Attack Surface Monitoring Tool for Continuous Discovery, Analysis, Remediation and Monitoring of Cyber Security Vulnerabilities and Potential Attack Vectors for Inventory

Abstract

Attack surface monitoring is a preventative cybersecurity strategy designed to continuously identify, assess, analyse and mitigate possible vulnerabilities or possible vulnerabilities and attack vectors at an organization's digital footprint. Attack surfaces have grown in scope as organizations continue to adopt more interconnectivity and increase reliance on cloud services and remote access; the larger the attack surface, the larger the cybersecurity issue organizations will experience in terms of potential attacks. Attack surface monitoring provides an organization a means to mitigate cybersecurity risk by maintaining an overall healthy security posture, maintaining regulatory compliance, and protecting secure systems and critical resources from being compromised.

To accomplish this, the main goal of this project is the creating of an Attack Surface Monitoring Tool which allows for continuous discovery, analyzing, remediation, and monitoring of cybersecurity vulnerabilities and attack vectors. The Attack Surface Monitoring Tool will automate the scanning of network assets, classifying open, closed and filtered ports and finding exposed services that an attacker could potentially use as part of an attack. By surprising actionable insights and suggested remediation(s), the Attack Surface Monitoring Tool could assist a security team in prioritizing and remediating vulnerabilities or security gaps before an attacker is able to exploit the vulnerability.

In terms of outcomes, this solution, which has the ability to enhance critical systems security, would periodically scan the networks identified in the inventory scan and provide the finding through a dashboard which is simple and intuitive to use. The modular architecture of the tool will allow the ability to add additional feature such as automate the schedule for scans, integrity and configuration checking, patch management integrations, or creating RESTful APIs for integrations with other parties and supporting both cloud.

Results

The Attack Surface Monitoring Tool was developed as a full-stack web application composed of a React-based front-end dashboard and a Python FastAPI back-end. Ultimately, the back-end uses the nmap utility for network scans. The front-end allows a user to enter their targets (e.g., scanme.nmap.org) and a range of ports for scanning. Once the user has entered their information and submitted the scan, the back-end component will first scan the targets, parse the results, and then send rich data structures back to the front-end to visualize the targets.

Workflow

1. The user enters their target(s) (i.e., scanme.nmap.org) and port range (i.e., 20-100).

2. The back-end runs a network scan using an nmap and identifies open ports, closed ports, filtered ports, and the services associated with each.

3. The scan results are returned to the front-end dashboard and are parsed to display on the front-end, including summary statistics, distributions of states of each port, and suggested remediation steps associated with any potential vulnerability that may have been identified.

The tool makes it easy to understand the security posture of any scanned assets. For instance, if someone scans scanme.nmap.org on ports 20 -100, they may see two ports (22, 80) were open, and others were filtered or closed. The dashboard clearly indicates the ports and may provide a recommendation if needed (i.e., disable any service that isn't used in production (as noted above) or update software that may be out of date).

Example Output:

- **Target:** scanme.nmap.org
- **Ports Scanned:** 1-1000 (Default)
- **Open Ports:** 22 (SSH), 25(SMTP), 80 (HTTP), 443 (HTTPS)
- **Filtered Ports:** 23, 25, 53, etc.
- **Closed Ports:** 70 (gopher)

Issues Found & Remediation (Summary)

1. Open SSH Port (22/tcp) – Weak SSH Config

- Disable weak ciphers/protocols.
- Require key-based authentication.
- Firewall rules restrict trusted IPs.
- Keep SSH updated.
- Disable root login if not needed.

2. Open SMTP Port (25/tcp) – Weak Default Credentials

- Remove weak/default credentials.
- Use a strong unique password.
- Use authentication & encryption (STARTTLS)
- Restrict trusted network access.
- Keep the SMTP server updated.

