Task 1 Network Discovery Challenge ~Sandesh Waghmare

Objective:
The objective of this network discovery task was to identify devices connected to the home network using the nmap network scanning tool. The report provides a detailed description of the task steps, commands used, and findings.

1. Introduction:
In modern home networks, multiple devices are connected, including computers, smartphones, smart TVs, printers, and IoT devices. Identifying these devices and their IP addresses is crucial for network management and security.

2. Tools Used:
The primary tool used for this network discovery task was nmap, a powerful network scanning tool available for Linux systems.

Nmap (Network Mapper) is a powerful open-source network scanning tool used for discovering hosts and services on a computer network. It's designed to scan large networks efficiently while providing a wide range of features for network exploration and security auditing. Here's some detailed information about Nmap:

1. **Scanning Techniques:**
    - **Ping Scan (-sn):** This is a basic scan that checks if hosts are online without scanning ports.
    - **TCP Connect Scan (-sT):** Establishes a full TCP connection to scan for open ports, useful for quick scans.
    - **TCP SYN Scan (-sS):** Sends SYN packets to determine open ports, stealthier than a full connection.
    - **UDP Scan (-sU):** Used for scanning UDP ports, which are commonly used for services like DNS and DHCP.
    - **ACK Scan (-sA):** Checks if ports are filtered by examining the response to ACK packets.

- **OS Detection (-O):** Attempts to determine the operating system of target hosts based on responses.
- **Service Version Detection (-sV):** Determines the version of services running on open ports.
- **Scripting Engine (-sC):** Runs Nmap scripts for additional information gathering and vulnerability detection.

2. **Host Discovery:** Nmap can use different methods to discover hosts on a network, such as ARP scanning, ICMP Echo requests, TCP and UDP scanning, and DNS resolution.
3. **Port Scanning:** Nmap can scan for open ports on target hosts using TCP, UDP, and other protocols. It can also scan specific ports or ranges of ports.
4. **Operating System Detection:** Using various techniques like TCP/IP stack fingerprinting and network responses, Nmap can often accurately detect the operating systems of scanned hosts.
5. **Service Detection:** Nmap can identify the services running on open ports by analyzing their responses, including identifying service banners and version information.
6. **Scripting Engine:** Nmap includes a scripting engine that allows users to write and execute scripts for specialized scanning tasks, vulnerability detection, and additional information gathering.
7. **Integration and Extensibility:** Nmap can be integrated with other tools and scripts, allowing for customized scanning workflows and automation of tasks. It also supports plugins and extensions for extending its functionality.
8. **Usage Examples:**
    - Basic Ping Scan: **nmap -sn 192.168.1.0/24**
    - TCP SYN Scan: **nmap -sS 192.168.1.1**
    - UDP Scan: **nmap -sU 192.168.1.1**
    - OS Detection: **nmap -O 192.168.1.1**
    - Service Version Detection: **nmap -sV 192.168.1.1**
    - Scripting Engine: **nmap -sC 192.168.1.1**

