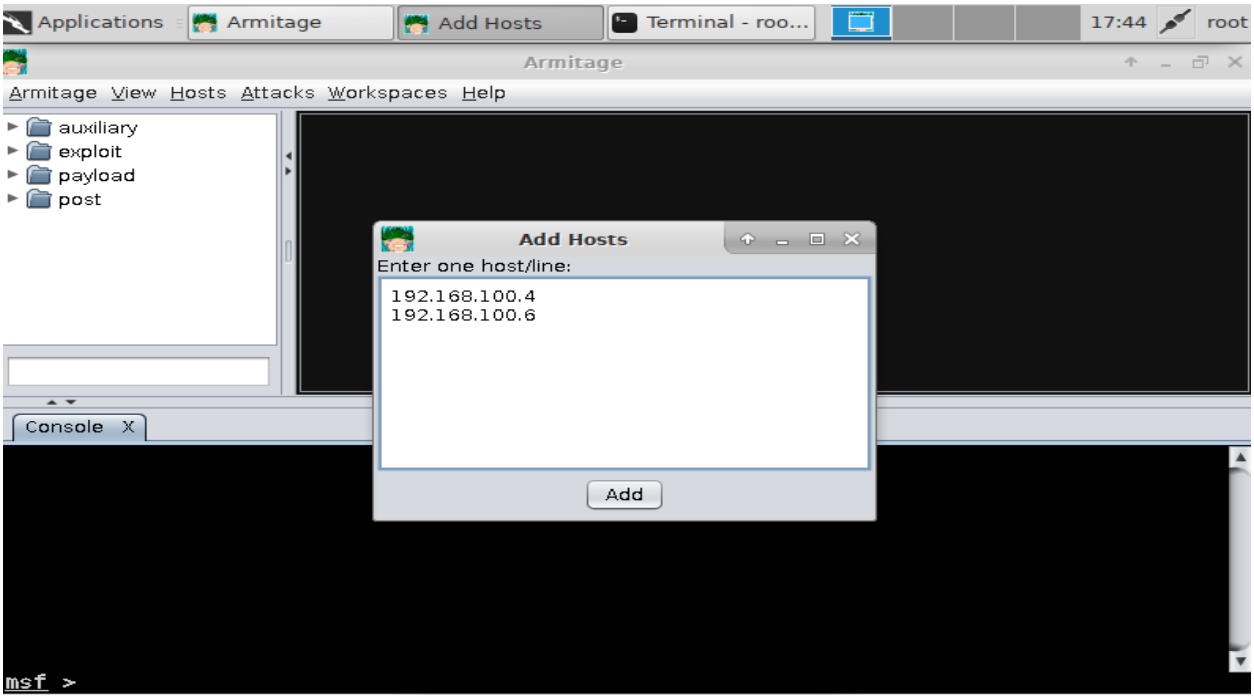
- **ping kali machine from clone to make sure they are talking.**

```
root@kali:~# msfdb reinit
[+] Starting database
[+] Deleting configuration file /usr/share/metasploit-framework/config/databa
se.yml
[+] Stopping database
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/datab
ase.yml'
[+] Creating initial database schema
root@kali:~#
```

