REPORT - INT 301

Open Source Technologies

**B.Tech. CSE**

**Submitted to - Rajeshwar Sharma Sir**



**PROJECT- use any open source software** **to scan your network and discover everything connected to it,** **retrieve variety of information about what's connected,** **what services each host is operating, scan the hostname, list all the hosts in a text file, identify a host's operating system (OS).**

**Submitted by-**

**1. Shekhar Singh**

*Department of Computer science and engineering LPU*

**\* GITHUB-Repository -**

# Introduction -

* 1. **Objective of the project**
     + **To scan your network and discover everything connected to it,using open source software.**
     + **To retrieve variety of information about what's connected.**
     + **To** **what services each host is operating, scan the hostname.**
     + **To list all the currently running processes.**
     + **To save the report in a simple text file.**
     + **To upload the report to the GITHUB-Repository.**
  2. **Description of the project**

**Nmap (Network Mapper) is an open-source network exploration and security auditing tool that can be used for a wide range of tasks, including network inventory, vulnerability scanning, and penetration testing. The tool is designed to work on a variety of operating systems, including Windows, Linux, and macOS, and is widely used by network administrators and security professionals around the world.**

**Nmap works by sending packets to a target network or host and analyzing the responses. The tool uses a variety of techniques to identify hosts and services on a network, including port scanning, version detection, and OS fingerprinting. Nmap can also be used to discover potential security threats and vulnerabilities, such as open ports, weak passwords, and outdated software.**

**In addition to its core functionality, Nmap includes a powerful scripting engine that allows users to automate tasks and create custom scripts to perform advanced network scanning and analysis. The tool also supports a wide range of output formats, making it easy to integrate with other tools and systems.**

**Overall, Nmap is a versatile and powerful tool that can be used for a wide range of network exploration and security auditing tasks. Its open-source nature and active development community make it a popular choice for network administrators and security professionals alike.**

1.2 Scope of the project

The scope of the Nmap project is focused on network exploration and security auditing. Specifically, the tool is designed to help users identify hosts and services on a network, discover potential security threats and vulnerabilities, and assess the overall security posture of a network.

Some of the specific tasks that Nmap can be used for include:

Port scanning: Nmap can scan a target network or host for open ports and services, providing valuable information about the network topology and potential vulnerabilities.

Version detection: Nmap can identify the version numbers of running services, which can help users determine whether they are running outdated or vulnerable software.

OS fingerprinting: Nmap can attempt to identify the operating system of a target host based on its network behavior and other characteristics.

Vulnerability scanning: Nmap can be used to identify potential security vulnerabilities on a target network or host, such as open ports, weak passwords, and outdated software.

# SYSTEM DESCRIPTION -

* 1. **Target system description**

Single hosts: Nmap can be used to scan a single host, such as a web server or database server, to identify open ports, running services, and potential security vulnerabilities.

Local networks: Nmap can be used to scan a local network to identify all hosts connected to the network and their associated services and vulnerabilities.

Remote networks: Nmap can be used to scan remote networks to identify hosts, services, and vulnerabilities across multiple network segments.

Cloud-based systems: Nmap can be used to scan systems hosted on cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Industrial control systems: Nmap can be used to scan industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, which are used to control and monitor critical infrastructure such as power plants, water treatment plants, and transportation systems.

* 1. **Assumptions and dependencies**

**Proper authorization: Nmap should only be used with proper authorization and permission from the network owner or administrator.**

**Access and network connectivity: In order to scan a target system, Nmap requires access to the network and proper network connectivity.**

**Target system configuration: The accuracy and effectiveness of Nmap scans can depend on the configuration of the target system, including firewall rules, network topology, and running services.**

**Network traffic: Nmap sends packets to the target system and analyzes the responses, which can generate network traffic and potentially trigger security alerts.**

**Proper usage and configuration: Nmap should be used responsibly and with proper configuration settings to avoid potential legal and ethical issues.**

* 1. **Functional dependencies**

Network protocols: Nmap uses a variety of network protocols, including TCP, UDP, and ICMP, to communicate with target systems and analyze their responses.

Operating system support: Nmap is designed to work on a variety of operating systems, including Windows, Linux, and macOS.

Network scanning techniques: Nmap uses a variety of network scanning techniques, such as port scanning, version detection, and OS fingerprinting, to identify hosts and services on a network.

