Task-1 Cybersecurity

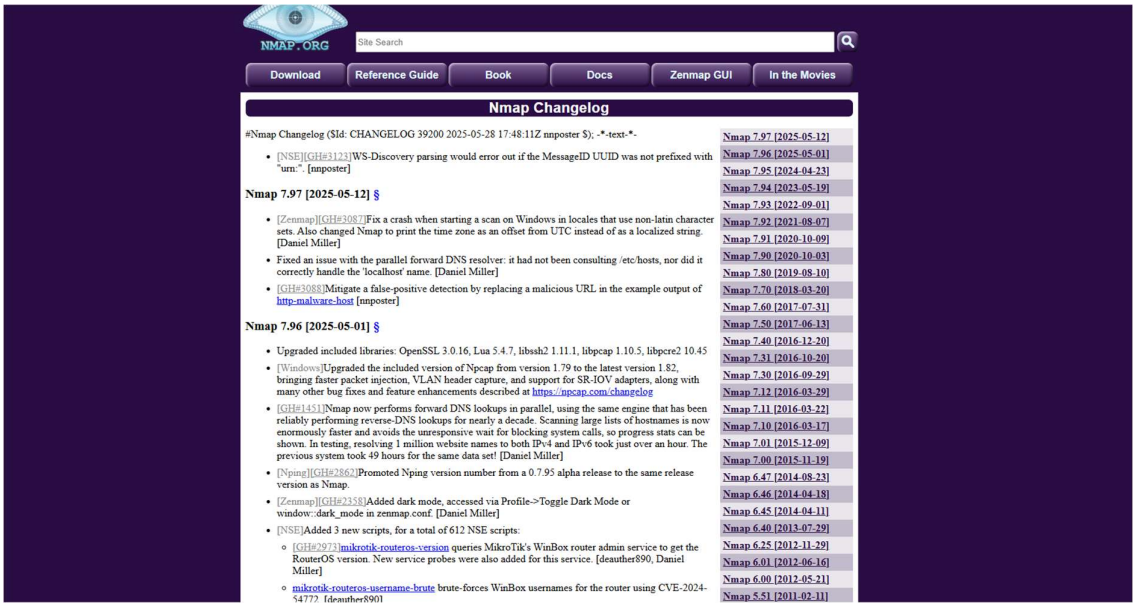
To Discover Open Ports On Devices In Your Local Network

