

PROFESSIONAL TRAINING REPORT - II

entitled

ProbCraft: Crafting Your Own Network Port Probing

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering with
Specialization in Cyber Security

by

**P NITHIN KUMAR [41614067]
PALERU VENKATESH [41614066]
CHUNDURU T V PRASANNA SRIDEVI [41614015]**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A++" by NAAC

**JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119**

MAY 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of **Mr. P NITHIN KUMAR (41614067)** who carried out the project entitled "**ProbCraft: Crafting Your Own Network Port Probing**" under my supervision from January 2024 to May 2024.

Internal Guide

Dr. D. Anu Disney, M.E., Ph.D.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 07/05/24

Internal Examiner

External Examiner

DECLARATION

I **Mr. P NITHIN KUMAR (41614067)** hereby declare that the Professional Training Report-II entitled "**ProbCraft: Crafting Your Own Network Port Probing**" done by me under the guidance of **Dr. D. Anu Disney, M.E., Ph.D.**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with Specialization in Cyber Security.

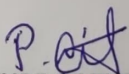
I would like to thank to **Dr. T. Sathish M.E., Ph.D.**, Dean, School of Computing, Dr. S. Sridharan M.E., Ph.D., Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive review.

I would like to express my sincere and deep sense of gratitude to my mentor, **Dr. D. Anu Disney, M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement, which paved way for the successful completion of my advanced professional training.

I would like to express my thanks to all Teaching and Non-teaching staff members of the Department of Computer Science and Engineering who were helpful in every way for the completion of the project.

DATE: 07/05/24

PLACE: Chennai


SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D., Dean, School of Computing, Dr. S.Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Dr. D. Anu Disney, M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

COURSE CERTIFICATE



Elite

NPTEL Online Certification

(Funded by the MoE, Govt. of India)



This certificate is awarded to

P NITHIN KUMAR

for successfully completing the course

Cloud Computing and Distributed Systems

with a consolidated score of **73** %

Online Assignments	20/25	Proctored Exam	52.5/75
--------------------	-------	----------------	---------

Total number of candidates certified in this course: **3244**

Prof. B. V. Ratish Kumar
Chairman, Centre for Continuing Education
IIT Kanpur

Jan-Mar 2024

(8 week course)

Prof. Satyaki Roy
NPTEL Coordinator
IIT Kanpur



Indian Institute of Technology Kanpur



Roll No: NPTEL24CS09S344100375

To verify the certificate



No. of credits recommended: 2 or 3

ABSTRACT

Port scanning is a fundamental aspect of network reconnaissance, pivotal in network security and system administration. It enables users to meticulously survey target systems for accessible ports, providing insights into potential vulnerabilities. The primary objective of this project is to architect a robust, command-line port scanning tool using Python, to be shared on GitHub for public access. This tool operates by accepting an IP address as input and conducting a comprehensive scan to unearth all open ports associated with the specified IP. The implementation leverages the socket and threading libraries, pivotal components in network programming. The socket library facilitates the establishment of TCP/IP connections, essential for port probing, while threading optimizes performance through parallel processing, significantly enhancing scanning efficiency. This concurrent execution strategy mitigates bottlenecks inherent in sequential scanning methods, thereby accelerating the discovery of open ports. The dynamism of modern cybersecurity landscapes necessitates proactive measures to fortify network defenses. This project not only addresses the exigency for effective port scanning tools but also underscores the imperative of network security awareness. By delving into the intricacies of port scanning methodologies within the Python ecosystem, it fosters a deeper understanding of network vulnerabilities and risk mitigation strategies. The port scanning tool developed herein extends beyond rudimentary scanning paradigms, integrating sophisticated techniques to ascertain not only open ports but also detailed insights into services running on target hosts. It boasts a user-friendly interface coupled with robust reporting functionalities, empowering network administrators and security professionals with actionable intelligence to discern and remediate vulnerabilities promptly. This initiative embodies a commitment to a secure digital milieu, characterized by resilience against evolving cyber threats.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	vi
	LIST OF FIGURES	viii
1	INTRODUCTION	1
	1.1 Overview	
	LITERATURE SURVEY	3
2	2.1 survey	
	2.2 Existing System	6
3	REQUIREMENTS ANALYSIS	
	3.1 Objective	15
	3.1 Requirements	16
	3.2.1 Hardware Requirements	16
	3.2.2 Software Requirements	16
4	DESIGN DESCRIPTION OF PROPOSED PRODUCT	
	Proposed methodology	
	4.1.1 Ideation Map/Architecture Diagram	17
4.1	4.1.2 Phases of Port Scanning Process	20
	4.1.3 Internal or Component Design Structure	22
	Features	
	4.2.1 NOVELTY OF THE PROPOSAL	23
4.2	4.2.2 Benefits	24
	4.2.3 Future Scope	25
5	CONCLUSION	26
	REFERENCES	27
6	APPENDIX	
	A. Research Paper	29
	B. Source code	38

