IT303 – Software Engineering

Project title: “Implementation of Port Scanning Techniques”

User Manual

Port scanning utility quick guide

Date: 28.10.25

Prepared By:

Anirudh S (231IT006)
Siddharth S Kolkar (231IT071)
T Srujan Swampy (231IT079)

Introduction:

Port scanner is a lightweight network tool designed to scan a target host for port behaviour, os/protocol discovery.

Purpose:

The purpose of this utility is to perform active network reconnaissance by scanning a target's ports. It is intended for educational use and authorized security assessments to map a system's attack surface and validate its network-level posture.

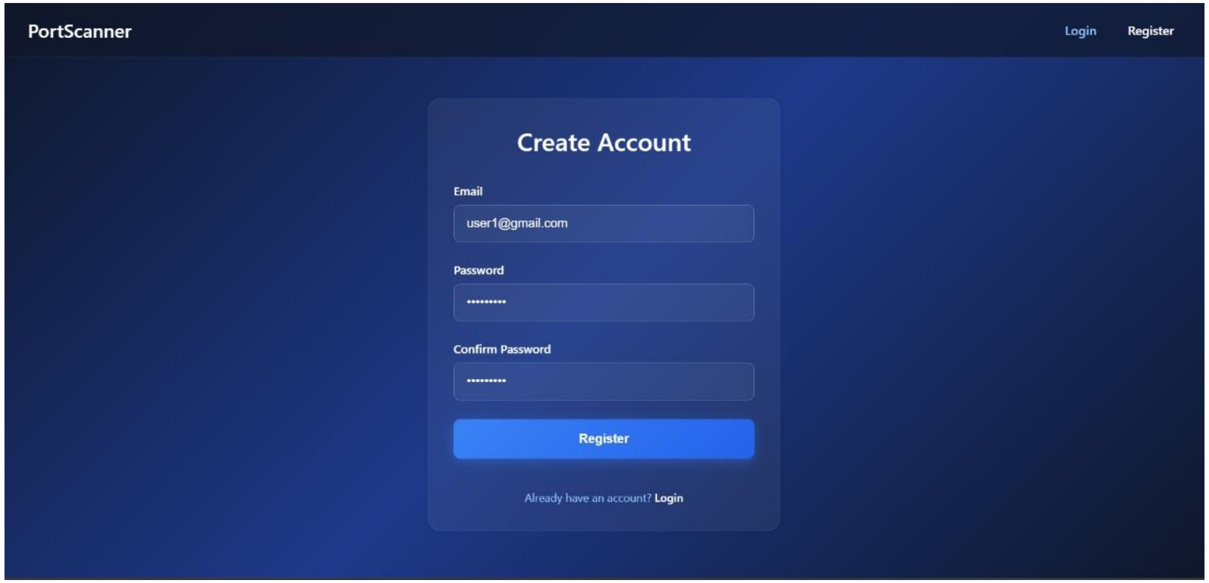
Ethical warning:

This tool should only be used on networks and systems for which you have explicit authorization. Unauthorized port scanning is illegal and unethical.

Procedure overview

1. User registration and verification using email
2. User log in
3. Select scan type
4. Input parameters for the target
5. Export results
6. User Log out