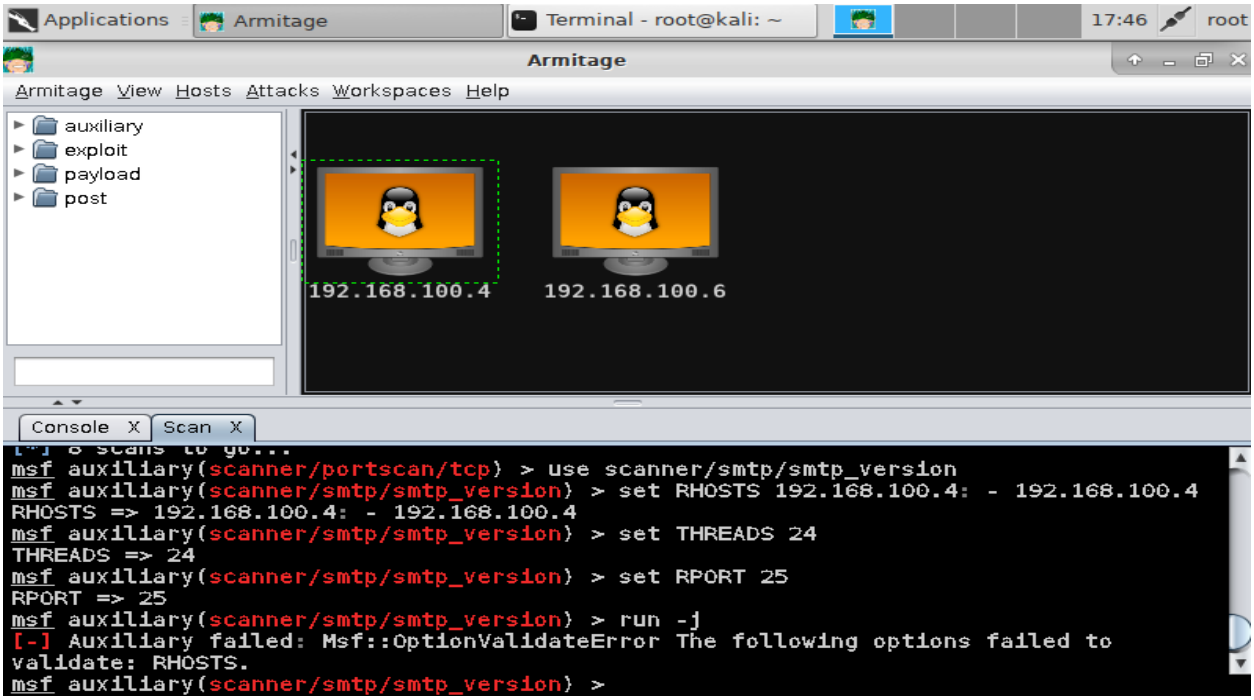
- **msfdb reinit to reinitiate the database setup.**



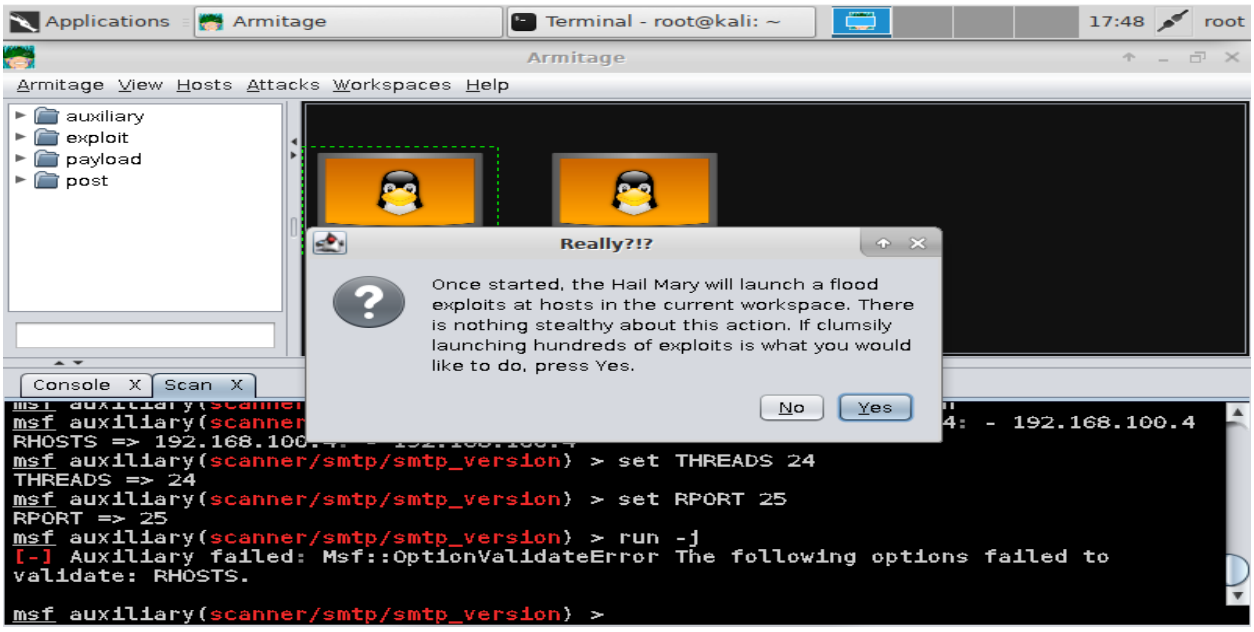
- **service postgresql start launch database management service.**
- **Armitage cybersecurity attack tool.**