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
4.1	System architecture	18
4.2	Common Ports and Services	19
4.3	Flowchart of Working of Port Scanner	21
4.4	Working Principles	22
B.1	Importing Packages	40
B.2	Implementing Port Scanner	40
B.3	Specific Port Scanning	41
B.4	Scanning All the Ports	41
B.5	Scanning Complete	42

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Port scanning is a fundamental technique used by network administrators, security professionals and ethical hackers to examine the accessibility of network services on a target system. The objective of this project is to create a port scanner using python as it is going to be a command line tool which is user-friendly and efficient tool that can probe a wide range of network ports on a given IP address uncovering open ports. Using python as the programming language of choice as it has huge list of libraries from which we are seeking socket and threading that we have used. This project aims to be a valuable asset for both professional and enthusiasts in the field of cybersecurity and network administration. The project serves as valuable resource enhancing network security and gaining a better understanding of vulnerabilities in your network.

Challenges and Limitations

- **Scalability and Elasticity:** As networks scale and evolve, the ability to scale scanning operations and adapt to changing network conditions becomes critical. Ensuring that scanning infrastructure can scale horizontally to accommodate growing network environments and dynamically adjust scanning parameters based on network elasticity requires robust architecture design and automation.
- **Network Complexity:** Modern networks often consist of diverse architectures, including cloud environments, virtualized infrastructure, and IoT devices. Managing and scanning these complex network environments can be challenging, as they may involve dynamic IP addresses, network segmentation, and heterogeneous systems with varying levels of accessibility.
- **Authentication and Credential Management:** Vulnerability scanning often requires authentication credentials to access target systems and perform authenticated scans. Managing and securely storing these credentials, especially in large-scale environments with numerous systems and accounts, presents challenges in terms of confidentiality, integrity, and access control.

Addressing these challenges and limitations requires a combination of technical solutions, operational best practices, and organizational policies to ensure effective integration of port scanning with vulnerability scanning for enhanced network security.

Ethical Considerations:

Ethical considerations play a crucial role in conducting port scanning with vulnerability scanning to ensure responsible and lawful use of these techniques. Here are some key ethical considerations:

- **Permission and Authorization:** Obtain explicit permission and authorization from the owner or administrator of the target network before conducting any scanning activities. Unauthorized scanning can be considered intrusive and may violate laws and regulations governing network security and privacy.
- **Data Privacy and Confidentiality:** Respect the privacy and confidentiality of sensitive information collected during scanning, such as IP addresses, system configurations, and vulnerability data. Handle and store scan results securely, and ensure compliance with applicable data protection regulations.
- **Responsible Disclosure:** If vulnerabilities are discovered during scanning, follow responsible disclosure practices by promptly notifying the affected parties and providing them with actionable recommendations for remediation. Avoid publicly disclosing vulnerabilities or exploit details until appropriate patches or mitigations are available.
- **Education and Awareness:** Promote education and awareness about ethical considerations in port scanning and vulnerability scanning among security professionals, researchers, and practitioners. Foster a culture of ethical behavior and responsible use of scanning techniques to uphold ethical standards in the cybersecurity community.

CHAPTER 2

LITERATURE REVIEW

2.1 SURVEY

A literature review or survey of a CLI-based port scanner developed using Python encompasses an exploration of existing research, projects, and tools in the domain of network scanning and port analysis. The various port scanning techniques such as TCP, UDP, SYN and more that are commonly used. Currently available tools are NMAP, SCAPY and more. Frameworks like click or ARGPARSE are used in Creating CLI interface. Libraries that are used in port scanning generally are socket, threading, pyfiglet. Parallel scanning, Asynchronous Programming are used to minimize the use of network resources. Port scanning is a network reconnaissance technique used to discover open, closed, or filtered ports on a target computer or network device. It involves sending network requests to various network ports to determine which ports are active and responding to the requests. Port scanning serves several important purposes in the field of computer networking and security.

Here's a continuation of the literature review:

Introduction to Network Port Probing:

Network port probing, a fundamental practice in cybersecurity, plays a pivotal role in identifying potential vulnerabilities within networked systems. It involves the systematic exploration of network devices to uncover open ports, which serve as entry points for communication between devices. The significance of port probing lies in its ability to uncover weaknesses in network configurations, thereby enabling proactive measures to strengthen cybersecurity defences. As the digital landscape continues to evolve, understanding the intricacies of network port probing becomes increasingly critical for both offensive and defensive cybersecurity strategies.