3. Open HTTP/HTTPS Ports (80/443) – SQL Injection Risk

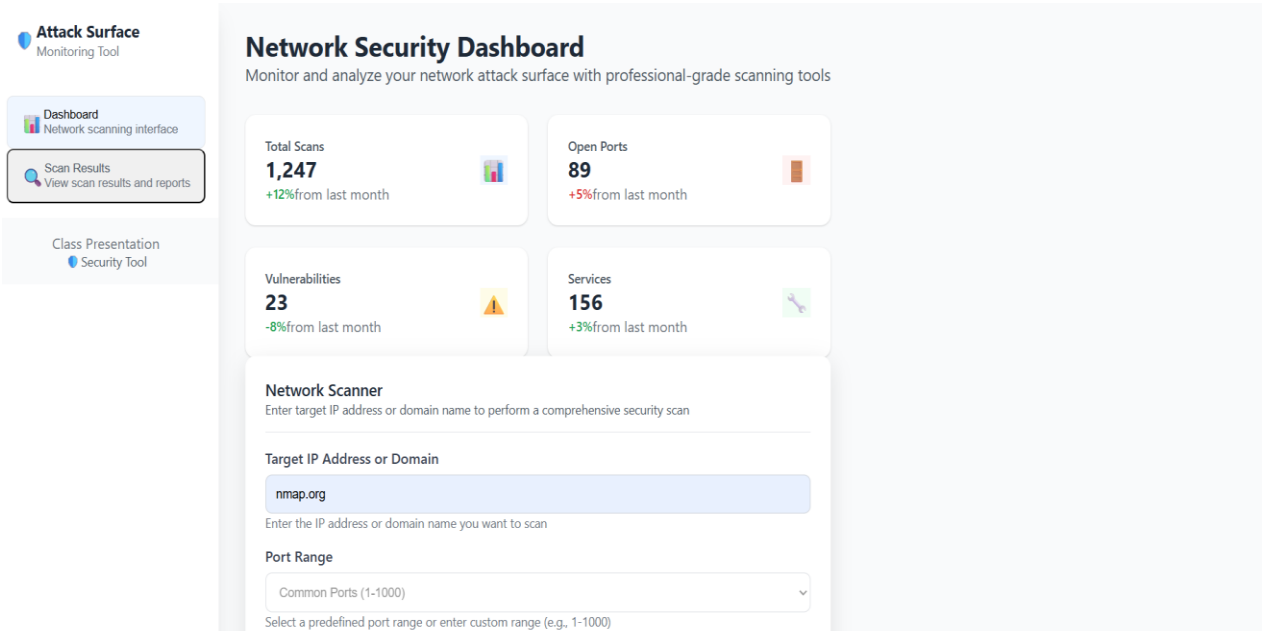
- Validate & sanitize inputs.
- Use parameterized queries/prepared statements.
- Regularly patch web server & framework software.
- Use a Web Application Firewall (WAF).
- Regularly penetration test.

