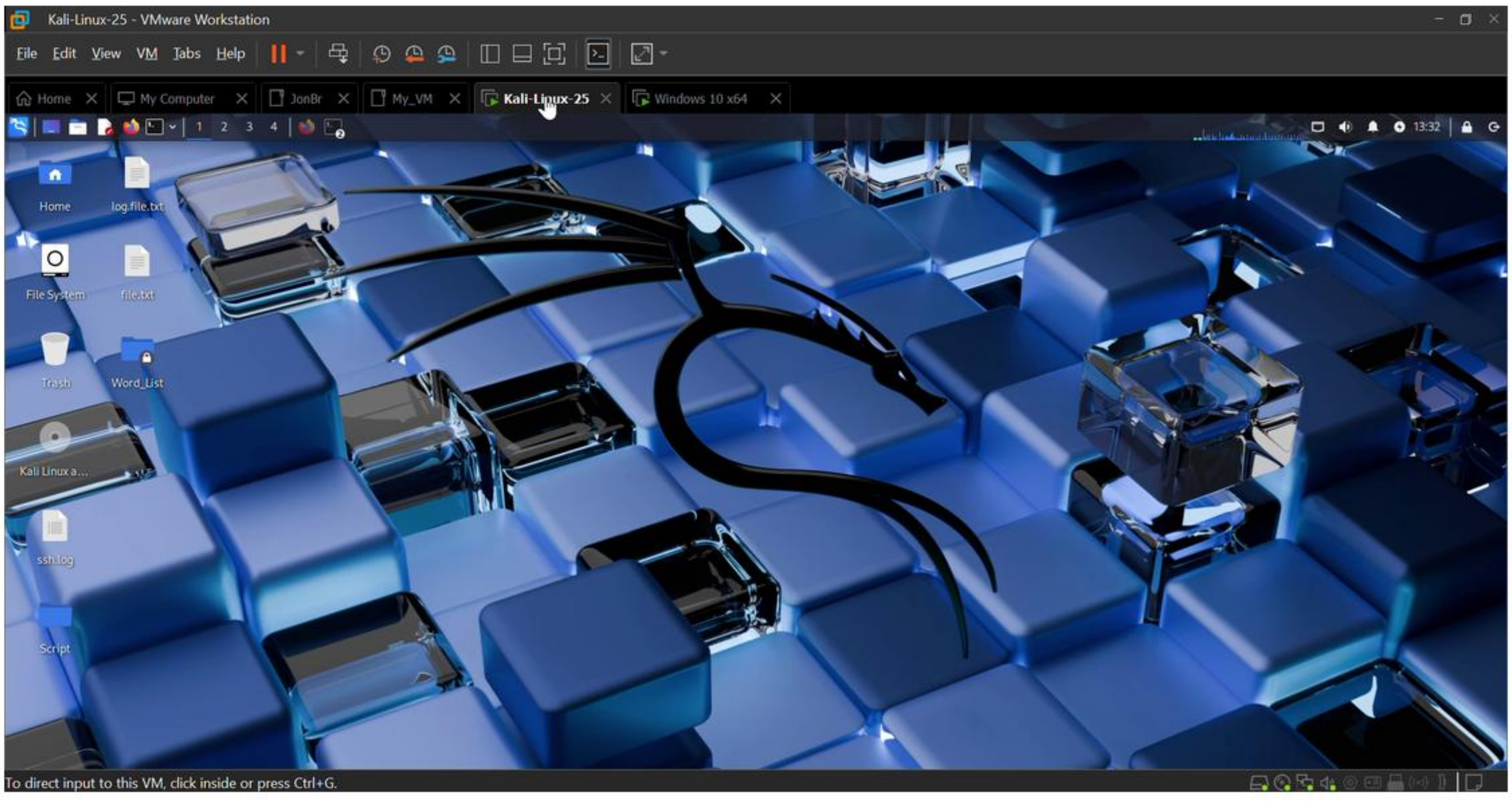
ARP Spoofing Proof of Concept (PoC)

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.

