

# 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                  | Nmap Command  | Purpose  |
|----------------------------|---|--|
| ICMP Ping Test             | <code>ping -c 4 10.201.76.90</code>                   | Determine if host responds to ICMP echo requests |
| Xmas Scan (first 999)      | <code>nmap -sX -p1-999 10.201.76.90</code>            | Identify stealth-detectable open                 |
| Xmas Scan w/ Verbosity     | <code>nmap -sX -p1-999 -vv 10.201.76.90</code>        | Confirm reasons for open                         |
| TCP SYN Scan (first 5000)  | <code>nmap -sS -p1-5000 10.201.76.90</code>           | Identify open TCP ports quickly                  |
| TCP Connect Scan (Port 80) | <code>nmap -sT -p80 10.201.76.90</code>               | Observe 3-way handshake in Wireshark             |
| FTP Anonymous Access Check | <code>nmap -p21 --script=ftp-anon 10.201.76.90</code> | Test for anonymous FTP login                     |

```
Application  Sun 10 Aug, 15:54 AttackBox IP:10.201.61.59

root@ip-10-201-61-59: ~
File Edit View Search Terminal Help
root@ip-10-201-61-59:~# ^C
root@ip-10-201-61-59:~# nmap -sX -p1-999 -vv 10.201.76.90
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 15:45 BST
Initiating ARP Ping Scan at 15:45
Scanning 10.201.76.90 [1 port]
Completed ARP Ping Scan at 15:45, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 0.00s elapsed
Initiating XMAS Scan at 15:45
Scanning ip-10-201-76-90.ec2.internal (10.201.76.90) [999 ports]
Completed XMAS Scan at 15:45, 21.07s elapsed (999 total ports)
Nmap scan report for ip-10-201-76-90.ec2.internal (10.201.76.90)
Host is up, received arp-response (0.00011s latency).
All 999 scanned ports on ip-10-201-76-90.ec2.internal (10.201.76.90) are
open|filtered because of 999 no-responses
MAC Address: 16:FF:D6:21:4B:A9 (Unknown)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
root@ip-10-201-61-59:~# ^C
root@ip-10-201-61-59:~# nmap -sS -p1-5000 10.201.76.90
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 15:47 BST
Nmap scan report for ip-10-201-76-90.ec2.internal (10.201.76.90)
```

```
Application  Sun 10 Aug, 15:55 AttackBox IP:10.201.61.59

root@ip-10-201-61-59: ~
File Edit View Search Terminal Help
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)
root@ip-10-201-61-59:~# ^C
root@ip-10-201-61-59:~# nmap -sS -p1-5000 10.201.76.90
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-10 15:47 BST
Nmap scan report for ip-10-201-76-90.ec2.internal (10.201.76.90)
Host is up (0.00033s latency).
Not shown: 4995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
MAC Address: 16:FF:D6:21:4B:A9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds
root@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).
```

```
root@ip-10-201-61-59: ~
File Edit View Search Terminal Help
Not shown: 4995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
MAC Address: 16:FF:D6:21:4B:A9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds
root@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:~#
```

### 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.

...

1

V

Learn > Nmap



# Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

Easy ⌚ 50 min

Share your achievement

Help ▾


Save Room

👍 19643

🗨

Options ▾

Room completed ( 100% )



Target Machine Information

| Title | Target IP Address | Expires |
|-------|-------------------|---------|
|-------|-------------------|---------|