

**Task-1 Cybersecurity**  
**To Discover Open Ports On Devices In Your Local**  
**Network**

*Report*

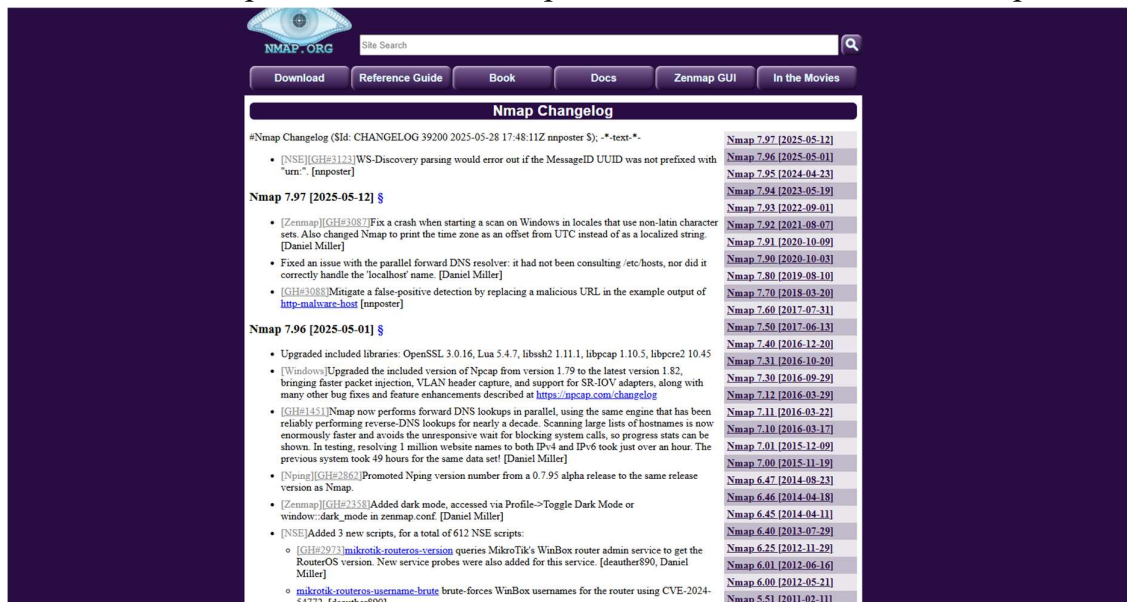
---

Table of Contents

1.Install Nmap from official website.....	
2.Find your local IP range (e.g., 192.168.1.0/24).....	
3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.....	
4.Note down IP addresses and open ports found.....	
5.Optionally analyze packet capture with Wireshark.....	
6.Research common services running on those ports.....	
7.Identify potential security risks from open ports.....	
8.Save scan results as a text or HTML file.....	

# Task-1 Install Nmap from official website

So in the first step I moved to the nmap official site and download nmap tool



# Task-2 Find your local IP range

To find the our local ip range we follow some steps need to -:

Step 1 first we need to know our own ip

Command -: if config(linux)

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.178 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 2405:201:a004:1a98:78bd:3e25:46c3:ddce prefixlen 64 scopeid 0x0<global>
    inet6 fe80::f7f9:425:faae:e7a6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 2535 bytes 334050 (326.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8014 bytes 510684 (498.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2008 bytes 84480 (82.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2008 bytes 84480 (82.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Output-: 192.168.29.178.

From the above we came to know our Ip range can be  
192.168.29.0/24

## Task-3 Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan

```
(kali@kali)-[~]
$ nmap -sS 192.168.29.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 07:25 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0030s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1900/tcp  open  upnp
2869/tcp  closed icslap
7443/tcp  open  oracleas-https
8002/tcp  closed teradataordbms
8080/tcp  open  http-proxy
8200/tcp  closed trivnet1
8443/tcp  open  https-alt
MAC Address: 20:89:8A:EB:8D:19 (Shenzhen Skyworth Digital Technology)

Nmap scan report for 192.168.29.5
Host is up (0.00043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: F8:89:D2:63:23:93 (Cloud Network Technology Singapore PTE.)

Nmap scan report for 192.168.29.12
Host is up (0.0082s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 7C:78:7E:3E:D5:FB (Samsung Electronics)

Nmap scan report for 192.168.29.37
Host is up (0.0052s latency).
All 1000 scanned ports on 192.168.29.37 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 5C:66:6C:8C:3B:69 (Guangdong Oppo Mobile Telecommunications)

Nmap scan report for 192.168.29.178
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.29.178 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.94 seconds
```

