**Mission Lab Alpha Recon 1**

**03/26/2024**

**By John Bradley Webb IV**

**Mission Objective:** You have been dropped into an unknown virtual environment and need to

identify your location and conduct reconnaissance to gather critical information about the

network. Your goal is to explore the environment, discover the size of the network, and

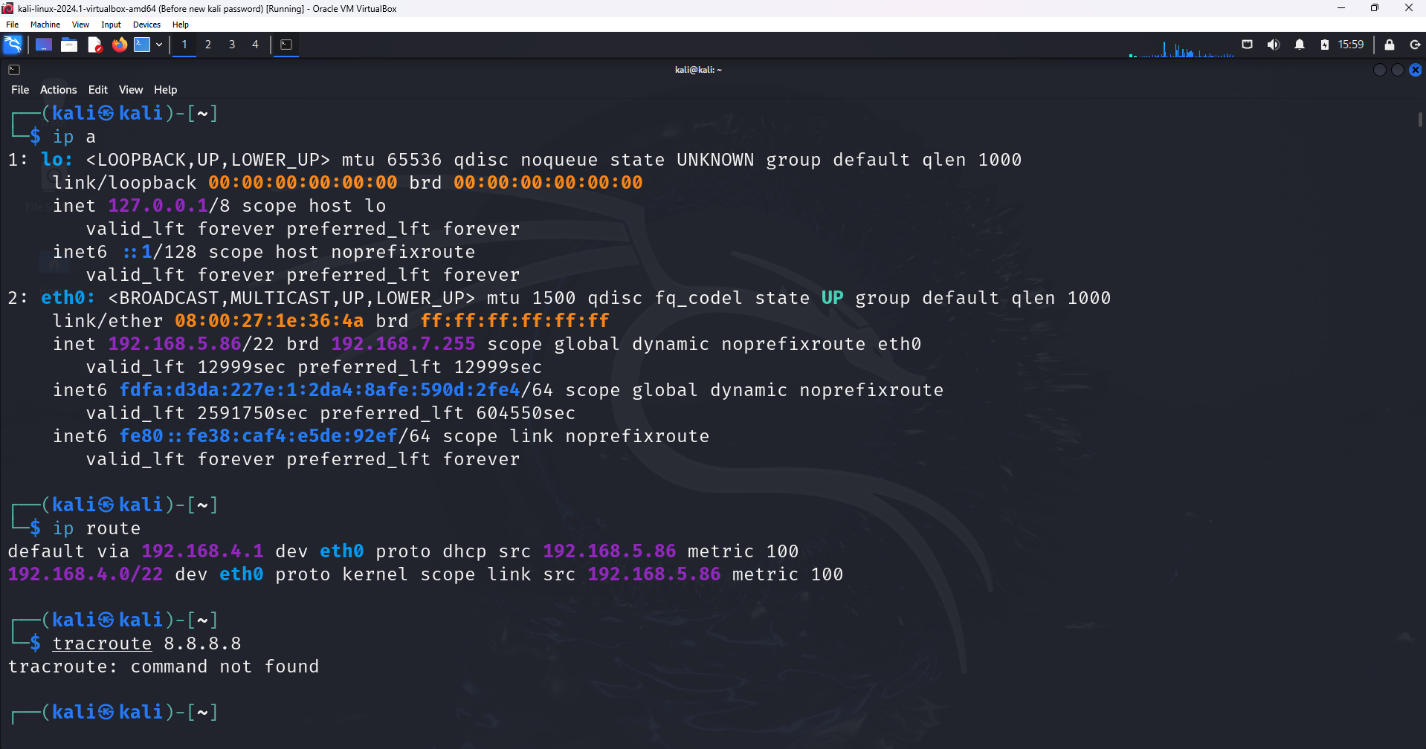
enumerate the systems present. Locate the Jumpbox system and initiate network mapping scans

to identify other active systems within the network.

