# Nmap Scanning Report – Target: 10.201.76.90

# Report submitted by SNEHA K

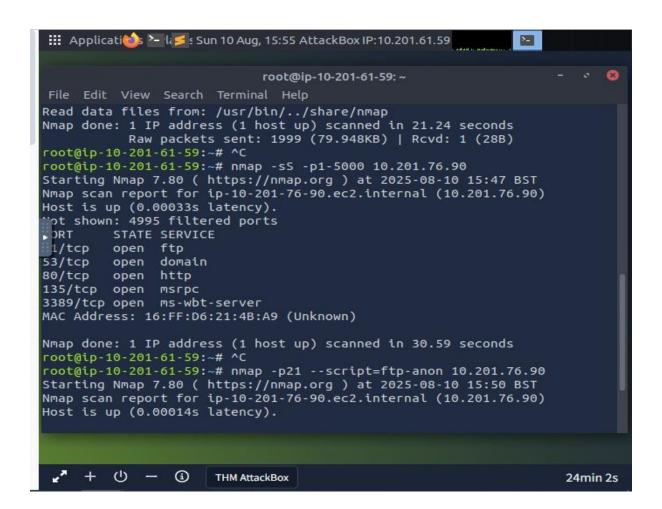
## 1. Objective

To perform reconnaissance and service enumeration on the target machine using Nmap, identifying open ports, services, and potential vulnerabilities, while applying various scan types and firewall evasion techniques.

## 2. Methodology

We applied the following Nmap techniques:

Scan Type	<b>Nmap Command</b>	Purpose
ICMP Ping Test	ping -c 4 10.201.76.90	Determine if host responds to ICMP echo requests
Xmas Scan (first 999)	nmap -sX -p1-999 10.201.76.90	Identify stealth-detectable open
Xmas Scan w/ Verbosity	nmap -sX -p1-999 -vv 10.201.76.90	Confirm reasons for open
TCP SYN Scan (first 5000)	nmap -sS -p1-5000 10.201.76.90	Identify open TCP ports quickly
TCP Connect Scan (Port 80)	nmap -sT -p80 10.201.76.90	Observe 3-way handshake in Wireshark
FTP Anonymous Access Check	nmap -p21script=ftp- anon 10.201.76.90	Test for anonymous FTP login



```
0
                                        root@ip-10-201-61-59: ~
 File Edit View Search Terminal Help
Not shown: 4995 filtered ports
           STATE SERVICE
21/tcp
53/tcp
            open ftp
open domain
           open http
80/tcp
135/tcp open msrpc
3389/tcp open ms-wbt-server
MAC Address: 16:FF:D6:21:4B:A9 (Unknown)
nap done: 1 IP address (1 host up) scanned in 30.59 seconds pot@ip-10-201-61-59:~# ^C
root@ip-10-201-61-59:~# nmap -p21 --script=ftp-anon 10.201.76.90
Starting Nmap 7.80 (https://nmap.org) at 2025-08-10 15:50 BST
Nmap scan report for ip-10-201-76-90.ec2.internal (10.201.76.90)
Host is up (0.00014s latency).
PORT STATE SERVICE
21/tcp open ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
MAC Address: 16:FF:D6:21:4B:A9 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 30.83 seconds root@ip-10-201-61-59:~# ■
      +
            () - (i)
                               THM AttackBox
                                                                                              23min 28s
```

#### 3. Findings

#### 3.1 ICMP Ping Test

- **Result:** Host **did not** respond to ICMP echo requests.
- **Conclusion:** ICMP blocked; -Pn switch needed for scans.

#### 3.2 Xmas Scan (Ports 1–999)

- **Result:** All **999 ports** reported as **open**|**filtered**.
- Reason: no-response (likely due to firewall rules blocking Xmas scan probes).

#### 3.3 TCP SYN Scan (Ports 1–5000)

• **Result:** 5 open ports detected:

Port Service
21/tcp FTP
53/tcp DNS
80/tcp HTTP
135/tcp MSRPC
3389/tcp RDP

#### 3.4 FTP Anonymous Login Test

• **Result:** Anonymous FTP access could allow unauthenticated file uploads or downloads.

#### 4. Observations

- Xmas scan results indicate that the host is filtering non-standard TCP flag combinations, typical of modern firewalls.
- SYN scan was successful despite ICMP blocking, revealing essential attack surface data.
- Multiple high-value services (RDP, MSRPC, FTP) are exposed externally, which is uncommon for hardened production systems.