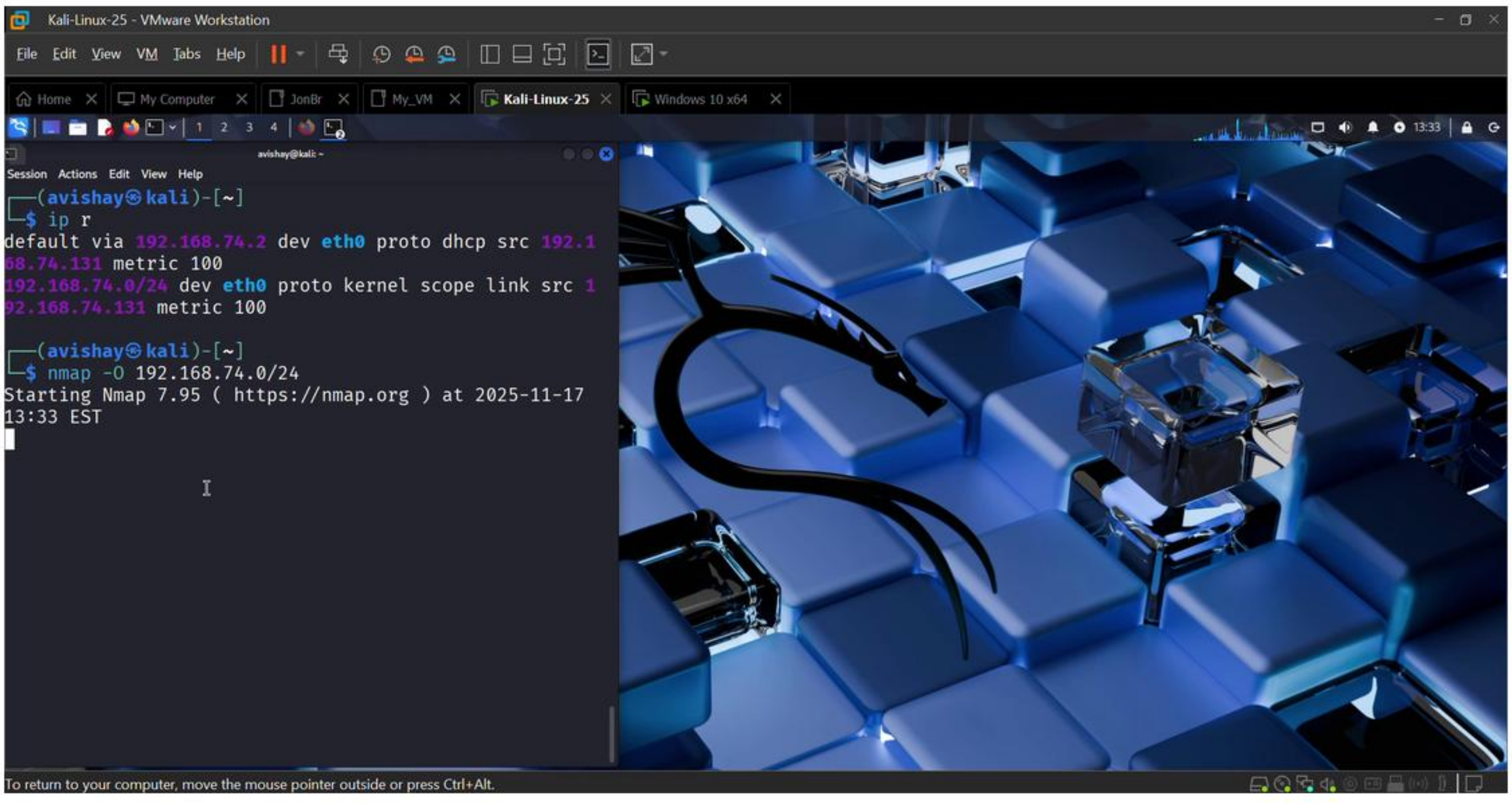
Step 1

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