**Task 1: Orientation in the Unknown Virtual Environment**

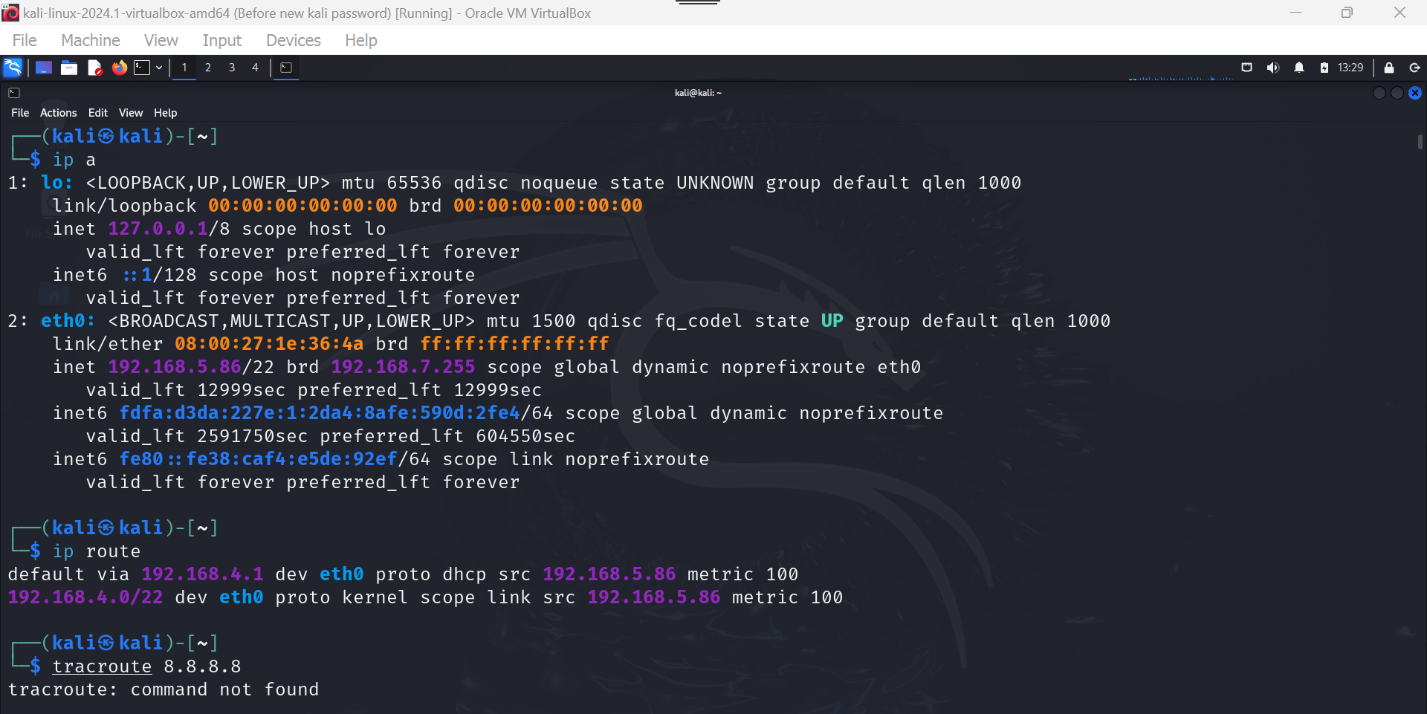
*(Use the ‘ip a’ command to check the network interfaces on your current system.)*

* **Network Interfaces Discovery**: The **ip a** command revealed several network interfaces, including one with an IP address indicating it's part of a larger, possibly segmented network.



*(Execute the ip route command to view the routing table and identify the default gateway.)*

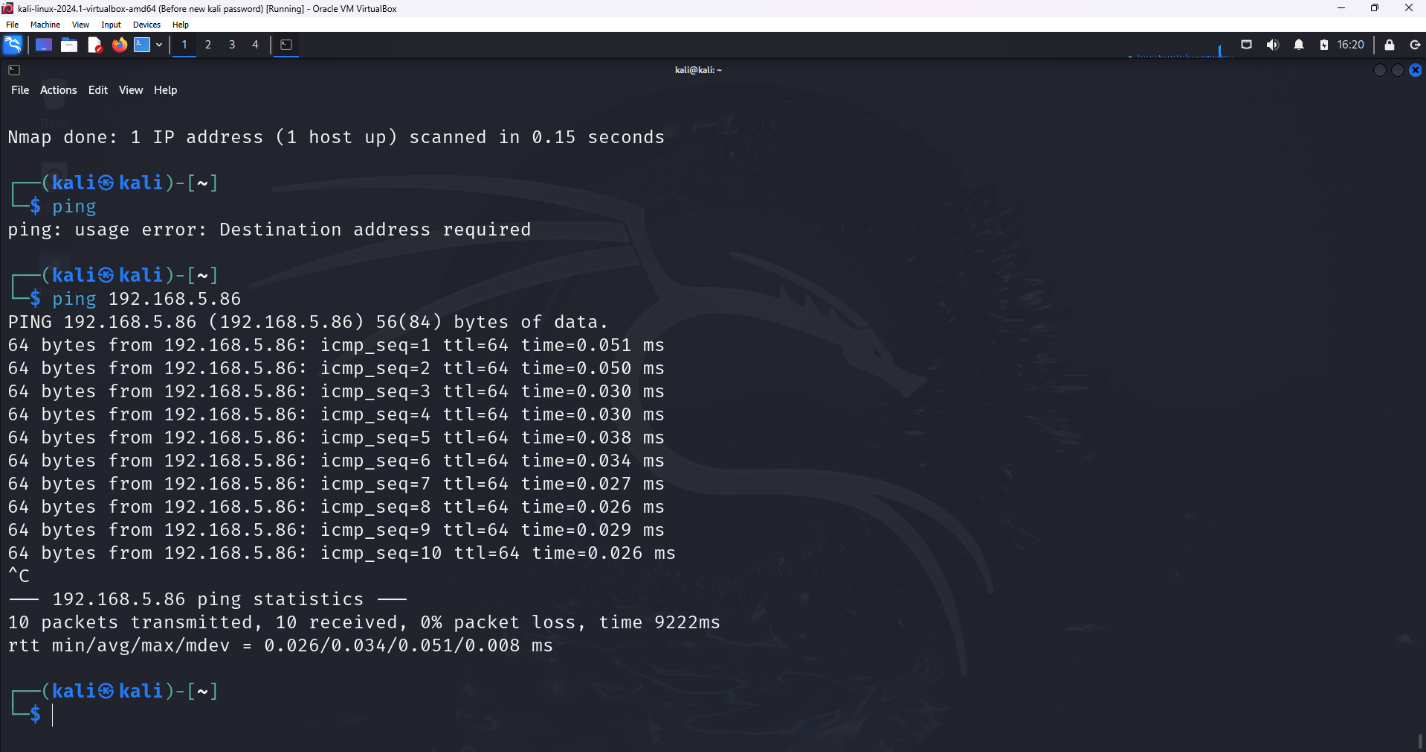
* **Default Gateway Identification**: Using **ip route**, the default gateway was identified, suggesting a pathway out of the local network and potentially to other network segments or the internet.



