# NMAP-VULNERABILITY SCANNER

**AIM:**To scan vulnerabilities using nmap in windows operating system

## DESCRIPTION:

Nmap vulnerability scanning is the process of using Nmap to scan for and identify known vulnerabilities. The goal of Nmap vulnerability scanning is to gather information about a target host, system, network, or an information technology asset, test it for weaknesses, attempt to exploit those weaknesses, and report on the findings so appropriate security measures can be taken to eliminate any reported problems. Nmap vulnerability scanning may also be conducted to check the effectiveness of an organization's security policy, adherence to compliance regulations, company-wide awareness of security measures, and the ability of an organization to flag and respond to security threats and violations.

Nmap is capable of:

- ✓ Scan Active IPs

  Get detailed reporting on every IP on your network to figure out if a certain IP address is compromised and needs further investigation. Nmap can flag compromised IPs and report on whether they're being used by a legitimate network service or a hacker.

- ✓ Scan Your Entire Network

  Nmap can help you visualize and map out your entire local network. It can also show you a list of active live hosts, available ports, and the operating systems running on every device connected.

- ✓ Scan for Vulnerabilities

  In addition to a number of network scanning functions, Nmap can also be used to identify vulnerabilities in your network. The tool gives you a front-row view of what attackers would see if they attempt to infiltrate your network defenses. This can help you prepare better for any future cybersecurity threats.

- ✓ Visualize Your Network

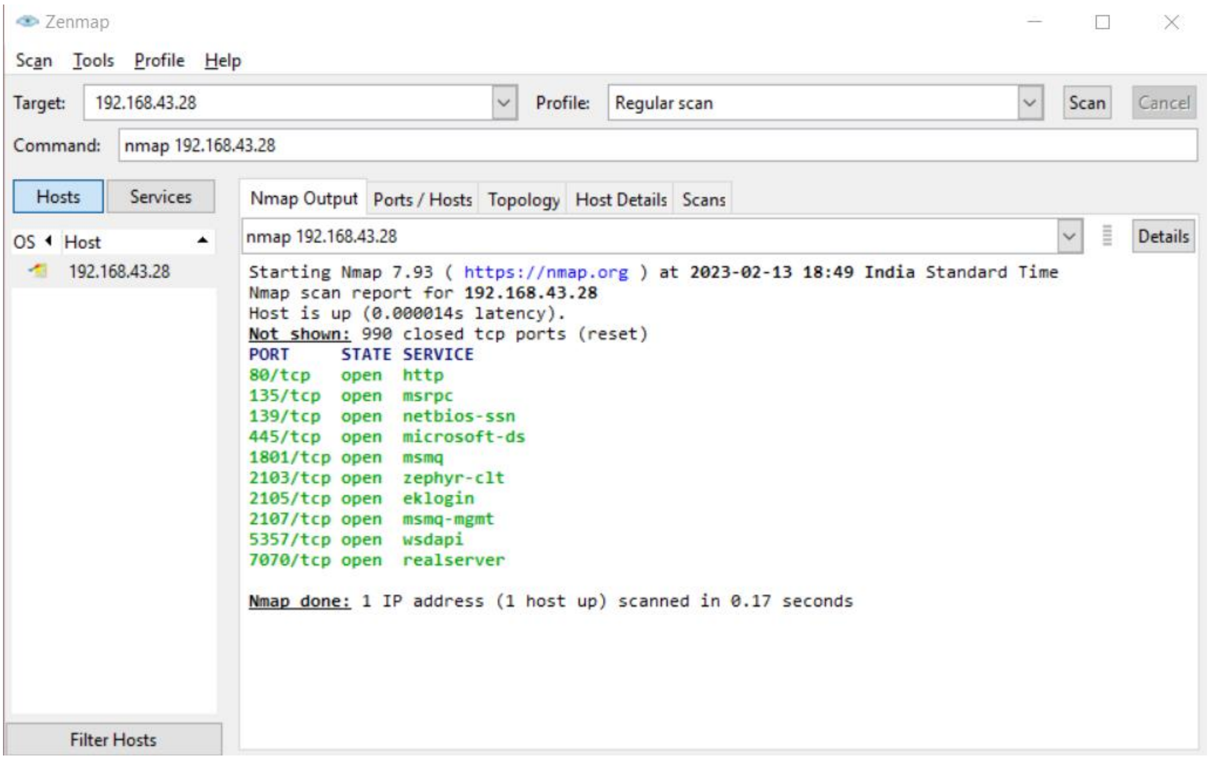
  Nmap is a command-line tool. But it has a graphical user interface called Zenmap that can help you visually map your network so you can understand it better and prepare reports that are easier to understand.