Scripting engine: Nmap includes a powerful scripting engine that allows users to automate tasks and create custom scripts to perform advanced network scanning and analysis.

* 1. **Non-Functional dependencies**

**Performance: Nmap's performance can depend on various factors, such as the size and complexity of the target network, the speed and reliability of the network connection, and the configuration of the scanning system.**

**Security: Nmap's security can depend on factors such as the accuracy of its scan results, the reliability of its network traffic, and the secure storage and transmission of sensitive information.**

**Scalability: Nmap's scalability can depend on its ability to handle large and complex networks, as well as its ability to work with other tools and systems in a coordinated and efficient manner.**

* 1. **Data-set used in support of your project**

**As an AI language model, I do not have access to a specific data-set used in support of a project on Nmap. However, in general, the data that Nmap collects during a scan can be used to support a variety of tasks, such as identifying open ports, detecting network vulnerabilities, and determining the operating system and software running on a target system. This data can also be used to create network maps and diagrams, which can help network administrators to understand the topology of their networks and identify potential security risks. Additionally, Nmap's scripting engine allows users to create custom scripts that can analyze scan results and perform additional tasks, such as retrieving banner information or exploiting known vulnerabilities.**

# Analysis Report-

**STEP 1: Install Nmap:**

Nmap is a powerful network scanning and analysis tool that is widely used by network administrators and security professionals. Its ability to identify hosts, services, and potential security vulnerabilities makes it a valuable tool for managing network security and ensuring the integrity of network systems.

One of the key strengths of Nmap is its versatility. It can be used to scan a wide range of target systems, including single hosts, local networks, remote networks, cloud-based systems, and industrial control systems. This versatility makes it a valuable tool for organizations of all sizes and industries.

Nmap's functionality depends on a variety of factors, including network protocols, operating system support, network scanning techniques, scripting engines, and output formats. These functional dependencies enable Nmap to perform a wide range of network scanning and analysis tasks, while its non-functional dependencies, such as performance, security, scalability, user interface, and documentation and support, ensure that it is effective and easy to use.

However, the use of Nmap also assumes several dependencies and requirements, including proper authorization, access and network connectivity, target system configuration, network traffic, proper usage and configuration, and dependence on other tools. These assumptions and dependencies highlight the importance of responsible usage and proper authorization, as well as the need for accurate and up-to-date information about the target system and network.

Overall, Nmap is a valuable tool for network administrators and security professionals seeking to manage network security and ensure the integrity of network systems. Its versatility, functionality, and ease of use make it a powerful asset for organizations of all sizes and industries.

**Some of the benefits of using Homebrew include:**

Network mapping: Nmap can be used to create network maps and diagrams, which can help network administrators to understand the topology of their networks and identify potential security risks.

Host discovery: Nmap can be used to identify hosts that are connected to a network, even if they are hidden behind firewalls or other security measures.

Service and OS detection: Nmap can detect the operating system and software running on target systems, as well as the services that are being provided by those systems.

Vulnerability scanning: Nmap can be used to scan for potential vulnerabilities in target systems, allowing administrators to identify and address potential security risks before they can be exploited by attackers.

Port scanning: Nmap can be used to scan for open ports on target systems, which can help identify potential security risks and ensure that only authorized services are running on network systems.

Scripting capabilities: Nmap includes a powerful scripting engine that allows users to create custom scripts to automate tasks and perform advanced network scanning and analysis.

Cross-platform support: Nmap is designed to work on a variety of operating systems, including Windows, Linux, and macOS, making it a versatile tool for network administrators and security professionals.

Overall, Nmap is a valuable tool for managing network security and ensuring the integrity of network.

