IS IA-2 Report

**Aryan Balpande-16010120002**

**Vinod Ghanchi-16010120016**

**Kaushik Iyer-16010120017**

# What is Zenmap?

Zenmap is a graphical user interface (GUI) for the network exploration and security auditing tool Nmap. It allows users to quickly and easily perform network scans, identify hosts and services, and discover potential security vulnerabilities. Zenmap provides a variety of scanning options, including ping sweeps, TCP and UDP port scans, and operating system detection. It also offers features such as host filtering and advanced scripting for custom scans.

# Features provided by Zenmap

Zenmap is a graphical user interface (GUI) for Nmap, a network exploration and security auditing tool. Zenmap provides an easy-to-use interface for users to quickly and easily scan their networks and identify potential security vulnerabilities. Some of the features of Zenmap include:

* Graphical representation of the network topology
* The ability to conduct various types of scans, including ping sweeps, TCP and UDP port scans, and operating system detection
* The ability to save and load scan results for future reference
* The ability to filter hosts and services based on various criteria
* The ability to create custom scripts to automate and streamline scanning processes
* The ability to compare and contrast scan results to identify changes over time
* The ability to export scan results in a variety of formats, including HTML and XML.

# What is Nmap?

Nmap is a free and open-source network exploration and security auditing tool that can be used to discover hosts and services on a computer network, thus creating a "map" of the network. It is commonly used by network administrators to identify potential vulnerabilities and to monitor network security. Nmap uses a variety of techniques to scan networks, including port scanning, host discovery, and operating system detection. It can also be used to gather information about hosts on a network, such as open ports, operating system versions, and service versions. Nmap includes advanced features like NSE (Nmap Scripting Engine), which allows users to create and execute custom scripts to automate tasks and customize their scanning processes.

# Technologies Used

Nmap uses various technologies to perform network exploration and security auditing tasks. Some of the key technologies used by Nmap include:

* Raw IP packets: Nmap sends and receives raw IP packets to discover hosts, identify open ports, and gather information about network services.
* TCP/IP stack fingerprinting: Nmap uses various techniques to identify the operating system and version of the TCP/IP stack running on target hosts. This can be used to identify potential vulnerabilities and to fine-tune scanning strategies.
* Port scanning: Nmap uses a variety of techniques to scan for open ports on target hosts. This can be used to identify potential security vulnerabilities and to monitor network traffic.
* NSE (Nmap Scripting Engine): NSE is a powerful feature of Nmap that allows users to create and execute custom scripts to automate tasks and customize their scanning processes. NSE scripts can be used to perform a variety of tasks, including vulnerability scanning, network discovery, and data collection.

# Uses of Zenmap

Some of the key use cases of Zenmap include:

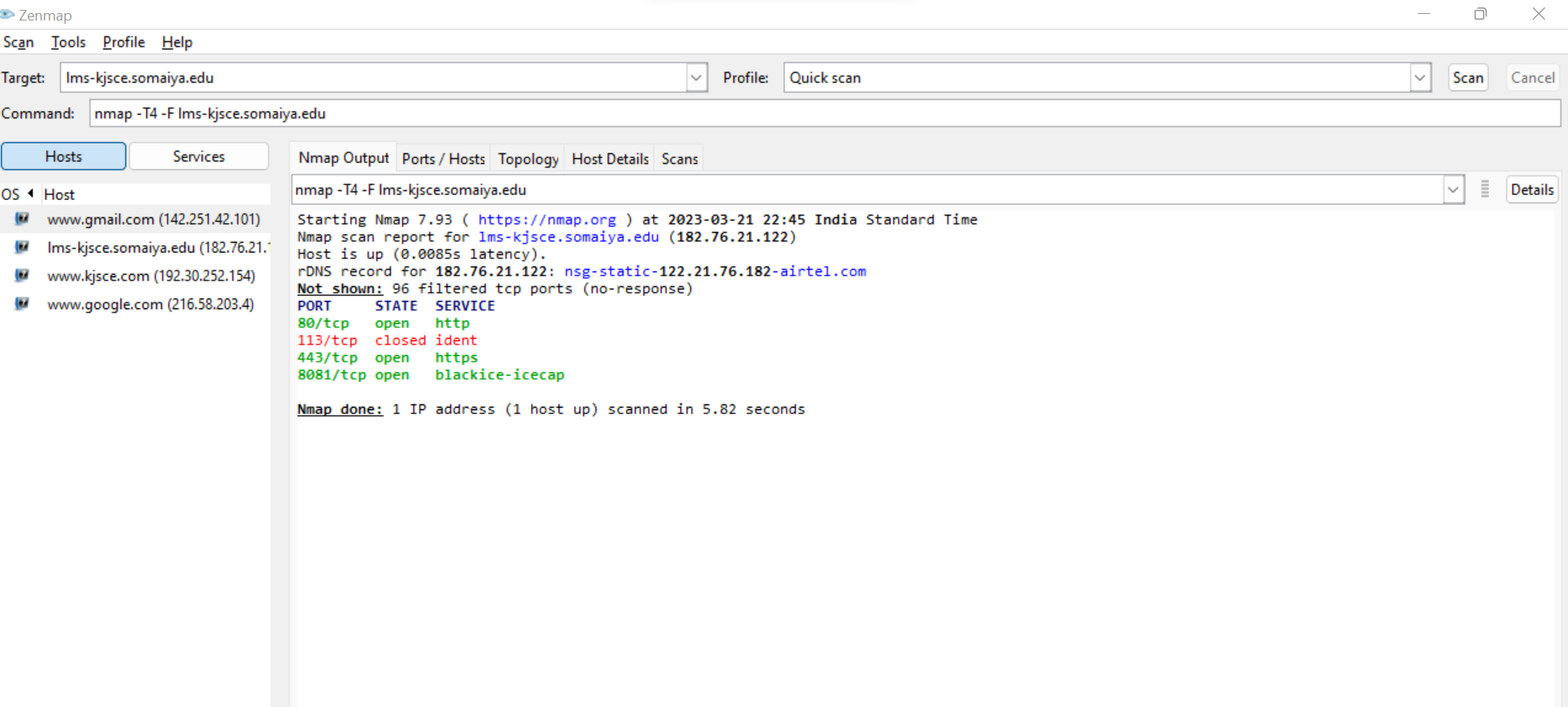
* Network mapping: Zenmap can be used to create a visual map of a network, identifying hosts, services, and potential vulnerabilities.
* Network inventory: Zenmap can be used to gather information about hosts on a network, including open ports, operating system versions, and service versions.
* Vulnerability scanning: Zenmap can be used to scan a network for potential vulnerabilities, helping administrators to identify and address security risks.
* Monitoring network security: Zenmap can be used to monitor network traffic and identify potential security threats, allowing administrators to take action to protect their network.
* Penetration testing: Zenmap can be used as part of a penetration testing process, helping to identify potential security weaknesses and vulnerabilities in a network.