Historical Overview:

The historical evolution of network port probing traces back to the nascent stages of computer networking when rudimentary tools were used to scan for open ports and services. Early methods such as simple TCP connect scans provided basic insights into network topology but

lacked sophistication. Over time, advancements in networking technology and cybersecurity practices spurred the development of more refined port scanning techniques. The advent of SYN scans, pioneered by researchers like Fyodor Vaskovich with the creation of Nmap, revolutionized the field by introducing stealthier and more efficient scanning methods. Subsequent innovations, including UDP scanning and application-layer probing, further expanded the arsenal of techniques available to both attackers and defenders.

Technical Foundations:

A deeper exploration of the technical foundations underlying network port probing reveals the intricacies of TCP/IP protocols and port classifications. The TCP/IP protocol suite governs communication between devices on the internet, with TCP and UDP serving as the primary transport layer protocols. Ports, identified by numerical values, facilitate the exchange of data between applications running on networked devices. Understanding the nuances of TCP handshake mechanisms, such as SYN, SYN-ACK, and ACK, is essential for comprehending the inner workings of port scanning techniques. Different scanning methodologies, including TCP connect scans, SYN scans, UDP scans, and stealth scans, leverage these protocol intricacies to varying degrees, each offering distinct advantages and limitations.

Applications and Use Cases:

The applications of network port probing extend across a spectrum of offensive and defensive cybersecurity practices. Malicious actors leverage port scanning techniques to identify potential targets for exploitation, probe for vulnerable services, and gather intelligence for targeted attacks. In contrast, network administrators employ port scanning tools as part of vulnerability assessments, penetration testing, and network reconnaissance activities. By systematically scanning networked devices for open ports and services, organizations can identify security weaknesses, prioritize remediation efforts, and bolster their overall security posture. Real-world examples underscore the critical role of port scanning in uncovering vulnerabilities, detecting unauthorized access attempts, and mitigating potential threats.

Countermeasures and Defence Strategies:

As the prevalence of port scanning attacks continues to rise, organizations must implement robust countermeasures and defence strategies to safeguard their networks. Firewall configurations, both at the perimeter and internal network levels, play a pivotal role in

controlling traffic flow and blocking unauthorized port access. Intrusion detection and prevention systems (IDPS) leverage signature-based and anomaly-based detection mechanisms to identify and thwart port scanning attempts in real-time. Network segmentation, access control policies, and regular security audits further enhance resilience against port probing attacks. However, effective defence against port scanning requires a multi-layered approach that integrates technological solutions with proactive threat intelligence and user education initiatives.

Ethical and Legal Considerations:

Ethical and legal considerations surrounding network port probing pose significant challenges for cybersecurity practitioners and researchers alike. While port scanning tools are indispensable for security testing and vulnerability assessment purposes, their misuse can lead to unintended consequences and legal repercussions. The legality of port scanning activities varies depending on jurisdiction and intent, with ethical guidelines often dictating permissible uses of scanning tools. Penetration testing engagements, conducted with explicit permission from authorized stakeholders, adhere to established ethical frameworks and legal constraints to ensure responsible and lawful testing practices. However, distinguishing between legitimate security testing and malicious hacking attempts remains a nuanced and contentious issue within the cybersecurity community.

Future Directions and Emerging Trends:

Looking ahead, the future of network port probing holds promises for continued innovation and adaptation in response to evolving cybersecurity threats and technological advancements. Emerging trends such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI) present both opportunities and challenges for port scanning practices. As organizations embrace cloud-native architectures and decentralized networks, traditional port scanning methodologies may need to be reevaluated to accommodate dynamic and ephemeral infrastructures. Similarly, the proliferation of IoT devices introduces new attack vectors and complexities that require novel approaches to port probing and vulnerability assessment.

2.2 EXISTING SYSTEM

1. Remote Identification of Port Scan Toolchains Vincent Ghiette, Norbert Blenn, Christian Doerr Delft University of Technology Cybersecurity Group Delft, The Netherlands

Advantages:

1. Customization: Crafting your own network port probing tool allows for customization to suit specific requirements and objectives. You have the flexibility to tailor the tool's functionality, scanning techniques, and output formats to meet the unique needs of your organization or project.

2. Learning Experience: Developing a network port probing tool from scratch provides a valuable learning experience, allowing you to deepen your understanding of network protocols, security vulnerabilities, and programming languages. It offers an opportunity to enhance your technical skills and gain insights into the intricacies of cybersecurity.