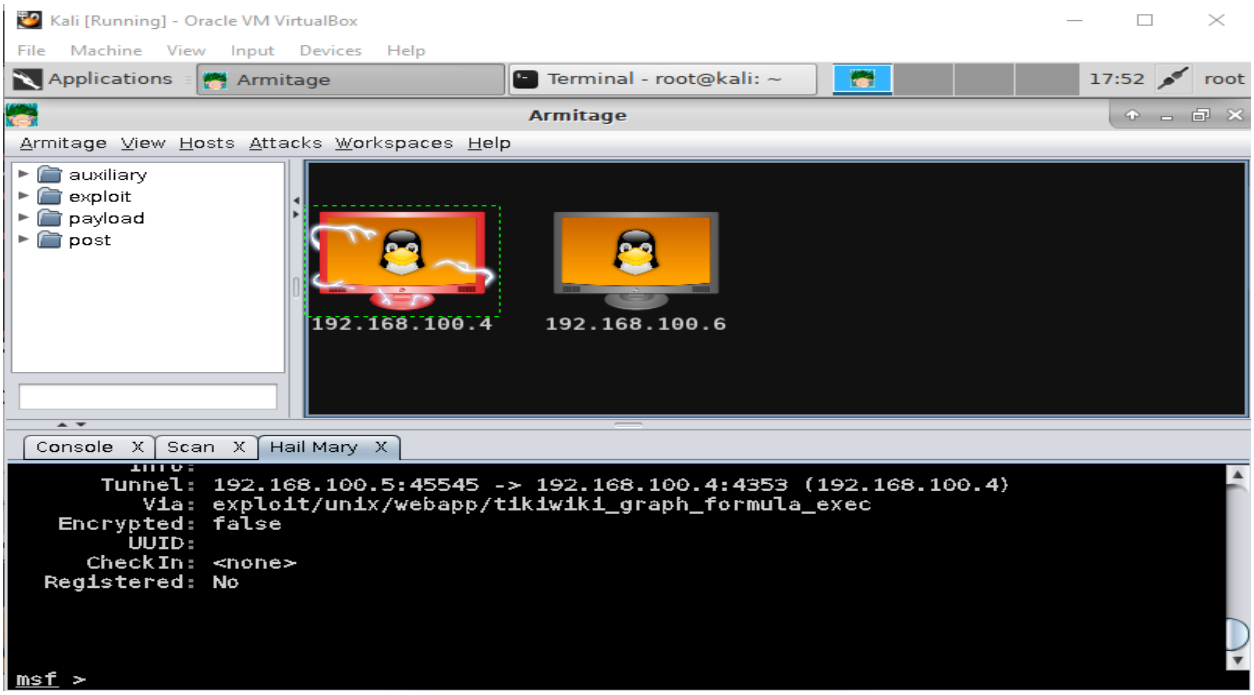
- **Designate hosts, the machines that will receive the payloads.**