Report

Table of Contents

Task-1 Install Nmap from official website

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

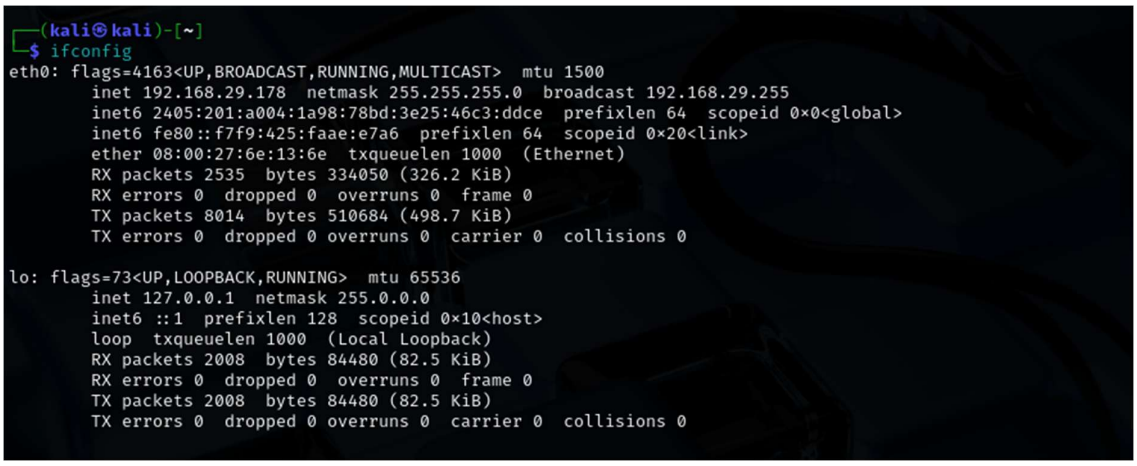


Task-2 Find your local IP range

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

Step 1 first we need to know our own ip

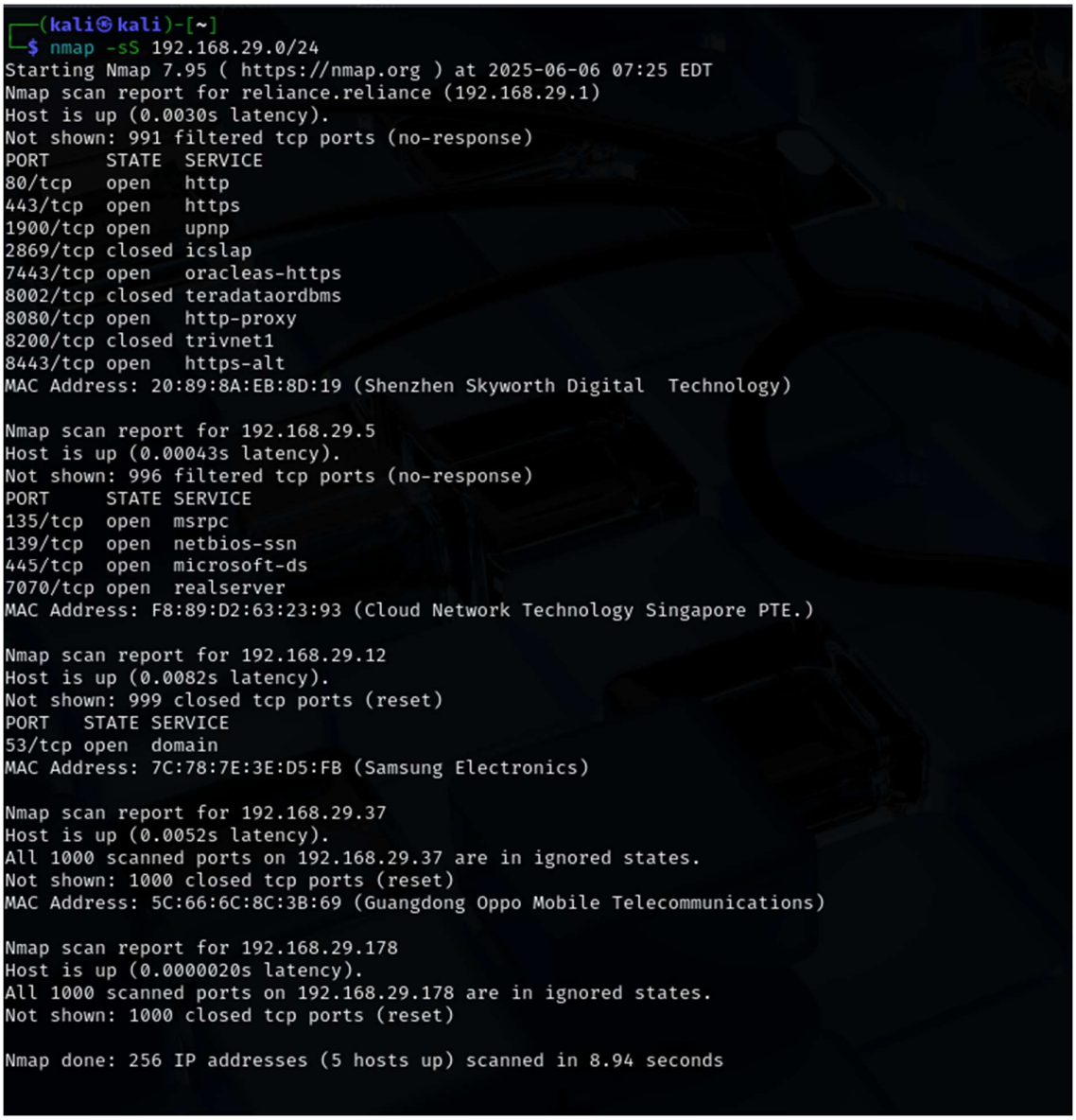
Command -: if config(linux)



