**Internal Assessment Report on**

# NMAP(ZenMap)

**by**

**Parth Pancholi 16010121128**
**Raheel H Parekh 16010121133**
**Ujjawal Patel 16010121139**

**For the subject**

**Information Security**

**Department of Computer Engineering**
**K. J. Somaiya College of Engineering**
**(Constituent College of Somaiya Vidyavihar University)**
**Academic Year 2023-24**

**Under the guidance of:**

**Prof. Swati Mali**

**Topic chosen: Nmap**

## Introduction

### WHAT IS ZENMAP?

Zenmap is a graphical user interface (GUI) for the Nmap network scanner. It provides an intuitive way to perform network discovery, host profiling, and security auditing tasks. Zenmap simplifies the process of running Nmap scans by providing a user-friendly interface with options for configuring scan parameters and viewing scan results.

### HOW DOES IT WORK?

Zenmap allows users to specify target hosts or networks for scanning by entering IP addresses, hostnames, or importing a list of targets. Users can configure scan types, intensity levels, and advanced options like OS detection. Once configured, Zenmap initiates the scan, sending probe packets to gather information about open ports, services, and vulnerabilities. Scan results are presented in interactive maps, tables, and textual formats for easy analysis and exploration.

### WHY USE ZENMAP?

- Ease of Use: Zenmap's graphical interface makes it accessible to users who may not be familiar with command-line tools like Nmap. It provides a point-and-click interface for performing complex network scans and analyzing the results.
- Comprehensive Scanning Capabilities: Zenmap leverages the powerful scanning engine of Nmap, allowing users to conduct a wide range of network reconnaissance and security auditing tasks. It supports various scan types, including TCP SYN scans, UDP scans, and comprehensive vulnerability detection scans.
- Visualization and Reporting: Zenmap offers visualization tools such as topology maps and graphical charts to help users understand the network layout and identify potential security issues. It also provides options for exporting scan results in various formats, including XML, HTML, and plain text, for further analysis or reporting purposes.

**IMPLEMENTATION DETAILS:**

- Installation: Zenmap is available for multiple platforms, including Windows, Linux, and macOS. Users can download and install Zenmap from the official Nmap website or package repositories for their respective operating systems.
- Configuration: Upon launching Zenmap, users can configure scan parameters, target specifications, and output options through the graphical interface. Zenmap also allows users to save scan profiles for reuse in future scans.
- Integration with Nmap: Zenmap utilizes the Nmap command-line tool under the hood, providing a GUI frontend for Nmap's functionality. Users can access advanced Nmap features and options through Zenmap's interface while benefiting from its ease of use.

**DEMONSTRATION:**

- Start by launching Zenmap from the installed application or command line.
- Enter the target IP address, hostname, or network range in the "Target" field.
- Choose a scan profile from the dropdown menu, such as "Intense Scan," "Quick Scan," or "Ping Scan."
- Optionally, configure additional scan options and parameters according to your requirements.
- Click the "Scan" button to initiate the scan.
- Monitor the scan progress in the output window and wait for the scan to complete.
- Once the scan is finished, explore the results using the various tabs and views available in the Zenmap interface.
- You can export the scan results to a file or generate a report for further analysis or presentation purposes.

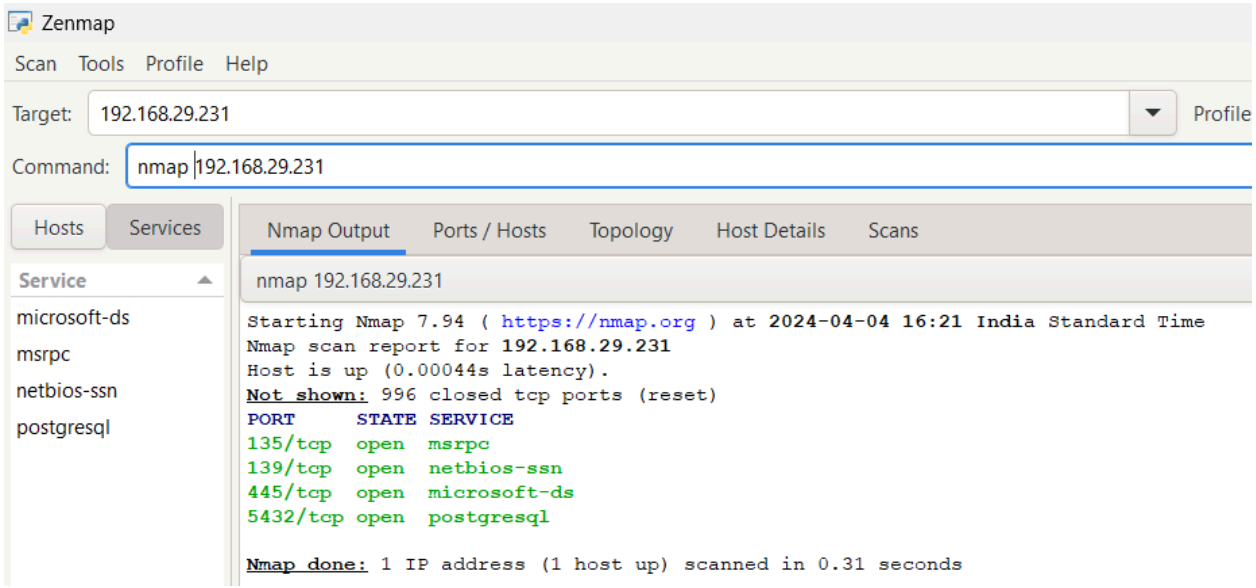
## Features/Characteristics:

- User-Friendly Interface: Zenmap offers an intuitive GUI for easy network scanning and analysis.
- Scan Profiles: Predefined profiles cater to various scanning needs.
- Customizable Options: Users can adjust scan parameters to fit their requirements.
- Network Discovery: Identifies hosts, open ports, and running services on a network.
- Service and OS Detection: Detects services and operating systems on scanned hosts.
- Vulnerability Assessment: Assesses security risks and vulnerabilities.

# Implementation Screenshots:

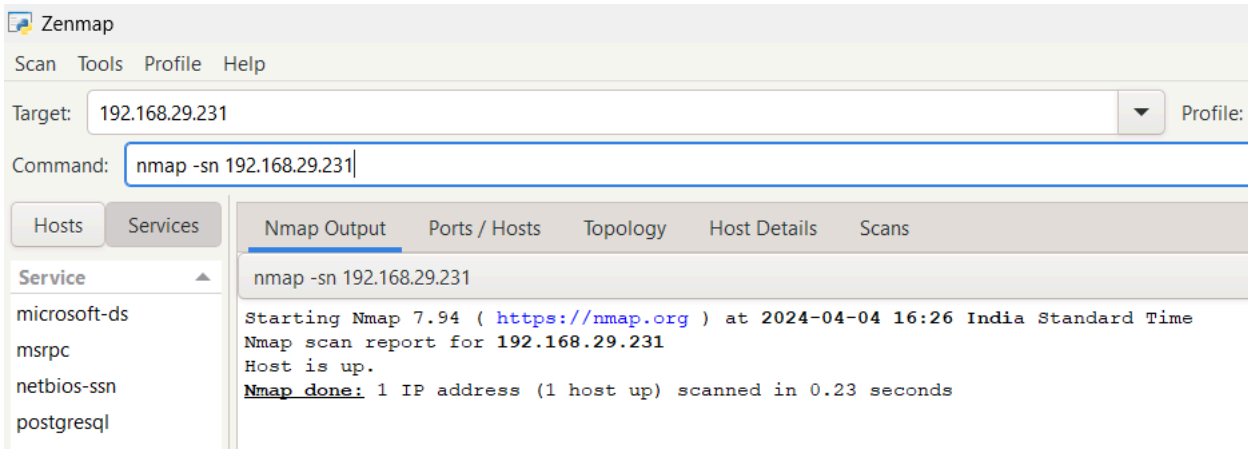
## Scanning IP:

nmap 192.168.29.231




## Pinging IP:

nmap -sn 192.168.29.231

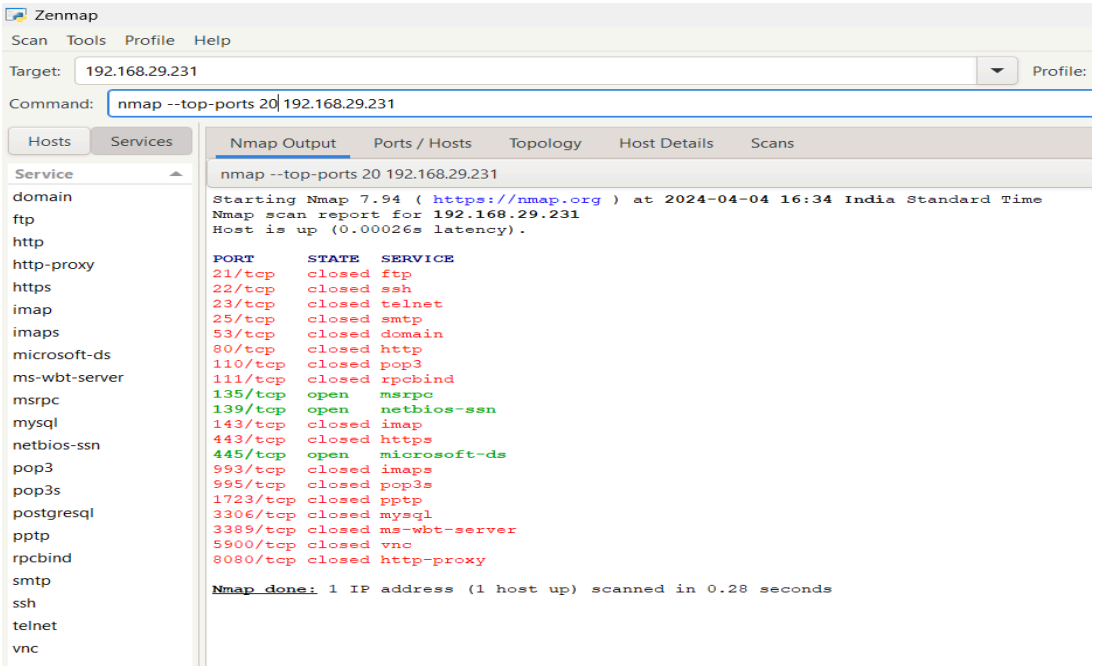


**Pinging Specific Ports:**

nmap -p 135 192.168.29.231

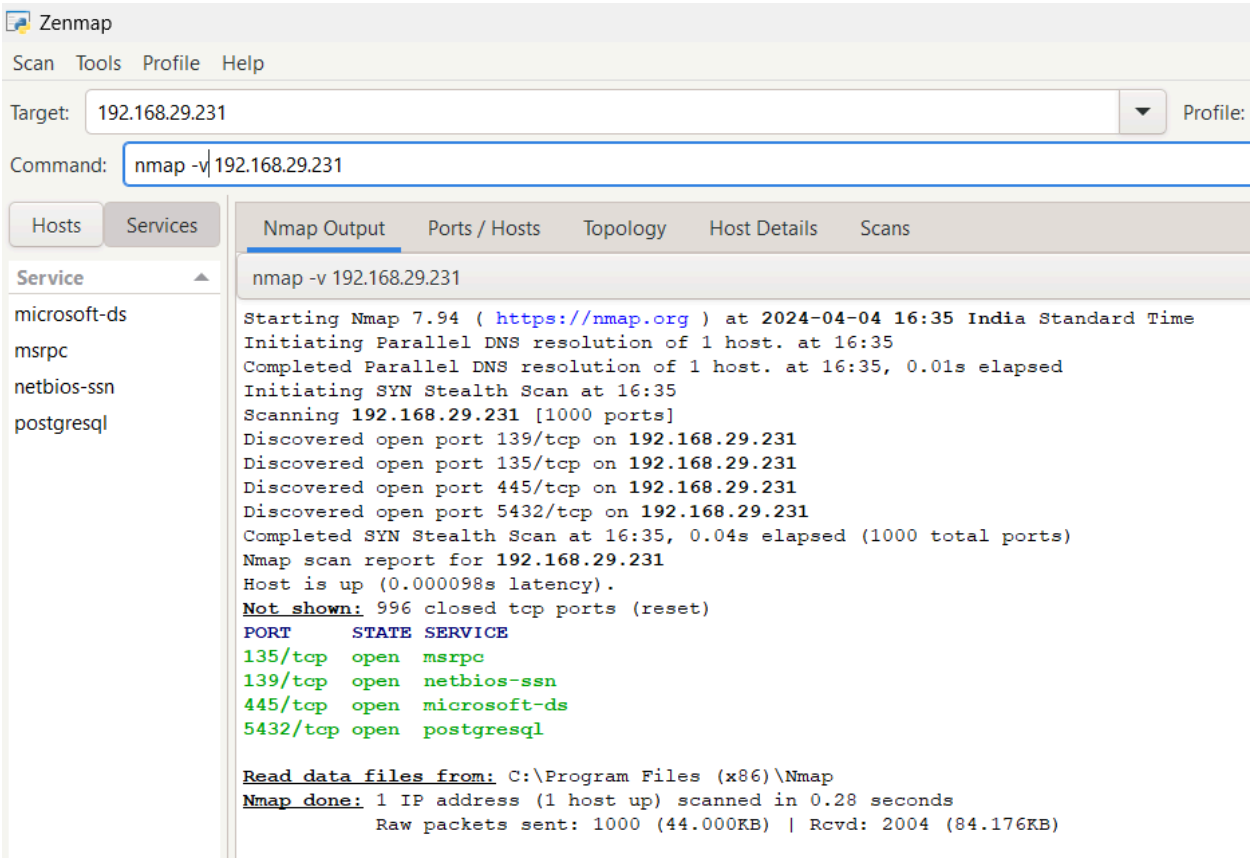

**Most Popular Ports:**

nmap --top-ports 20 192.168.29.231



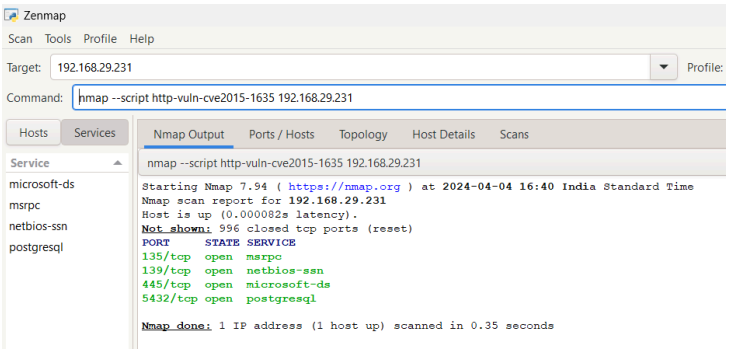
**Scanning with verbosity - Provides a detailed information:**