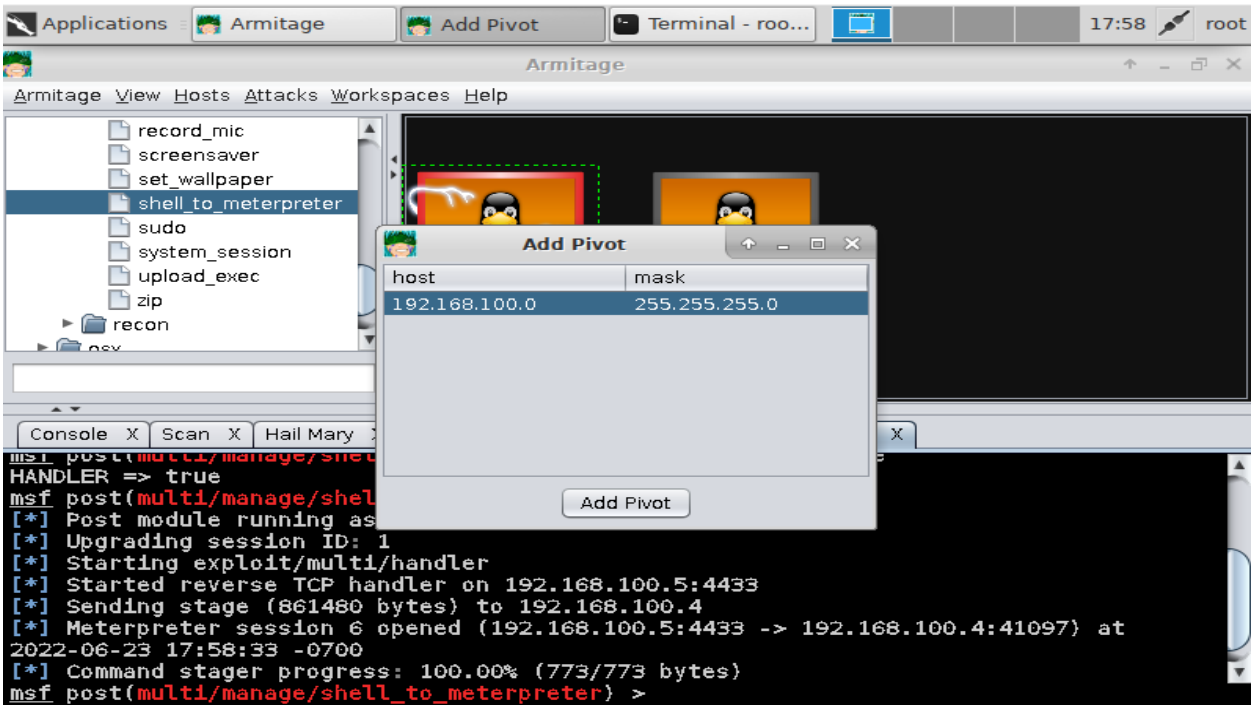
- **Scan the hosts, to verify the available payloads per machine.**



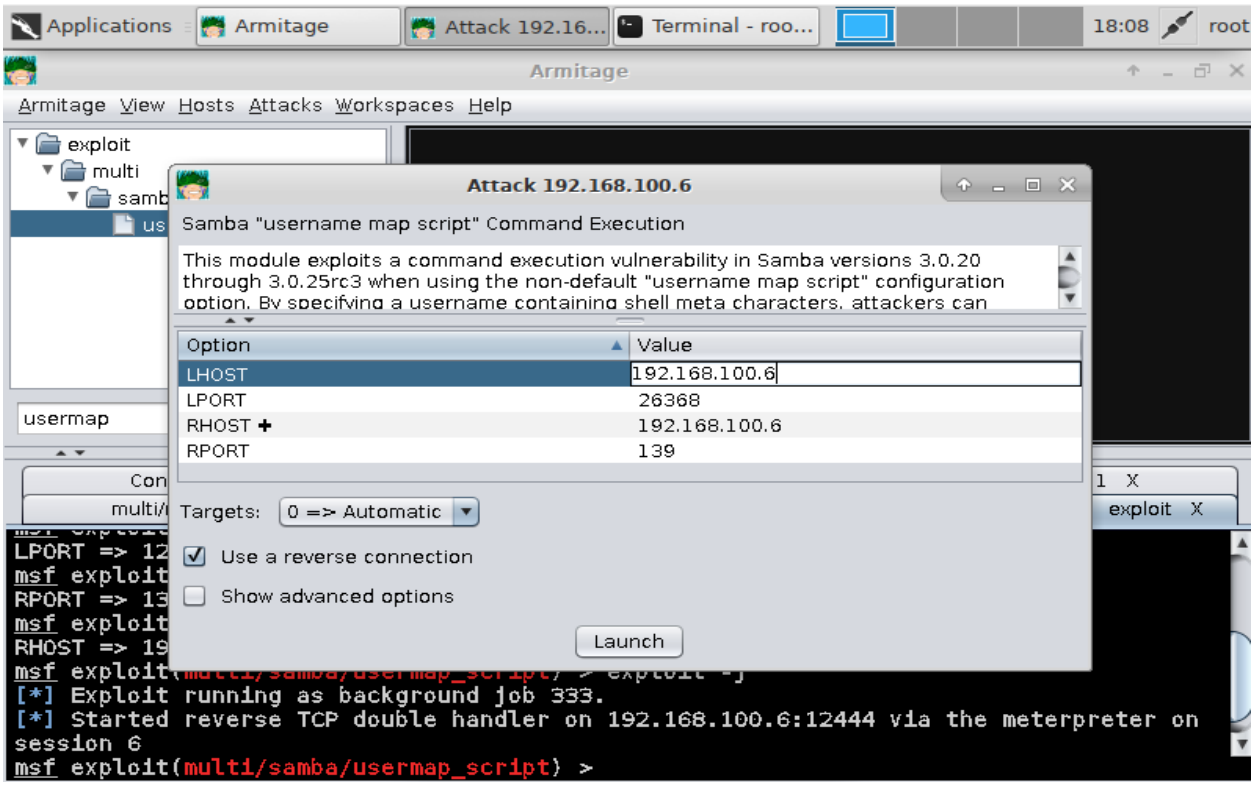
- **Deploy the Hail Mary attack, every available payload will be launched at the designated machine, very sloppy.**