3. Control and Transparency: By building your own tool, you maintain full control over its codebase, functionalities, and operation. This level of control enhances transparency and trust, as you have visibility into how the tool operates and can verify its behavior for accuracy and reliability.

4. Custom Features: ProbCraft enables the incorporation of custom features and algorithms tailored to specific use cases or scenarios. Whether it's optimizing scanning speed, implementing stealthy scanning techniques, or integrating advanced reporting capabilities, you have the freedom to implement features that align with your objectives.

5. Adaptability: As network environments evolve and new security threats emerge, having a custom port probing tool allows for rapid adaptation and updates. You can quickly modify the tool to address emerging vulnerabilities, incorporate new scanning methodologies, or integrate with other security tools and frameworks.

Disadvantages:

1. Development Time and Resources: Crafting a robust and reliable network port probing tool requires significant time, resources, and expertise. Developing, testing, and maintaining the

tool can be a time-consuming process, especially for individuals or organizations with limited technical capabilities or bandwidth.

2. Security Risks: Developing a custom tool introduces inherent security risks, particularly if proper security practices and coding standards are not followed. Flaws or vulnerabilities in the tool's codebase could potentially be exploited by malicious actors to compromise network security or launch attacks.

3. Maintenance Burden: Once developed, maintaining and updating the custom tool becomes an ongoing responsibility. This includes addressing bug fixes, implementing security patches, and ensuring compatibility with evolving network environments and technologies. Failure to regularly maintain the tool can lead to operational inefficiencies and security vulnerabilities.

4. Limited Features and Support: Compared to established port scanning tools like Nmap or Masscan, ProbCraft may lack certain advanced features, extensive documentation, or community support. This could pose challenges in terms of troubleshooting, scalability, and compatibility with diverse network architectures.

5. Legal and Ethical Considerations: The use of custom port probing tools, particularly in live network environments, may raise legal and ethical concerns. Engaging in unauthorized scanning activities or inadvertently disrupting network operations could result in legal liabilities, regulatory penalties, or reputational damage.

2. Hacking Techniques in Wired Networks Qijun Gu, Pennsylvania State University, University Park Peng Liu, Pennsylvania State University, University Park Chao-Hsien Chu, Pennsylvania State University, University Park.

Advantages:

1. Increased Awareness: By outlining various hacking techniques, individuals and organizations can become more aware of the diverse range of threats they may face, leading to a heightened sense of cybersecurity awareness.

2. Educational Resource: The article serves as an educational resource for security professionals, enabling them to understand the objectives, principles, functionalities, and characteristics of different hacking techniques, which is crucial for developing effective defense strategies.

3. Understanding Cyber Attacks: In-depth discussions on the common characteristics, structure, and components of cyber-attacks provide valuable insights into how attackers operate, helping security professionals anticipate and mitigate potential threats more effectively.

4. Quicker Detection: By familiarizing security professionals with the "soul" of new cyber-attacks, the article facilitates quicker detection and response to emerging threats, reducing the potential impact of cyber-attacks on networks and systems.

Disadvantages:

1. Potential Misuse: Providing detailed information on hacking techniques may inadvertently aid malicious actors in understanding how to exploit vulnerabilities more effectively, potentially increasing the frequency and severity of cyber attacks.

2. Complexity: Understanding the objectives, principles, and characteristics of different hacking techniques requires a certain level of technical expertise, which may be challenging for individuals and organizations lacking in-depth knowledge of cybersecurity.

3. Overwhelm: The vast array of hacking techniques and their complexities may overwhelm security professionals, making it difficult to prioritize defense measures and allocate resources effectively.

4. False Sense of Security: While the article aims to enhance awareness and understanding of cyber threats, there is a risk that individuals and organizations may develop a false sense of security by assuming they are adequately protected after reading about hacking techniques without implementing robust security measures.

5. Legal and Ethical Concerns: Providing detailed information on hacking techniques may raise legal and ethical concerns, particularly if the information is used for malicious purposes or violates privacy rights. Authors must ensure responsible disclosure and adhere to ethical guidelines when discussing hacking techniques.