**Task 2: Identifying Live Systems**

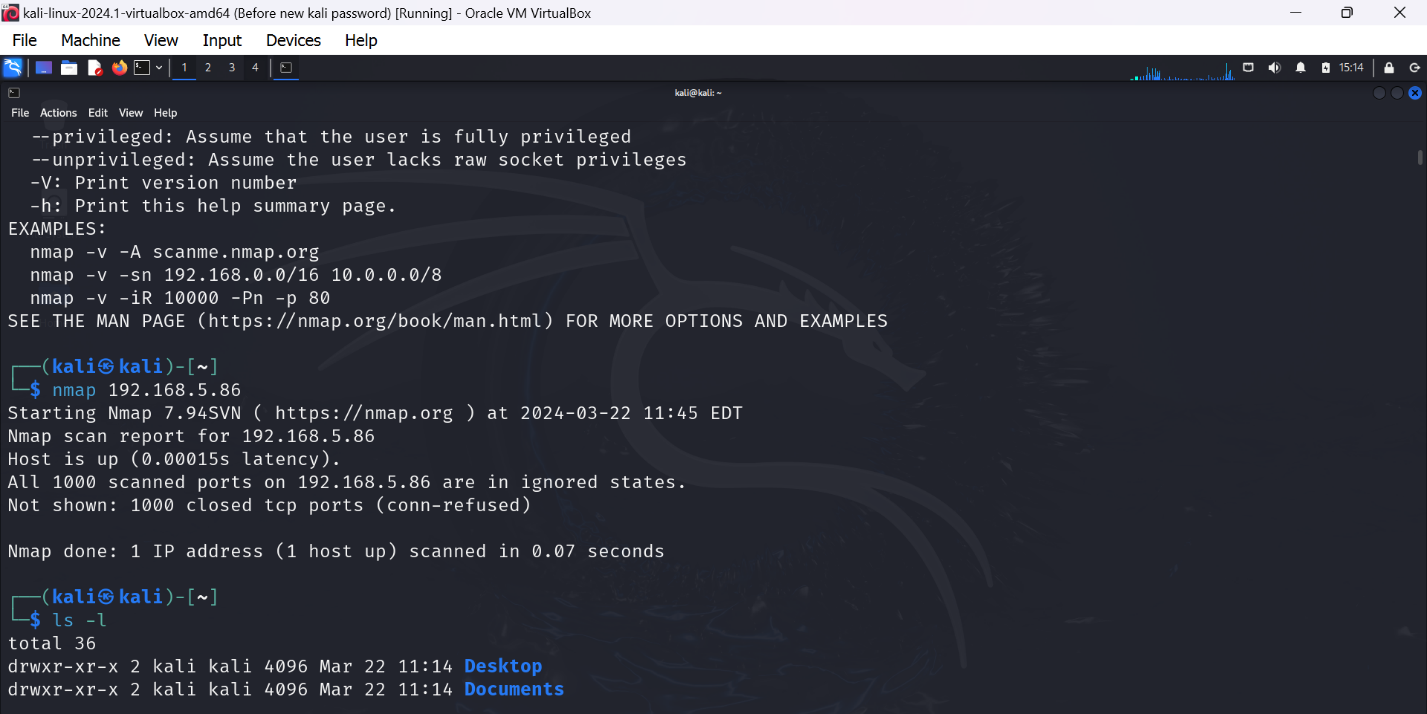
*(Scan the network to identify live hosts using the ‘ping’ command.)*

* **Live Hosts Detection**: The execution of the ping command across the network range highlighted several responsive hosts, indicating active systems within the network.



*(Use ‘nmap’ to perform a port scan and identify open ports on the live hosts. (optional))*

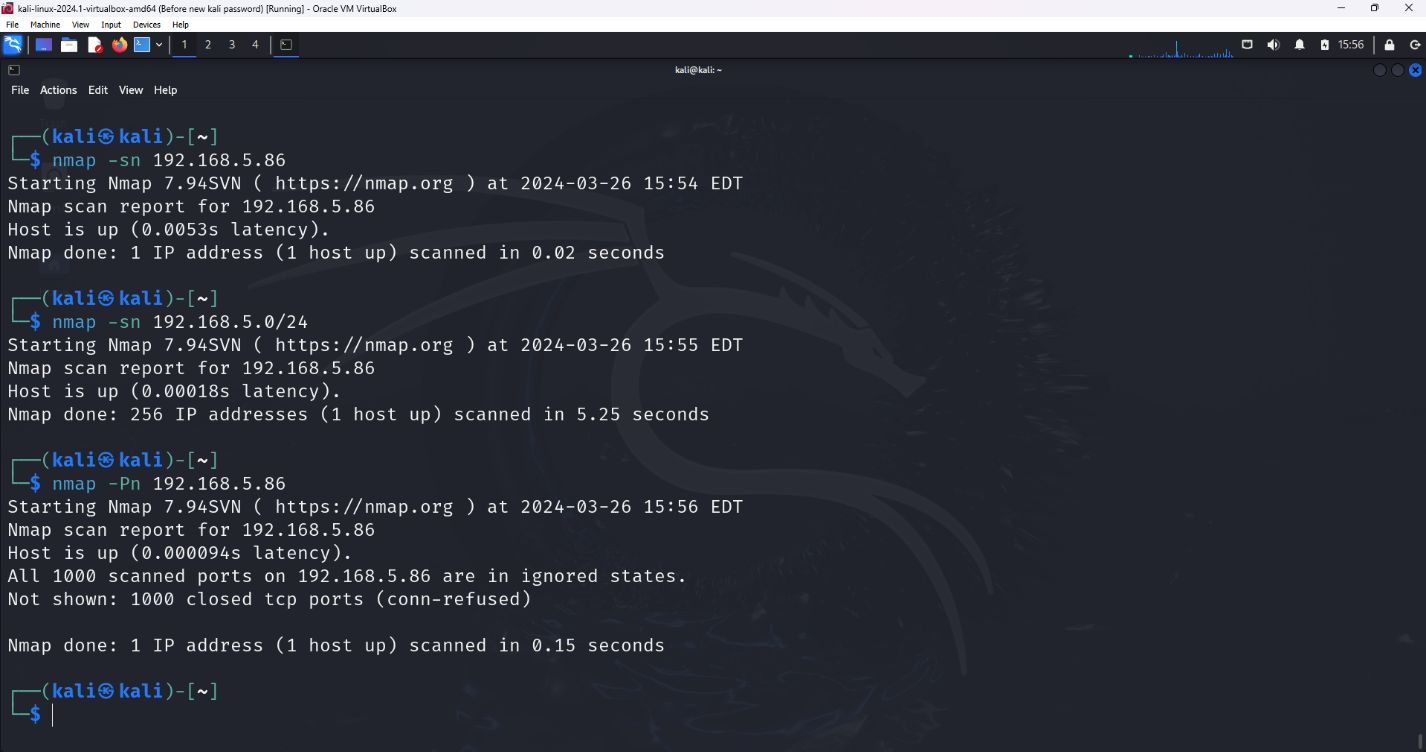
* **Open Ports Discovery**: An optional nmap port scan on discovered live hosts listed open ports, hinting at running services that could be gateways for further exploration or exploitation.