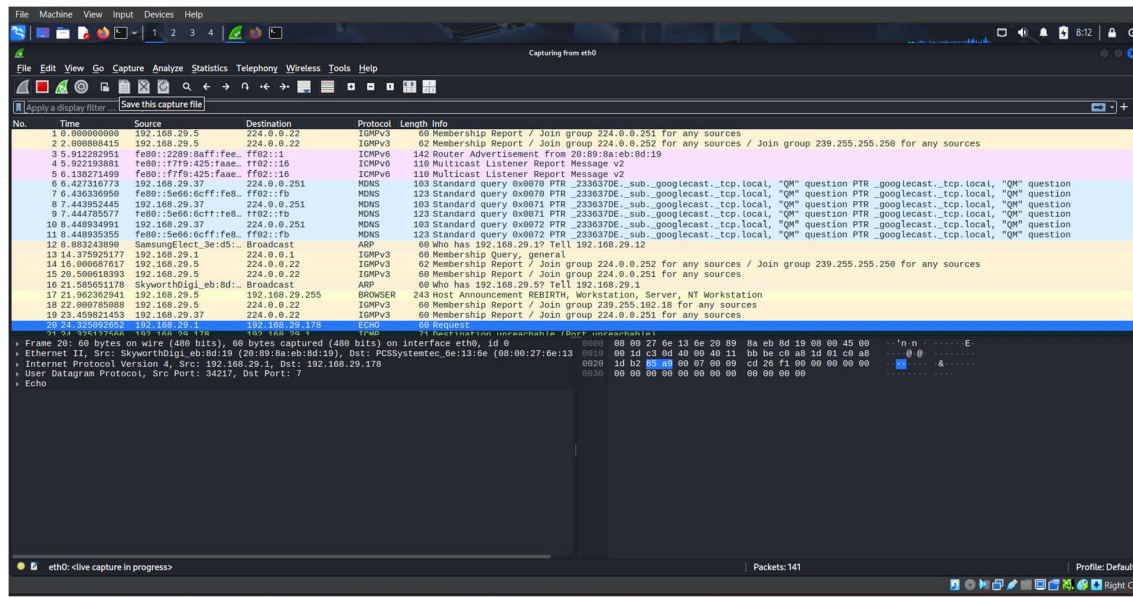
## 4.Note down IP addresses and open ports found

Output:-

1. 192.168.29.1
2. 192.168.29.5
3. 192.168.29.12
4. 192.168.29.37

5. 192.168.29.178

## 5.Optionaly analyze packet capture with Wireshark



Here the screenshort of analyzed packet capture with Wireshark

## Task 6 Research common services running on those ports

For finding all the open ports running in those system we use nmap command

Command -: `nmap -sC -sV 192.168.29.0/24`

Output-:

## Nmap scan report for reliance.reliance (192.168.29.1)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	http	lighttpd
--------	------	------	----------

443/tcp	open	ssl/http	lighttpd
---------	------	----------	----------

2869/tcp closed icslap  
7443/tcp open ssl/oracleas-https  
8002/tcp closed teradataordbms  
8080/tcp open http-proxy  
8200/tcp closed trivnet1  
8443/tcp open ssl/https-alt

### **Nmap scan report for 192.168.29.5**

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
7070/tcp	open	ssl/realserver?	

### **Nmap scan report for 192.168.29.12**

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	dnsmasq 2.62

```
(kali@kali)~$ sudo nmap -sC -sV 192.168.29.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 08:20 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0039s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         lighttpd
|_ http-title: Jio Centrum Home Gateway :
|_ http-server-header: Web Server
443/tcp    open  ssl/http     lighttpd
|_ ssl-cert: Subject: commonName=RILSELFECERT/organizationName=Reliance Jio Infocomm Limited
|_ Not valid before: 2018-06-27T00:00:02
|_ Not valid after: 2028-06-24T00:00:02
|_ ssl-date: TLS randomness does not represent time
1900/tcp    open  upnp
|_ fingerprint-strings:
|_   FourOhFourRequest, GetRequest:
|_     HTTP/1.1 404 Not Found
|_     Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance
|_     Content-Length: 48
|_     Content-Type: text/html
|_     <HTML><BODY><H1>404 Not Found</H1></BODY></HTML>
|_   HTTPOptions:
|_     HTTP/1.1 405 Method Not Allowed
|_     Server: Linux UPnP/1.0 DLNADOC/1.50 AccessTwine/1.0-RAS Device/reliance.reliance
|_     Content-Length: 57
|_     Content-Type: text/html
|_     <HTML><BODY><H1>405 Method Not Allowed</H1></BODY></HTML>
2869/tcp    closed  icslap
7443/tcp    open  ssl/oracleas-https?
|_ ssl-date: TLS randomness does not represent time
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.0 503 Service Unavailable
|_     Content-Length: 19
|_     Content-Type: text/html
|_     Connection: close
|_     Server: JCOW407/JUICEJFV-1.3.31
|_     Service Unavailable
|_   HTTPOptions:
|_     HTTP/1.0 501 Not Implemented
|_     Content-Length: 15
|_     Content-Type: text/html
|_     Connection: close
|_     Server: JCOW407/JUICEJFV-1.3.31
|_     implemented
|_   ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms Limited/stateOrProvinceName=KA/countryName=IN
```

## **Task-7 Identify potential security risks from open ports**

On identifying some and checking some of the open ports

Service version if they are outdated I found it for 1 ip address that is 192.168.29.5

And vulnerable port service and version is

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

Vulnerability is CVE:

2019-1089

The screenshot shows the Exploit Database interface for a specific vulnerability. The title is 'Microsoft Windows 10 1903/1809 - RPCSS Activation Kernel Security Callback Privilege Escalation'. The entry includes fields for EDB-ID (47135), CVE (2019-1089), Author (GOOGLE SECURITY RESEARCH), Type (LOCAL), Platform (WINDOWS), and Date (2019-07-18). It also indicates 'EDB Verified: ✓', 'Exploit: 📄 / 📄', and 'Vulnerable App:'. The main content area contains a detailed description of the vulnerability, including the summary, description, and a note about the actkernel RPC service.

## Task-8 Save scan results as a text or HTML file

For the out put in txt format

Command we can we use is-;

```
nmap -sV 192.168.1.0/24 -oN scan_output.txt
```

For the output in html format

Command we can use is -:

```
nmap -sV 192.168.1.0/24 -oN scan_output.txt
```

```
xsltproc scan_output.xml -o scan_output.html
```