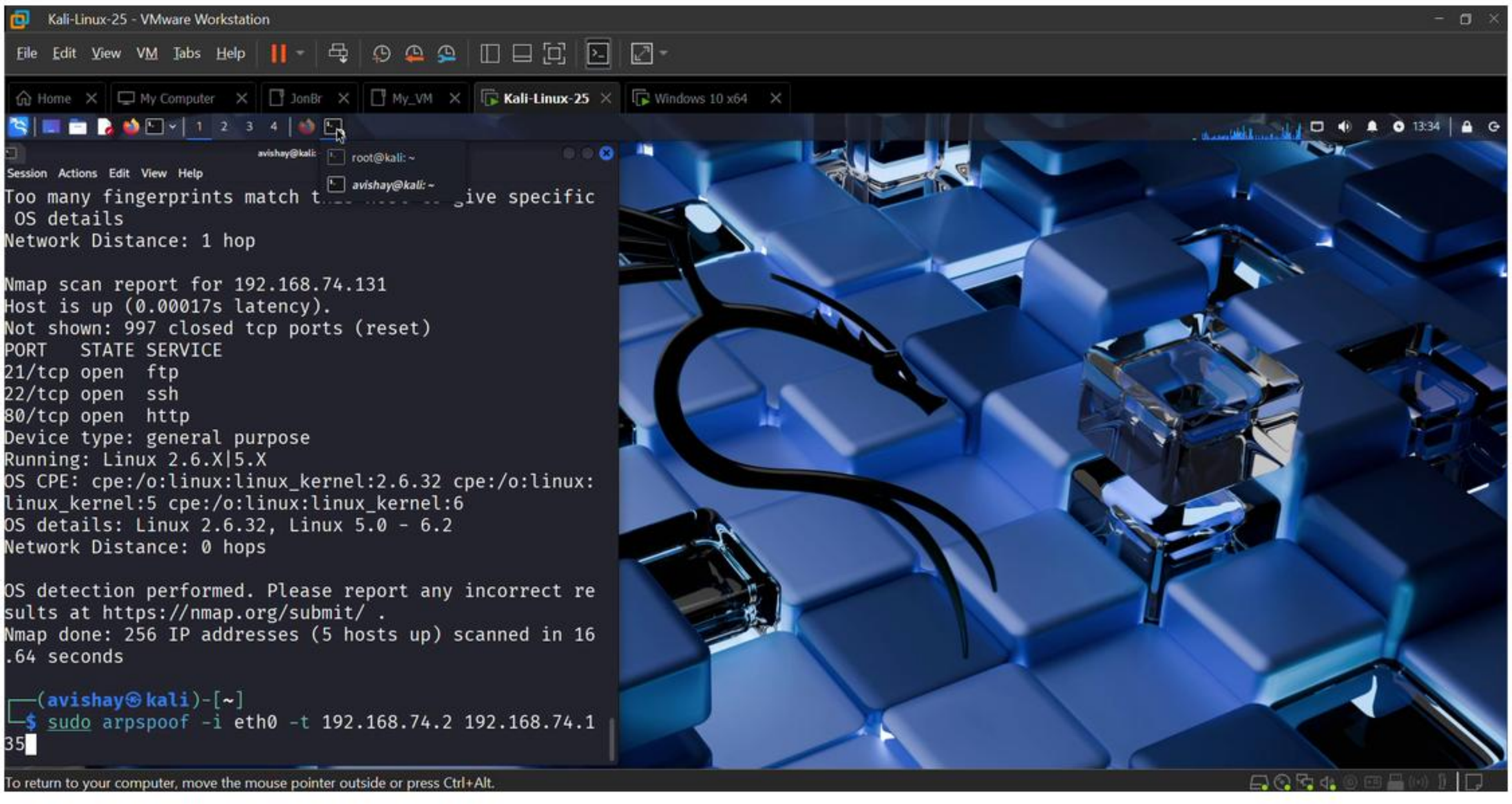
Step 2

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



