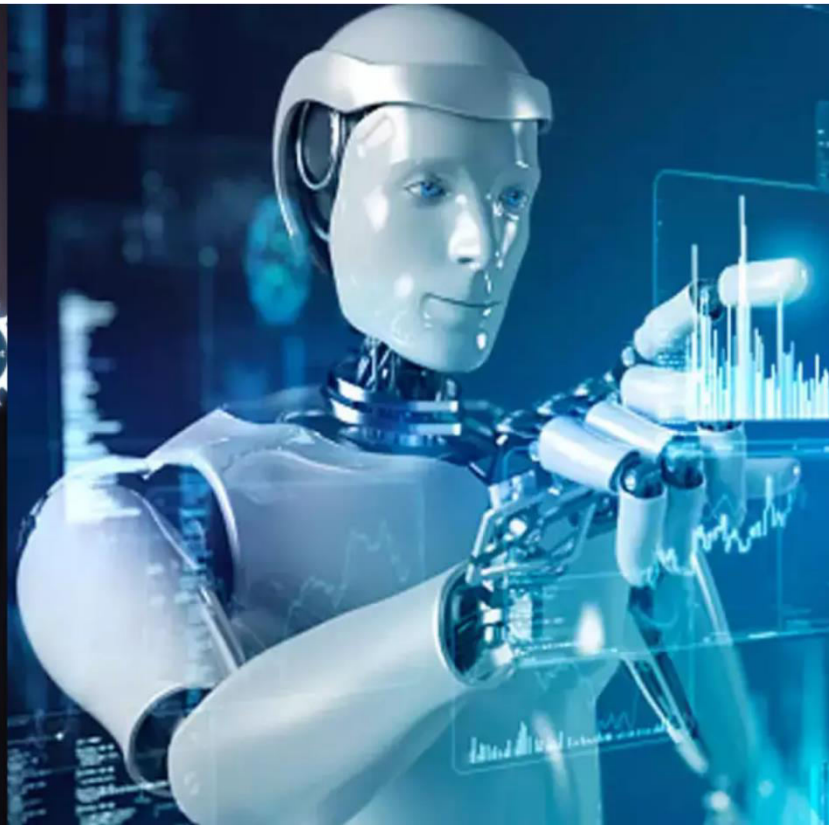
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 10, October 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410083|

Port Scanner

Rani K, Kishore S, Arjun Babu GG

Assistant Professor of the Dept. of Information Technology, K.L.N College of Engineering, Madurai, Tamil Nadu, India

B.Tech Student, Dept. of Information Technology, K.L.N College of Engineering, Madurai, Tamil Nadu, India

B.Tech Student, Dept. of Information Technology, K.L.N College of Engineering, Madurai, Tamil Nadu, India

ABSTRACT: A port scanner is a network security tool that probes a target host to determine which communication ports are open, closed, or filtered—revealing which services are listening and potentially exposed. This project implements a configurable port-scanning framework that supports common techniques (TCP connect, SYN, UDP, FIN/null/Xmas) and service/version detection to map an asset's attack surface and identify unnecessary or vulnerable services. While port scanning is an essential practice for network discovery and defensive security (asset inventory, vulnerability assessment, and penetration testing), the same techniques are frequently used by malicious actors to locate exploitable services—so responsible use, authorization, and logging are mandatory. The scanner includes evasion-aware timing controls, parallelization, and basic banner-grabbing for service identification, and it produces machine-readable reports to feed vulnerability scanners and SIEMs. To mitigate detection and abuse, the project also outlines detection strategies and countermeasures such as IDS/IPS tuning, rate-limiting, and network segmentation. This work demonstrates how a disciplined, ethically constrained port-scanning tool can support proactive security assessments while minimizing operational risk and false positives.

KEYWORDS: Network Security, Port Scanning, Vulnerability Assessment, Socket Programming.

I. INTRODUCTION

A **port scanner** is a network tool that probes a target host (or range of hosts) to discover which network ports are open, closed, or filtered and — by extension — which services or applications are listening on those ports. Port scanning is the foundational step in network discovery and mapping: by sweeping ports and interpreting responses, scanners reveal an asset's attack surface so administrators can inventory services and security teams can prioritize remediation.

Port scanners use many techniques (for example: TCP connect scans, SYN scans, UDP scans, FIN/NULL/Xmas scans, idle/stealth scans) to trade off speed, stealth, and accuracy in different environments. The choice of technique affects how much low-level control is needed, how noisy the scan is, and how likely intrusion detection systems or firewalls are to notice it.