****

**Task 3: Network Mapping and System Discovery**

(*Perform a detailed network scan using nmap to identify all active systems and their open ports.)*

* **Comprehensive Network Scan**: A detailed nmap scan was executed, revealing all active systems in the network along with their open ports. This scan was crucial for understanding the network's layout and the services running on each host.

****

*(Use nmap to discover the operating system and service versions on the identified systems.)*

* **System Identification**: The same nmap scan also shed light on the operating systems and service versions on the identified systems, offering clues about the network's potential vulnerabilities and the types of systems protected within its boundaries.

**Example Scenario Observables**

* **Initial Configuration Checks**: The **ip a** and **ip route** commands provided a clear picture of the starting system's network configuration and its place within the larger network.

****

* **Pinpointing the Jumpbox**: A system, identified through a ping scan as "172.18.0.4", was recognized as the Jumpbox. A targeted nmap scan on this system unveiled its role and open services.
* **Network-Wide Enumeration**: A ping sweep, followed by targeted nmap scans, cataloged the active systems, their services, and security postures.

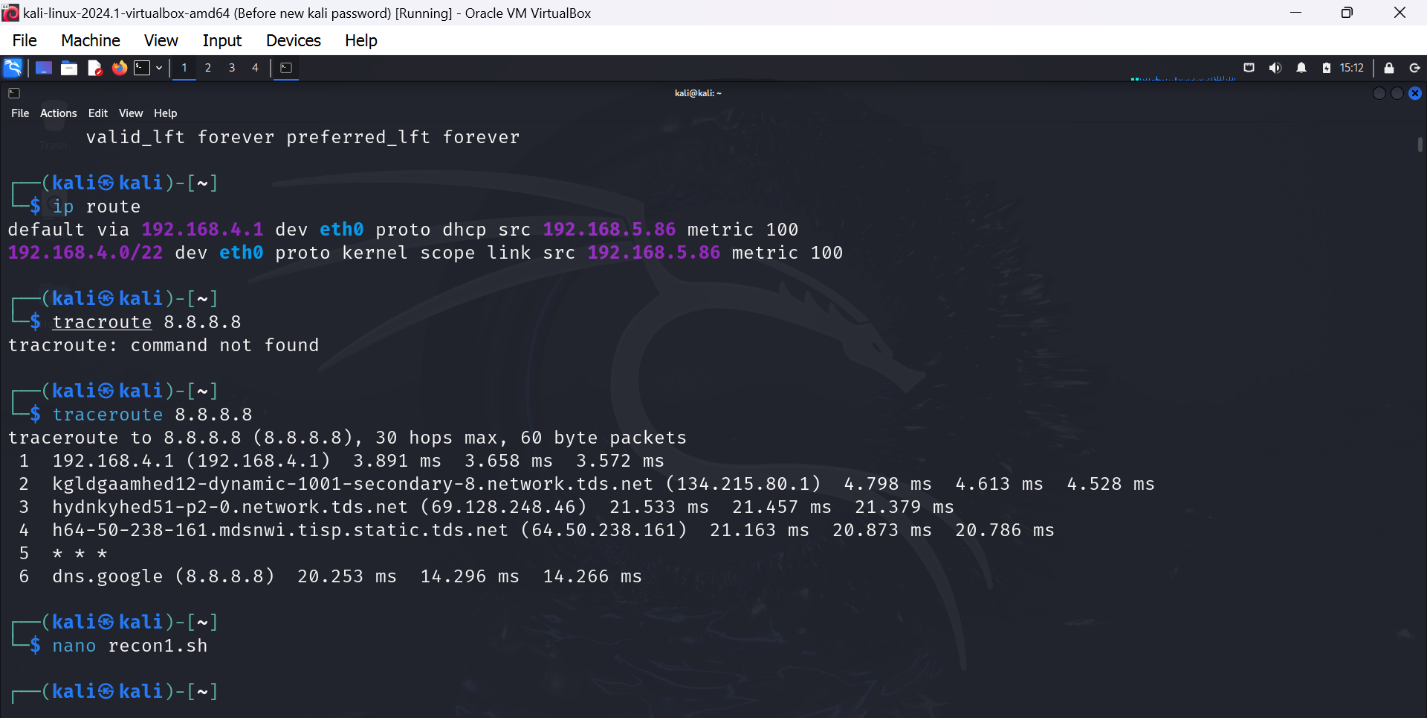
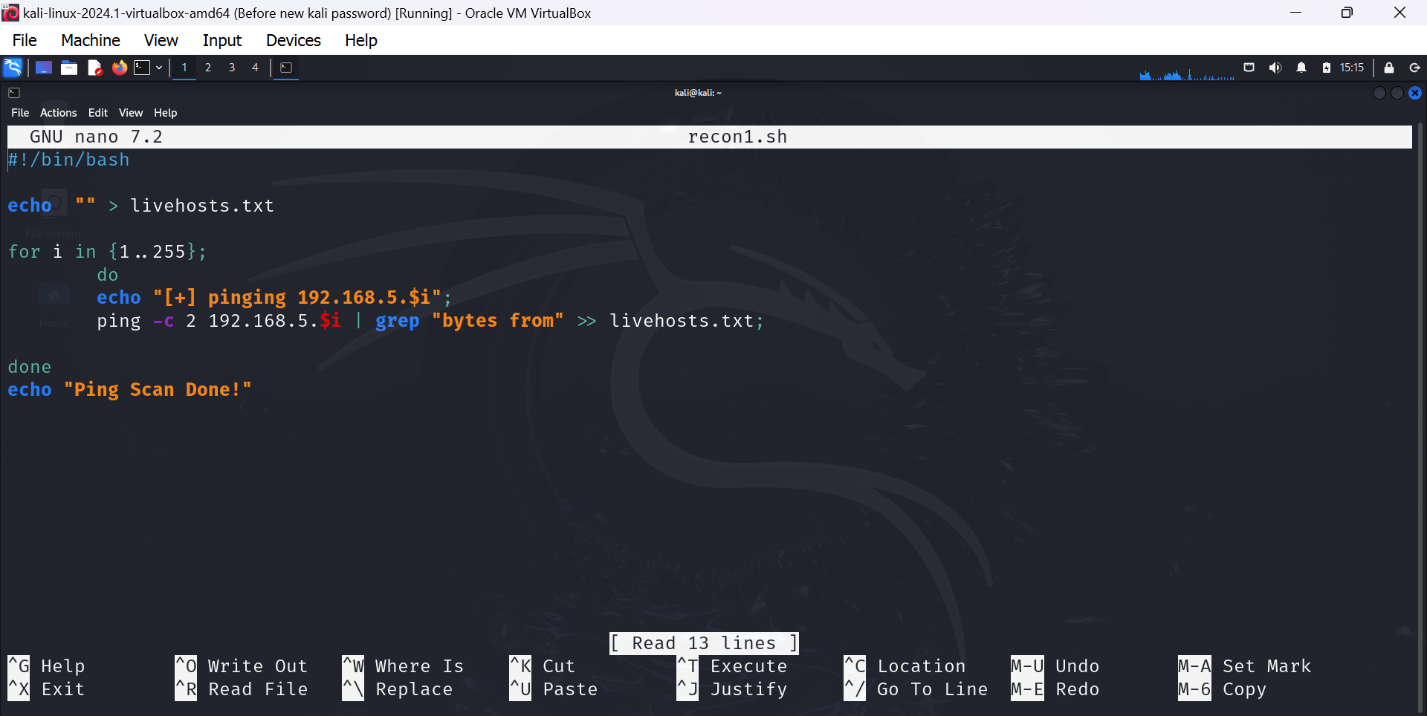
**Task 4: ASSIGNMENT**

*(Create a bash script called “recon1.sh” that will contain the for loop provided above that*

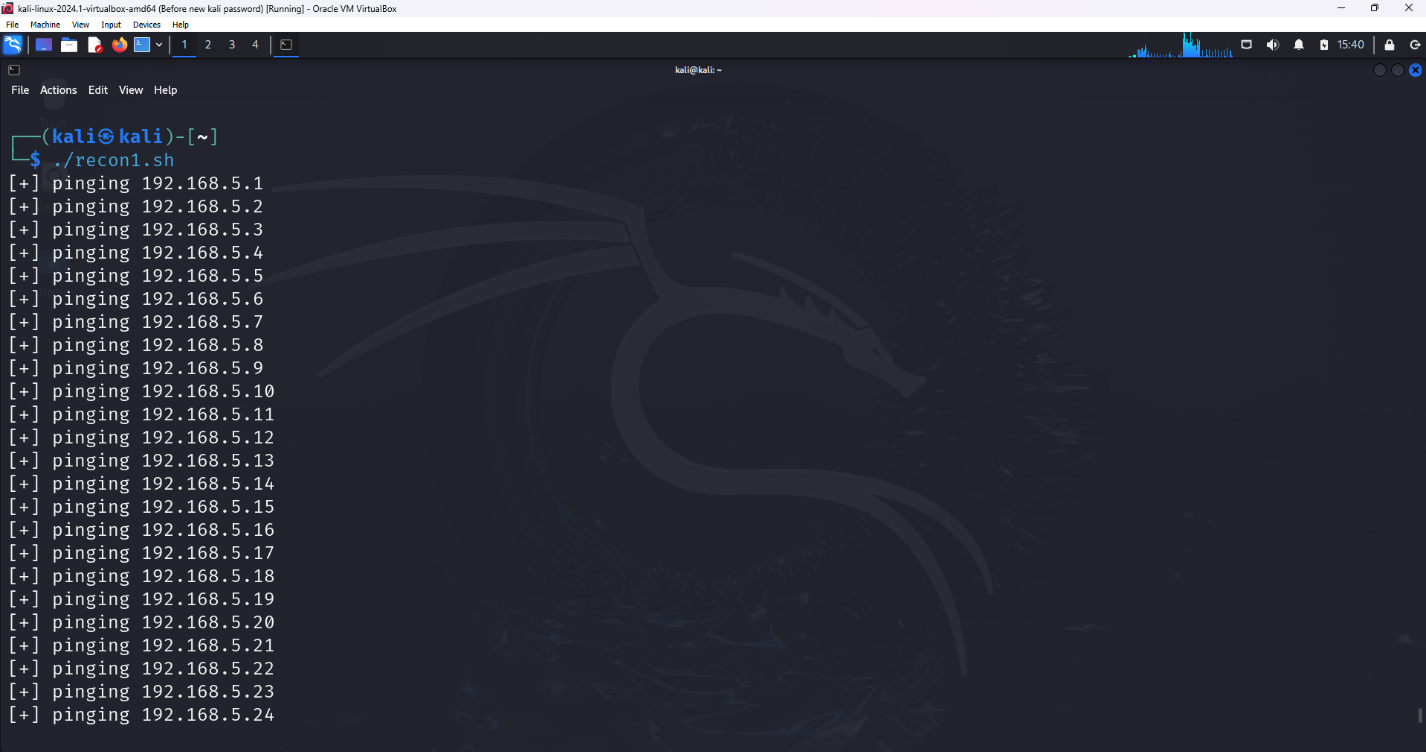
*will run and create an output file on the results. Please write down a short list of the*