## PROCEDURE

The primary uses of Nmap can be broken into three core processes.

- ✓ First, the program gives you detailed information on every IP active on your networks, and each IP can then be scanned. This allows administrators to check whether an IP is being used by a legitimate service, or by an external attacker.
- ✓ Secondly, Nmap provides information on your network as a whole. It can be used to provide a list of live hosts and open ports, as well as identifying the OS of every connected device. This makes it a valuable tool in ongoing system monitoring, as well as a critical part of pentesting.
- ✓ Thirdly, Nmap has also become a valuable tool for users looking to protect personal and business websites. Using Nmap to scan your own web server, particularly if you are hosting your website from home, is essentially simulating the process that a hacker would use to attack your site.

# OBSERVATION



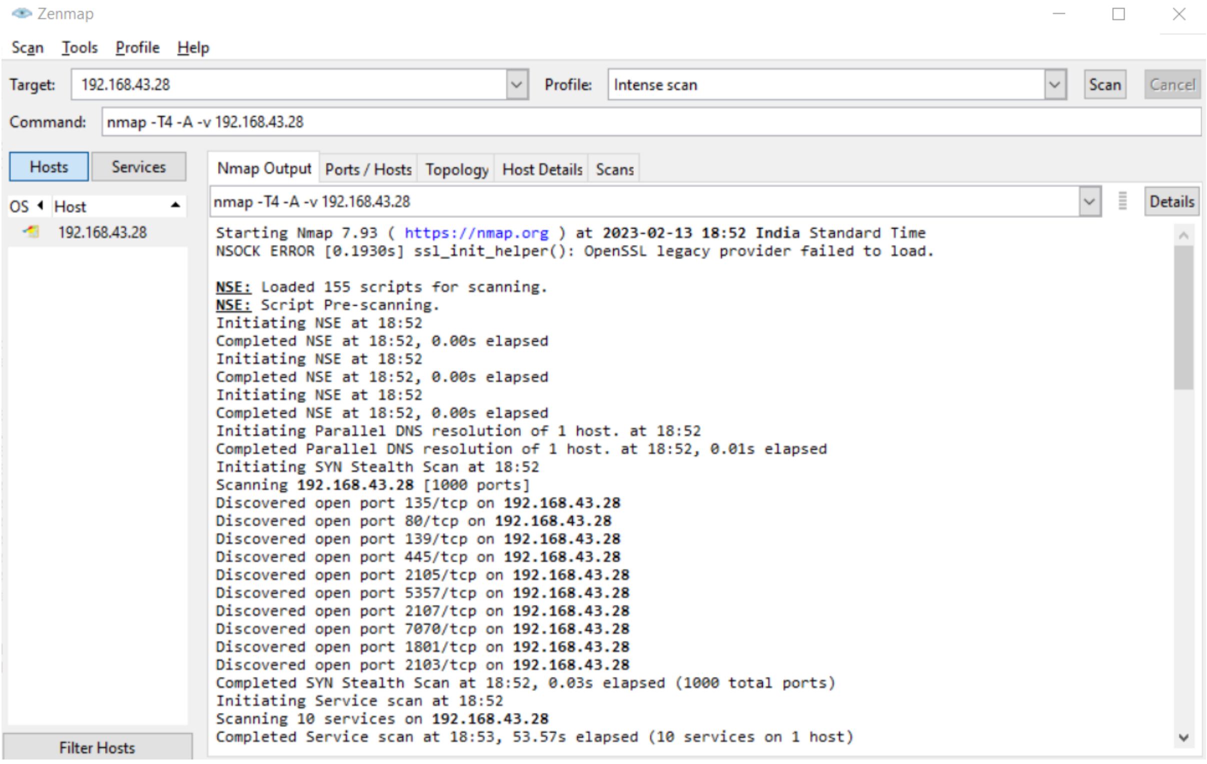
Target: 192.168.43.28

Profile: Regular scan

Command: nmap 192.168.43.28

```
nmap 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 18:49 India Standard Time
Nmap scan report for 192.168.43.28
Host is up (0.000014s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```



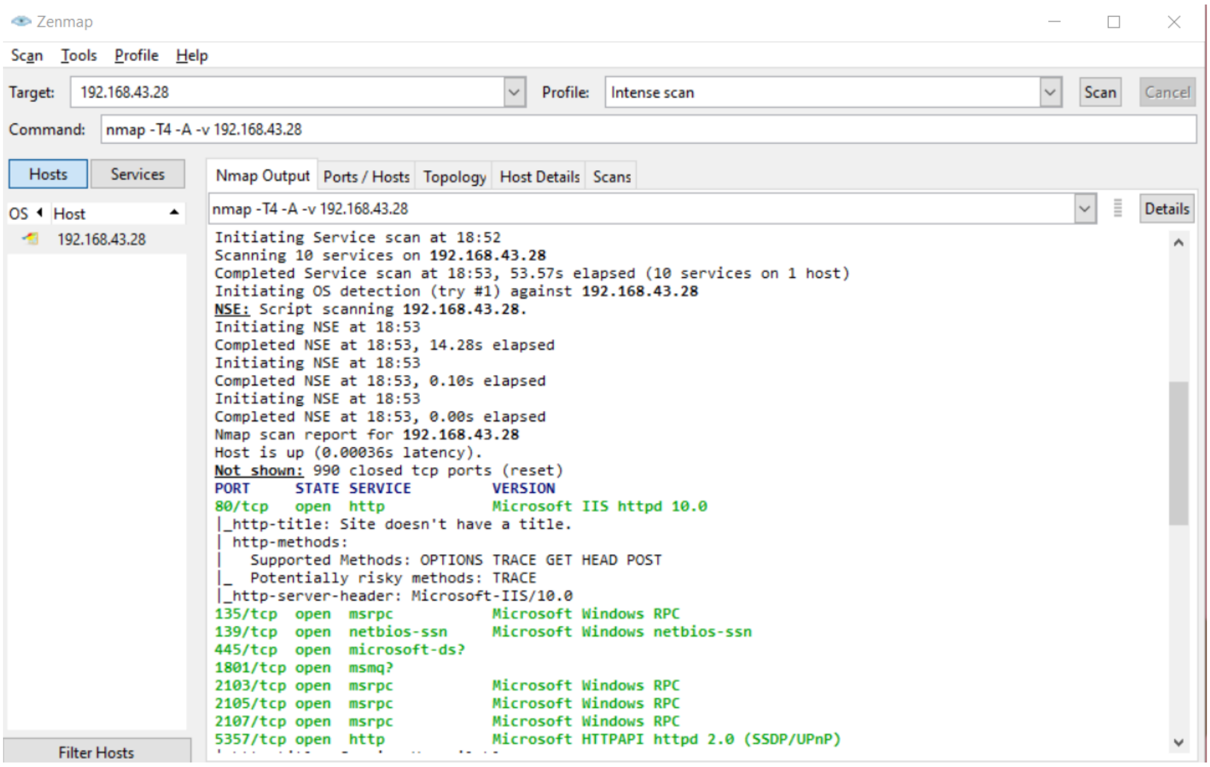
Target: 192.168.43.28

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.43.28