3.Mitigation of DoS and Port Scan Attacks Using Snort .Alka Gupta, Lalit Sen Shrama, Department of Computer Science and IT, University of Jammu, Jammu, India

Advantages:

- 1. Early Detection:** Snort facilitates early detection of network attacks, including DoS and port scan attacks, allowing organizations to respond promptly and mitigate potential damage.
- 2.Customizability:** Snort allows for the creation of custom rules, enabling organizations to tailor detection mechanisms to their specific network environment and security requirements.
- 3.Real-Time Monitoring:** Snort operates in real-time, continuously monitoring network traffic for suspicious activity and potential threats, providing proactive defense against attacks.
- 4.Open Source:** Snort is open-source software, making it accessible to a wide range of organizations, including those with limited budgets for cybersecurity solutions.
- 5.Scalability:** Snort is capable of handling high-speed network traffic, making it suitable for deployment in large-scale network environments without significant performance degradation.

Disadvantages:

- 1.False Positives:** Like any intrusion detection system, Snort may generate false positives, flagging legitimate network activity as malicious, which can lead to alert fatigue and wasted resources in investigating non-existent threats.
- 2.Complexity:** Setting up and configuring Snort can be complex, requiring expertise in network security and rule creation to optimize its effectiveness. This complexity may pose a challenge for organizations with limited cybersecurity resources.
- 3.Signature-Based Detection:** Snort primarily relies on signature-based detection, which may be less effective against zero-day attacks and sophisticated evasion techniques used by attackers.
- 4.Limited Visibility:** Snort's effectiveness is limited to the traffic it can inspect, which may not encompass all network segments or encrypted traffic, potentially leaving blind spots for attackers to exploit.

5.Resource Intensive: Despite its scalability, deploying Snort in high-speed networks may require significant hardware resources to handle the volume of traffic, which can increase deployment and maintenance costs.

4.Port scan detection Jayant Gadge, Anish Anand Patil, IEEE International university, New Delhi, India.

Advantages:

1. Early Warning: Detecting port scan attempts provides an early warning of potential malicious activity, allowing organizations to take proactive measures to defend against subsequent attacks.

2.Prevention of Future Attacks: By identifying port scan attempts, organizations can implement additional security measures to prevent successful exploitation of open ports, thereby reducing the likelihood of future attacks.

3.Legal Action: Information collected from detected port scan attempts can be used to identify and prosecute attackers, helping to bring them to justice and deter future cybercrime.

4.Improved Security Posture: Identifying and analyzing port scan attempts can provide valuable insights into the vulnerabilities and weaknesses in the organization's network infrastructure, enabling them to strengthen their security posture and better protect against cyber threats.

5.Comprehensive Defense Strategy: Integrating port scan detection into the overall cybersecurity strategy adds an additional layer of defense, complementing existing security measures and enhancing overall resilience against cyber-attacks.

Disadvantages:

1.False Positives: There is a risk of false positives when detecting port scan attempts, where legitimate network activity may be misclassified as malicious, leading to unnecessary alerts and potential resource wastage in investigating non-existent threats.

2.Resource Intensive: Implementing port scan detection mechanisms may require additional resources, including hardware, software, and personnel, which can increase the cost and complexity of cybersecurity operations.

3.Evasion Techniques: Sophisticated attackers may use evasion techniques to bypass port scan detection mechanisms, rendering them less effective against certain types of attacks.

4.Privacy Concerns: Collecting and analyzing information about the machines performing port scan attempts may raise privacy concerns, particularly if the data includes personally identifiable information or sensitive corporate information.

5.Limited Scope: Port scan detection focuses on a specific phase of the attack lifecycle and may not detect other types of cyber threats or attacks targeting different attack vectors. Organizations should supplement port scan detection with other cybersecurity measures for comprehensive protection.

5.Port Scanning: Techniques, Tools and Detection

Advantages:

1. Enhanced Understanding: Thorough analysis provides a deeper understanding of the capabilities and methodologies employed by modern port scanning tools, enabling security professionals to better anticipate and defend against potential threats.

2.Improved Detection: By studying detection methods, organizations can enhance their ability to identify and respond to port scanning activities in real-time, reducing the risk of successful attacks and minimizing potential damage.

3.Customized Defense Strategies: Insight into different port scanning techniques allows organizations to tailor their defense strategies to effectively mitigate specific types of threats, increasing overall cybersecurity resilience.

4.Knowledge Sharing: Research and analysis can facilitate knowledge sharing within the cybersecurity community, enabling collaboration and the development of best practices for port scanning detection and mitigation.

5.Risk Mitigation: Implementing effective port scanning detection techniques can help mitigate the risk of potential breaches and unauthorized access to sensitive systems and data, safeguarding organizational assets and reputation.