User registration



Create Account

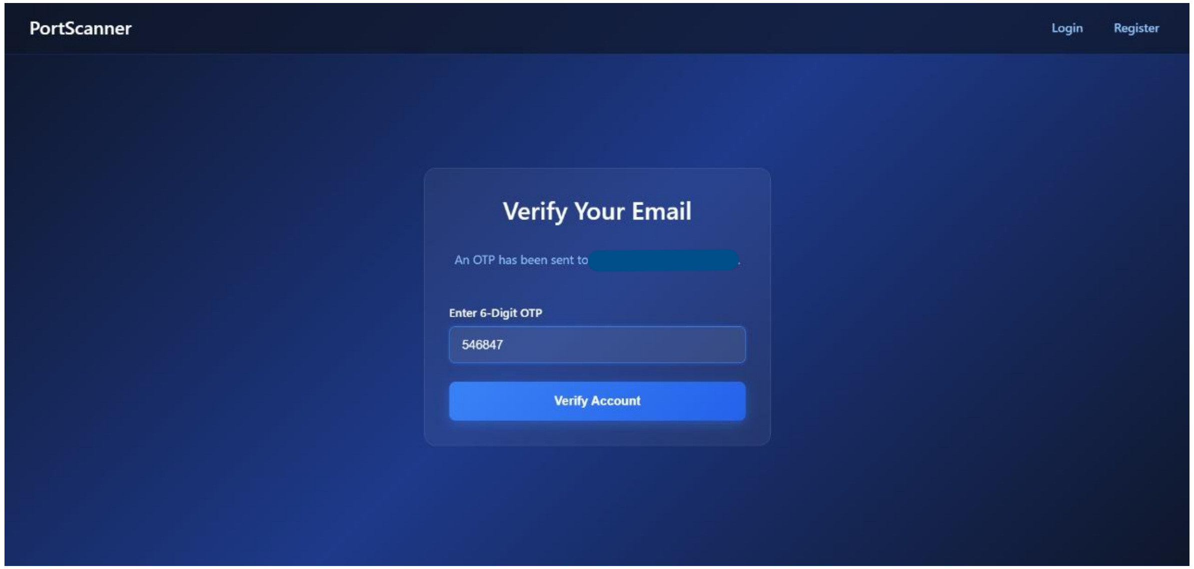
Email: user1@gmail.com

Password: •••••••••

Confirm Password: •••••••••

- Enter your email and create a password
- Confirm the password and click on register
- You should wait for 10 mins before re-registering a previously unverified account

Account Verification



Verify Your Email

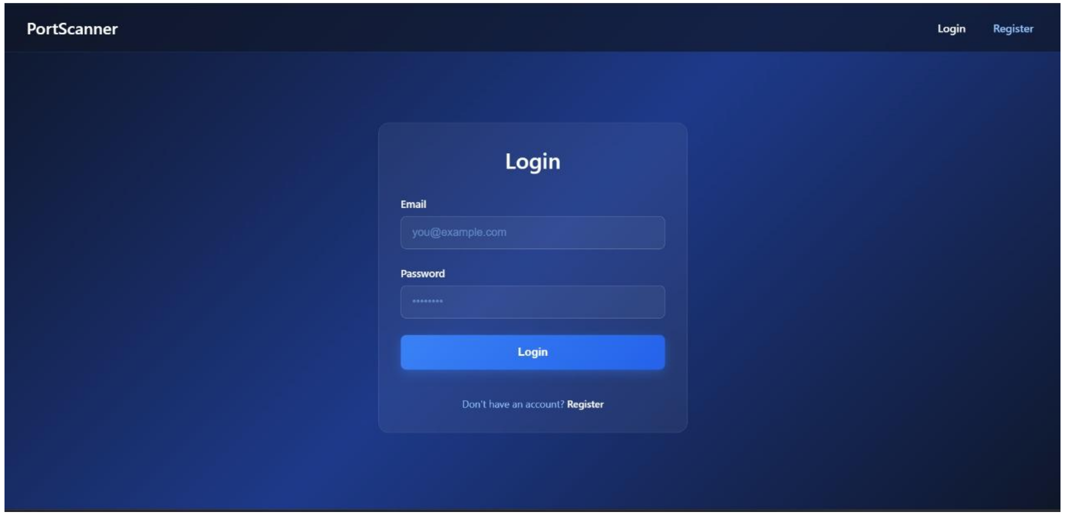
An OTP has been sent to [redacted].

Enter 6-Digit OTP

546847

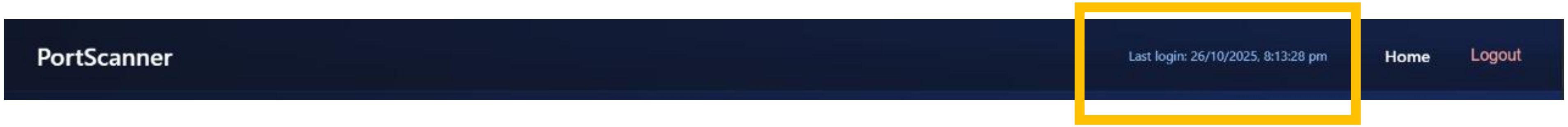
- A 6-digit One time password (OTP) will be sent to the email you are registering.
- OTP will be valid until 10 minutes

