

California State
University, Sacramento

Lab 3-Pentesting

Elliot Turner

Professor Dr. Jun Dai

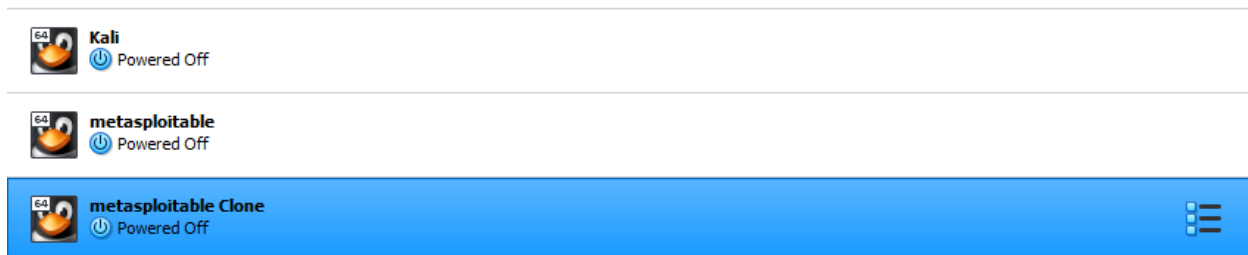
CSC 154

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.

```

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Terminal - root@kali: ~ 17:31 root

Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.5 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:feea:8422 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ea:84:22 txqueuelen 1000 (Ethernet)
    RX packets 53 bytes 9748 (9.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1998 (1.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 156 (156.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 156 (156.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
  
```

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

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:9d:0e
          inet addr:192.168.100.4  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:9d0e/64 Scope:Link
          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:~$ _

```

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

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a6:49:cc
          inet addr:192.168.100.6  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea6:49cc/64 Scope:Link
          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:~$ _