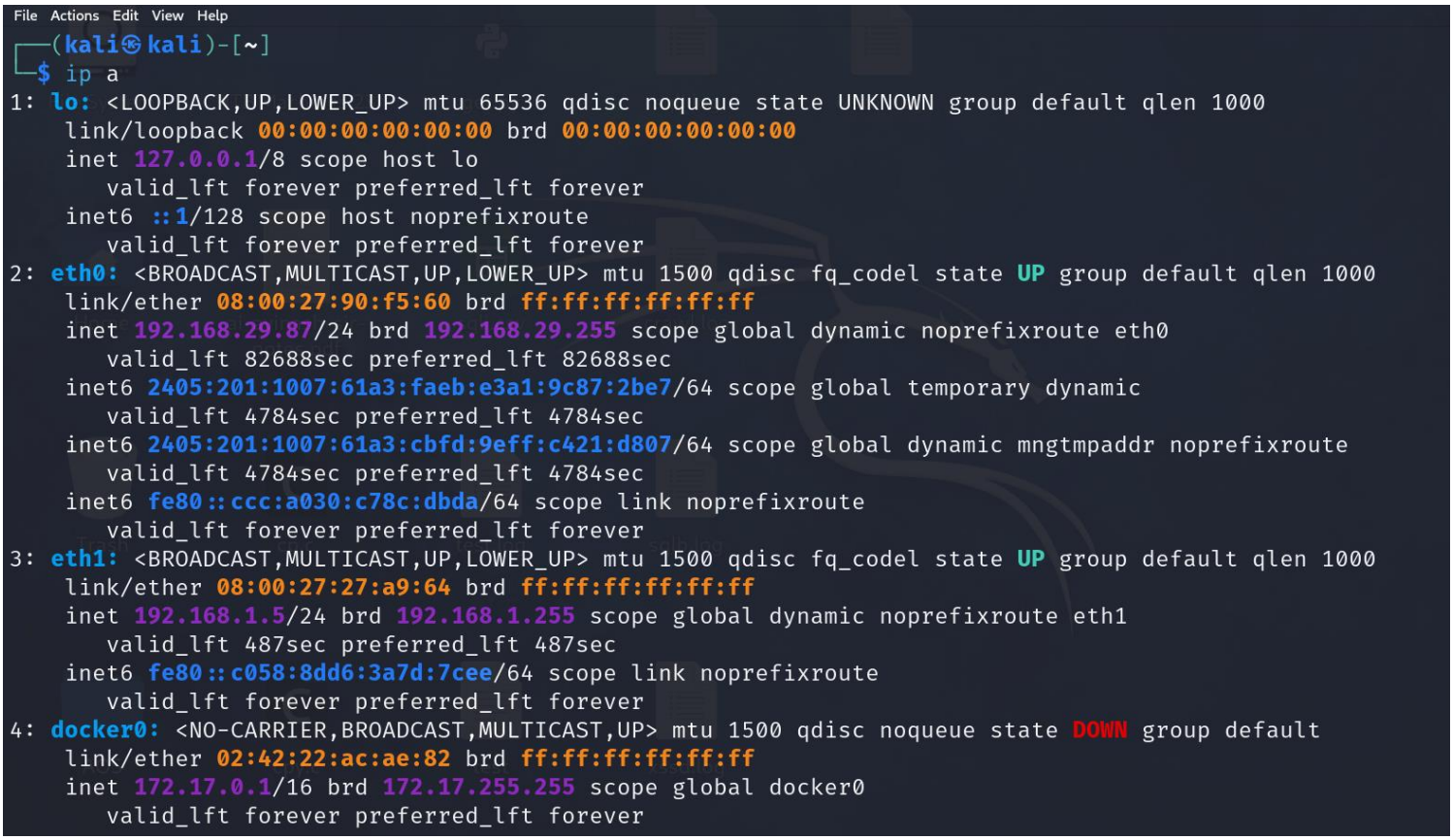
9. **Security and Ethical Considerations:** While Nmap is a valuable tool for network administrators and security professionals, it's important to use it responsibly and ethically. Unauthorized scanning of networks without permission is illegal and unethical, and users should always ensure they have the appropriate authorization before conducting network scans.

Overall, Nmap is a versatile and widely used network scanning tool known for its reliability, flexibility, and extensive feature set, making it an essential tool in network reconnaissance, security auditing, and troubleshooting.

