IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network Scanner

[1]Chris Gonsalves, [2]Soni Vishwakarma, [3]Sharon Gaspar, [4]Erica D’Cruz, [5]Prof. Nilambari Narkar

[1]U.G. Student, [2]U.G. Student, [3]U.G. Student, [4]U.G. Student, [5]Assistant Professor
[1]Department of Computer Engineering,
[1]Xavier Institute of Engineering, Maharashtra, India

Abstract: The evolution of network security tools has enabled us to address vulnerabilities in innovative ways. Our project focuses on developing a Python-based Network Scanner that enhances network security by providing essential functionalities such as port scanning, local network scanning, and intrusion detection. By leveraging a user-friendly interface, this tool simplifies the process of identifying open ports and discovering devices within a network. Our aim is to automate device discovery and improve operational efficiency while enabling real-time monitoring of network health. This project is designed to empower users with accessible and effective solutions for safeguarding their networks.

***Index Terms* - Port Scanning, Local Area Network (LAN), Intrusion Detection, User Datagram Protocol (UDP), Address Resolution protocol (ARP), Scan Detection System (SDS), Time-to-live (TTL).**

I. INTRODUCTION

The exponential growth of interconnected devices and networks has drastically heightened the need for effective network security measures. Modern cybersecurity threats demand tools that are efficient, accessible, and adaptable. Current solutions often require advanced expertise, making them inaccessible to a wider audience.

This project introduces a Python-based network security tool designed to simplify essential security tasks, including port scanning, local network scanning, and intrusion detection. By providing a user-friendly interface, the tool empowers users with varying levels of technical expertise to safeguard their networks. The focus is on creating an accessible, cost effective, and scalable solution to address the challenges posed by evolving network environments.

The significance of the project lies in its ability to detect and manage network intrusions effectively. The system is designed to monitor network traffic, identify anomalies, and distinguish between normal and malicious activities. This is crucial for maintaining network security, preventing unauthorized access, and ensuring the integrity of data within a network. Port scanning and local network scanning are integral components of the system. Port scanning allows the tool to identify open, closed, and filtered ports on devices within the network, helping to detect potential vulnerabilities. Local network scanning enables the discovery of devices on the network, providing detailed information such as IP addresses, MAC addresses, and device names. This helps in mapping the network layout and identifying unauthorized devices. By providing real-time feedback and alerts, the system helps network administrators respond promptly to potential threats, minimizing the risk of security breaches. The integration of advanced technologies such as machine learning and IoT enhances the system’s adaptability and accuracy, making it a valuable tool for safeguarding network environments. Overall, the project represents a significant step toward improving network security, protecting sensitive information from cyber threats, and ensuring a safer and more accessible network environment.

II. RESEARCH METHODOLOGY

2.1 Selection of Research Papers

The selection process targeted peer-reviewed studies published in journals and conferences, emphasizing assistive technologies such as identifying port scanning, local network scanning (LAN), and detection of malicious activity, these tools enhance the capabilities of network administrators and improve overall network security The user-friendly interfaces make them accessible to both experts and beginners, allowing for easy customization of scan parameters. However, feedback from users highlights the need for better handling of large file transfers and optimization for larger networks to improve overall usability and performance, thus, papers focusing on these identified limitations were prioritized for detailed examination. Therefore, studies addressing these specific technical and usability challenges were given precedence in the review.

2.2 Data Extraction and Categorization

Key information from each research paper was extracted and categorized into the following sections:

- **Findings**: Key achievements, technological advancements, and system functionalities.
- **Research Gaps**: Limitations identified in the studies, including usability challenges, dataset constraints, and optimization issues.
- **Future Work Suggestions**: Recommendations proposed by authors for addressing existing gaps and enhancing system performance.

2.3 Thematic Analysis

The extracted data highlight advancements in network security tools, showcasing efficient and user-friendly solutions for identifying open ports, LAN scanners and Intrusion Detection. However, challenges such as potential misuse, resource intensity, and hardware requirements limit scalability and usability. User feedback is positive, but improvements are needed for large file transfers and network optimization. Integrating advanced technologies like multithreading and contrastive learning enhances tool capabilities, but further research is needed to address resource usage and scalability challenges.

2.4 Comparative Evaluation

A comparative evaluation was conducted to assess the strengths and limitations of various solutions proposed in the reviewed papers. Network security tools provide efficient and user-friendly solutions for identifying open ports and detecting network errors. However, they face challenges like potential misuse, resource intensity, and hardware requirements. Advanced technologies such as multithreading and contrastive learning enhance their capabilities, but further research is needed to address scalability and usability issues.