```

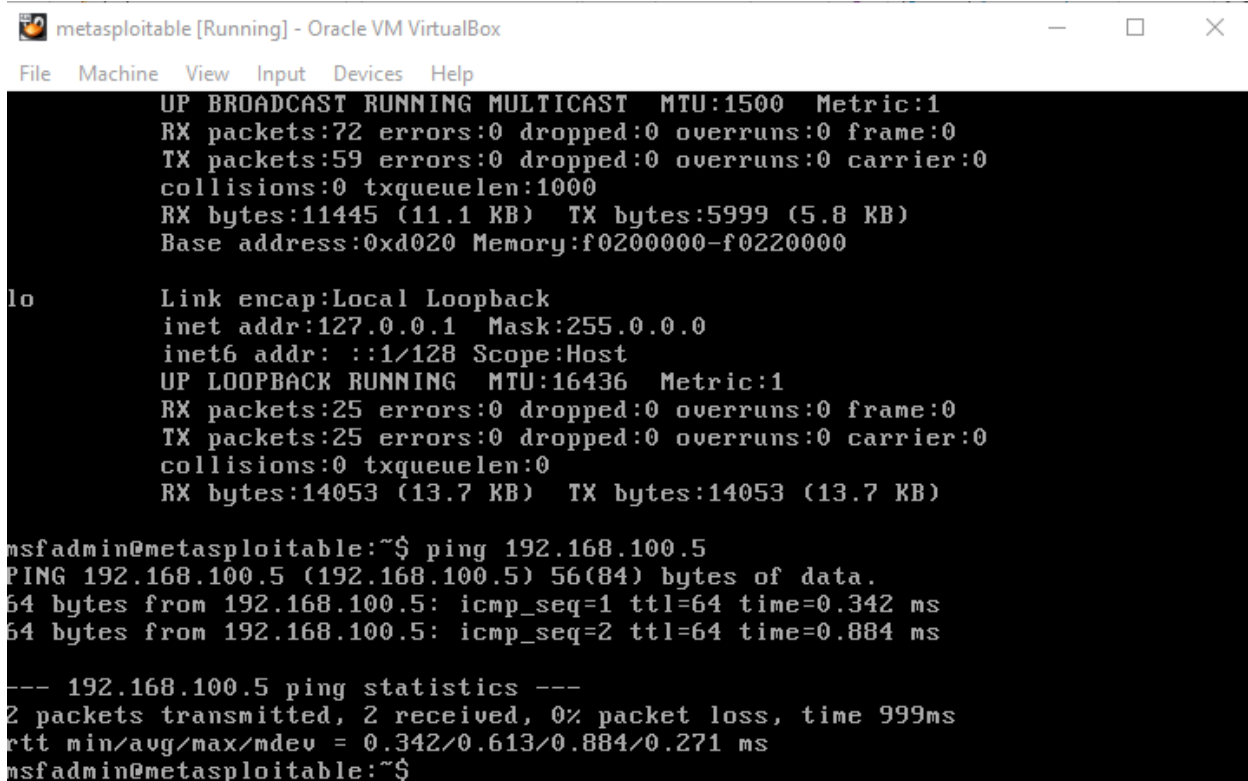
- `ifconfig` to determine inet on metasploitable clone virtual machine.

```

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

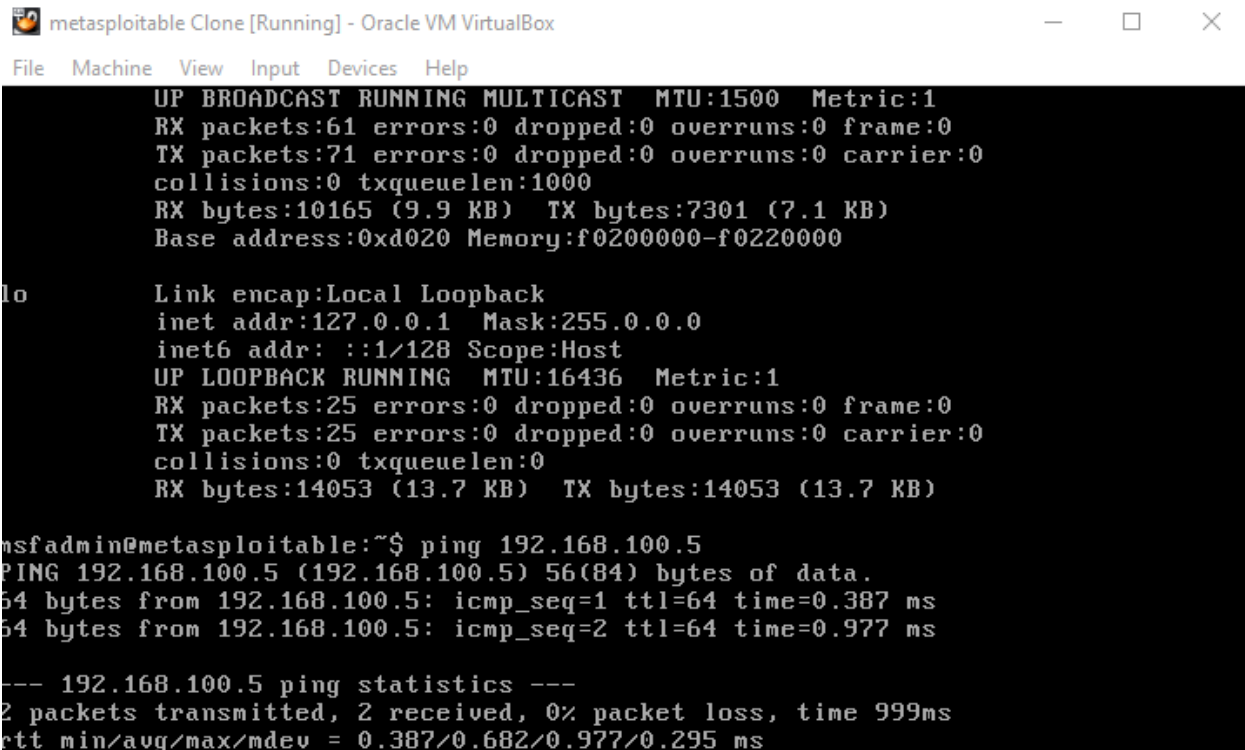
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:72 errors:0 dropped:0 overruns:0 frame:0
TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:11445 (11.1 KB) TX bytes:5999 (5.8 KB)
Base address:0xd020 Memory:f0200000-f0220000

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.



