**PROBLEM STATEMENT:**

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine.

Hacker Machine : Windows 10

Victim machine : Kali Linux and Windows

**SOLUTION:**

**WHAT IS NMAP?**

**Nmap** is an open-source utility for network discovery. Network Mapper is a security auditing and network scanning independent tool developed by **Gordon Lyon**. It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Many systems and network administrators are used for managing **network inventory, service upgrade schedules, monitoring hosts** and **service uptime**.

### DEFINITION OF NMAP:

### At the top-level, [Nmap](https://www.educba.com/nmap-commands/" \t "_blank) is defined as a tool that can detect or diagnose services that are running on an **Internet-connected system** by a network administrator in their networked system used to identify potential security flaws. It is used to automate redundant tasks, such as monitoring the service.

WORKING OF NMAP

Nmap is convenient [during penetration testing](https://www.educba.com/penetration-testing/) of networked systems. Nmap provides the network details, and also helps to determine the security flaws present in the system. Nmap is **platform-independent** and runs on popular **operating systems** such as [**Linux**](https://www.javatpoint.com/linux-tutorial)**,**[**Windows**](https://www.javatpoint.com/windows) and **Mac**.

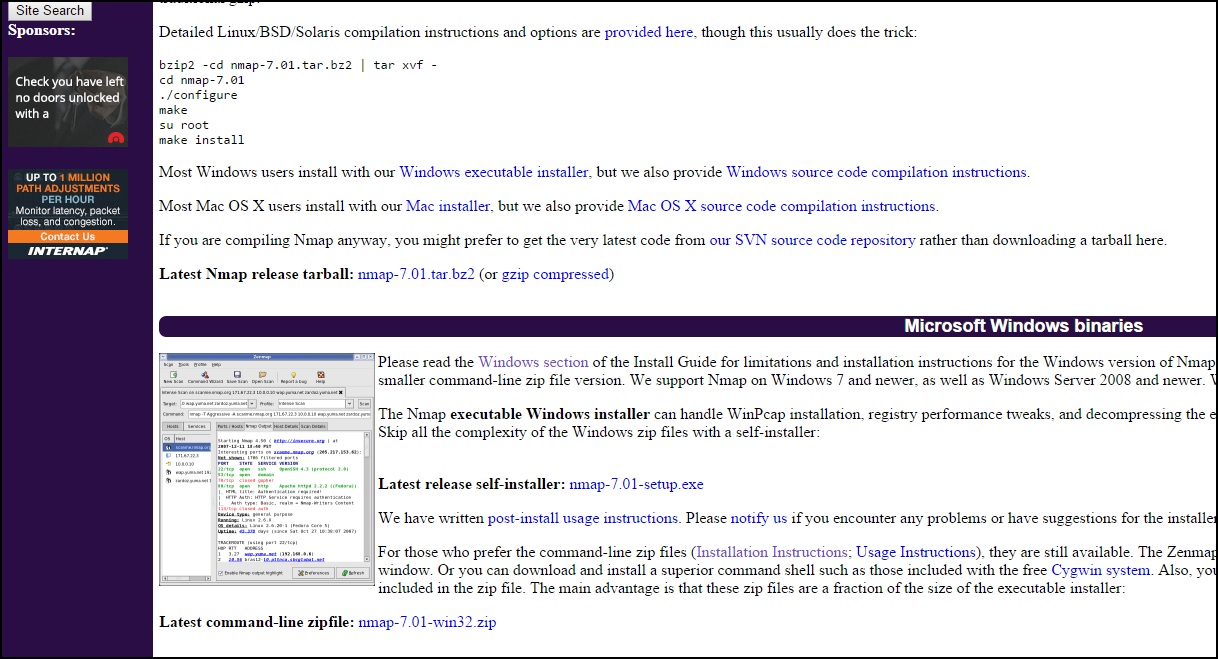
Nmap is a useful tool for network scanning and auditing purposes.

* It can search for hosts connected to the Network.
* It can search for free ports on the target host.
* It detects all services running on the host with the help of **operating system**.
* It also detects any **flaws** or **potential vulnerabilities** in networked systems.