2.5 Synthesis and Reporting

Python-based network security tools, such as open port scanners and LAN scanners, provide efficient and user-friendly solutions for identifying open ports, detecting network errors and malicious activity. These tools benefit from advanced technologies like multithreading and contrastive learning, enhancing their capabilities. However, challenges such as potential misuse, resource intensity, and hardware requirements remain. Further research is needed to address scalability and usability issues to improve overall performance and user experience. This methodology ensures a structured and thorough examination of existing research, enabling the identification of critical gaps and opportunities for advancing assistive technologies.

III. RESULTS AND DISCUSSION

3.1 Results of Functional Performance and Validation

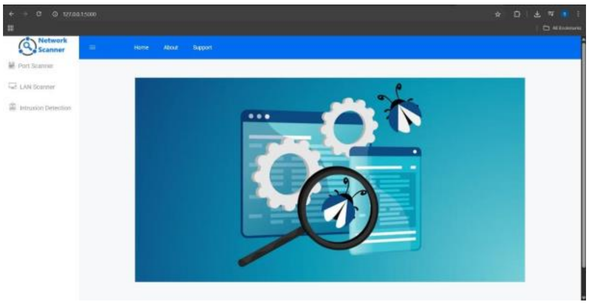
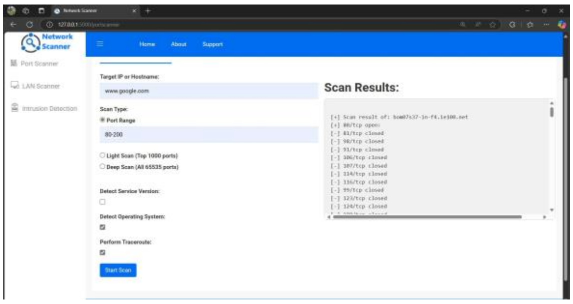


Figure 3.1: Home Page

Figure 3.1 shows the Home page of the Network Scanner application. This page includes a Top Menu (Home, About & Support) and a left menu (Port Scanner, LAN Scanner & Intrusion Detection). These menus help users navigate between different modules easily and access the desired functionality based on their requirements.



Target IP or Hostname: www.google.com

Scan Type:

● Port Range

80-200

○ Light Scan (Top 1000 ports)

○ Deep Scan (All 65535 ports)

Detect Service Version: □

Detect Operating System: ☑

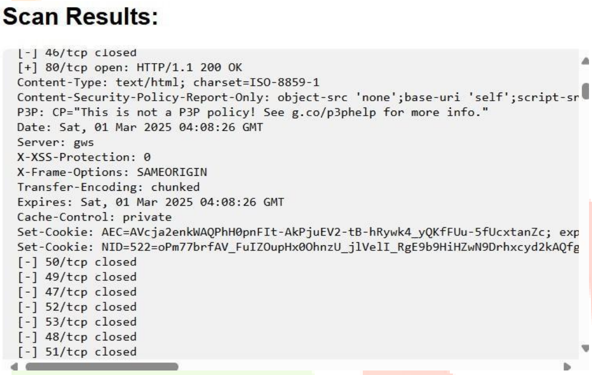
Perform Traceroute: ☑

Scan Results:

```
[+] Scan result of: bom07s37-in-f4.1e100.net
[+] 80/tcp open:
[-] 81/tcp closed
[-] 90/tcp closed
[-] 91/tcp closed
[-] 106/tcp closed
[-] 107/tcp closed
[-] 114/tcp closed
[-] 116/tcp closed
[-] 99/tcp closed
[-] 123/tcp closed
[-] 124/tcp closed
```

Figure 3.2: Port Scanner

Figure 3.2 shows the interface of Port Scanner. Identifies open ports, detects and retrieves OS and traceroute details for given IP addresses.

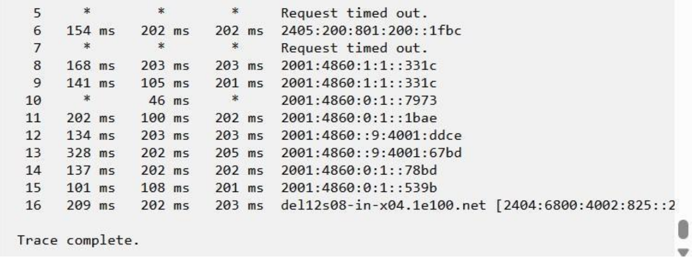


Scan Results:

```
[-] 46/tcp closed
[+] 80/tcp open: HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-sr
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Sat, 01 Mar 2025 04:08:26 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Expires: Sat, 01 Mar 2025 04:08:26 GMT
Cache-Control: private
Set-Cookie: AEC=AVcja2enkWAQPhH0pnFIt-AkPjuEV2-tB-hRywk4_yQKfFUu-5fUcxtanZc; exp
Set-Cookie: NID=522=oPm77brfAV_FuIZOupHx0OhnzU_jlVelI_RgE9b9HiHZwN9Drhxcyd2kAQfg
[-] 50/tcp closed
[-] 49/tcp closed
[-] 47/tcp closed
[-] 52/tcp closed
[-] 53/tcp closed
[-] 48/tcp closed
[-] 51/tcp closed
```