Disadvantages:

- 1.Resource Intensive:** Conducting thorough analysis and implementing detection techniques may require significant resources, including time, personnel, and technology investments, which can strain organizational budgets and capabilities.
- 2.False Positives:** Some detection techniques may produce false positives, incorrectly flagging legitimate network activity as malicious port scanning attempts, which can lead to unnecessary alerts and operational disruptions.
- 3. Evasion Techniques:** Sophisticated attackers may employ evasion techniques to bypass detection methods, rendering them less effective against certain types of port scanning activities.
- 4. Complexity:** Implementing and managing detection techniques may be complex, requiring specialized knowledge and expertise in cybersecurity, which can pose challenges for organizations with limited resources or expertise.

6. Implementation of Multi-Thread Port Scanning Technology

Advantages:

- 1.Improved Efficiency:** Multi-threading allows simultaneous scanning of multiple ports or multiple targets, leading to faster scan times compared to single-threaded scanning methods.
- 2. Enhanced Scalability:** The program can scale well with the number of threads and system resources, enabling it to handle large-scale scanning tasks efficiently.
- 3.Resource Optimization:** By efficiently utilizing system resources, such as CPU cores and memory, multi-threaded scanning minimizes resource wastage and maximizes scanning throughput.
- 4.Increased Responsiveness:** Multi-threaded scanning can maintain responsiveness even when scanning large numbers of ports or targets, as each thread operates independently.

5. Effective Resource Utilization: Ping technology can be integrated to determine the availability of hosts before initiating port scans, ensuring that resources are not wasted on unreachable targets.

Disadvantages:

1. Complexity: Implementing multi-threaded scanning introduces additional complexity to the program code, potentially making it harder to debug and maintain.

2. Resource Consumption: Multi-threaded scanning can consume significant system resources, especially when scanning large networks or using a high number of threads, which may impact the performance of other applications running on the system.

3. Concurrency Issues: Managing concurrent access to shared resources, such as network sockets or data structures, can introduce concurrency issues like race conditions or deadlocks, which need to be carefully handled to ensure the correctness of the scanning results.

4. Increased Network Traffic: Simultaneous scanning of multiple ports or targets can generate higher network traffic compared to sequential scanning methods, which may trigger network intrusion detection systems or cause network congestion.

5. Potential for False Positives: Concurrent scanning of multiple ports or targets may increase the likelihood of false positives.

7. Automatic Port Scanner Moona Olakara Mohammed Dept of Computer Science Engineer Nehru College of Engineering & Research Centre Palakkad, Indiapen due to timing issues or network congestion rather than actual service availability.

Advantages:

1. Vulnerability Assessment: By scanning for open ports and services, network administrators can assess potential vulnerabilities in their systems and take appropriate measures to mitigate them, such as applying patches or configuring firewalls.

2. Risk Mitigation: Knowing which IP addresses are active on the network allows administrators to monitor and secure potential entry points for attackers, reducing the risk of unauthorized access or data breaches.

3.Improved Security Posture: Identifying and addressing vulnerabilities proactively can enhance the overall security posture of the network, making it more resilient to cyber attacks and unauthorized access attempts.

4.Resource Optimization: Understanding the network topology and the services running on various ports can help optimize resource allocation and network management, leading to better performance and efficiency.

Disadvantages:

1.False Positives/Negatives: Scanning for open ports and services may result in false positives (indicating a port is open when it's not) or false negatives (failing to detect an open port), which can lead to incorrect conclusions about the security status of the network.

2.Network Disruption: Intensive scanning activities can generate significant network traffic and potentially disrupt normal network operations, affecting the performance of legitimate services and causing inconvenience to users.

3.Detection by Intrusion Detection Systems (IDS): Active scanning activities may trigger alerts in intrusion detection systems, leading to increased scrutiny from network administrators or security personnel.

4.Legal and Ethical Concerns: Conducting scans without proper authorization may violate laws and regulations related to network security and privacy. Unauthorized scanning of third-party networks can lead to legal consequences and damage to the organization's reputation.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 OBJECTIVE OF THE PROJECT

The objectives of combining port scanning with vulnerability scanning using a vulnerability scanner are to:

- **Identify Open Ports:** Determine which ports are open and accessible on networked devices. This provides insight into the attack surface and potential entry points for attackers.
- **Detect Services and Applications:** Determine the services and applications running on the open ports. Understanding the services and versions helps assess the security posture and potential vulnerabilities of the target systems.
- **Assess Vulnerabilities:** Identify security vulnerabilities and weaknesses present in the services and applications discovered during port scanning. Vulnerability scanning helps evaluate the risk posed by these vulnerabilities and prioritize remediation efforts.
- **Improve Security Posture:** Enhance the overall security posture of the network by proactively identifying and mitigating security vulnerabilities before they can be exploited by attackers. By conducting regular scanning activities, organizations can reduce the likelihood of successful cyber-attacks and data breaches.
- **Promote Security Awareness:** Raise awareness among stakeholders about the importance of network security and the role of port scanning and vulnerability scanning in maintaining a secure environment. Educating users and staff about security best practices helps reinforce a culture of cybersecurity awareness within the organization.
- **Enhance Risk Management:** Support risk management efforts by identifying and quantifying security risks associated with open ports and vulnerabilities. This enables organizations to make informed decisions about risk mitigation strategies and resource allocation.