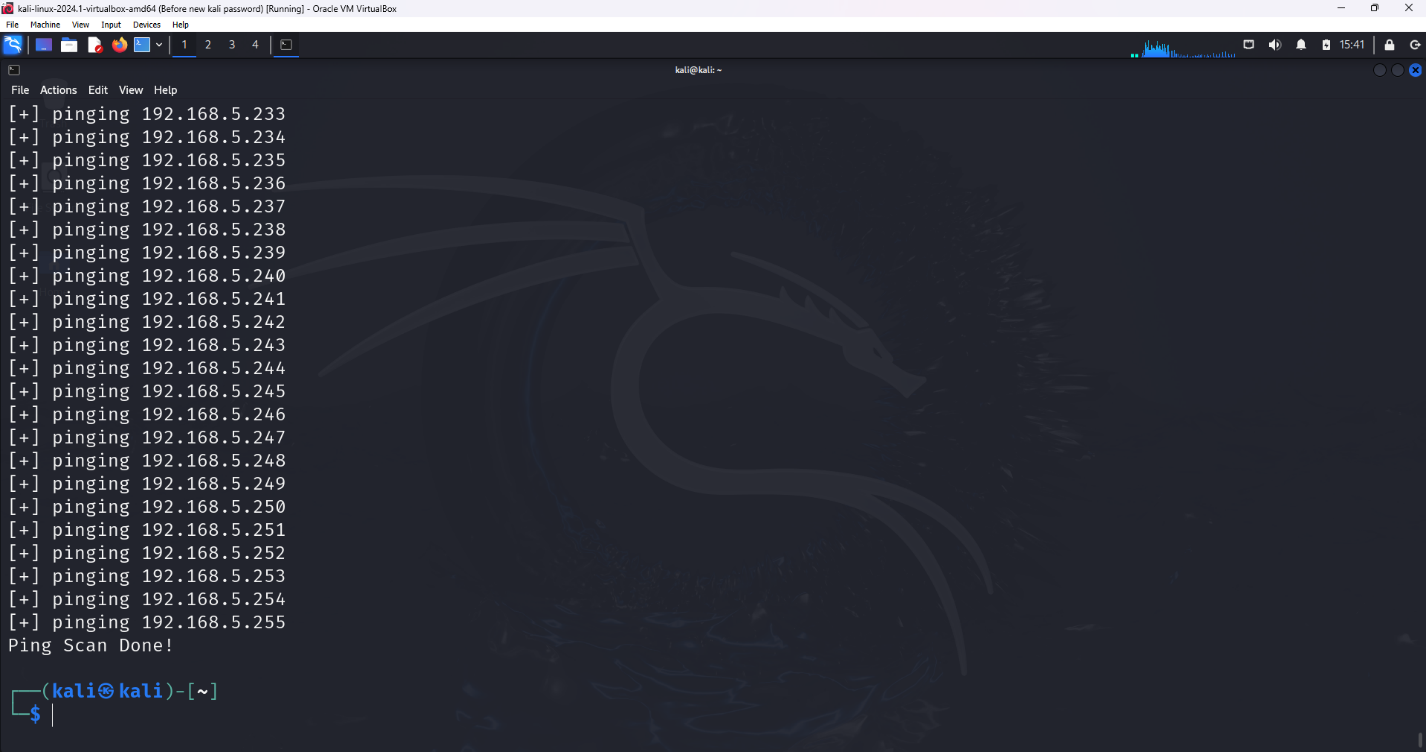
*commands and tools we used during the mission. Store your output in a file called*