4. General Recommendations

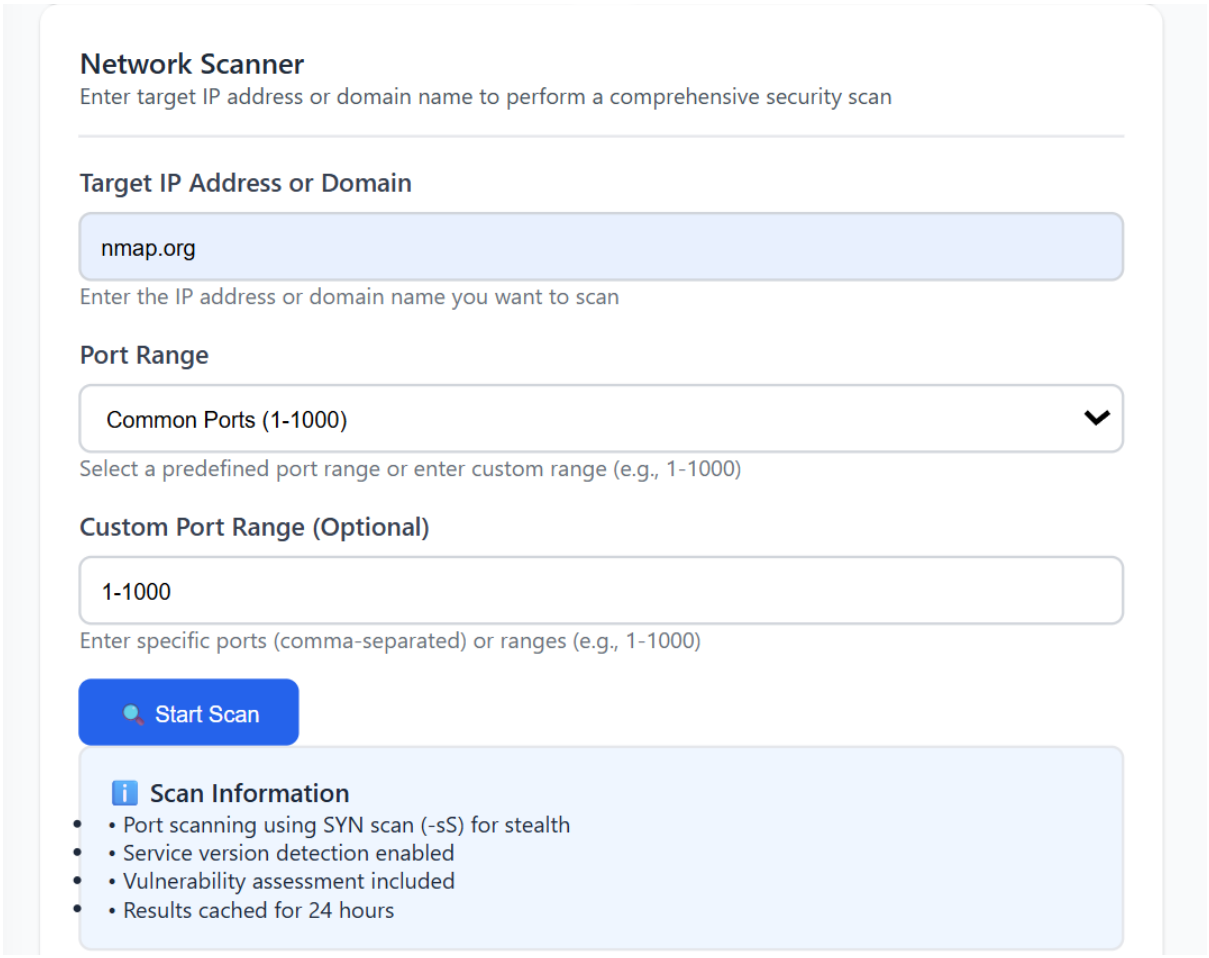
- Close/disable unused ports & services.
- Update firewall rules regularly.
- Review logs for suspicious activity.
- Apply security patches promptly.
- Remove unneeded software.

SCREENSHOTS :

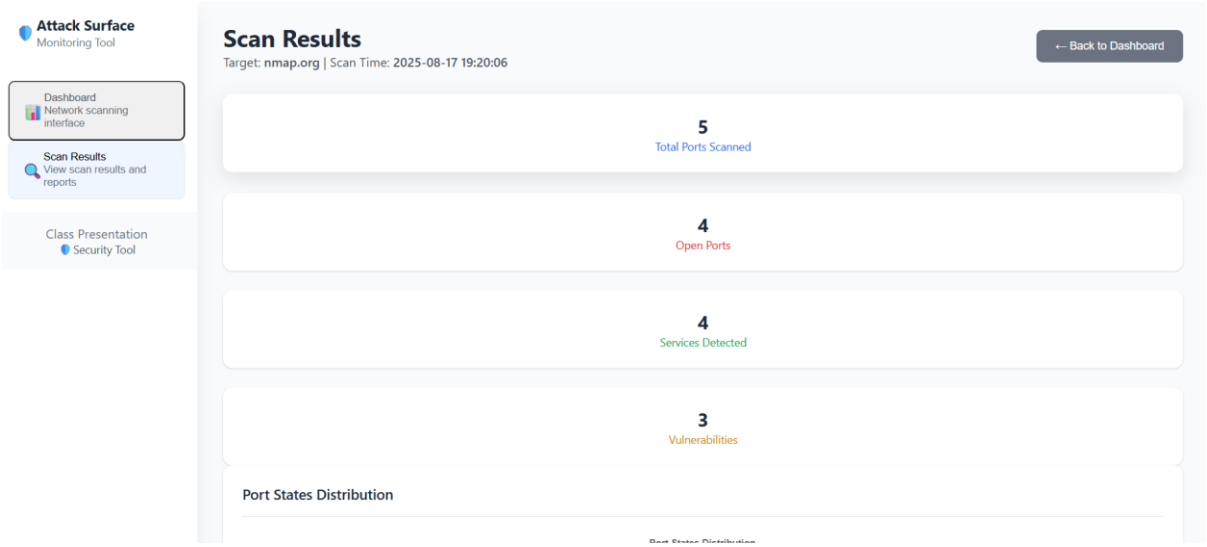
1) Monitoring Dashboard (Image 1)