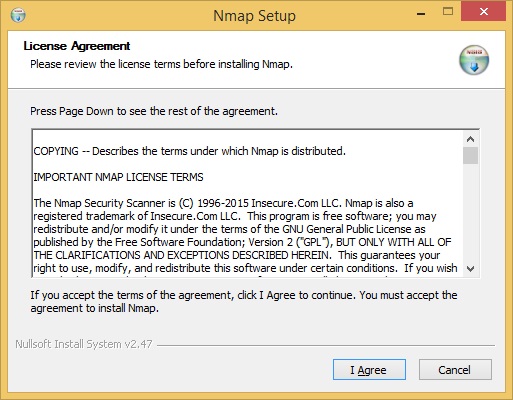
It is effortless to work with the Nmap. With the release of a new graphical user interface called **GenMap User**, it performs many tasks such as saving and comparing scan results, scanning the results in a database, and visualize the network system topology graphically, etc.

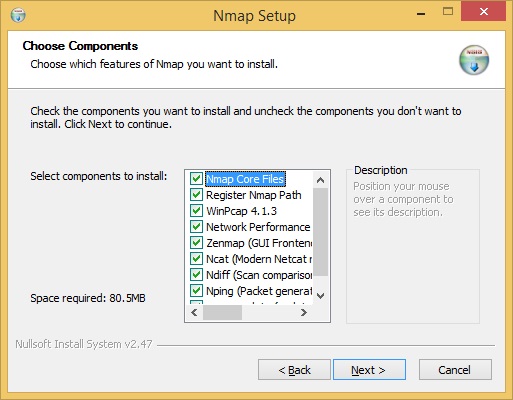
steps to install Nmap on Windows:

**1.**Browse to <https://nmap.org/download.html> and download the latest self-installer.

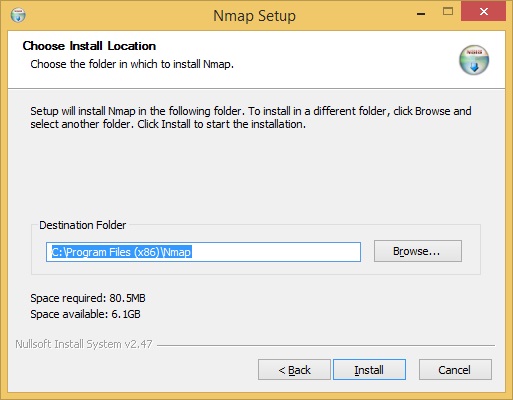


1. Run the downloaded**.exe** file. In the window that opens, accept the license terms:

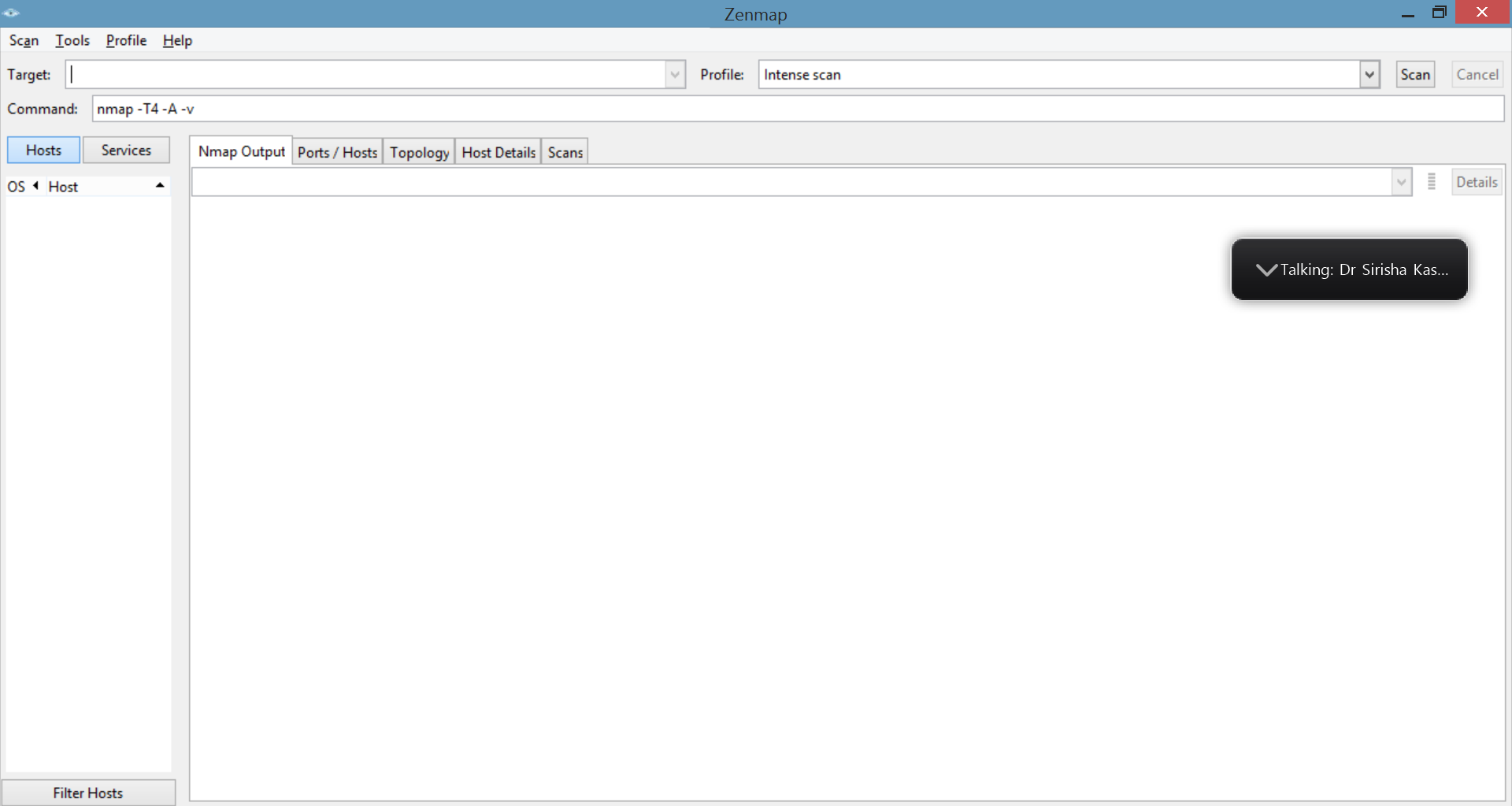


1. Choose the components to install. By default, the**Zenmap GUI** will be installed: ****

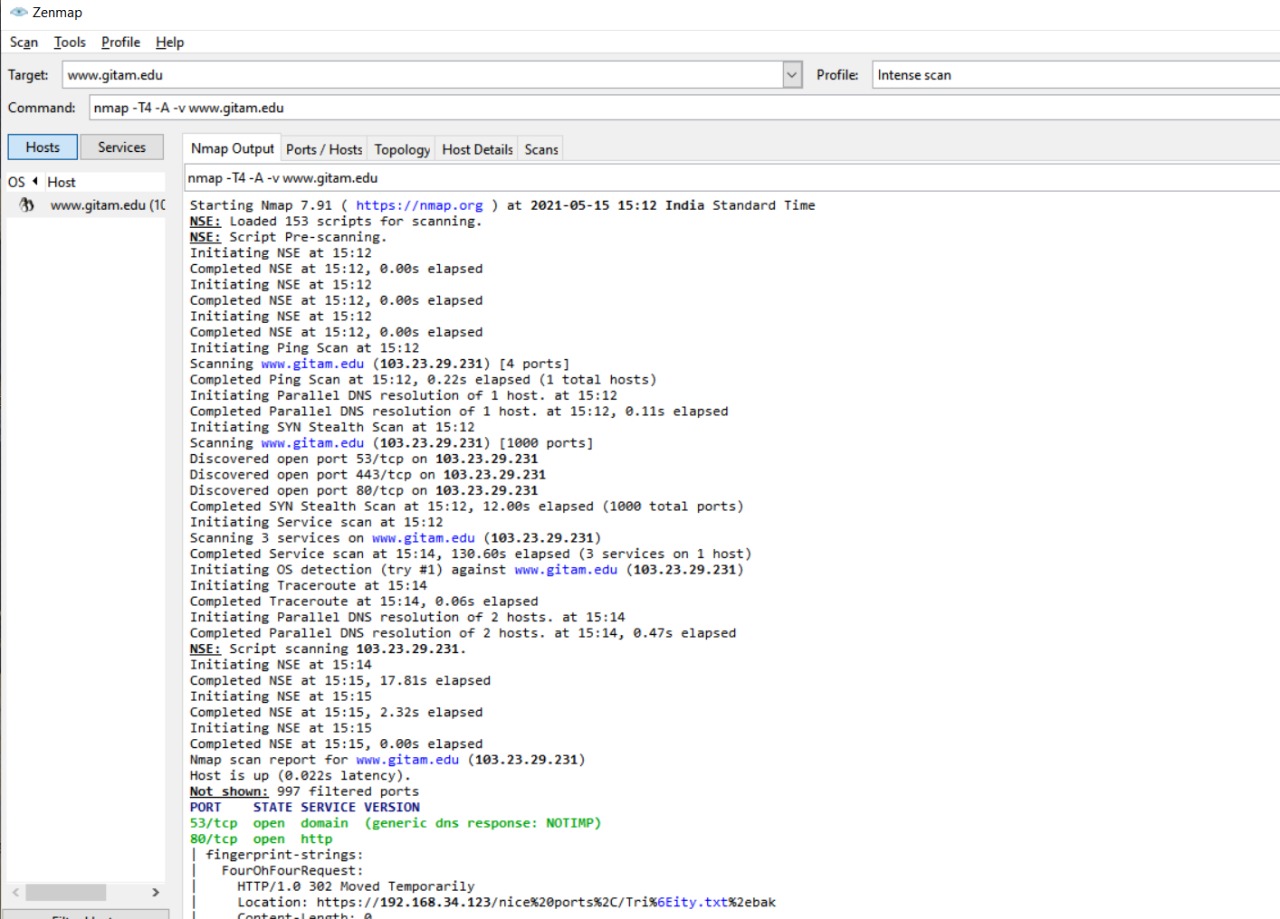
4. Select the install location and click **Install**:

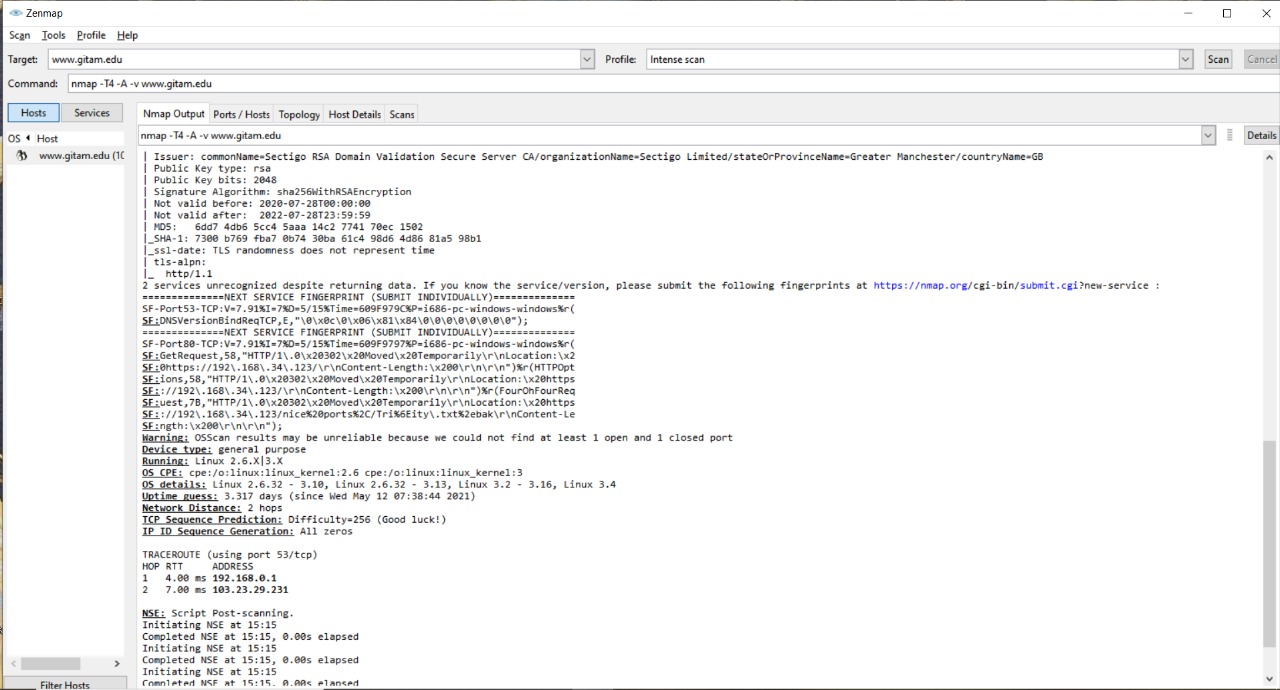
****

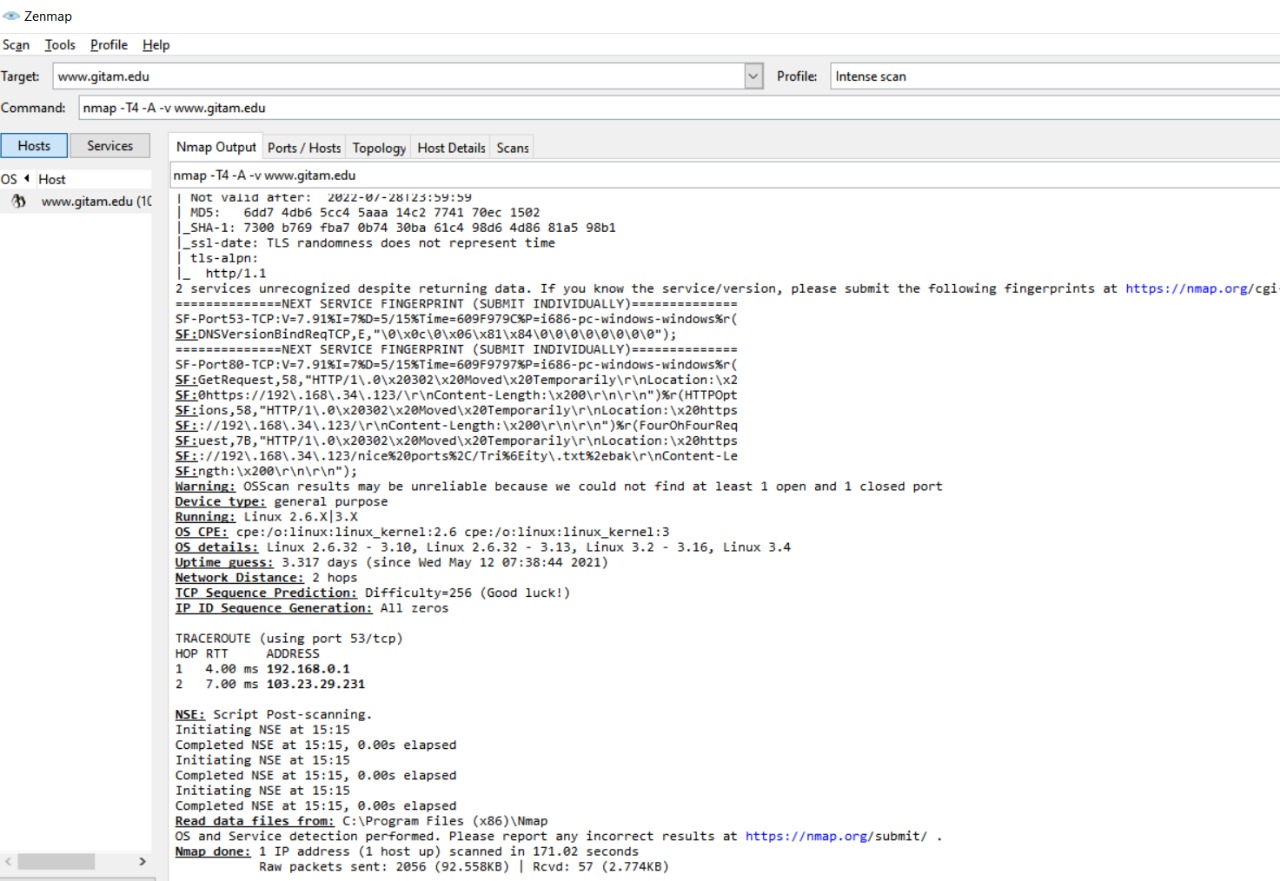
1. The installation should be completed in a couple of minutes. After installation it will show like this:

****

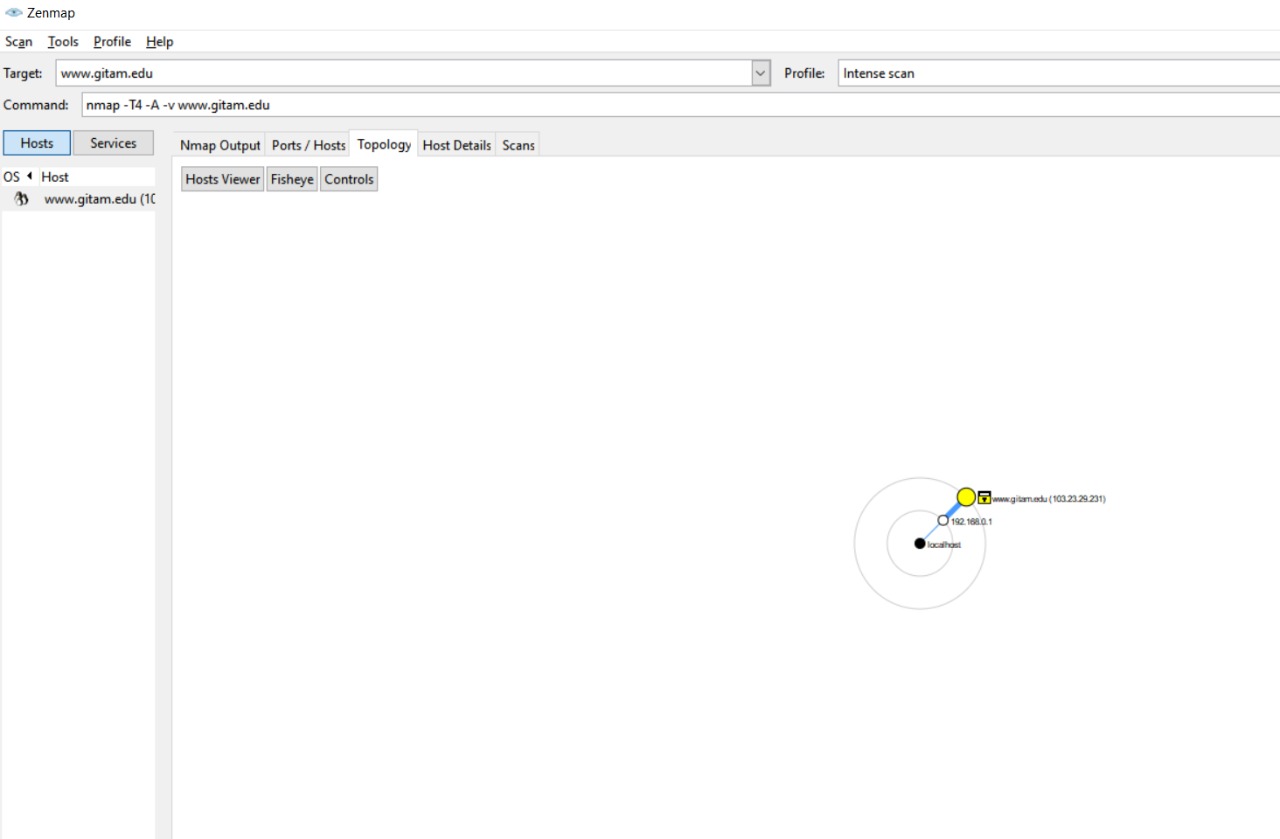
1. **Now ,** **find the open/closed ports** **on** [**www.gitam.edu**](http://www.gitam.edu) **website.**







7.Topology of the Githam websie.



8.Open ports on the gitam website.