```

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

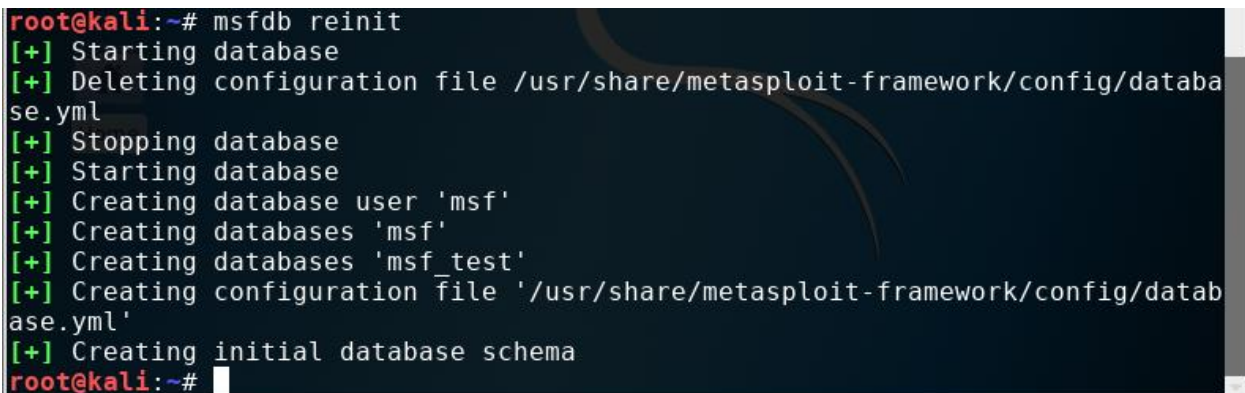
lo
Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:25 errors:0 dropped:0 overruns:0 frame:0
TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:14053 (13.7 KB)  TX bytes:14053 (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/database.yml
[+] Stopping database
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:~#

```

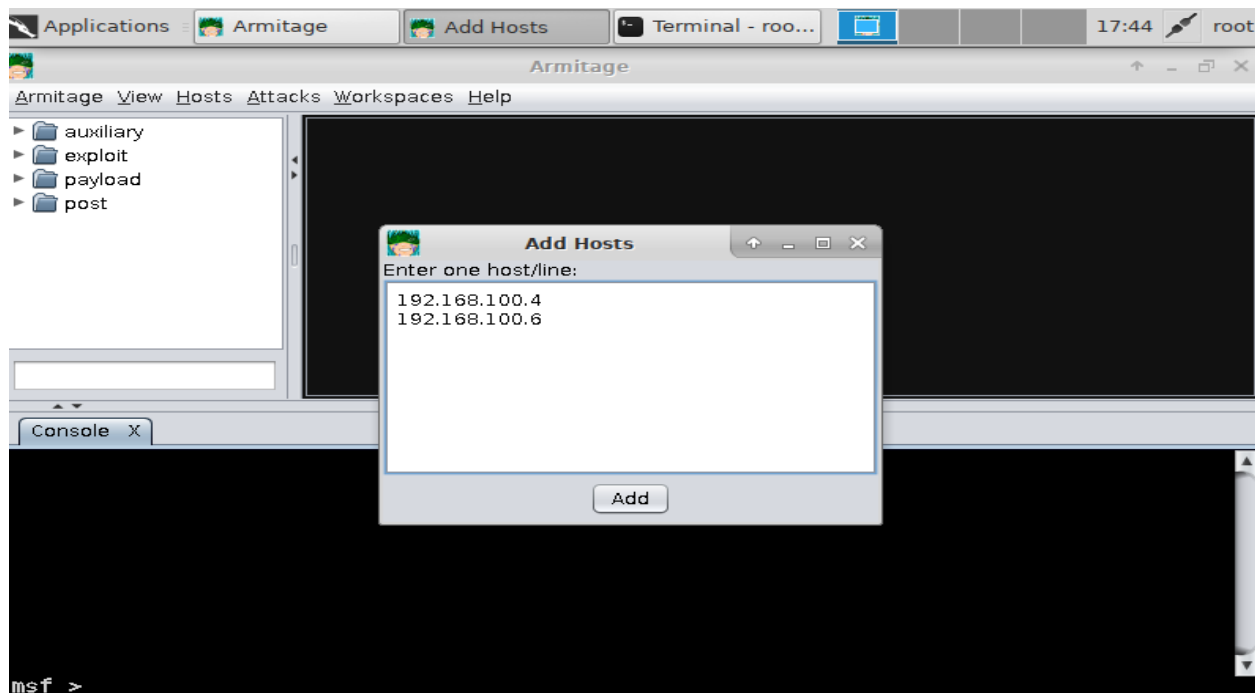
- `msfdb reinit` to reinitiate the database setup.

