Vidyavardhini’s College of Engineering & Technology

Department of Computer Engineering
Academic Year : 2023-24

Experiment No 4

Aim: Perform network discovery using discovery tools (eg. Nmap, mrtg)

Theory:

1. To install NMAP on Ubuntu, run the command:

    ```
    sudo apt-get install nmap
    ```

2. After that open terminal and write

    ```
    nmap --version
    ```

3. Type nmap <ip address> and nmap <url>.
4. Next we will perform nmap operation on list of IP addresses.

    For that we need to type nmap and all the ip addresses eg. nmap 115.96.26.154,115.96.26.153, 115.96.26.152, 115.96.26.151

    You will get details regarding the IP addresses passed.

    We can also give range of IP Addresses

    It can be done by typing 56.78.29.10-30. This example will perform nmap operation on 20 ip addresses

5. Now let’s perform nmap using file

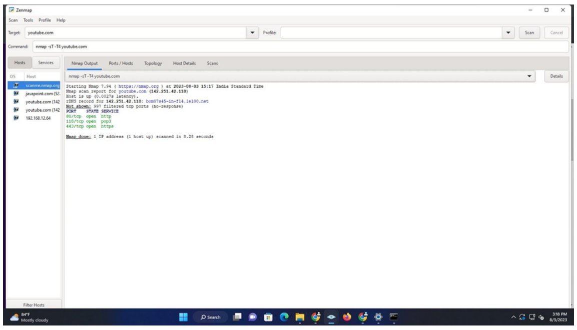
    Create a text file and in that paste ip address one below another

    Save the file and run nmap -iL filename.txt command.

    After a few minutes you will be able to see all available details of the sites mentioned .

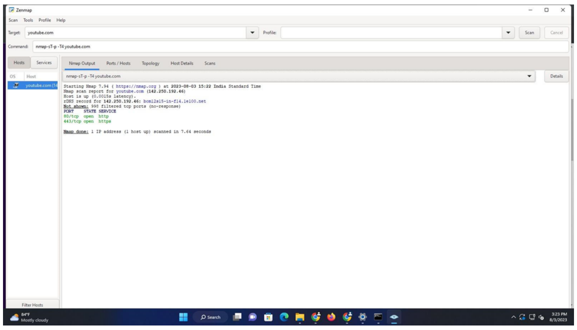
Output:

IP and URL address:



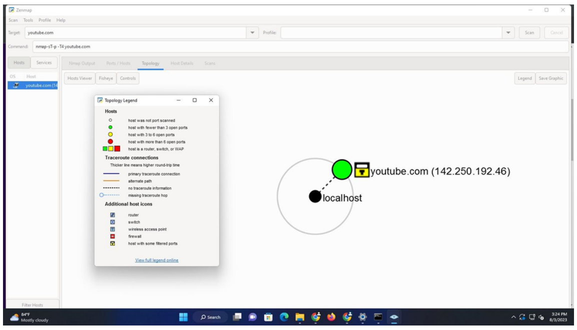
Command: nmap -sT -T4 youtube.com

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 15:17 India Standard Time
Nmap scan report for youtube.com (142.251.42.110)
Host is up (0.0027s latency).
rDNS record for 142.251.42.110: bom07s45-in-f14.1e100.net
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
110/tcp open  pop3
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds
```



Command: nmap-sT-p -T4 youtube.com

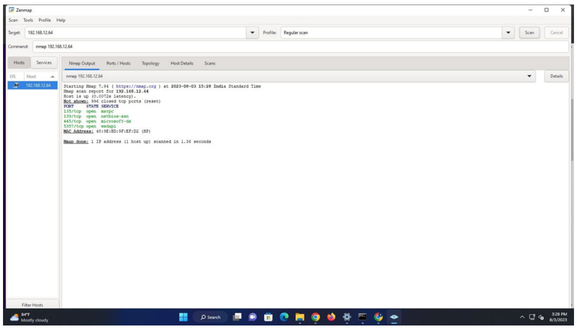
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 15:22 India Standard Time
Nmap scan report for youtube.com (142.250.192.46)
Host is up (0.0015s latency).
rDNS record for 142.250.192.46: bom12s15-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.64 seconds
```