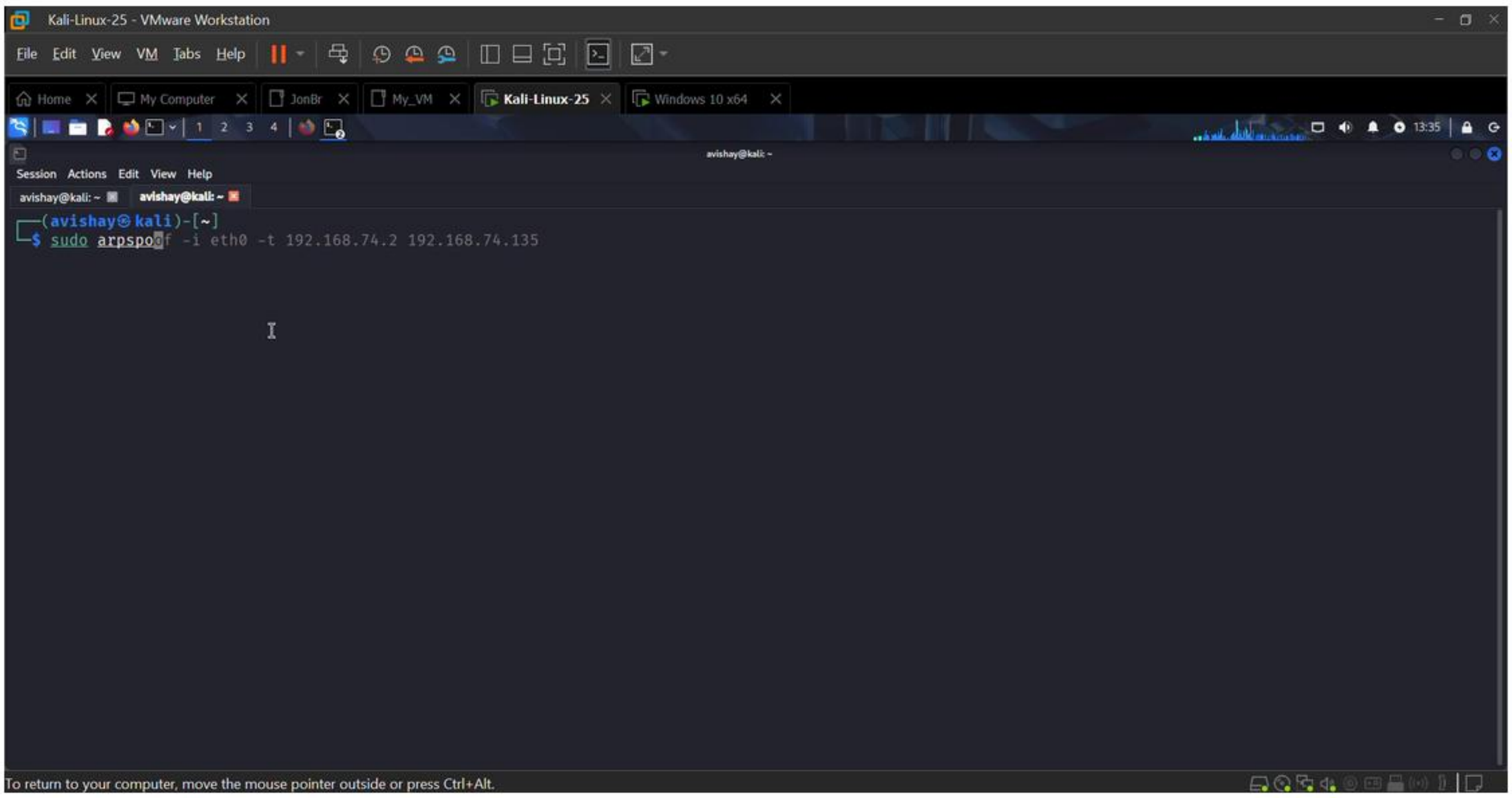
Step 3

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