```
nmap -T4 -A -v 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 18:52 India Standard Time
NSOCK ERROR [0.1930s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating NSE at 18:52
Completed NSE at 18:52, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:52
Completed Parallel DNS resolution of 1 host. at 18:52, 0.01s elapsed
Initiating SYN Stealth Scan at 18:52
Scanning 192.168.43.28 [1000 ports]
Discovered open port 135/tcp on 192.168.43.28
Discovered open port 80/tcp on 192.168.43.28
Discovered open port 139/tcp on 192.168.43.28
Discovered open port 445/tcp on 192.168.43.28
Discovered open port 2105/tcp on 192.168.43.28
Discovered open port 5357/tcp on 192.168.43.28
Discovered open port 2107/tcp on 192.168.43.28
Discovered open port 7070/tcp on 192.168.43.28
Discovered open port 1801/tcp on 192.168.43.28
Discovered open port 2103/tcp on 192.168.43.28
Completed SYN Stealth Scan at 18:52, 0.03s elapsed (1000 total ports)
Initiating Service scan at 18:52
Scanning 10 services on 192.168.43.28
Completed Service scan at 18:53, 53.57s elapsed (10 services on 1 host)
```



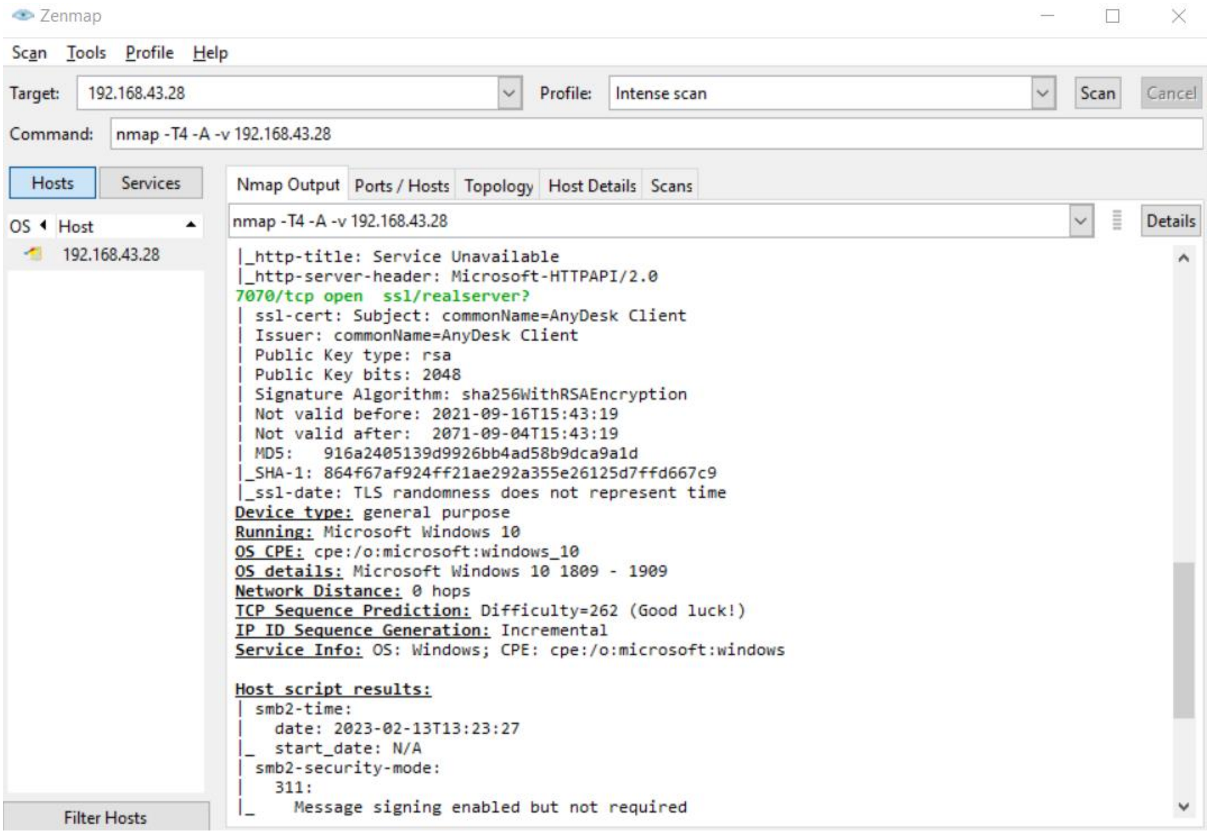
Target: 192.168.43.28

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.43.28

192.168.43.28