User Login



Don't have an account? Register

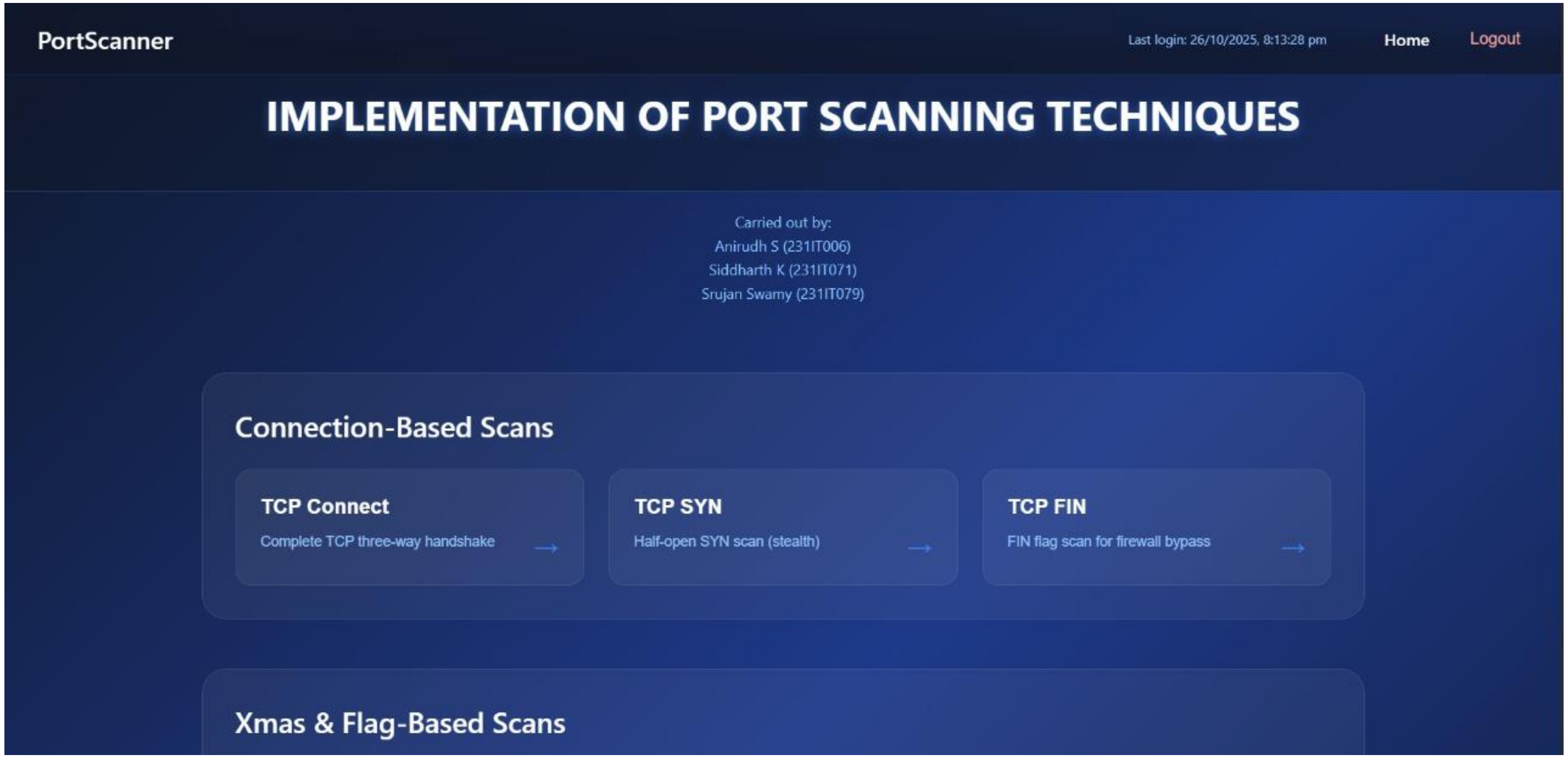
Login with valid credentials



Last login: 26/10/2025, 8:13:28 pm

You can see your last login date and time on the navigation bar in top-right.