Figure 3.3: Port Scanner - Service Version Output

Figure 3.3 shows Port Scanner- Service Version Output. Identifies the Service Version of the open port numbers and displays the details.

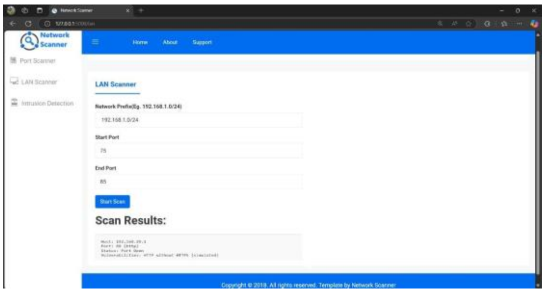


```
  5     *        *        *     Request timed out.
  6   154 ms   202 ms   202 ms  2405:200:801:200::1fbc
  7     *        *        *     Request timed out.
  8   168 ms   203 ms   203 ms  2001:4860:1:1::331c
  9   141 ms   105 ms   201 ms  2001:4860:1:1::331c
 10     *       46 ms     *     2001:4860:0:1::7973
 11   202 ms   100 ms   202 ms  2001:4860:0:1::1bae
 12   134 ms   203 ms   203 ms  2001:4860::9:4001:ddce
 13   328 ms   202 ms   205 ms  2001:4860::9:4001:67bd
 14   137 ms   202 ms   202 ms  2001:4860:0:1::78bd
 15   101 ms   108 ms   201 ms  2001:4860:0:1::539b
 16   209 ms   202 ms   203 ms  del12s08-in-x04.1e100.net [2404:6800:4002:825::2

Trace complete.
```

Figure 3.4: Port Scanner- OS & Traceroute Results Output

Figure 3.4 shows Port Scanner - OS & Traceroute Results Output. Identifies the **OS & Traceroute** of the given Domain/IP address and displays the details.



LAN Scanner

Network Prefix(Eg. 192.168.1.0/24)

192.168.1.0/24

Start Port

75

End Port

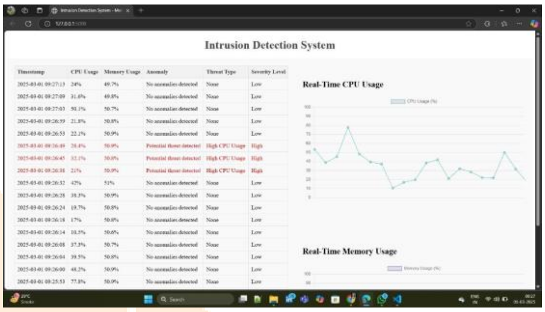
85

Scan Results:

```
Host: 192.168.29.1
Port: 80 (http)
Status: Port Open
Vulnerabilities: HTTP without HTTPS (simulated)
```

Figure 3.5: LAN Scanning

Fig. 3.5 shows the interface of the LAN Scanner. The local network detection(LAN) feature displays the vulnerabilities of all connected devices along with their IP addresses within the specified range.



Intrusion Detection System

Timestamp	CPU Usage	Memory Usage	Anomaly	Threat Type	Severity Level
2025-03-01 09:27:13	24%	49.7%	No anomalies detected	None	Low
2025-03-01 09:27:09	31.6%	49.8%	No anomalies detected	None	Low
2025-03-01 09:27:03	50.1%	50.7%	No anomalies detected	None	Low
2025-03-01 09:26:59	21.8%	50.8%	No anomalies detected	None	Low
2025-03-01 09:26:53	22.1%	50.9%	No anomalies detected	None	Low
2025-03-01 09:26:49	28.4%	50.9%	Potential threat detected	High CPU Usage	High
2025-03-01 09:26:45	32.1%	50.8%	Potential threat detected	High CPU Usage	High
2025-03-01 09:26:38	21%	50.9%	Potential threat detected	High CPU Usage	High
2025-03-01 09:26:32	42%	51%	No anomalies detected	None	Low
2025-03-01 09:26:28	38.3%	50.9%	No anomalies detected	None	Low
2025-03-01 09:26:24	19.7%	50.8%	No anomalies detected	None	Low
2025-03-01 09:26:18	17%	50.8%	No anomalies detected	None	Low
2025-03-01 09:26:14	10.5%	50.6%	No anomalies detected	None	Low
2025-03-01 09:26:08	37.3%	50.7%	No anomalies detected	None	Low
2025-03-01 09:26:04	39.5%	50.8%	No anomalies detected	None	Low
2025-03-01 09:26:00	48.2%	50.9%	No anomalies detected	None	Low
2025-03-01 09:25:53	77.8%	50.9%	No anomalies detected	None	Low