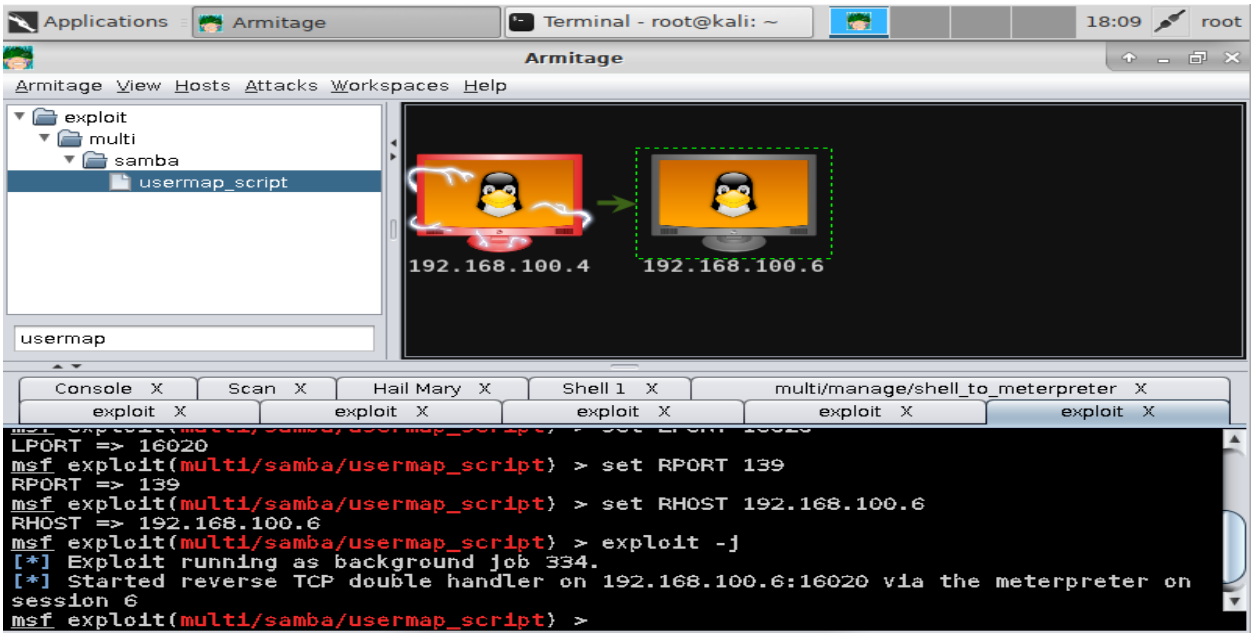
- **Successful Hail Mary, gained access to shells.**



- **Add pivot.**



- **Usermap module to prepare attack on 192.168.100.6 machine.**



- **Attempted command execution vulnerability.**