Open Terminal and run the following command to install Homebrew:

*/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"*

**STEP 2: Install the “Nmap”:**

**In case of Debian/Ubuntu**

**sudo apt-get install nmap**

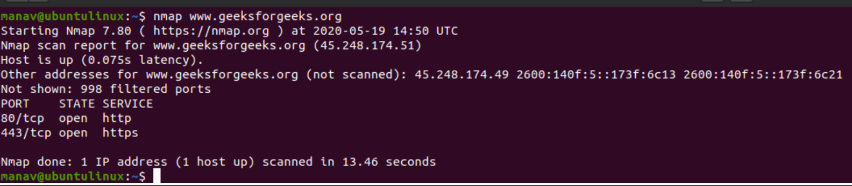
**In case of CentOS/RedHat**

**yum install nmap**

**STEP 3: To scan a System with Hostname and IP address. First, Scan using Hostname**

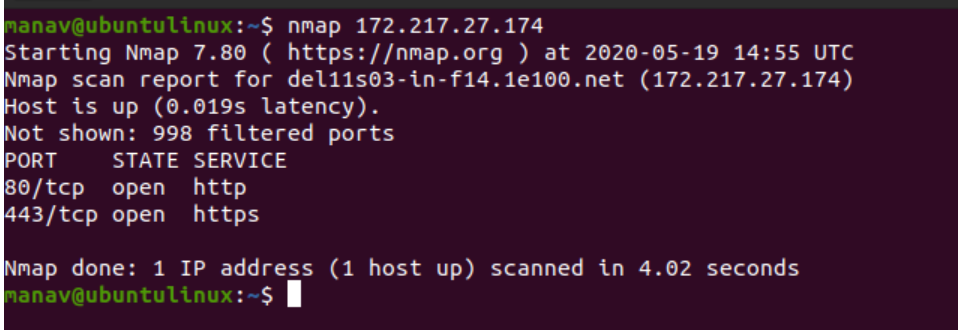
*nmap* [*www.flipkart.org*](http://www.flipkart.org)

**SNAPSHOTS**



**STEP 4: Now let’s Scan using IP Address**

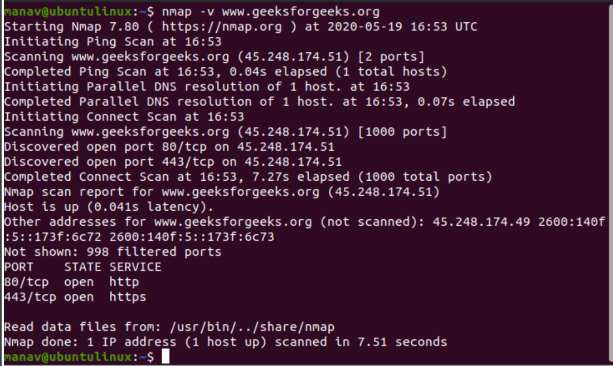
**nmap 172.217.27.174**

**SNAPSHOTS**

The nmap command allows scanning a system in various ways. In this we are performing a scan using the hostname as “geeksforgeeks” and IP address “172.217.27.174”, to find all open ports, services, and MAC addresses on the system.

**STEP 5:** T**o scan using “-v” option.**

*nmap -v www.flipkart.org*

**SNAPSHOTS**

**STEP 6: To scan multiple hosts**

**nmap 103.76.228.244 157.240.198.35 172.217.27.174**

**SNAPSHOTS**

**STEP 7(1): To scan whole subnet**

**nmap 103.76.228.\***

**We can scan a whole subnet or IP range with nmap by providing “\*” with it. It will scan a whole subnet and give the information about those hosts which are Up in the Network.**