Home Page:



IMPLEMENTATION OF PORT SCANNING TECHNIQUES

Carried out by:
Anirudh S (231IT006)
Siddharth K (231IT071)
Srujan Swamy (231IT079)

Connection-Based Scans

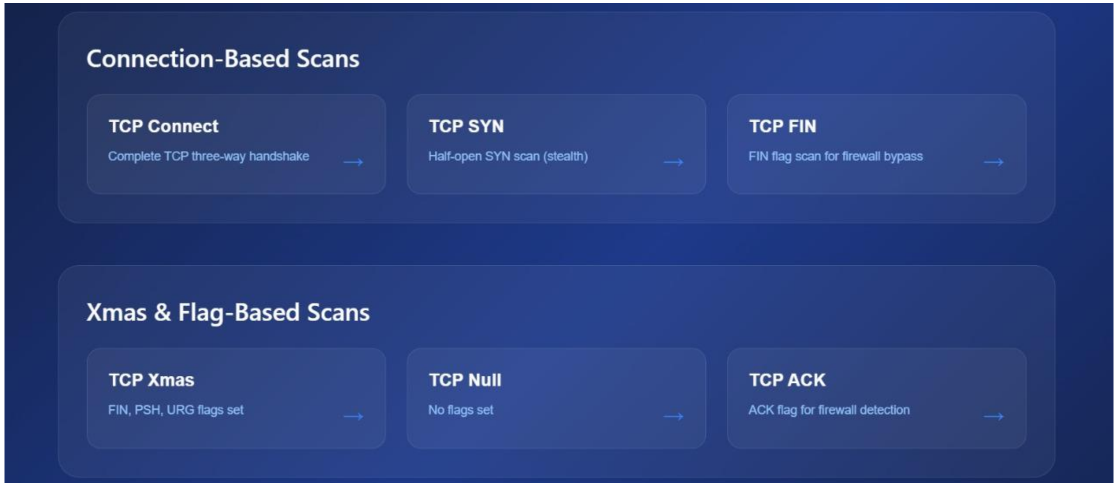
TCP Connect
Complete TCP three-way handshake →

TCP SYN
Half-open SYN scan (stealth) →

TCP FIN
FIN flag scan for firewall bypass →

Xmas & Flag-Based Scans

Scan techniques:



Connection-Based Scans

TCP Connect
Complete TCP three-way handshake →

TCP SYN
Half-open SYN scan (stealth) →

TCP FIN
FIN flag scan for firewall bypass →

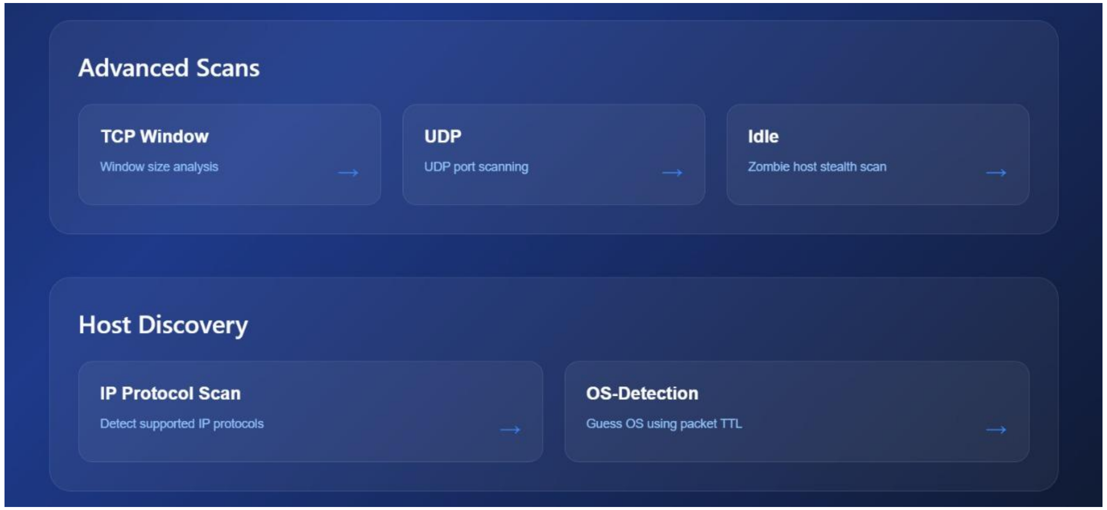
Xmas & Flag-Based Scans

TCP Xmas
FIN, PSH, URG flags set →

TCP Null
No flags set →

TCP ACK
ACK flag for firewall detection →

There are 11 scan techniques that have been implemented.