# 

# Screenshots

## 

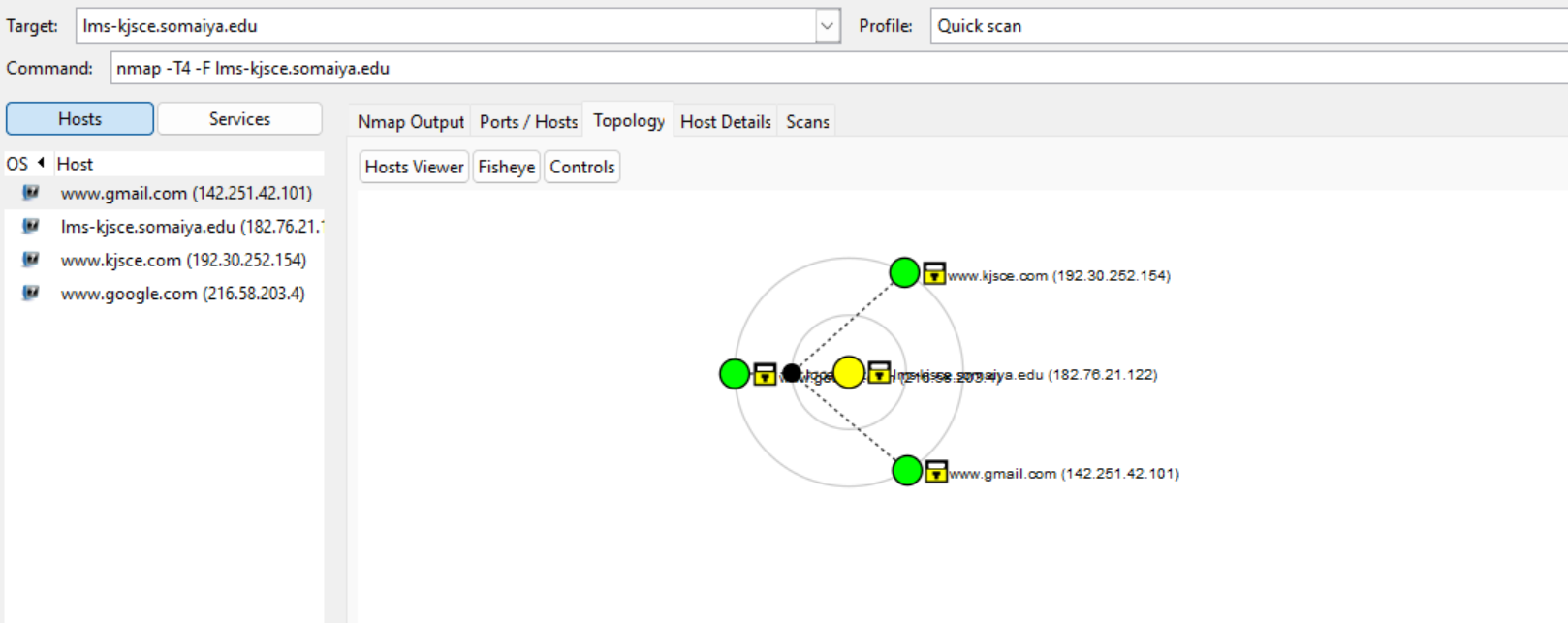
## Quick Scan of LMS



## HOSTS/PORT STATUS