Target: youtube.com

Command: nmap-sT-p -T4 youtube.com

Zenmap
Scan Tools Profile Help
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
Topology Legend
Hosts
○ host was not port scanned
● host with fewer than 3 open ports
● host with 3 to 6 open ports
● host with more than 6 open ports
🟩🟨🟥 host is a router, switch, or WAP
Traceroute connections
Thicker line means higher round-trip time
primary traceroute connection
alternate path
no traceroute information
missing traceroute hop
Additional host icons
router
switch
wireless access point
firewall
host with some filtered ports
View full legend online
youtube.com (142.250.192.46)
localhost
Filter Hosts

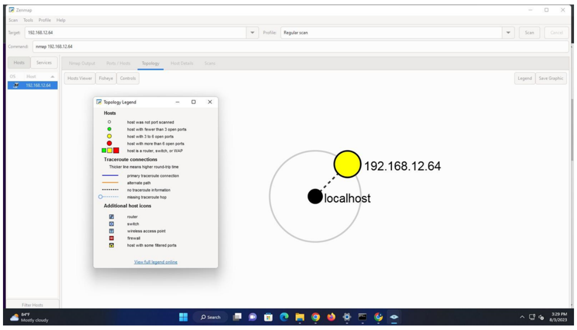


Target: 192.168.12.64

Profile: Regular scan

Command: nmap 192.168.12.64

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 15:28 India Standard Time
Nmap scan report for 192.168.12.64
Host is up (0.0072s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 48:9E:BD:9F:EF:D2 (HP)

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

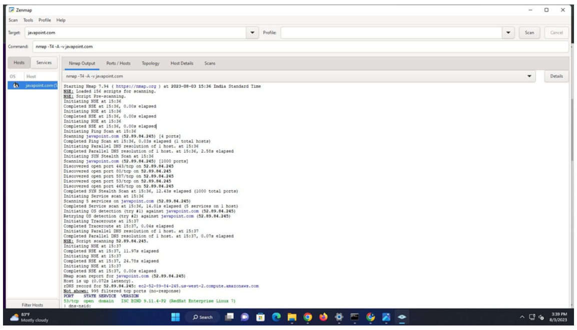


Target: 192.168.12.64

Profile: Regular scan

Command: nmap 192.168.12.64

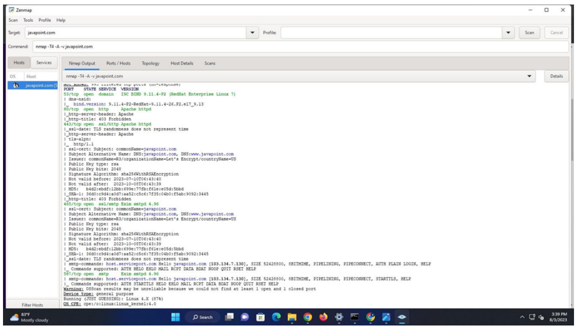
Topology Legend
Hosts
○ host was not port scanned
● host with fewer than 3 open ports
● host with 3 to 6 open ports
● host with more than 6 open ports
🟩🟨🟥 host is a router, switch, or WAP
Traceroute connections
Thicker line means higher round-trip time
primary traceroute connection
alternate path
no traceroute information
missing traceroute hop
Additional host icons
router
switch
wireless access point
firewall
host with some filtered ports
View full legend online
192.168.12.64
localhost