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



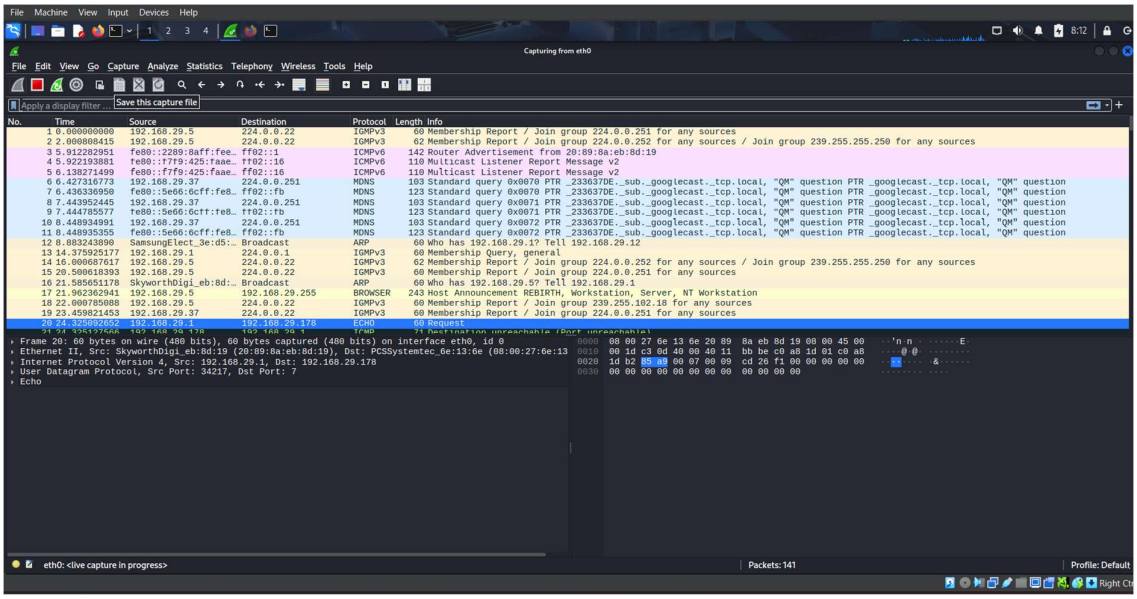
4.Note down IP addresses and open ports found

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

Task-7 Identify potential security risks from open ports

On identifying some and checking some of the open ports

Service version if they ae outdated the I found it for 1 ip address that is 192.168.29.5

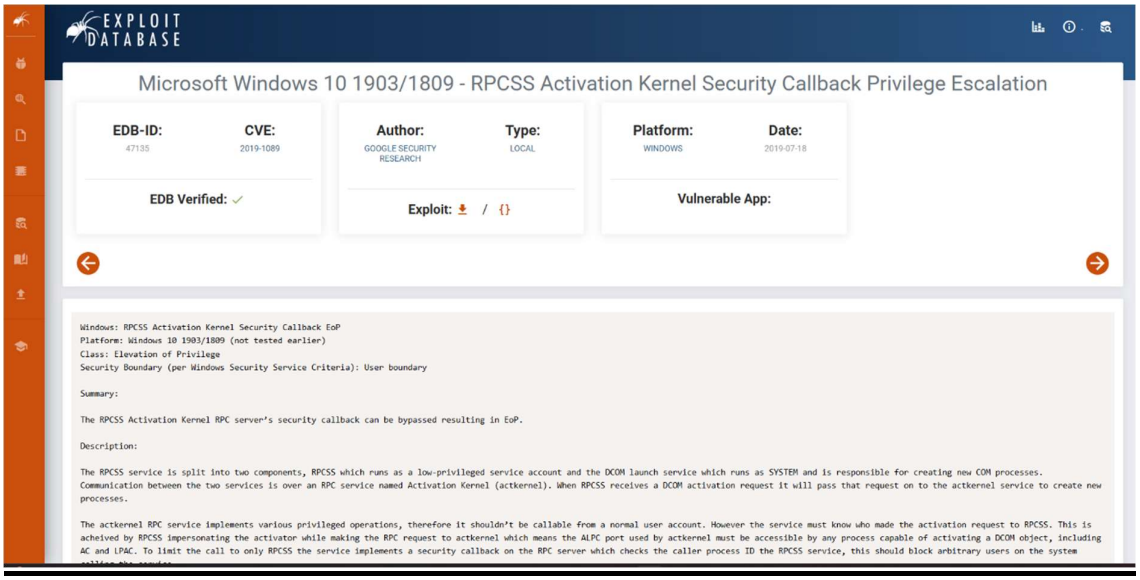
And vulnerable port service and version is

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

Vulnerability is CVE:

2019-1089



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