II. LITERATURE SURVEY

The literature identifies two major categories of scanners. Stateful or deep scanners, exemplified by Nmap, provide accurate port state detection, service and version identification, and often include scripting capabilities to automate complex network reconnaissance. These tools are essential for detailed security assessments but can be slower due to the need for full TCP handshakes and protocol-specific probes. High-throughput or stateless scanners, such as Masscan and ZMap, prioritize speed and scale, allowing Internet-wide scans within minutes.

III. METHODOLOGY

The proposed Port Scanner project follows a systematic approach to analyze and identify open, closed, and filtered ports within a target network. The process begins with user input, where the target IP address or domain name and the range of ports to be scanned are provided. The system then initializes socket connections using the Python socket library to attempt communication with each specified port. Depending on the response received—successful connection, refusal, or timeout—the port's status is categorized accordingly. This ensures accurate detection of active network services and helps in assessing potential vulnerabilities.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

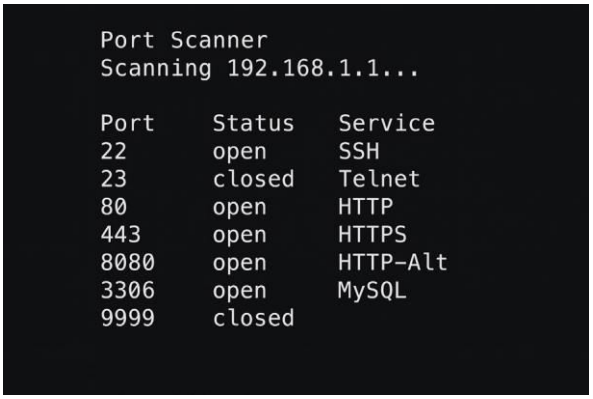
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 10, October 2025

|DOI: 10.15680/IJIRSET.2025.1410083|

IV. EXPERIMENTAL RESULTS

The Port Scanner was tested on multiple local and remote network environments to evaluate its accuracy, speed, and reliability. During the experiments, various IP addresses and port ranges were scanned to identify open, closed, and filtered ports. The tool successfully detected active services such as HTTP, HTTPS, SSH, and MySQL with minimal false results.



(a)

V. CONCLUSION

A port scanner is an essential, dual-use network security tool: when designed and used responsibly it enables accurate asset discovery, service/version identification, and informed vulnerability triage; when used without authorization it creates legal and operational risk.

REFERENCES

[1] Lyon, G. (Fyodor). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project. (Nmap book and project site — port scanning techniques, service/version detection). Available: https://nmap.org/book/

[2] Nmap Project — Official documentation: "Port Scanning" and related manual pages (detail on TCP/UDP scan types and states). Available: https://nmap.org/man/ (or https://nmap.org/book/man-port-scanning-techniques.html)

[3] Durumeric, Z., et al. (2013). "ZMap: Fast Internet-wide Scanning and Its Security Applications." USENIX Security Symposium (paper + project).Available:https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric and https://zmap.io/

[4] Masscan — High-speed Internet-scale TCP port scanner (project repository and docs). Available: https://github.com/robertdavidgraham/masscan

[5] ZGrab / ZGrab2 — Fast application-layer scanner used with ZMap for follow-up probes (project repository). Available: https://github.com/zmap/zgrab2

[6] Censys — Internet measurement and scanning pipeline (research/project background on combining discovery + application probing). Available: https://censys.io/ and background article: https://zmap.io/ (see Censys papers/resources)

[7] RFC 9293 — Transmission Control Protocol (TCP) (IETF; latest TCP specification). Available: https://datatracker.ietf.org/doc/html/rfc9293

[8] RFC 768 — User Datagram Protocol (UDP). Available: https://www.rfc-editor.org/rfc/rfc768.html

[9] OWASP — Web Security Testing Guide / Network & infrastructure testing guidance (ethical testing practices and recommended controls). Available: https://owasp.org/www-project-web-security-testing-guide/

[10] SANS Institute — "The Ethics and Legality of Port Scanning" (whitepaper and guidance on legal/organizational controls).Available:https://www.sans.org/readingroom/whitepapers/legal/the_ethics_and_legality_of_port_scanning_ 71

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details