3. Steps Taken:

Step 1: Getting to know the IP address

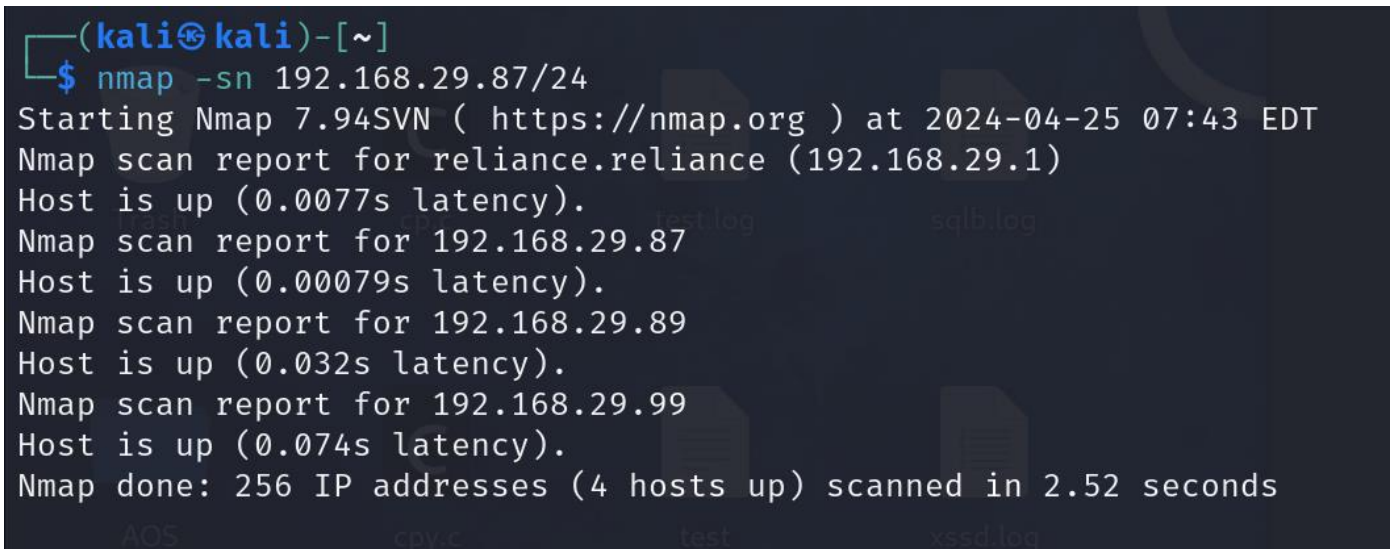
Using ip a command

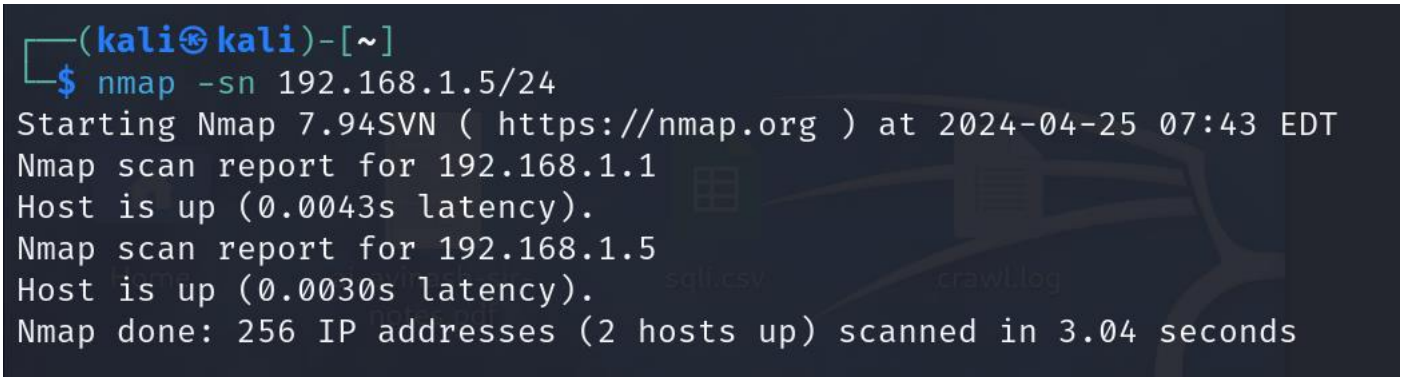


Step 2: Scan the Home Network
A ping scan was performed on the home network using nmap. The command used was:

As there were 2 ethernets present

- eth0: inet 192.168.29.87/24
- eth1: inet 192.168.1.5/24





This command instructs nmap to perform a ping scan (`-sn`) on all IP addresses in the range **192.168.29.87** to **192.168.29.255**and addresses in the range **192.168.1.5** to **192.168.1.255**