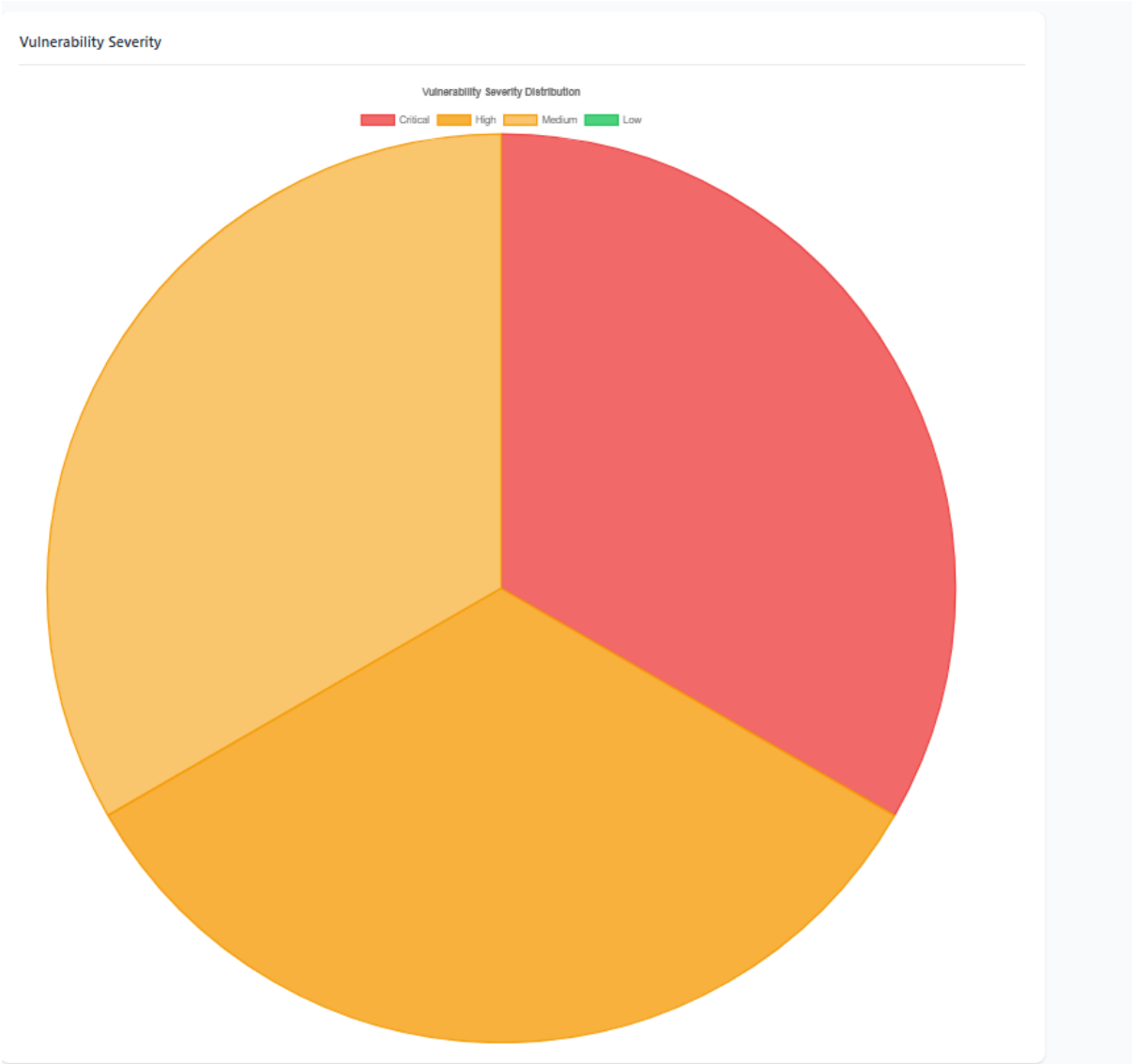
2) Network Scanner (Image 2)