Advanced Scans

TCP Window
Window size analysis →

UDP
UDP port scanning →

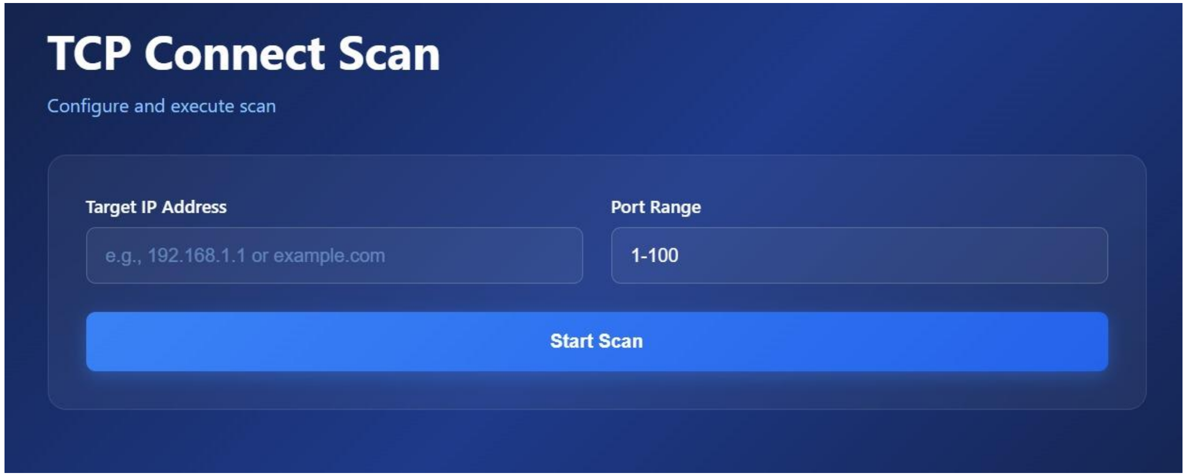
Idle
Zombie host stealth scan →

Host Discovery

IP Protocol Scan
Detect supported IP protocols →

OS-Detection
Guess OS using packet TTL →

Input parameters for various scans:



TCP Connect Scan

Configure and execute scan

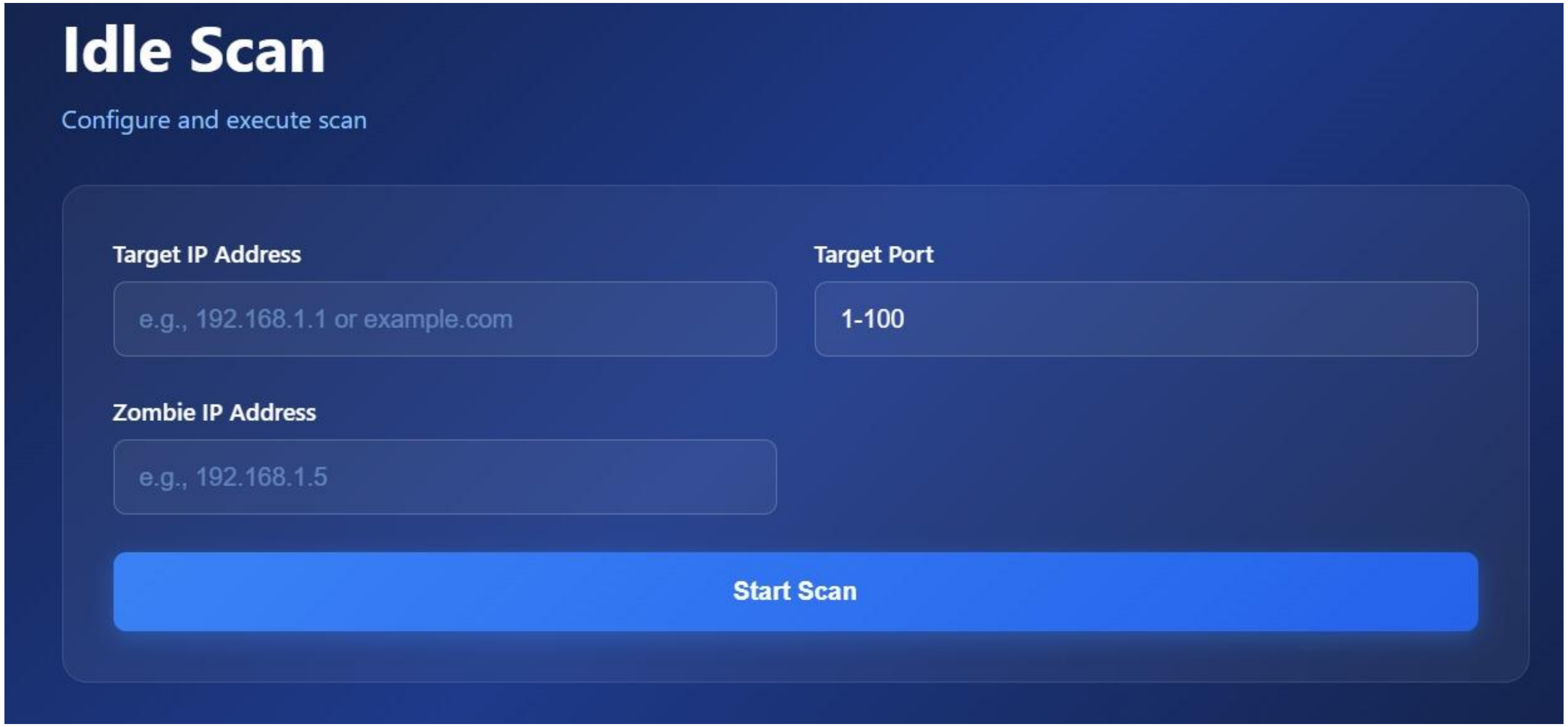
Target IP Address: e.g., 192.168.1.1 or example.com