Step 3: Review Scan Results

Upon completion of the scan, nmap displayed a list of discovered devices along with their IP addresses and MAC addresses. Sample output from the scan included:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.29.87/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 07:21 EDT
Nmap scan report for reliance.reliance (192.168.29.1)
Host is up (0.0056s 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-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=RILSELFCERT/organizationName=Reliance Jio Infocomm
Limited
| Not valid before: 2018-06-27T00:00:05
|_Not valid after:  2028-06-24T00:00:05
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
| ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms
Limited/stateOrProvinceName=KA/countryName=IN
| Not valid before: 2021-11-22T04:56:50
|_Not valid after:  2121-10-29T04:56:50
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 503 Service Unavailable
```

| Content-Length: 19
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.30
|_   Service Unavailable
8002/tcp closed teradataordbms
8080/tcp open http-proxy   JCOW414/JUICEJFV-1.3.30
|_http-server-header: JCOW414/JUICEJFV-1.3.30
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 400 Bad Request
| Content-Length: 11
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.30
| Request
| GetRequest:
| HTTP/1.0 503 Service Unavailable
| Content-Length: 19
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.30
| Service Unavailable
| HTTPOptions:
| HTTP/1.0 501 Not Implemented
| Content-Length: 15
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.30
|_   implemented
8200/tcp closed trivnet1
8443/tcp open ssl/https-alt   JCOW414/JUICEJFV-1.3.30
|_ssl-date: TLS randomness does not represent time
|_http-server-header: JCOW414/JUICEJFV-1.3.30
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.0 400 Bad Request
| Content-Length: 11
| Content-Type: text/html
| Connection: close
| Server: JCOW414/JUICEJFV-1.3.30
| Request
| HTTPOptions:
| HTTP/1.0 501 Not Implemented
| Content-Length: 15
| Content-Type: text/html

```
|     Connection: close
|     Server: JCOW414/JUICEJFV-1.3.30
|     implemented
|   JavaRMI, LANDesk-RC, LDAPBindReq, SMBProgNeg, WMSRequest, afp, oracle-tns:
|     (null) 400 Bad Request
|     Content-Length: 11
|     Content-Type: text/html
|     Connection: close
|_    Request
| ssl-cert: Subject: commonName=jiofiber.local.html/organizationName=Jio Platforms
Limited/stateOrProvinceName=KA/countryName=IN

Nmap scan report for 192.168.29.87
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.29.87 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.29.89
Host is up (0.016s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Cisco/3com IPSSHd 6.6.0 (protocol 2.0)
| ssh-hostkey:
|_  512 63:45:c4:f3:f0:c4:fa:53:bd:ce:14:c5:f6:79:2f:c3 (DSA)
80/tcp open  http
|_http-title: Opening...
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 401 Unauthorized
|     Content-Type: text/html;charset=UTF-8
|     Content-Length: 0
|     Connection: close
|     Cache-control: no-cache
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/html;charset=UTF-8
|     Content-Length: 0
|     Connection: close
|     Cache-control: no-cache

└─$ nmap -sV -A -sC  192.168.1.5/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 07:46 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE    SERVICE VERSION
53/tcp filtered domain
```

The scan results included devices such as the router, desktop computer, smartphone, smart TV.

Step 4: Describe Devices' Purposes

- **Router (reliance.reliance (192.168.29.1)):** The router serves as the gateway to the internet, managing network traffic.
- **Desktop Computer (192.168.29.87):** This device is a desktop computer used for general computing tasks.
- **Smartphone (192.168.29.99):** The smartphone is used for communication, browsing, and mobile applications.
- **Smart TV (192.168.1.1):** This device connects to online streaming services and provides entertainment content.

4. Conclusion:
The network discovery task using nmap successfully identified and listed devices on the home network, providing insights into their IP addresses, MAC addresses, and purposes. This information is valuable for network management, security monitoring, and device inventory.

This report provides a comprehensive overview of the Network Discovery Challenge, detailing the steps taken, commands used, scan results, device descriptions, and recommendations for network management and security.