```

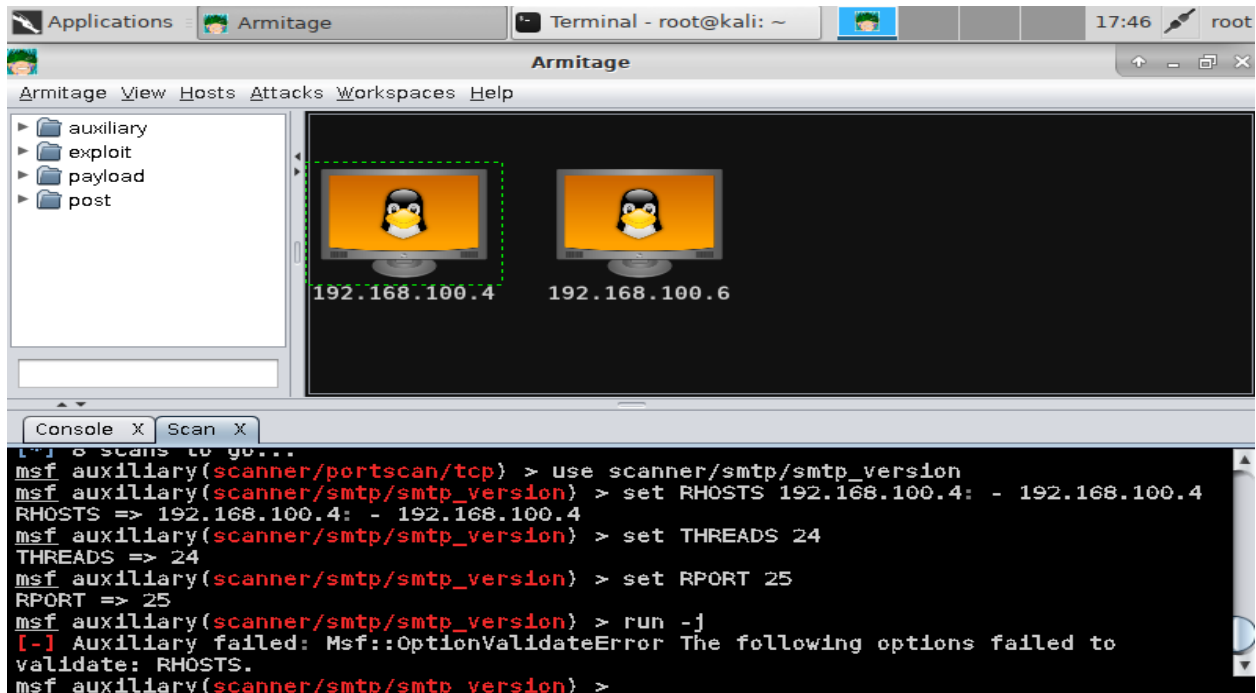
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = (
root@kali:~# msfb reinit
bash: msfb: command not found
root@kali:~# msfdb reinit
[+] Starting database
[+] Deleting configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Stopping database