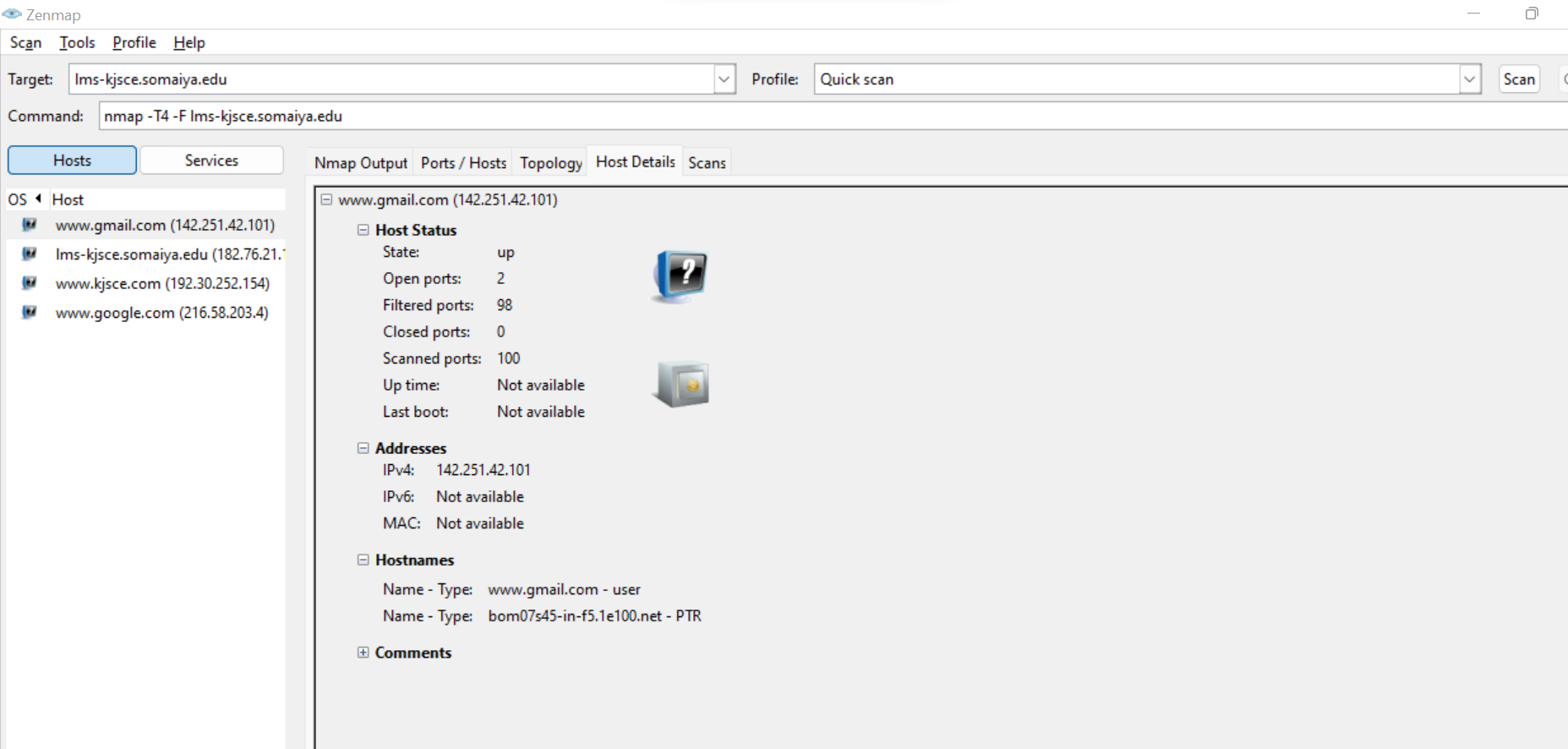
## 

## TOPOLOGY

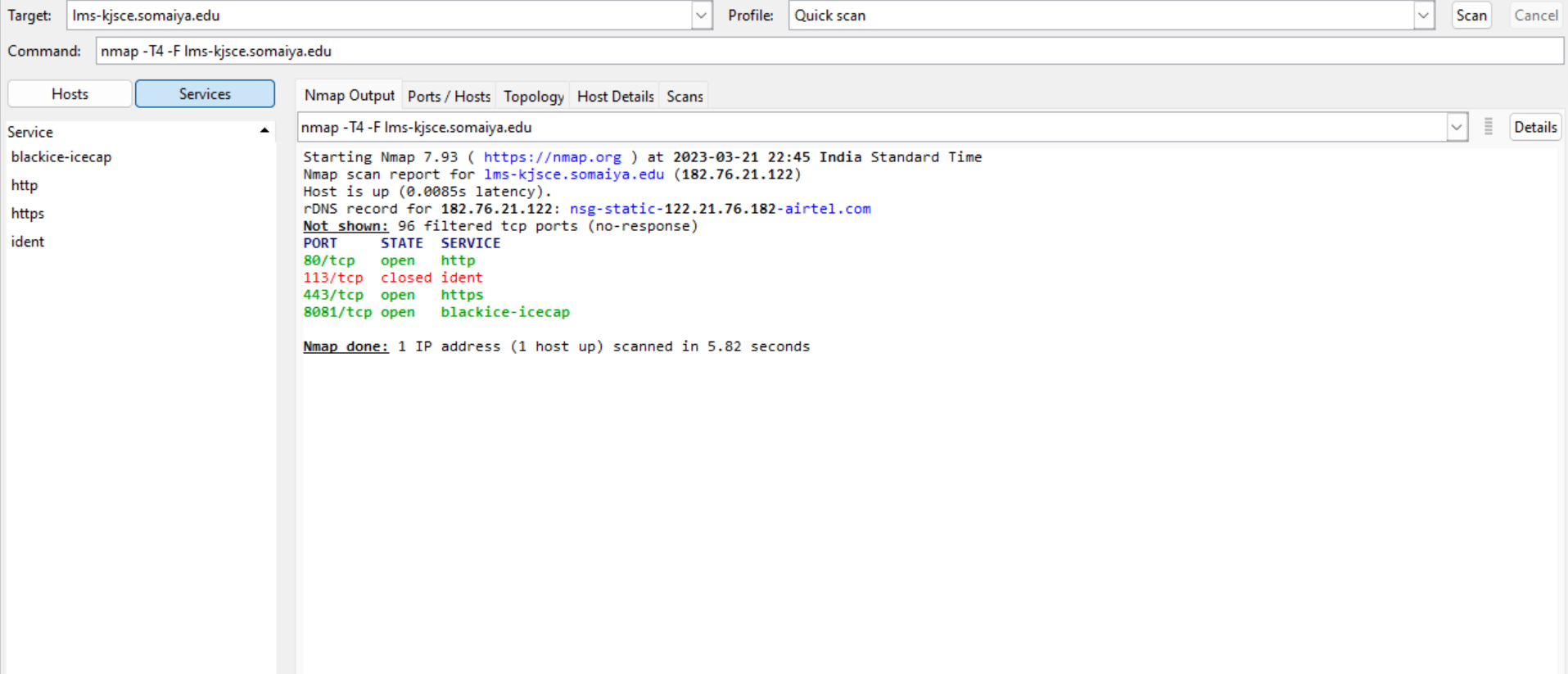