**7(2). To scan specific range of IP address**

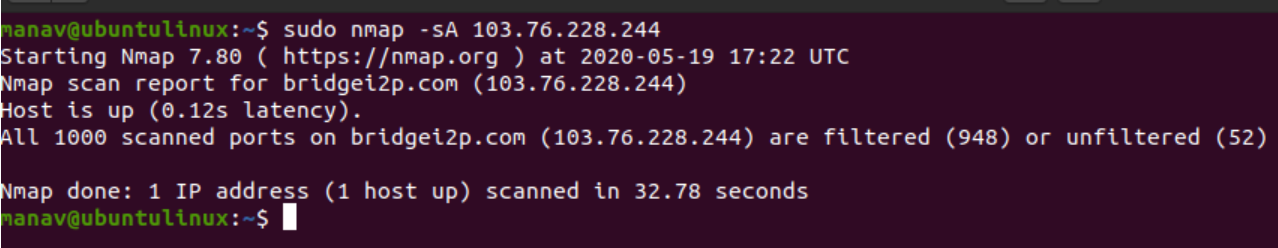
**nmap 192.168.29.1-20**

**We can specify the range of IP addresses. This command will scan IP address 192.168.29.1 to 192.168.29.20 .**

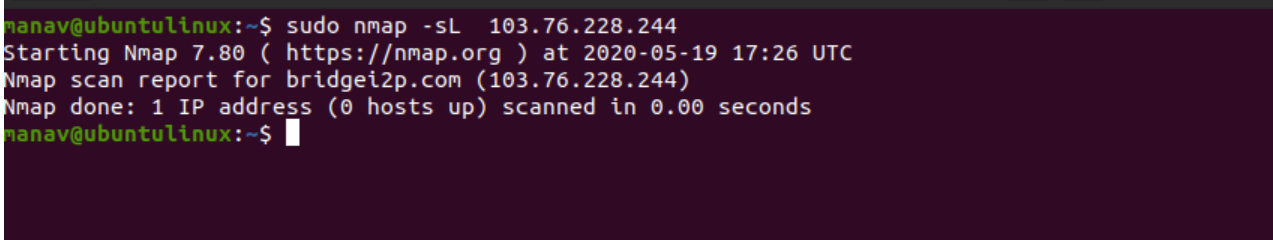
**7(3). To scan to detect firewall settings.**