[+] Starting database
[+] Creating database user
[+] Creating databases
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali:~# service postgresql start
root@kali:~# armitage

```

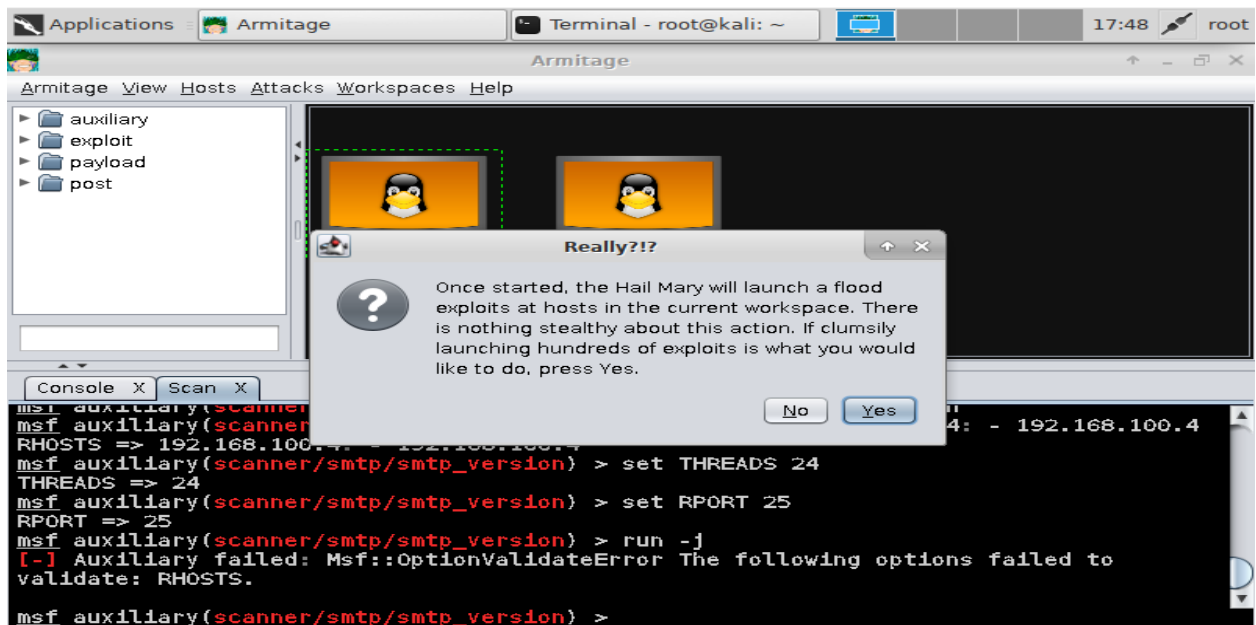
- `service postgresql start` launch database management service.
- `Armitage` cybersecurity attack tool.