Target: javapoint.com

Command: nmap -T4 -A -v javapoint.com

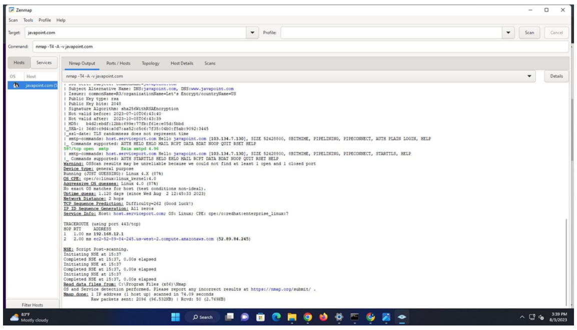
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 15:36 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating NSE at 15:36
Completed NSE at 15:36, 0.00s elapsed
Initiating Ping Scan at 15:36
Scanning javapoint.com (52.89.84.245) [4 ports]
Completed Ping Scan at 15:36, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:36
Completed Parallel DNS resolution of 1 host. at 15:36, 2.58s elapsed
Initiating SYN Stealth Scan at 15:36
Scanning javapoint.com (52.89.84.245) [1000 ports]
Discovered open port 443/tcp on 52.89.84.245
Discovered open port 80/tcp on 52.89.84.245
Discovered open port 587/tcp on 52.89.84.245
Discovered open port 53/tcp on 52.89.84.245
Discovered open port 465/tcp on 52.89.84.245
Completed SYN Stealth Scan at 15:36, 12.43s elapsed (1000 total ports)
Initiating Service scan at 15:36
Scanning 5 services on javapoint.com (52.89.84.245)
Completed Service scan at 15:36, 14.01s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against javapoint.com (52.89.84.245)
Retrying OS detection (try #2) against javapoint.com (52.89.84.245)
Initiating Traceroute at 15:37
Completed Traceroute at 15:37, 0.04s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:37
Completed Parallel DNS resolution of 1 host. at 15:37, 0.07s elapsed
NSE: Script scanning 52.89.84.245.
Initiating NSE at 15:37
Completed NSE at 15:37, 11.97s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 24.78s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Nmap scan report for javapoint.com (52.89.84.245)
Host is up (0.072s latency).
rDNS record for 52.89.84.245: ec2-52-89-84-245.us-west-2.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
```



Target: javapoint.com

Command: nmap -T4 -A -v javapoint.com

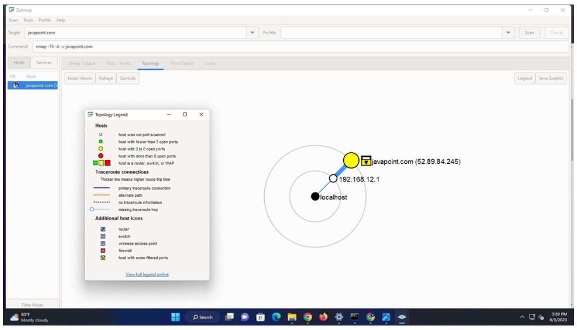
```
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.13
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
|_http-title: 403 Forbidden
443/tcp open  ssl/http Apache httpd
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=javapoint.com
| Subject Alternative Name: DNS:javapoint.com, DNS:www.javapoint.com
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-10T06:43:40
| Not valid after:  2023-10-08T06:43:39
| MD5:   b4d2:ebdf:12bb:699e:77fb:f61e:e05d:5bbd
|_SHA-1: 36d0:c9d4:a0d7:aa52:c5c6:7f35:04b0:f5ab:9092:3445
|_http-title: 403 Forbidden
465/tcp open  ssl/smtp Exim smtpd 4.96
| ssl-cert: Subject: commonName=javapoint.com
| Subject Alternative Name: DNS:javapoint.com, DNS:www.javapoint.com
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-10T06:43:40
| Not valid after:  2023-10-08T06:43:39
| MD5:   b4d2:ebdf:12bb:699e:77fb:f61e:e05d:5bbd
|_SHA-1: 36d0:c9d4:a0d7:aa52:c5c6:7f35:04b0:f5ab:9092:3445
|_ssl-date: TLS randomness does not represent time
| smtp-commands: host.serviceport.com Hello javapoint.com [103.134.7.130], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
587/tcp open  smtp     Exim smtpd 4.96
| smtp-commands: host.serviceport.com Hello javapoint.com [103.134.7.130], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
```



Target: javapoint.com

Command: nmap -T4 -A -v javapoint.com

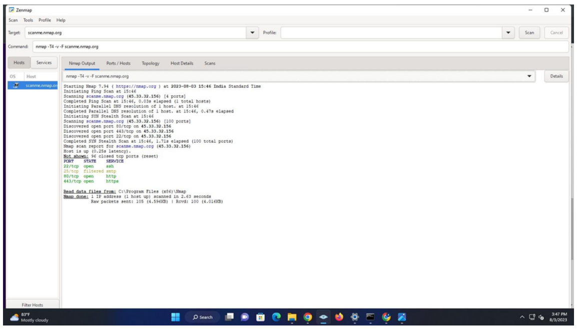
```
| ssl-cert: Subject: commonName=javapoint.com
| Subject Alternative Name: DNS:javapoint.com, DNS:www.javapoint.com
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-10T06:43:40
| Not valid after:  2023-10-08T06:43:39
| MD5:   b4d2:ebdf:12bb:699e:77fb:f61e:e05d:5bbd
|_SHA-1: 36d0:c9d4:a0d7:aa52:c5c6:7f35:04b0:f5ab:9092:3445
|_ssl-date: TLS randomness does not represent time
| smtp-commands: host.serviceport.com Hello javapoint.com [103.134.7.130], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
587/tcp open  smtp     Exim smtpd 4.96
| smtp-commands: host.serviceport.com Hello javapoint.com [103.134.7.130], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
Aggressive OS guesses: Linux 4.0 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.120 days (since Wed Aug  2 12:45:33 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: host.serviceport.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   1.00 ms 192.168.12.1
2   2.00 ms ec2-52-89-84-245.us-west-2.compute.amazonaws.com (52.89.84.245)

