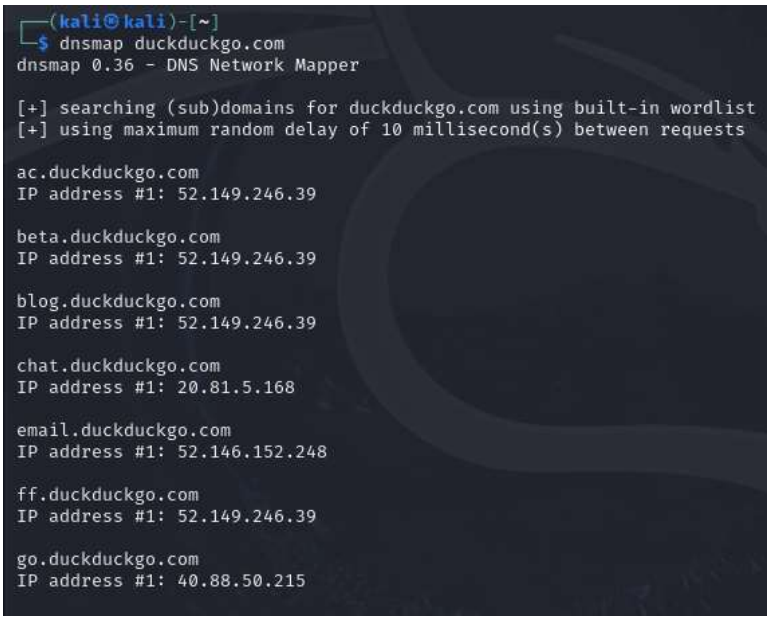
This project focuses on gathering network information using tools like dnsrecon for DNS enumeration, Nmap for scanning ports and services, and Nessus for vulnerability scanning. It provides essential skills for identifying live hosts, open ports, and potential vulnerabilities in a network. Here's a summary of the key components and steps:

DNS Enumeration

Understanding DNS: Learn how DNS resolves hostnames to IP addresses, zones, and resource records.

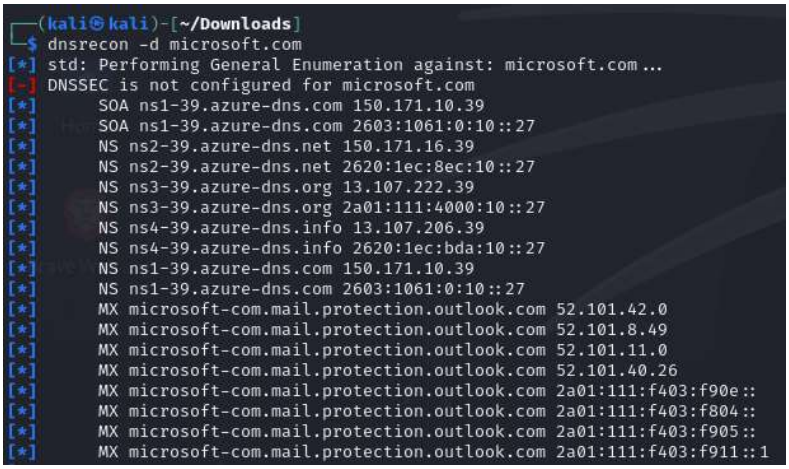
Using DNSmap



Performing Enumeration:

Use dnsrecon and host commands to gather DNS records for a target domain.

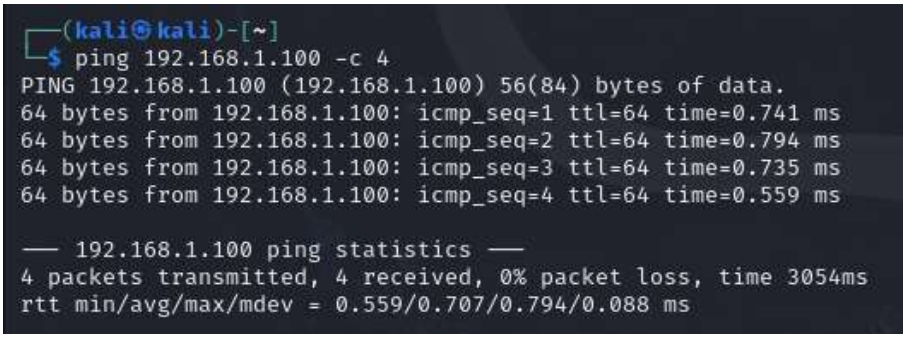
Practice zone transfer using tools like host and dnsenum.



Network Scanning

Discover Live Hosts:

Use tools like ping, arp-scan, and Nmap.



Basic and Advanced Nmap Scans:

Conduct scans to identify open ports, services, and operating systems.

Use options like -sS, -sU, -sV, and the NSE scripting engine.

-sS scans a range of IP addresses