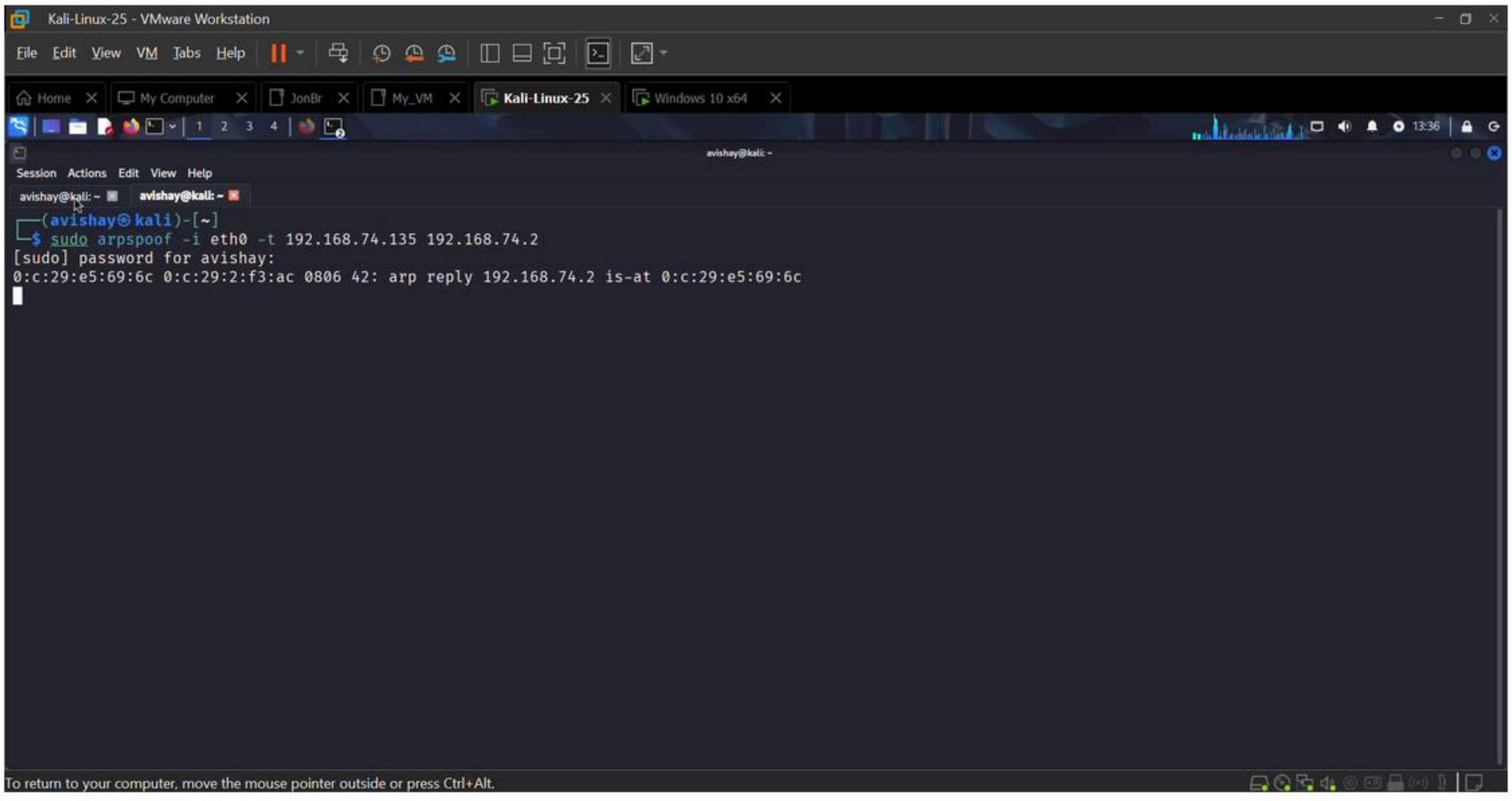
Step 4

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