Figure 3.6: Intrusion Detection System

Figure 3.6 shows the output of the Intrusion Detection System. This module was able to capture and display real-time alerts for suspicious or abnormal activities & also shows the Real Time CPU and Memory usage.

IV ACKNOWLEDGMENT

We would like to express our sincere gratitude to Prof. Nilambari Narkar for her invaluable guidance, mentorship, and continuous support throughout this research. We also thank the Department of Computer Engineering at Xavier Institute of Engineering, Mumbai, for providing the necessary resources for this study.

.

REFERENCES

[1] Kensuke Fukuda and John Heidemann. “Detecting Malicious Activity with DNS Backscatter”. In International Conference on Communications, Control, and Computing (ICCCC) IEEE 2021.

[2] Goni and Osman. “Implementation of Local Area Network (LAN) and Build a Secure LAN System for Atomic Energy Research Establishment (AERE)”. In International Journal of Modern Communication Technologies Research (IJMCTR), 2020.

[3] Xueying Han et al. “ContraMTD: An Unsupervised Malicious Network Traffic Detection Method Based on Contrastive Learning”. In IEEE International Conference on Communications, Control, and Computing (ICCCC), IEEE. 2021.

[4] Jafar Haadi Jafarian, Masoumeh Abolfathi, and Mahsa Rahimian. “In Detecting Network Scanning Through Monitoring and Manipulation of DNS Traffic”. In International Conference on Communications, Control, and Computing (ICCCC), IEEE 2021.

[5] K˝ov´ari et al. “Area Scanning with Reinforcement Learning and MCTS in Smart City Applications”. In: International Journal of Modern Communication Technologies Research (IJMCTR) 2020.

[6] Shehab et al. “Improving Port Scan Cybersecurity Risks Detection Using Features Selection Techniques with ML Algorithms”. In: Journal of Theoretical and Applied Information Technology 2024.

[7] Theofanous et al. “Fingerprinting the Shadows: Unmasking Malicious Servers with Machine Learning-Powered TLS Analysis”. In ACM Web Conference 2024.

[8] Nmap Security Scanner. “Nmap: The Network Mapper– Free Security Scanner for Network Exploration & Security Audits.” In https://nmap.org, 2024.

[9] Yaniv Miron et al. “Port Scanning Detection Techniques and Algorithms in Cybersecurity.” In International Journal of Computer Applications, Volume 182, No. 20, 2019.

[10] Hafeez Anwar, Zubair Baig, and Sherali Zeadally. “Network Scanning Techniques and the Detection of Scanners.” In IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 843–867, 2020.

[11] Muhammad Rizwan, Imran Khan, and Tauseef Rana. "A Comparative Study of Network Scanning Tools: Nmap, Angry IP Scanner, and Advanced IP Scanner." In International Journal of Computer Applications, vol. 182, no. 4, 2021.

[12] S. Dhanalakshmi and M. Padmavathi. "Detection of Network Scanners Using Machine Learning Techniques." In International Journal of Computer Science and Information Security (IJCSIS), vol. 18, no. 5, 2021.

[13] Qasem Abu Al-Haija et al. "A Survey of Network Scanning Tools: Scope, Capabilities, and Performance." In Journal of Network and Computer Applications, vol. 163, 2020.

[14] I. S. Al-Shaikhli and A. S. Hasan. "Evaluation and Analysis of Popular Network Scanning Tools." In International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 2, 2020.

[15] Asim Qayyum et al. "Network Security Threats and Countermeasures in the Context of Scanning Attacks." In IEEE Access, vol. 10, pp. 45021–45042, 2022.

[16] Yash Mehta, Sneha Rathi, and Rohan Sharma. "Intelligent Port Scanning Detection Using Supervised Machine Learning." In Proceedings of the International Conference on Cybersecurity Trends (ICCT), IEEE, 2023.