## 

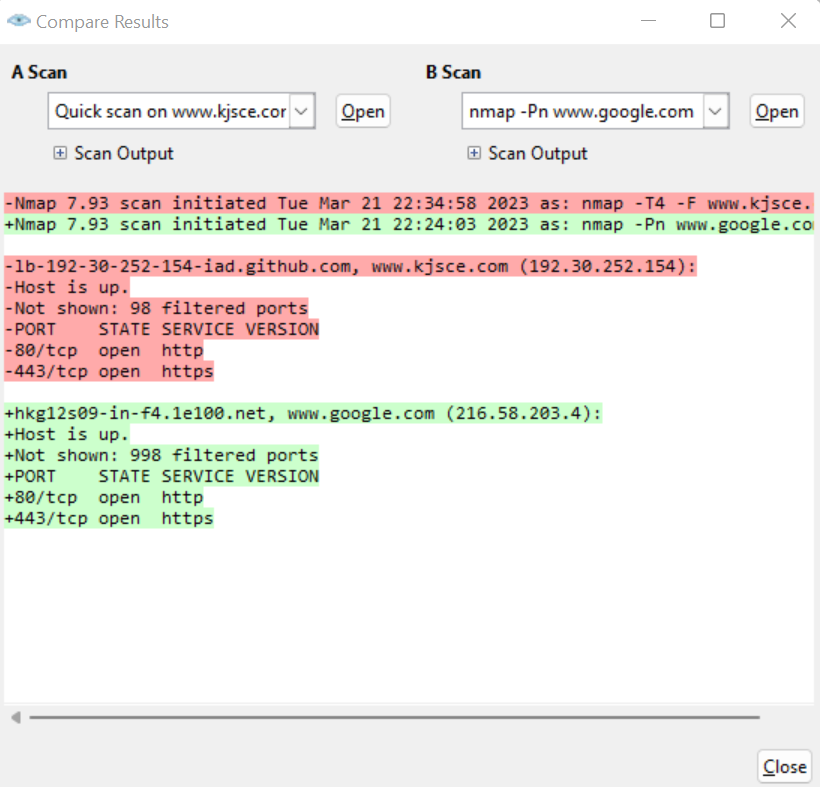
## HOST DETAILS



## Services



## Compare Results



## INTENSE SCAN