*“TargetList.txt” and upload this file with your assignment submission.)*

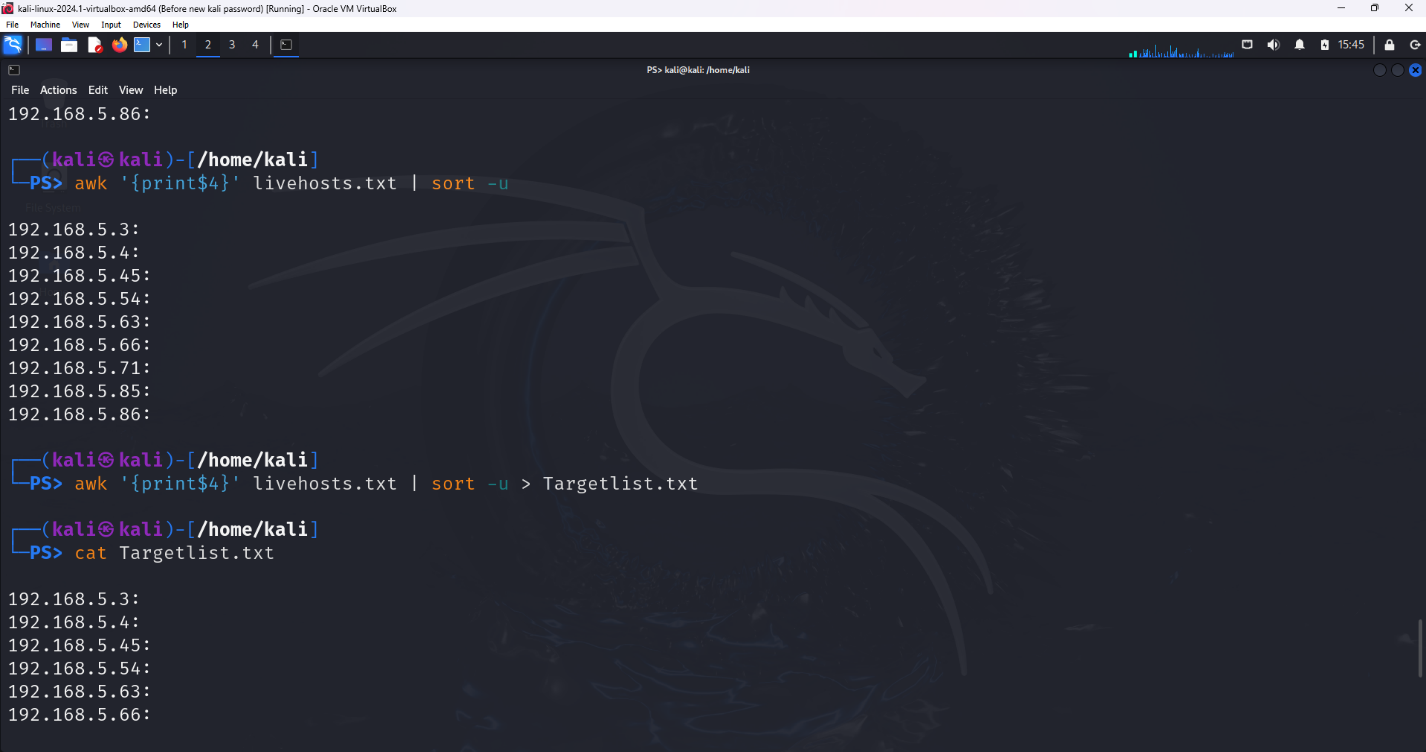
********

* **Script Execution**: Running the **recon1.sh** script automated the scanning process, efficiently mapping out the network's active systems and notable ports.

****



* **Findings Documentation**: The output, captured in "TargetList.txt", provided a comprehensive list of the network's hosts, their open ports, operating systems, and running services, forming a basis for further analysis or action.