nmap -v 192.168.29.231



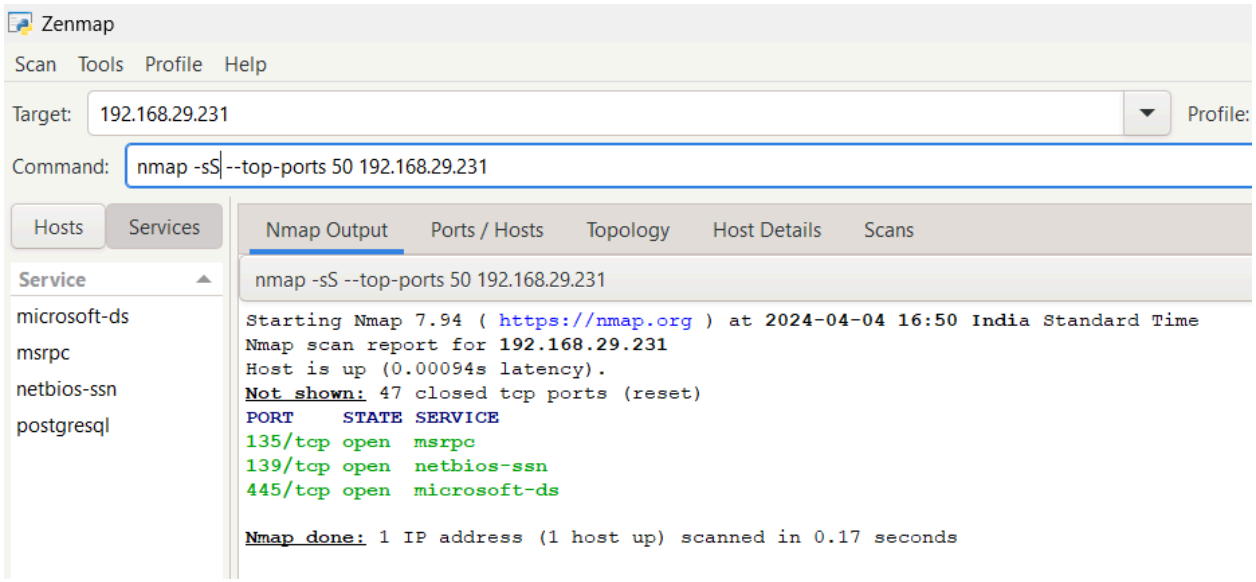

**Detects Malware Infections**

nmap –script http-vuln-cve2015-1635 192.168.29.231



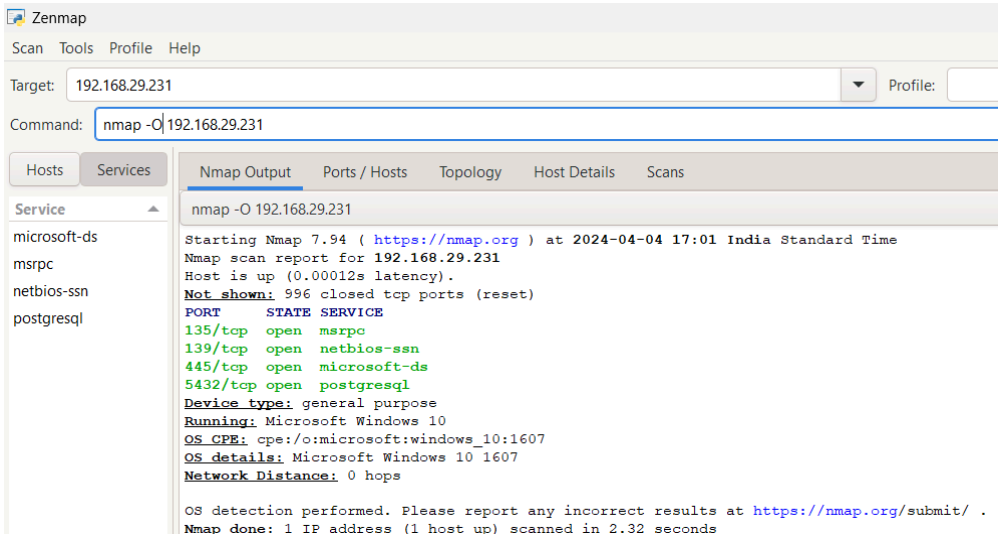
**Syn Scan-**This command can be useful for quickly identifying open ports and services on a target system, which can help in identifying potential vulnerabilities. However, it is important to note that this type of scan may be detected by intrusion detection systems (IDS) or firewalls, and may be considered a hostile act in some contexts.