Port Range: 1-100

For the scans:

TCP Connect scan, TCP SYN scan, TCP FIN scan, TCP Xmas scan, TCP Null scan, TCP ACK scan, TCP Window scan and UDP scan the input parameters should be:

1. IP address of the target system in same network with permission to scan.
2. Port(s) or port range. eg:3000, 3500-4000 etc.



Idle Scan

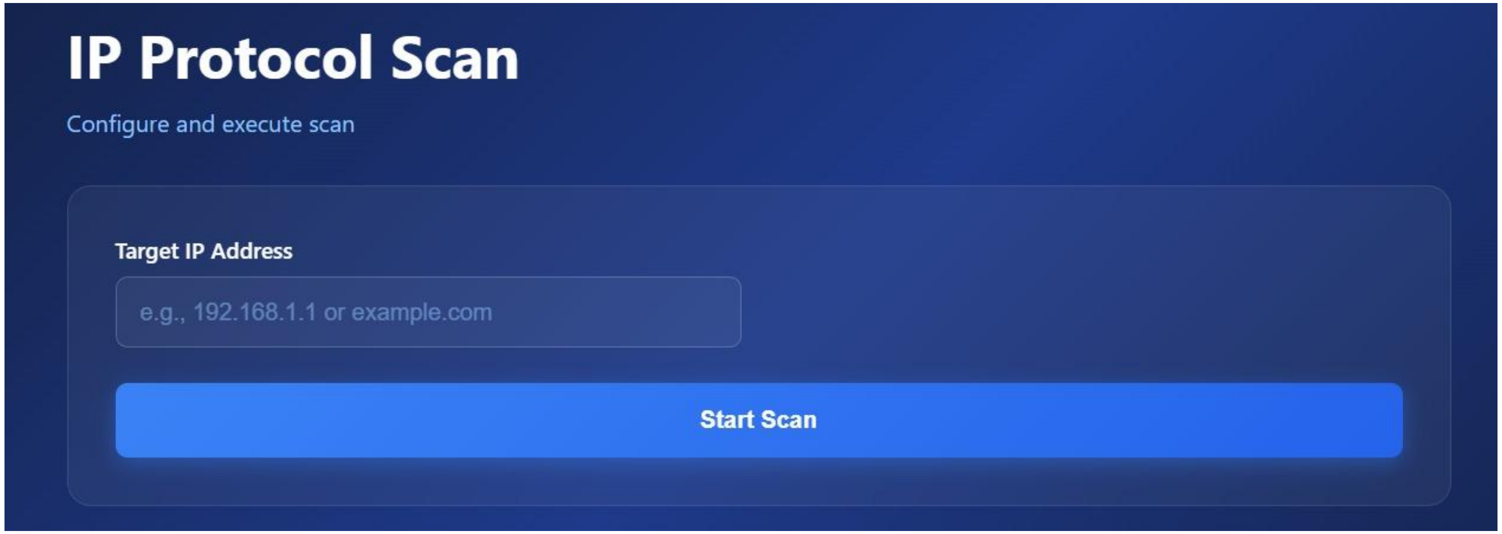
Configure and execute scan

Target IP Address: e.g., 192.168.1.1 or example.com

Target Port: 1-100

Zombie IP Address: e.g., 192.168.1.5

For **IDLE scan** along with target ip address and port, you need to also give the Zombie IP address. A 'Zombie' is a separate, idle machine on the network (like PC or Virtual Machine with older version of OS like FreeBSD 4.10 etc.)