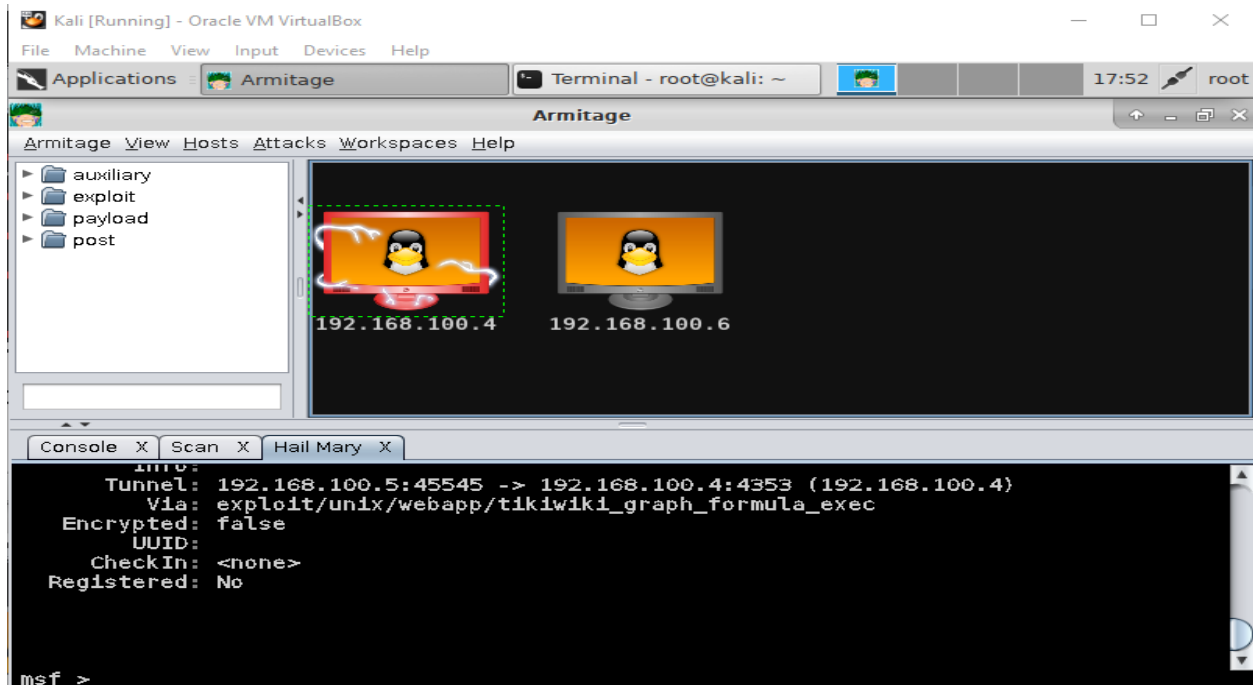
- Designate hosts, the machines that will receive the payloads.



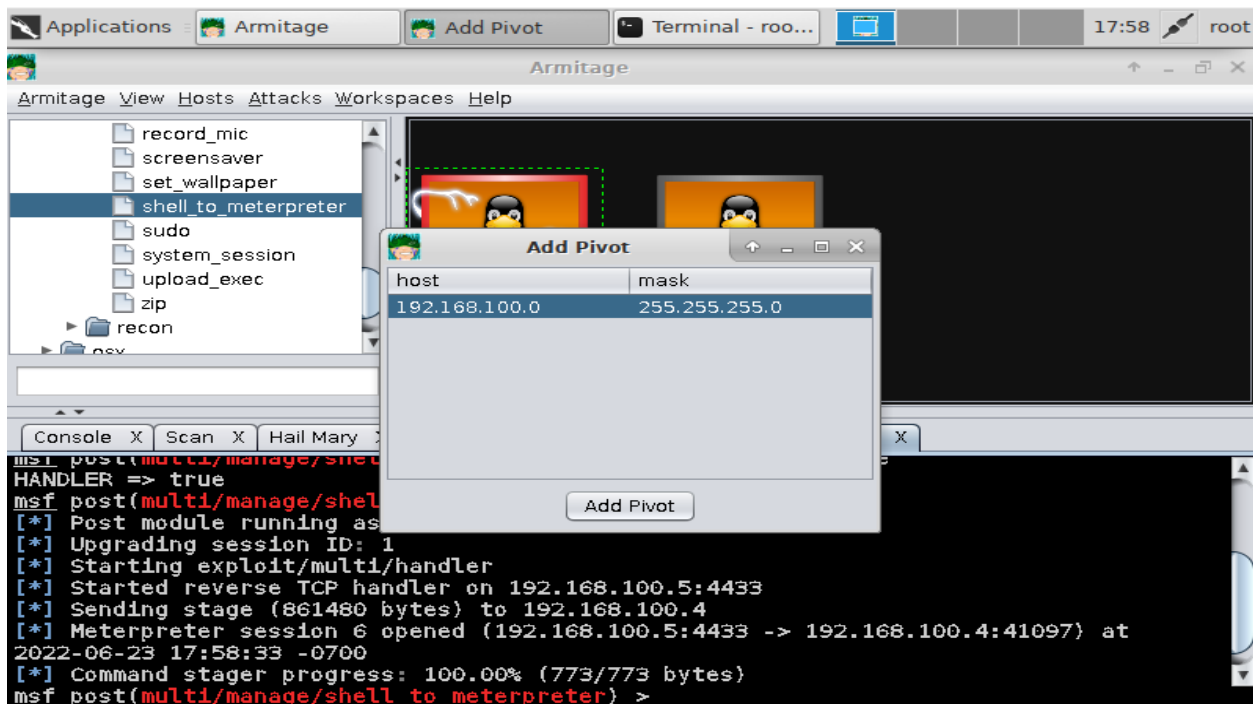
- Scan the hosts, to verify the available payloads per machine.



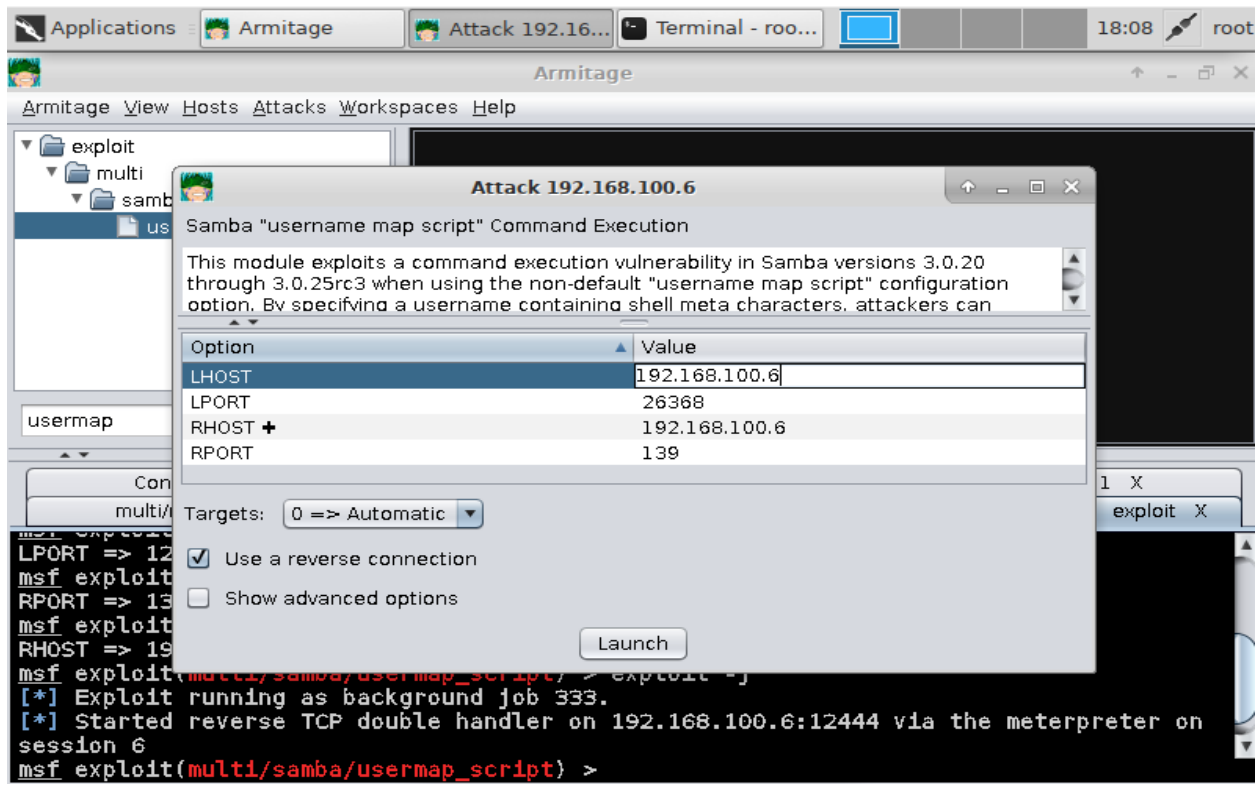