```
nmap -T4 -A -v 192.168.43.28
Initiating Service scan at 18:52
Scanning 10 services on 192.168.43.28
Completed Service scan at 18:53, 53.57s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against 192.168.43.28
NSE: Script scanning 192.168.43.28.
Initiating NSE at 18:53
Completed NSE at 18:53, 14.28s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.10s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Nmap scan report for 192.168.43.28
Host is up (0.00036s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
80/tcp   open  http            Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc           Microsoft Windows RPC
2105/tcp open  msrpc           Microsoft Windows RPC
2107/tcp open  msrpc           Microsoft Windows RPC
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```



Target: 192.168.43.28

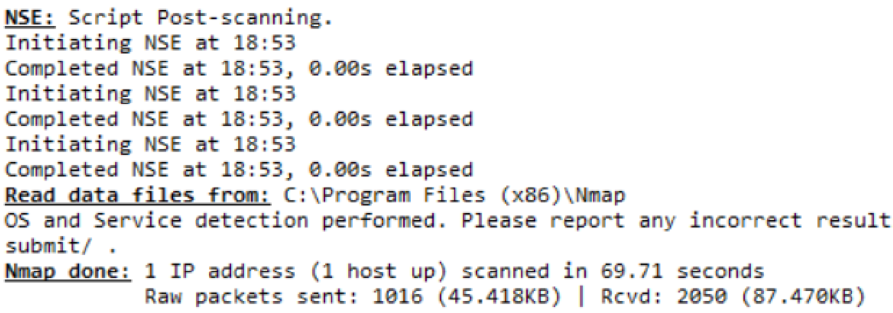
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.43.28

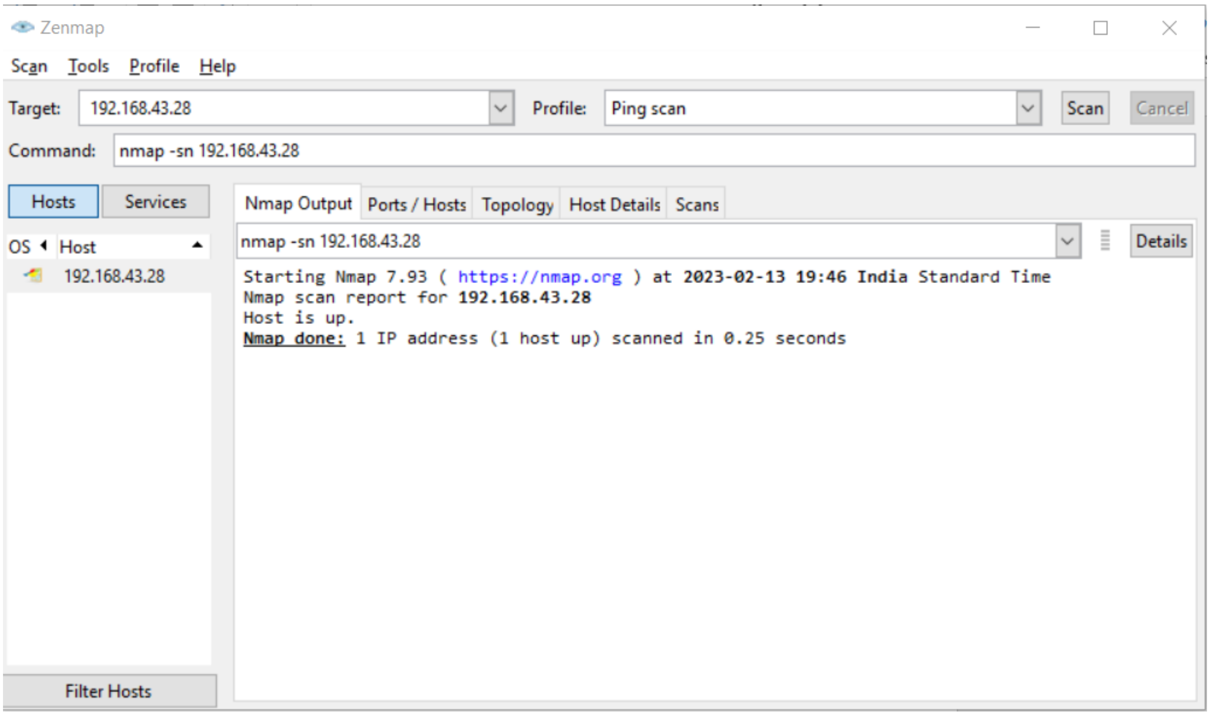
192.168.43.28

```
nmap -T4 -A -v 192.168.43.28
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
7070/tcp open  ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Issuer: commonName=AnyDesk Client
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-09-16T15:43:19
| Not valid after:  2071-09-04T15:43:19
| MD5:   916a2405139d9926bb4ad58b9dca9a1d
|_SHA-1: 864f67af924ff21ae292a355e26125d7ffd667c9
|_ssl-date: TLS randomness does not represent time
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-02-13T13:23:27
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
```



```
NSE: Script Post-scanning.
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Initiating NSE at 18:53
Completed NSE at 18:53, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 69.71 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2050 (87.470KB)
```