IP Protocol Scan

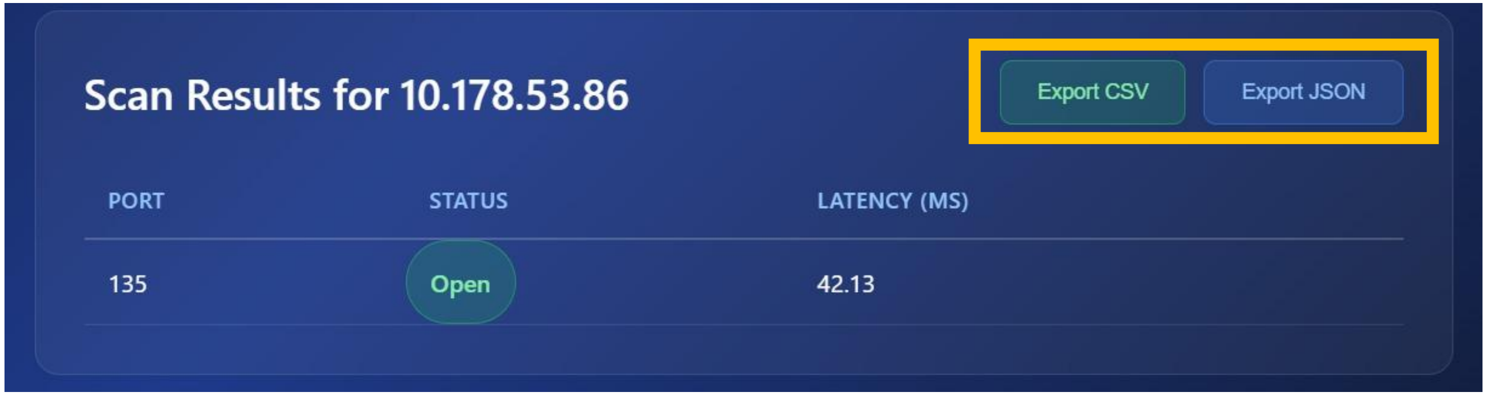
Configure and execute scan

Target IP Address

e.g., 192.168.1.1 or example.com

For IP Protocol Scan and OS-Detection scan, give only target IP address.

Export Results:

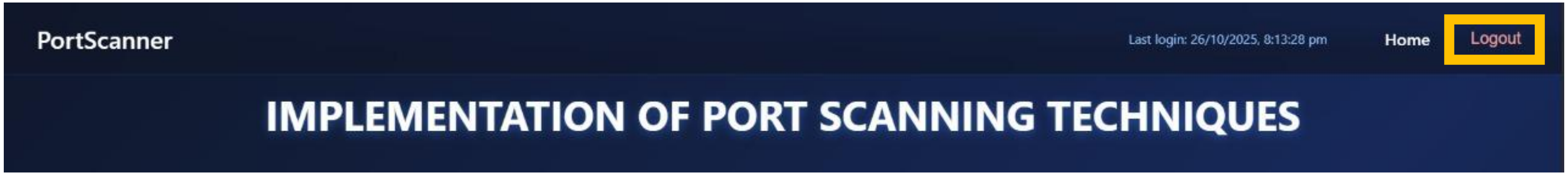


Scan Results for 10.178.53.86

PORT	STATUS	LATENCY (MS)
135	Open	42.13

Optionally choose required file type (.csv or .json) to export the results displayed on the screen.

Logout:



Last login: 26/10/2025, 8:13:28 pm

IMPLEMENTATION OF PORT SCANNING TECHNIQUES

Finally, the user can opt to logout by clicking on the Logout Button in the top right corner.

Else, the login of the user will be persistent for 24 hours.