Assignment 2

**Nmap-scanning**

Nmap is a powerful open-source tool used to scan websites and network hosts by sending packets and analyzing their responses. It helps discover open ports, running services, and potential vulnerabilities, assisting security professionals in network auditing and protection tasks. To properly submit your Nmap scan as a GitHub report or assignment, include the following sections: Introduction, Methodology (scan commands used), Results (with open ports and explanations), and Analysis. Save outputs in plain text or XML and attach these files as evidence in your repository or assignment folder.

**Nmap Assignment Report**

**1. Introduction**

This report documents an Nmap scan performed on the TryHackMe website to identify open ports and running services. The objective is to gain insights into the public-facing services for security assessment and documentation purposes.

**2. Methodology**

**Scan Command Used:**

nmap [www.tryhackme.com](http://www.tryhackme.com/) -oN tryhachmereport\_nmap.txt

* -oN outputs in normal text format for documentation.

**3. Results**

**Scan Output Summary:**

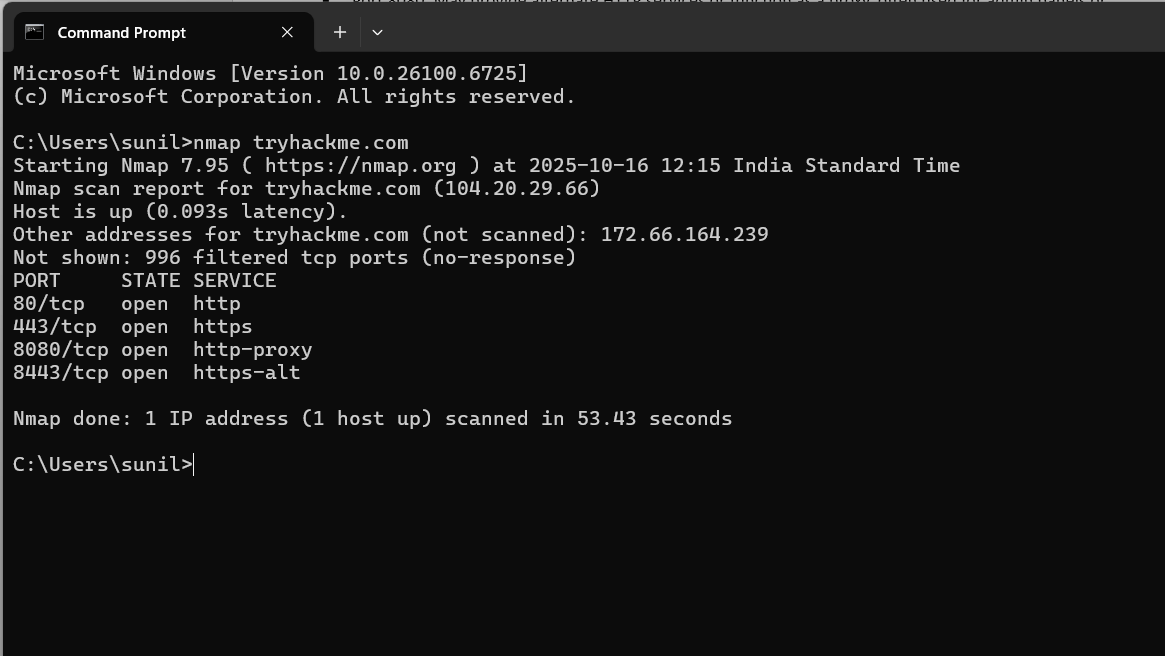
| **Port** | **State** | **Service** | **Description** |
| --- | --- | --- | --- |
| 80/tcp | open | http | Standard web server port for unencrypted web traffic |
| 443/tcp | open | https | Secure port for encrypted SSL/TLS web traffic |
| 8080/tcp | open | http-proxy | Often used for development, web proxies, or alternate HTTP services |

The scan identified three open ports: 80 (HTTP), 443 (HTTPS), and 8080 (HTTP-proxy), all serving web-based content/services.

**4. Analysis**

* Port 80: Hosts the default web page; traffic is unencrypted.
* Port 443: Provides encrypted, secure web traffic via HTTPS.
* Port 8080: May provide alternate HTTP services or function as a proxy, often used for admin panels or alternate web applications.

****

****