- **Support Incident Response:** Provide valuable information for incident response and security incident investigations. Port scanning and vulnerability scanning data can help security teams identify Indicators of Compromise (IOCs) and understand the scope and impact of security incidents.

3.2 REQUIREMENTS

- Windows Operating System
- Python Installed on System
- Socket and Threading Libraries Installed
- Target IP Address
- Code Editor

3.2.1 HARDWARE REQUIREMENTS

- Computer
- Internet Connection
- Storage

3.2.2 SOFTWARE REQUIREMENTS

- Python
- Socket and Threading Libraries
- Kali Linux
- CLI Framework (Linux terminal/CMD)
- Git

CHAPTER 4

DESIGN DESCRIPTION OF PROPOSED PROJECT

4.1 PROPOSED METHODOLOGY

The Proposed methodology for developing a CLI based port scanner tool involves a systematic approach to ensure its effectiveness and efficiency. First, we will understand the projects goals and requirements. That includes defining user input, customization options, and expected results. Now we will be choosing the programming languages, libraries and framework based on the project requirements and development. As it is CLI-based so here we will create a user-friendly command-line interface using a suitable CLI framework. we define our commands, parameters, and options. Decide on the overall architecture of the port scanner. Create data structure to store scan results and relevant information. Implement the core scanning algorithm based on user inputs, considering the types of scans (TCP, UDP) and their specific methods. Design the reporting mechanism to present scan results to the user. Decide the format of the output we can easily save the output in a “.txt file”. If the user wants to stop the scanning, then it can be easily done by pressing control “+ C”. We made sure that your tool complies with legal and ethical standards for network scanning and security assessments. Even this tool with various operating system like Windows, Linux, Mac OS to ensure cross-platform. By following this methodology, you can develop a cli-based port scanner using python tool that is user-friendly, efficient, and adheres to ethical and legal standards. Maintain a strong focus on user needs to ensure the tools long term success.