- Deploy the **Hail Mary** attack, every available payload will be launched at the designated machine, very sloppy.



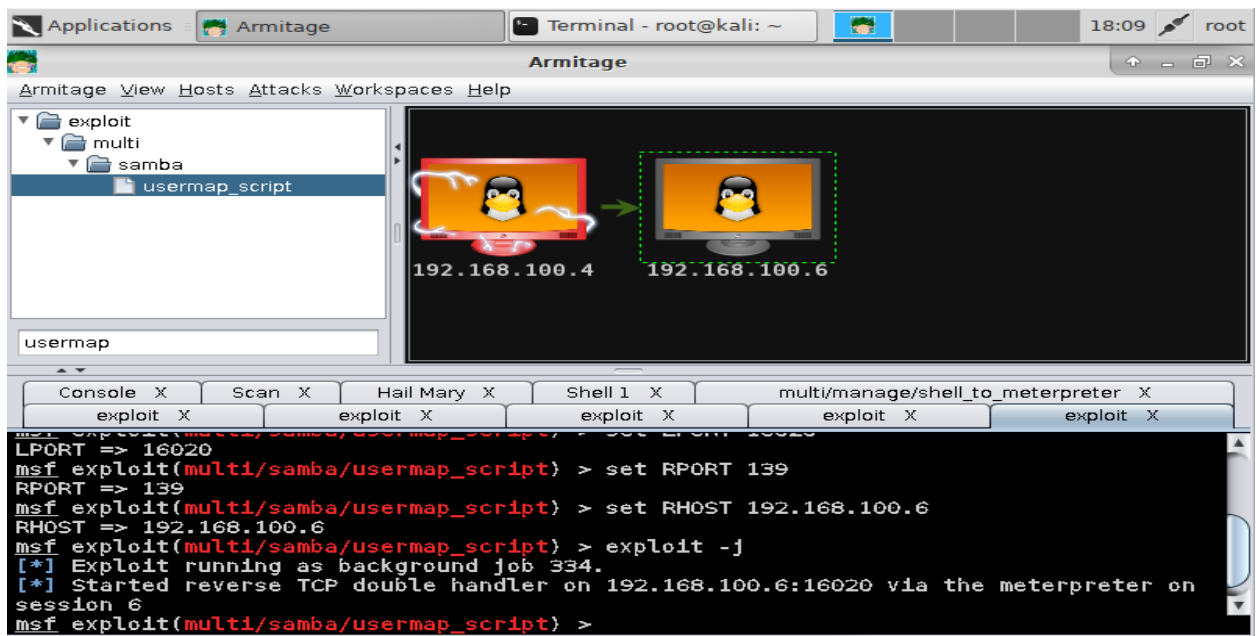
- Successful Hail Mary, gained access to shells.



- Add pivot.



- Usermap module to prepare attack on 192.168.100.6 machine.



- Attempted command execution vulnerability.