Nmap

An Open-Source Network Scanning Tool

Presented By:
Nafis Karim - 1805027
Mamun Munshi - 1805028

What is Nmap?

- Nmap is a powerful security scanner
- Discovers devices running on a network and identify various aspects of those devices
- Can scan for known vulnerabilities in the services that are running on open ports.

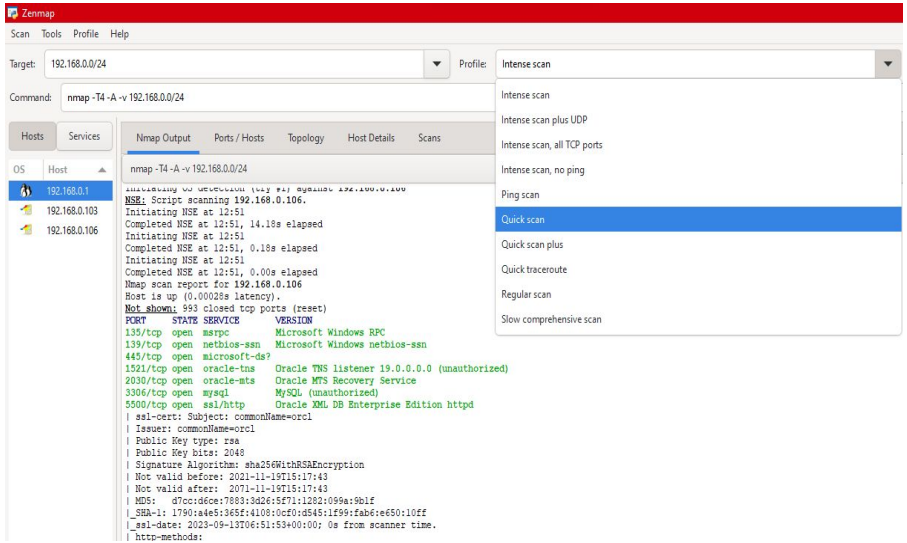
Nmap Using Commands

1. **-A** to enable OS and version detection
2. **-T4** for faster execution
3. **Hostname** which we want to explore

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

A Better Alternative : Zenmap GUI

1. **Target,** network we want to scan
2. **Profile**, defines the way scan should be done



Network Scanning Using Nmap

- **Host Discovery:** Identifies active hosts in the network.
- **Port Scanning:** Can discover which application is running on which port
- **OS and Version Detection:** Determines the operating system and services running on the target host.

Bypass Firewalls Using Nmap

Nmap can bypass firewalls by using techniques like:

- Fragmented packets
- Custom TCP flag
- No ping Scan
- Decoy scan
- Spoofing source MAC address
- By changing source port

By using Fragmented packets

- Avoid signature based detection
- Some firewalls can’t detect out-of-order fragmented packets
- The fragmented packets are then merged at the receiver.

By using custom TCP flags

- Some flag combinations less likely to be blocked
- Uses non standard flag combination
- Can learn about the behavior of a firewall(which flags it receives,which ones it blocks etc.)

By using no ping scan

- Ping used to find whether a device is active or running.
- Some firewalls block ICMP echo requests or ping requests.
- This technique avoids ICMP echo requests.
- Stealth technique.

By using decoy scan

- A way to hide the real source of the scan.
- Sends a series of fake source ips along with the real ips.
- Make it challenging to detect.

By spoofing MAC address

- Very similar to IP spoofing
- Changes the source MAC address
- Avoid detection by spoofing the MAC address
- Can select a particular MAC address to be used for spoofing or can select a random one.

By changing source port

- Can specify the port from which packets are sent.
- Done using —source-port or -g option.
- Can use a privileged source port(0-1023) too if we have root privilege.

Thank You