nmap -sS –top-ports 50 192.168.29.231



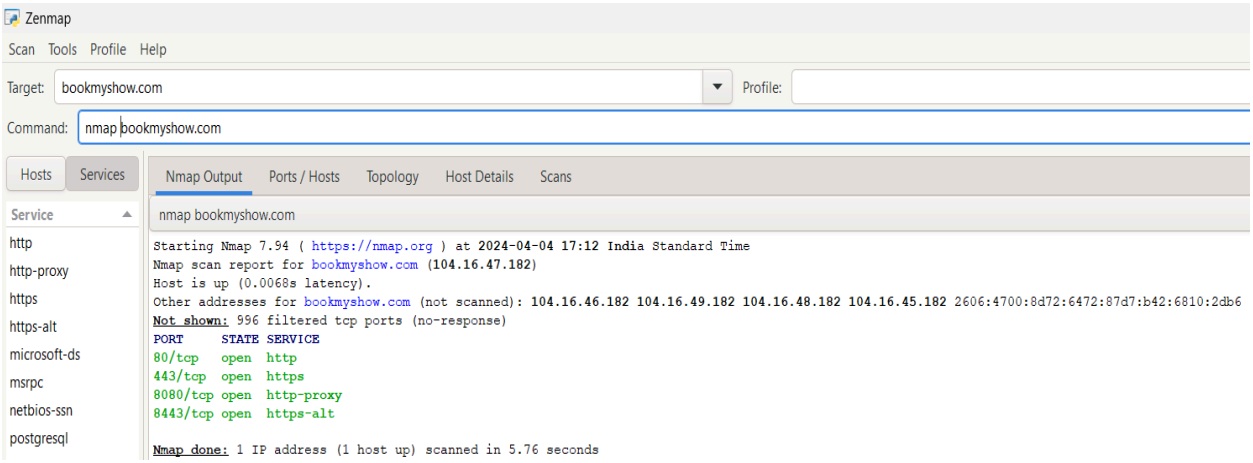

## Finding the OS of the Host

nmap -O 192.168.29.231



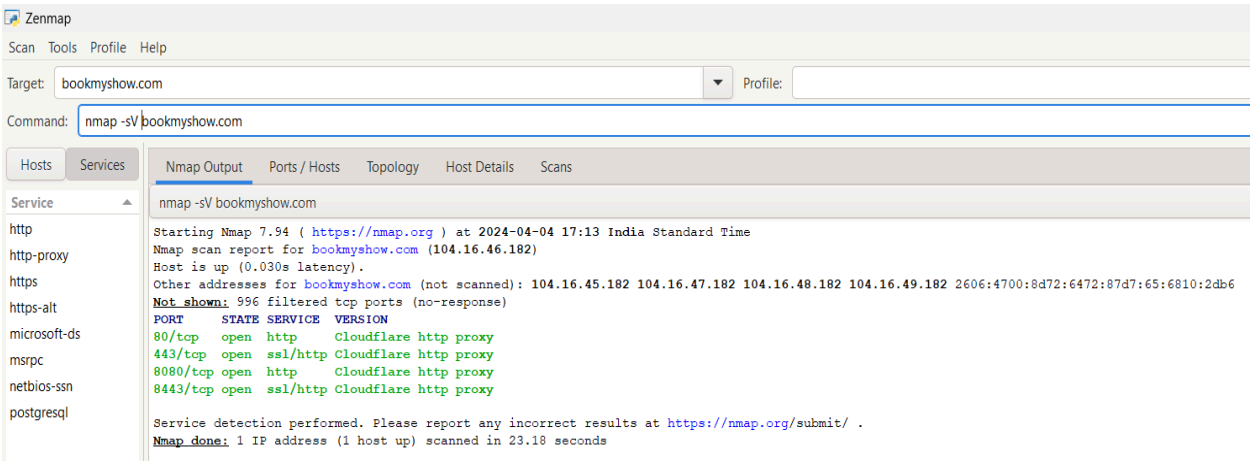
## Finding the open ports of a target IP