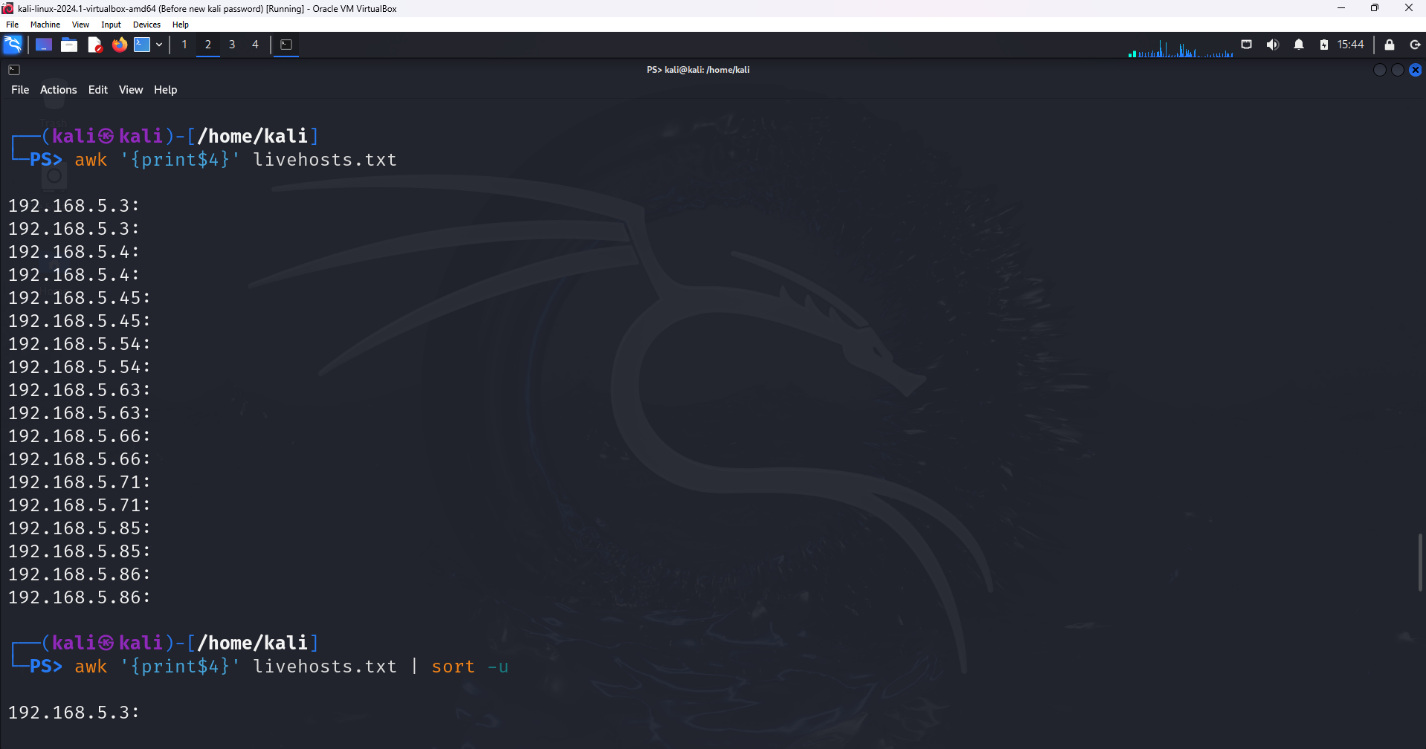
****

* **Operational Commands and Security Posture**: Post-execution commands (e.g., **ping 8.8.8.8**, **ip addr**) confirmed network connectivity and context, while a privilege check ensured the operations were conducted within the appropriate security context.



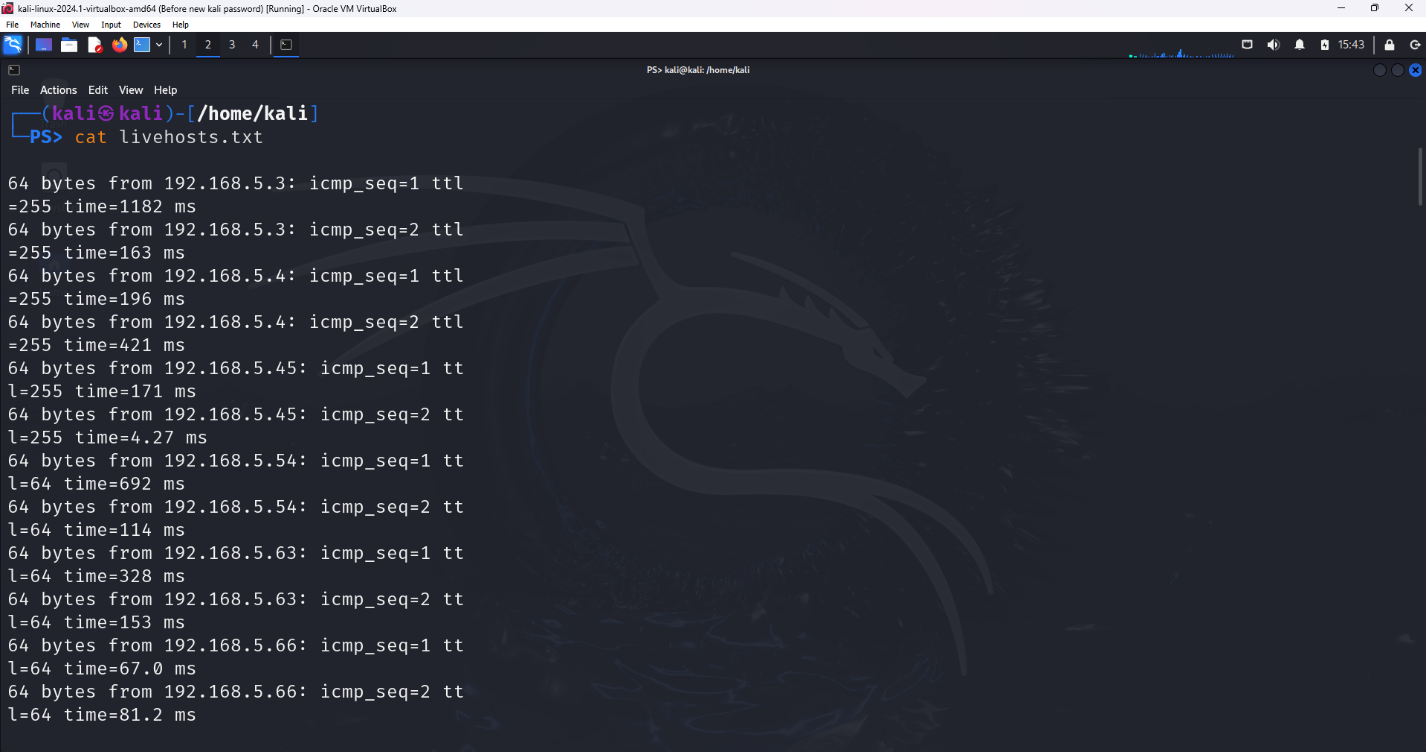
**Bonus: Network Exploration Depth**

*(Use Awk and sort commands to grab and sort to unique values.)*

**

* **Iterative Discovery Requirement**: To ensure no host within the network's various segments was overlooked, the script was run multiple times, adjusting targets to systematically cover the entire network space. Each iteration revealed new hosts or services, gradually completing the picture of the network's architecture and vulnerabilities.

*(Look in your recon file for the clue to complete this MISSION!)*

**

This sequential documentation of observables from conducting Mission Lab ALPHA Recon1 provides insights into the network's structure, security posture, and potential areas for further investigation or hardening.