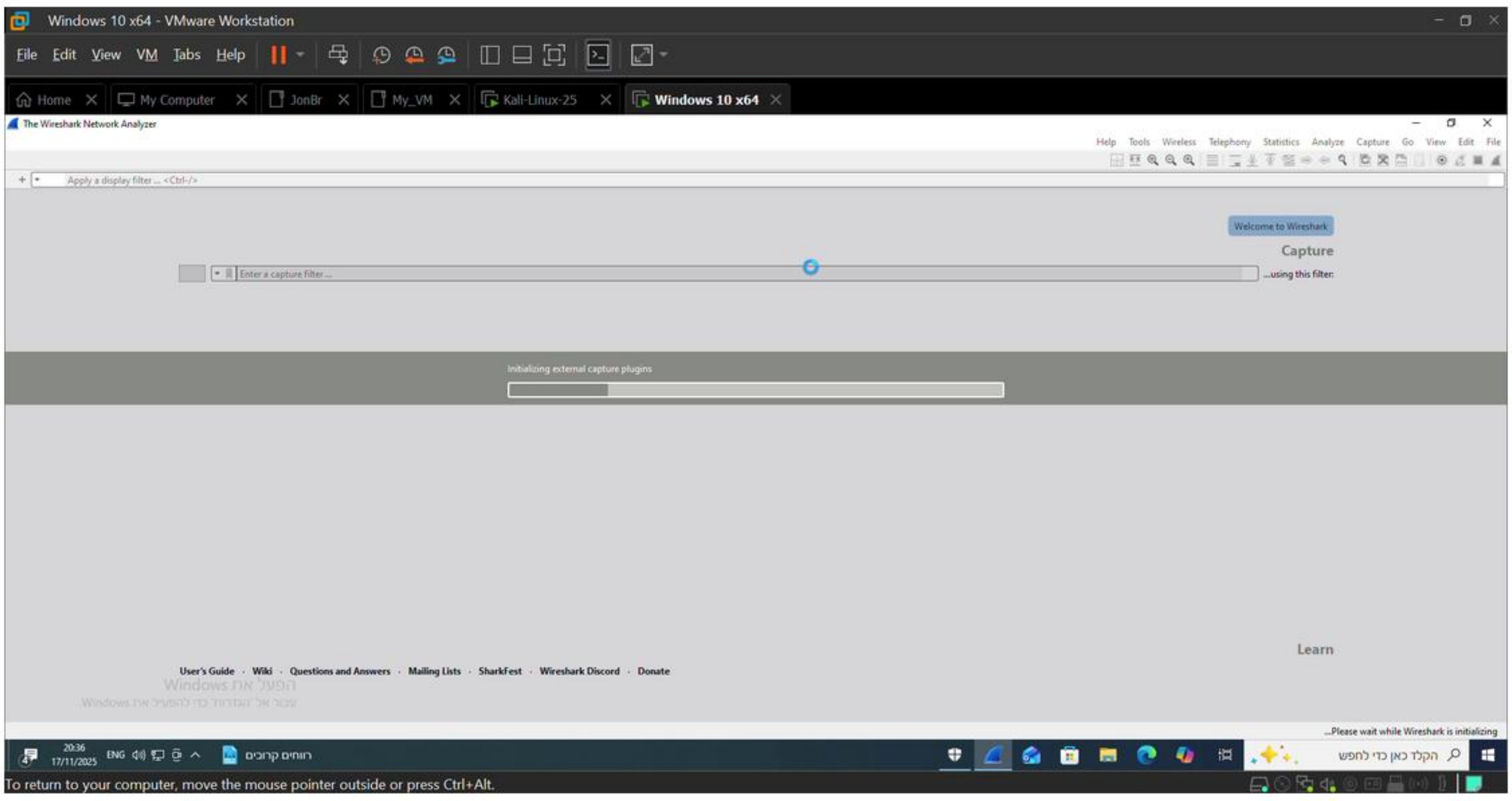
Step 5

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