nmap bookmyshow.com



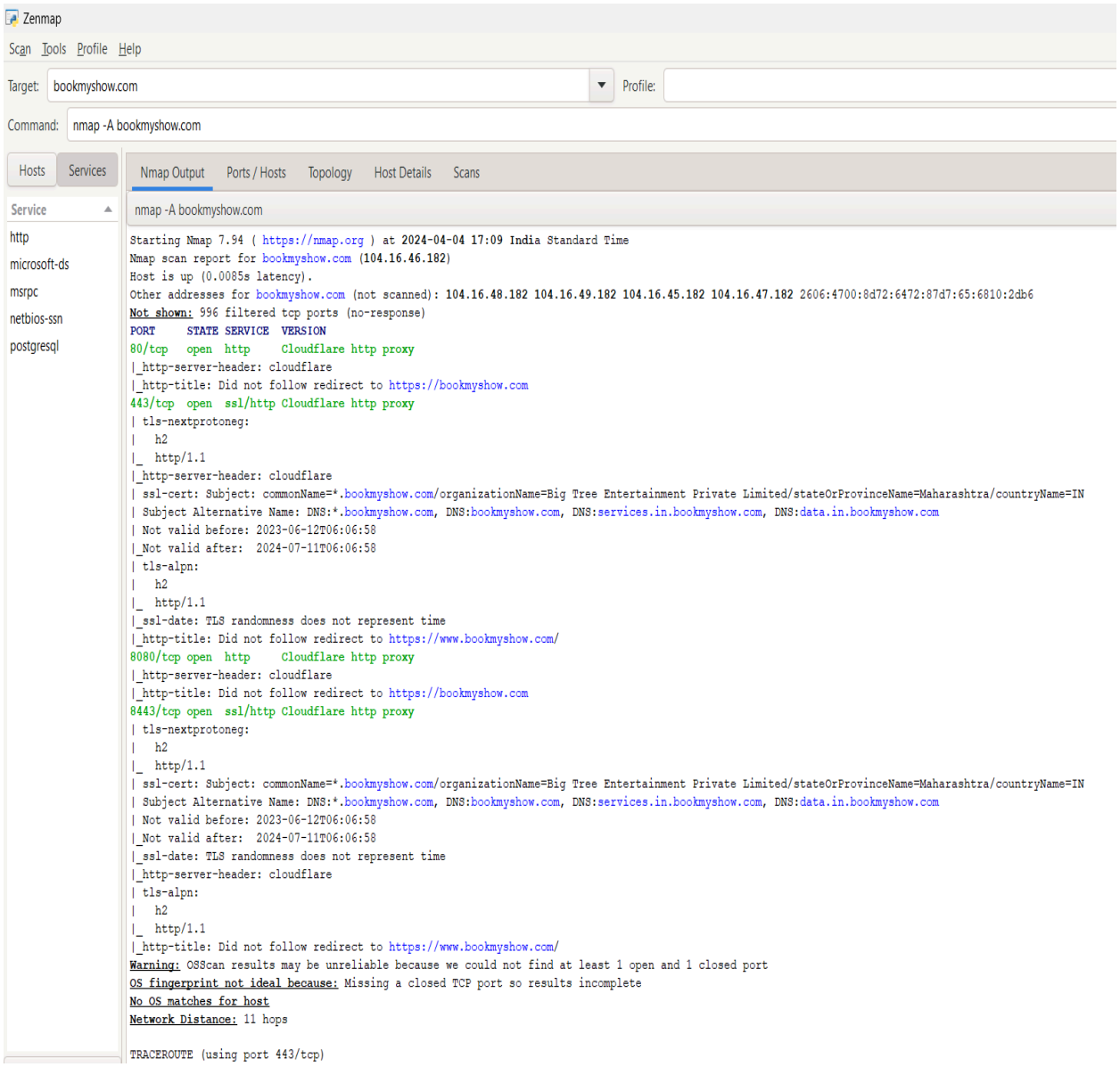

## Finding the versions of the open ports of the target IP

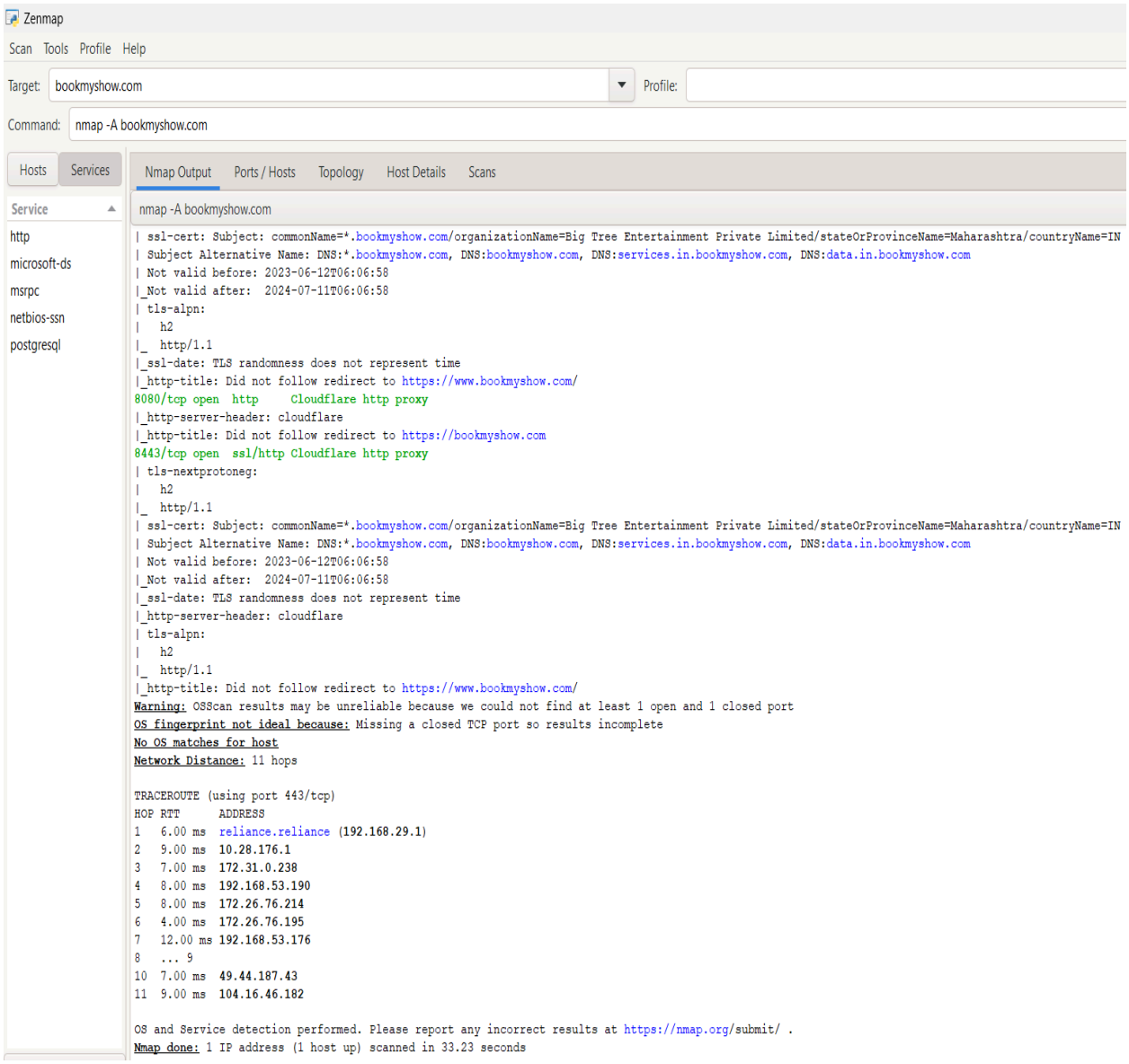
nmap -sV bookmyshow.com



**Aggressive Scan performed on the target IP to know detailed information about the DNS configuration and the Host OS**

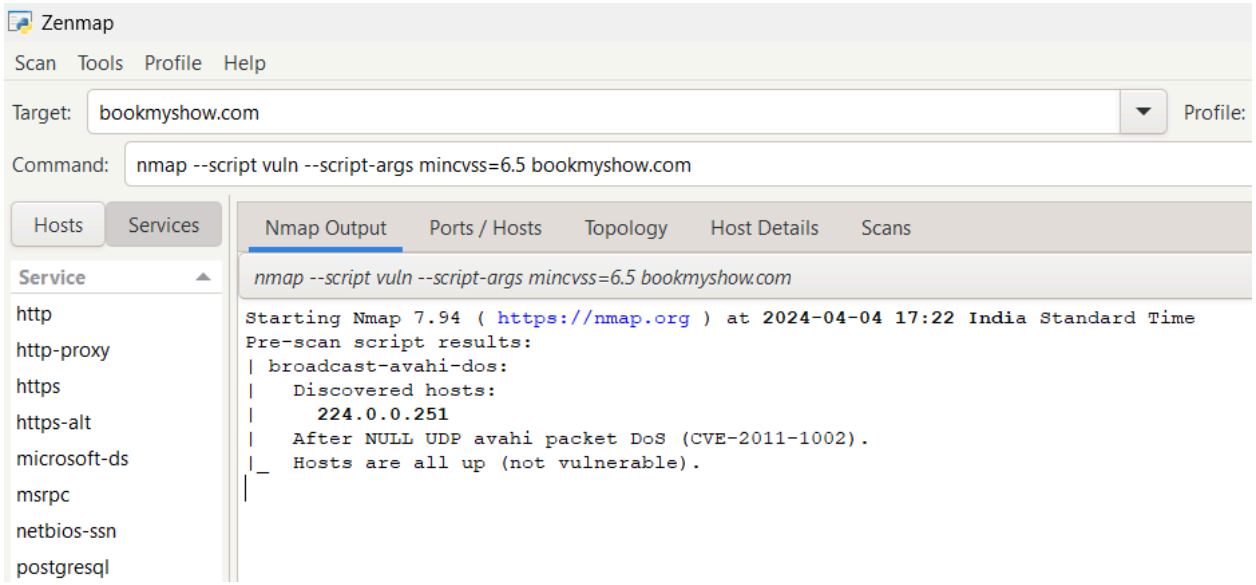
nmap -A bookmyshow.com



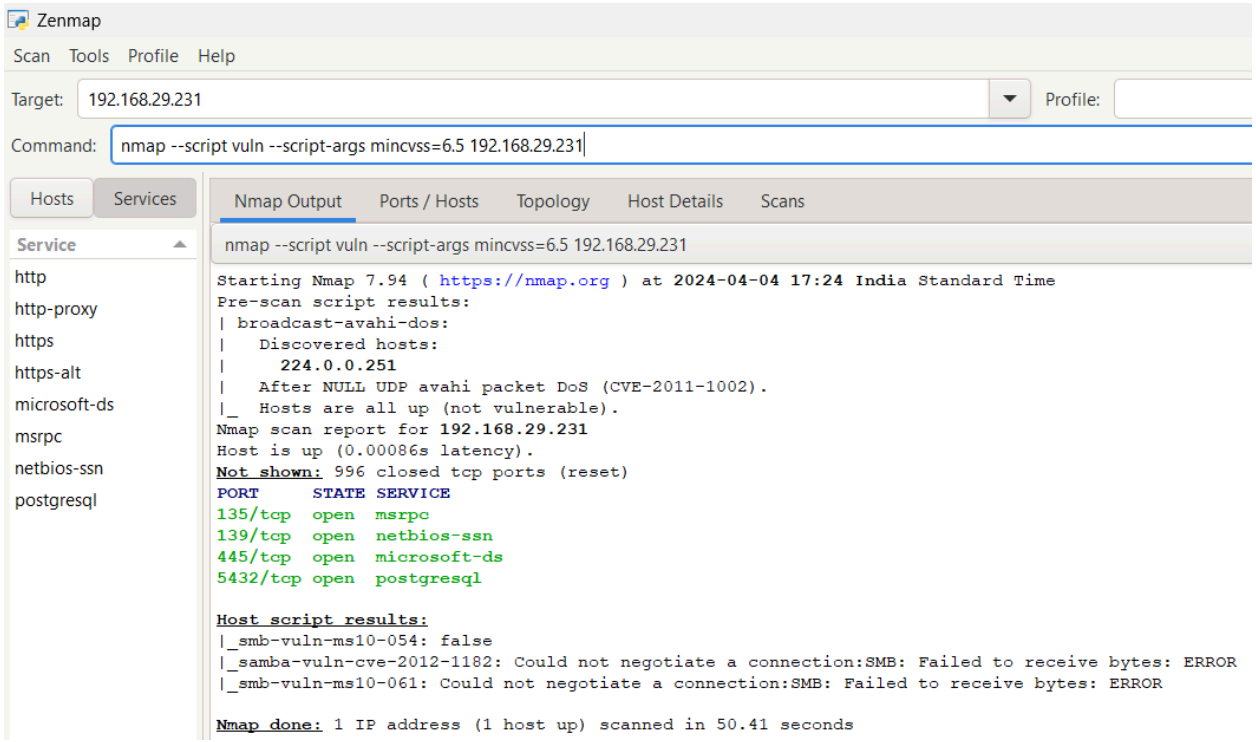

Zenmap
Scan Tools Profile Help
Target: bookmyshow.com
Profile:
Command: nmap -A bookmyshow.com
Hosts Services
Service
http
microsoft-ds
msrpc
netbios-ssn
postgresql
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -A bookmyshow.com
| ssl-cert: Subject: commonName=*.bookmyshow.com/organizationName=Big Tree Entertainment Private Limited/stateOrProvinceName=Maharashtra/countryName=IN
| Subject Alternative Name: DNS:*.bookmyshow.com, DNS:bookmyshow.com, DNS:services.in.bookmyshow.com, DNS:data.in.bookmyshow.com
| Not valid before: 2023-06-12T06:06:58
|_Not valid after: 2024-07-11T06:06:58
| tls-alpn:
| h2
|_ http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to https://www.bookmyshow.com/
8080/tcp open http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://bookmyshow.com
8443/tcp open ssl/http Cloudflare http proxy
| tls-nextprotoneg:
| h2
|_ http/1.1
| ssl-cert: Subject: commonName=*.bookmyshow.com/organizationName=Big Tree Entertainment Private Limited/stateOrProvinceName=Maharashtra/countryName=IN
| Subject Alternative Name: DNS:*.bookmyshow.com, DNS:bookmyshow.com, DNS:services.in.bookmyshow.com, DNS:data.in.bookmyshow.com
| Not valid before: 2023-06-12T06:06:58
|_Not valid after: 2024-07-11T06:06:58
|_ssl-date: TLS randomness does not represent time
|_http-server-header: cloudflare
| tls-alpn:
| h2
|_ http/1.1
|_http-title: Did not follow redirect to https://www.bookmyshow.com/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 11 hops
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 6.00 ms reliance.reliance (192.168.29.1)
2 9.00 ms 10.28.176.1
3 7.00 ms 172.31.0.238
4 8.00 ms 192.168.53.190
5 8.00 ms 172.26.76.214
6 4.00 ms 172.26.76.195
7 12.00 ms 192.168.53.176
8 ... 9
10 7.00 ms 49.44.187.43
11 9.00 ms 104.16.46.182
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.23 seconds

**Scanning for Vulnerabilities:**

nmap --script vuln --script-args mincvss=6.5 bookmyshow.com




nmap --script vuln --script-args mincvss=6.5 192.168.29.231



## Conclusion:

Zenmap serves as a powerful tool for network scanning and security auditing, offering a user-friendly interface, customizable scanning options, and comprehensive analysis capabilities. With features such as network discovery, vulnerability assessment, and topology mapping, Zenmap enables users to identify and address potential security risks in their network infrastructure. Its cross-platform compatibility and support for various output formats make it a valuable asset for IT professionals and security experts alike. Overall, Zenmap empowers users to enhance their network security posture and mitigate potential threats effectively.