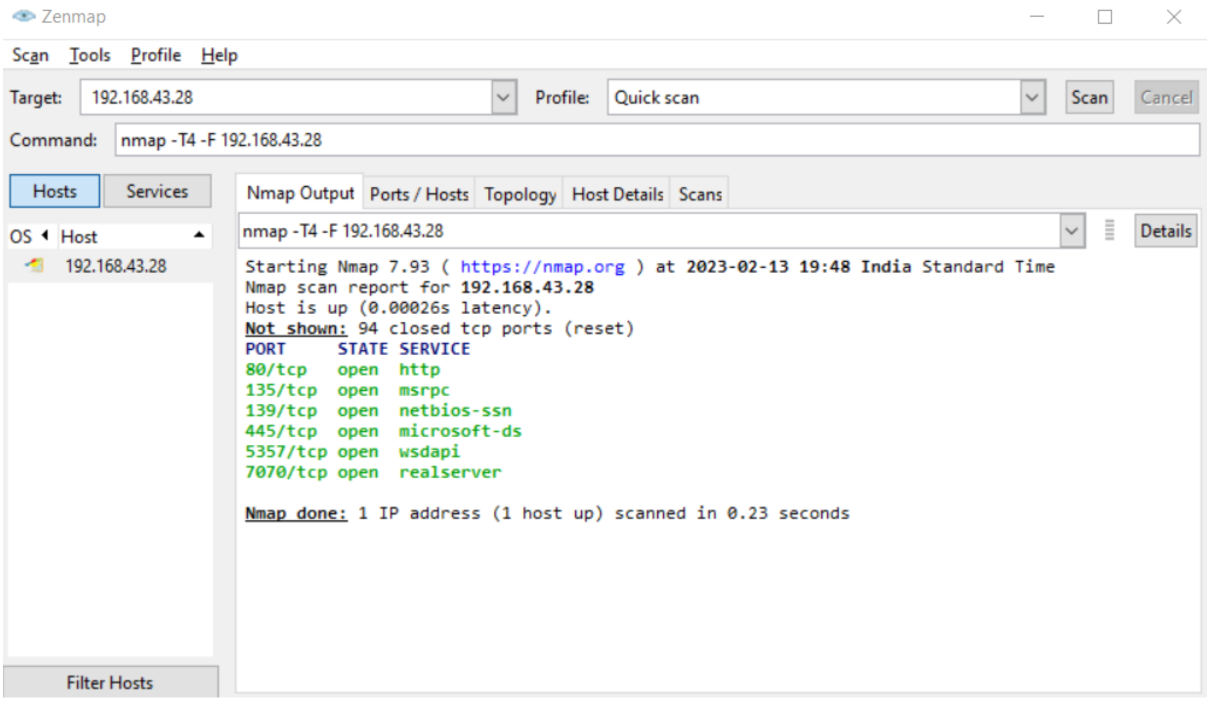
Target: 192.168.43.28

Profile: Ping scan

Command: nmap -sn 192.168.43.28

192.168.43.28

```
nmap -sn 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 19:46 India Standard Time
Nmap scan report for 192.168.43.28
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```



Target: 192.168.43.28

Profile: Quick scan

Command: nmap -T4 -F 192.168.43.28

192.168.43.28

```
nmap -T4 -F 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-13 19:48 India Standard Time
Nmap scan report for 192.168.43.28
Host is up (0.00026s latency).
Not shown: 94 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```