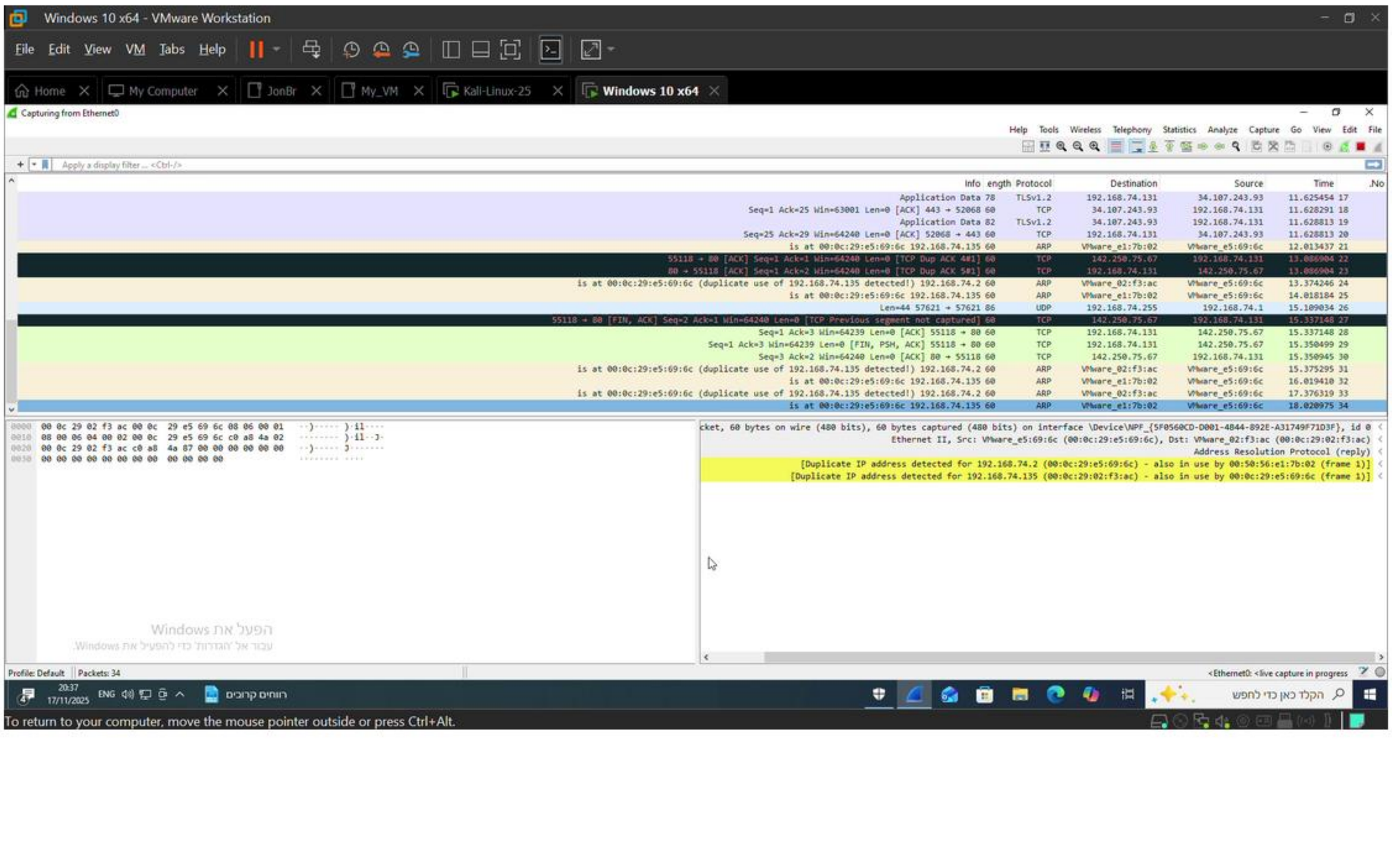
Step 6

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.