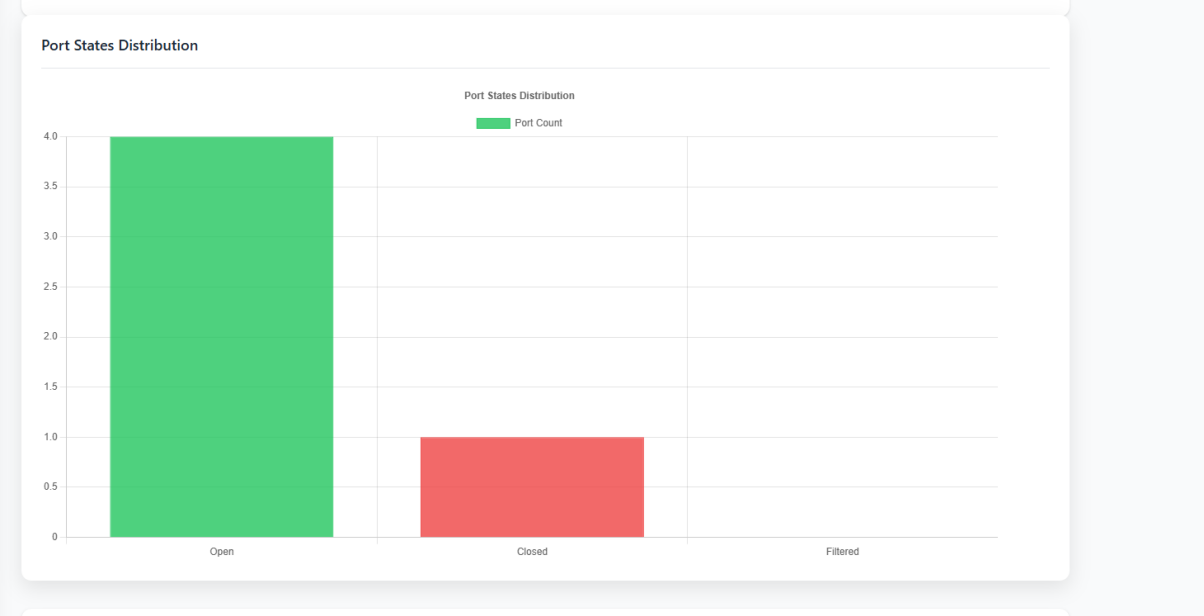
3) Scan Results (Image 3)



4) Vulnerability Severity (Image 4)



5) Port States Distribution Graph (Image 5)



6) Report of Open Port, Services and Vulnerability (Image 6)

Open Ports & Services

4 services detected on open ports

Port	Service	Version	Protocol	Status
22	SSH	Version 10.8	tcp	open
25	SMTP	Version 1.1	tcp	open
80	HTTP	Version 1.5	tcp	open
443	HTTPS	Version 4.2	tcp	open

Vulnerability Report

3 vulnerabilities detected

Weak SSH Configuration — Medium CVSS: 6.8
CVE: CVE-2023-5678
Description:
SSH service allows weak authentication methods and outdated protocols.
Affected Service:
SSH (Port 22)
Recommendation:
Disable weak ciphers and enforce strong authentication.

SQL Injection in Web Application — High CVSS: 8.5
CVE: CVE-2023-1234
Description:
The web application is vulnerable to SQL injection attacks through user input fields.
Affected Service:
HTTP (Port 25)
Recommendation:
Implement input validation and use parameterized queries.

Default Credentials — Critical CVSS: 9.1
CVE: CVE-2023-9012
Description:
Service is running with default or easily guessable credentials.
Affected Service:
Telnet (Port 80)
Recommendation:

7) Port Scan Status (Image 7)