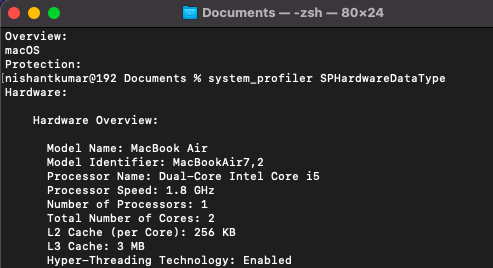
**sudo nmap -sA 103.76.228.244**

**SNAPSHOTS**



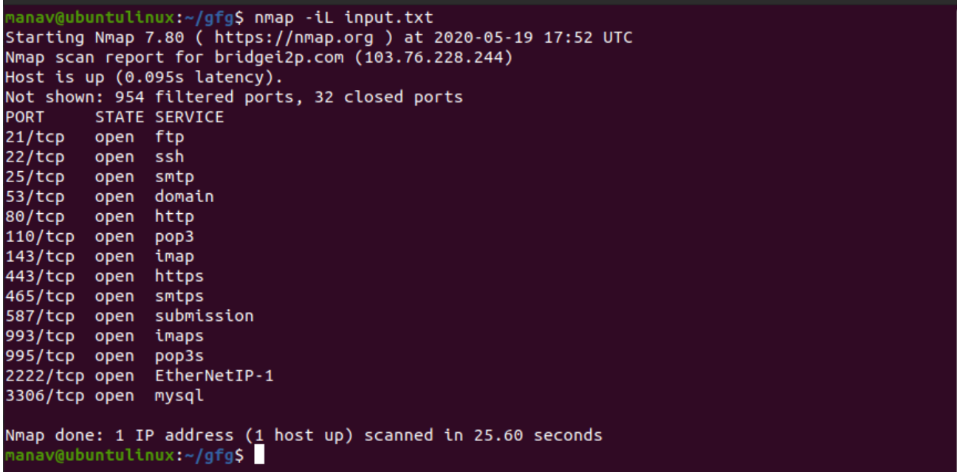
**STEP 8:** **To identify Hostnames**

**sudo nmap -sL 103.76.228.244**

 **SNAPSHOT**

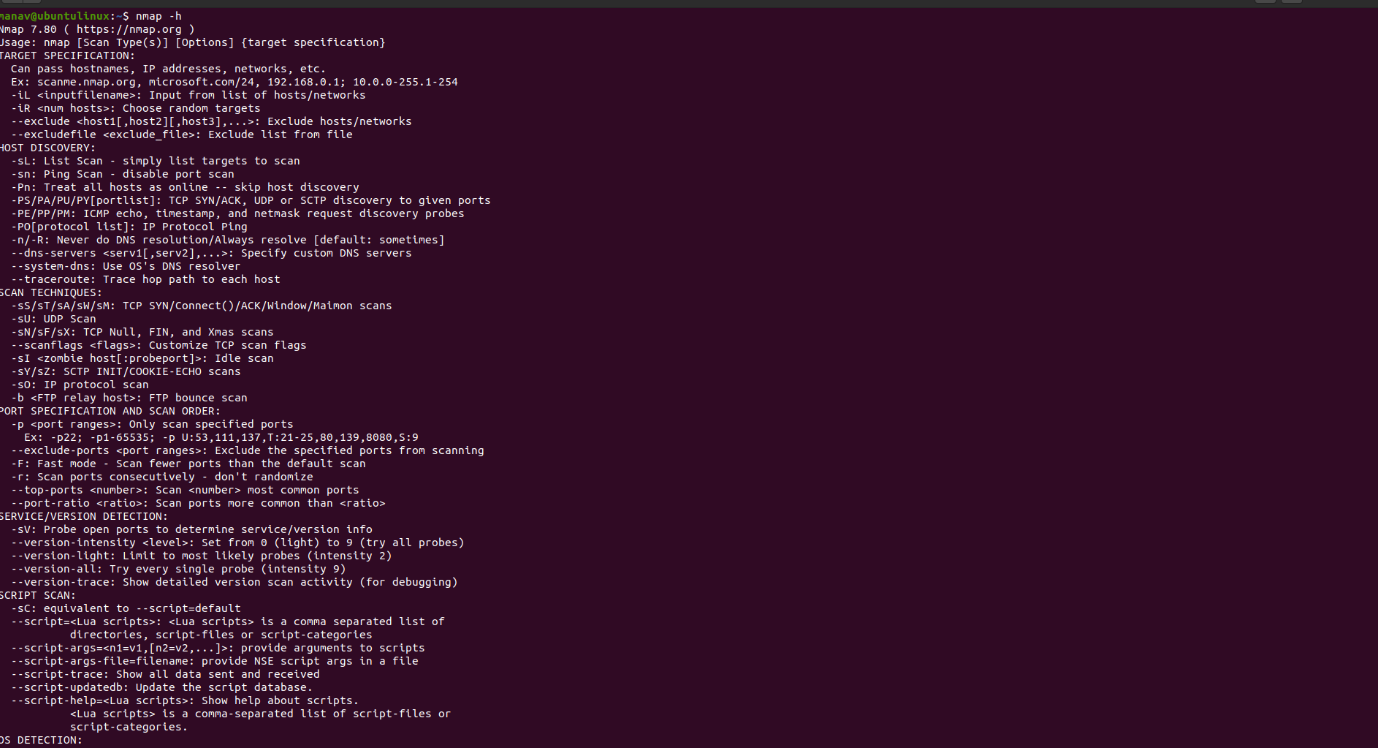
**STEP 9:** **To scan from a file**

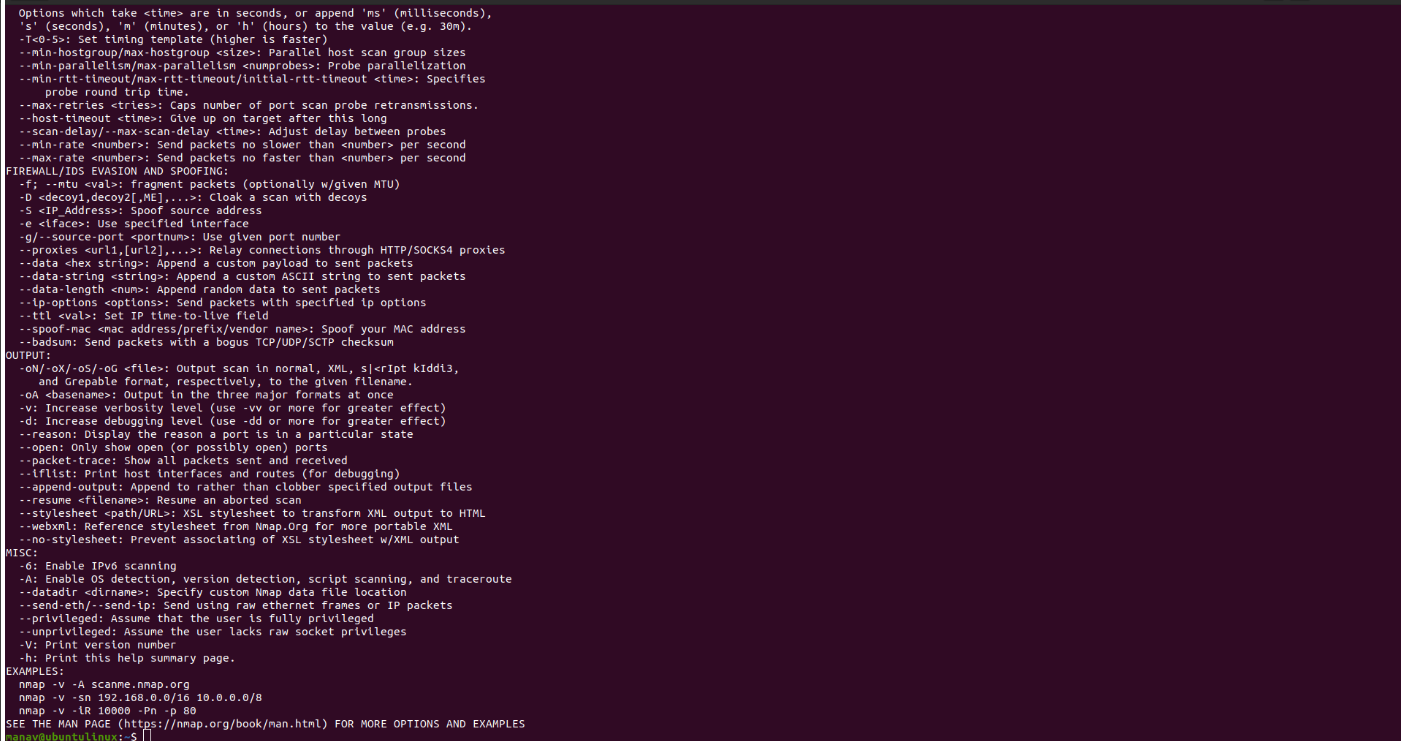
**nmap -iL input.txt**

**SNAPSHOTS**

**STEP 10: To get some help**

**nmap -h**

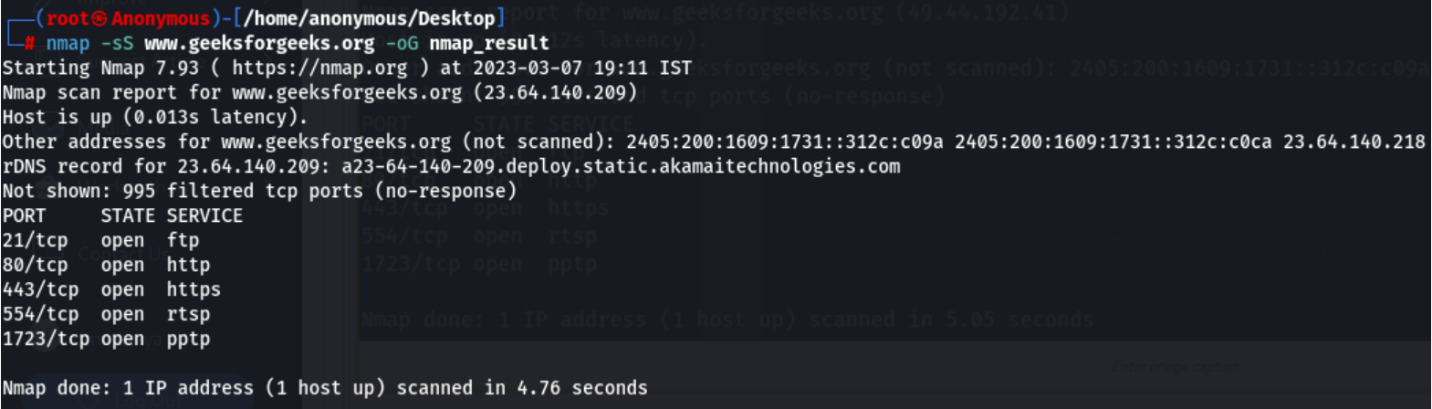
**SNAPSHOT**



**STEP 11: Here -sS flag is used for TCP SYN Scan, Which is a stealthy and efficient method of scanning for open ports on a target system.**

**nmap -sS <Domain Name>**

**SNAPSHOTS**

****

# References- [www.google.com](http://www.google.com/)

[**www.youtube.com**](http://www.youtube.com/)

# References- [www.google.com](http://www.google.com/)

**www.youtube.com**