NSE: Script Post-scanning.
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 0.00s elapsed
Initiating NSE at 15:37
Completed NSE at 15:37, 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 74.09 seconds
           Raw packets sent: 2096 (96.532KB) | Rcvd: 50 (2.769KB)
```



Target: javapoint.com

Command: nmap -T4 -A -v javapoint.com

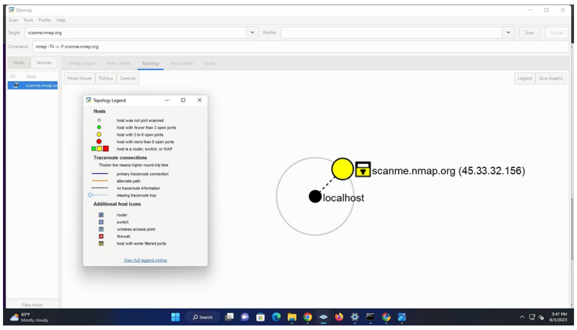
Topology Legend
Hosts
○ host was not port scanned
● host with fewer than 3 open ports
● host with 3 to 6 open ports
● host with more than 6 open ports
🟩🟨🟥 host is a router, switch, or WAP
Traceroute connections
Thicker line means higher round-trip time
primary traceroute connection
alternate path
no traceroute information
missing traceroute hop
Additional host icons
router
switch
wireless access point
firewall
host with some filtered ports
View full legend online
avapoint.com (52.89.84.245)
192.168.12.1
localhost



Target: scanme.nmap.org

Command: nmap -T4 -v -F scanme.nmap.org

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-03 15:46 India Standard Time
Initiating Ping Scan at 15:46
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 15:46, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:46
Completed Parallel DNS resolution of 1 host. at 15:46, 0.47s elapsed
Initiating SYN Stealth Scan at 15:46
Scanning scanme.nmap.org (45.33.32.156) [100 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 443/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Completed SYN Stealth Scan at 15:46, 1.71s elapsed (100 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 96 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
80/tcp  open     http
443/tcp open     https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
           Raw packets sent: 105 (4.596KB) | Rcvd: 100 (4.016KB)
```



Target: scanme.nmap.org

Command: nmap -T4 -v -F scanme.nmap.org

Conclusion:

In this experiment, we used Nmap, a potent network discovery tool, to identify active hosts and services on a local network. Employing options like -sn for host discovery and -PE for TCP SYN probing, we successfully gathered information about operating systems and software versions.

The outcomes help enhance network security by detecting devices and vulnerabilities, aiding in troubleshooting network issues.

Nmap proves valuable for administrators and security professionals, with recommendations including regular scans for monitoring and security assessments.

Additional notes highlight Nmap's versatility, availability of graphical interfaces, applicability, and customization options.