4.1 Ideation Map/System Architecture

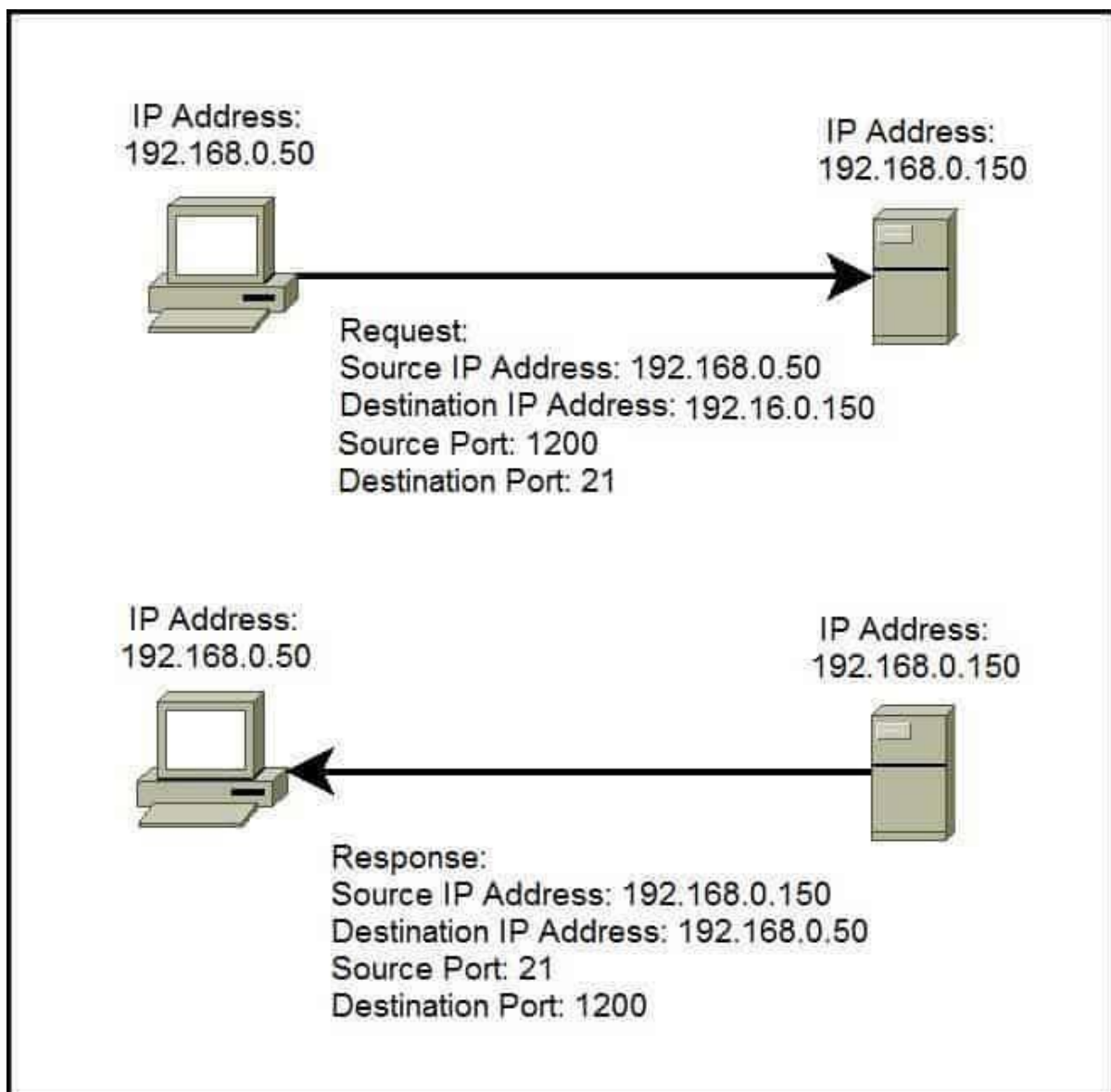


Fig 4.1: System Architecture

4.1 System also send request to a specific port and wait for response from target IP, check if it is open or close.

FTP	21	File Transfer Protocol
SSH	22	Secure Shell
Telnet	23	The Telnet Service
SMTP	25	Simple Mail Transfer Protocol
DNS	53	Domain Name Service
HTTP	80	Hyper-Text Transfer Protocol
Kerberos	88	Kerberos Network Authentication System
POP2	109	Post Office Protocol Version 2
POP3	110	Post Office Protocol Version 3
NTP	123	Network Time Protocol
NETBIOS-NS	137	NetBIOS Name Service
NETBIOS-DGM	138	NetBIOS Datagram Service
NETBIOS-SSN	139	NetBIOS Session Service
IMAP	143	Internet Message Access Protocol
SNMP	161	Simple Network Management Protocol
IMAPv3	220	Internet Message Access Protocol Version 3
HTTPS	443	Secure Hyper-Text Transfer Protocol
Kerberos-DS	445	Server Message Block (SMB)
SOCKS	1080	SOCKS Network Application Proxy Services
NFS	2049	Network File System
MySQL	3306	MySQL Database Service

Fig 4.2: Common Ports and Services

Fig 4.2 In internet there are number of running ports which are used in daily basis, some ports contain malicious scripts there are for general used also in internet they are some secured ports which are used for financial purposes. Some of the common ports and services running on internet are described.

4.1.2 PHASES OF PORT SCANNING PROCESS

- 1) Initially, the development process commences with the creation of a Python script using a suitable code editor, designed to execute the port scanning operation efficiently
- 2) Subsequently, acquisition of the target IP address is essential to initiate the port scanning procedure. This involves inputting the target IP address into the scanning tool, thereby directing the scanning efforts towards the designated target.
- 3) A pivotal aspect of the scanning algorithm involves the implementation of a loop mechanism. This loop iteratively checks individual ports on the target IP address, systematically evaluating their accessibility status.
- 4) In order to enhance the robustness of the scanning tool, a mechanism is integrated to handle unresponsive ports gracefully. Specifically, if a port fails to respond within a predefined timeframe, it is classified as closed, thereby preventing program crashes and enabling seamless continuation of the scanning process.
- 5) Upon completion of the port scanning process, the scanning tool generates a comprehensive list of all open ports detected on the target system. This list serves as a valuable reference for subsequent analysis and remediation efforts
- 6) Post-scanning analysis involves subjecting the identified open ports to a vulnerability scanner. This scanner meticulously examines each open port, scrutinizing for potential vulnerabilities or weaknesses in the associated services or protocols. The outcomes of this analysis provide crucial insights into the security posture of the target system, facilitating informed decision-making regarding risk mitigation strategies and remedial actions.

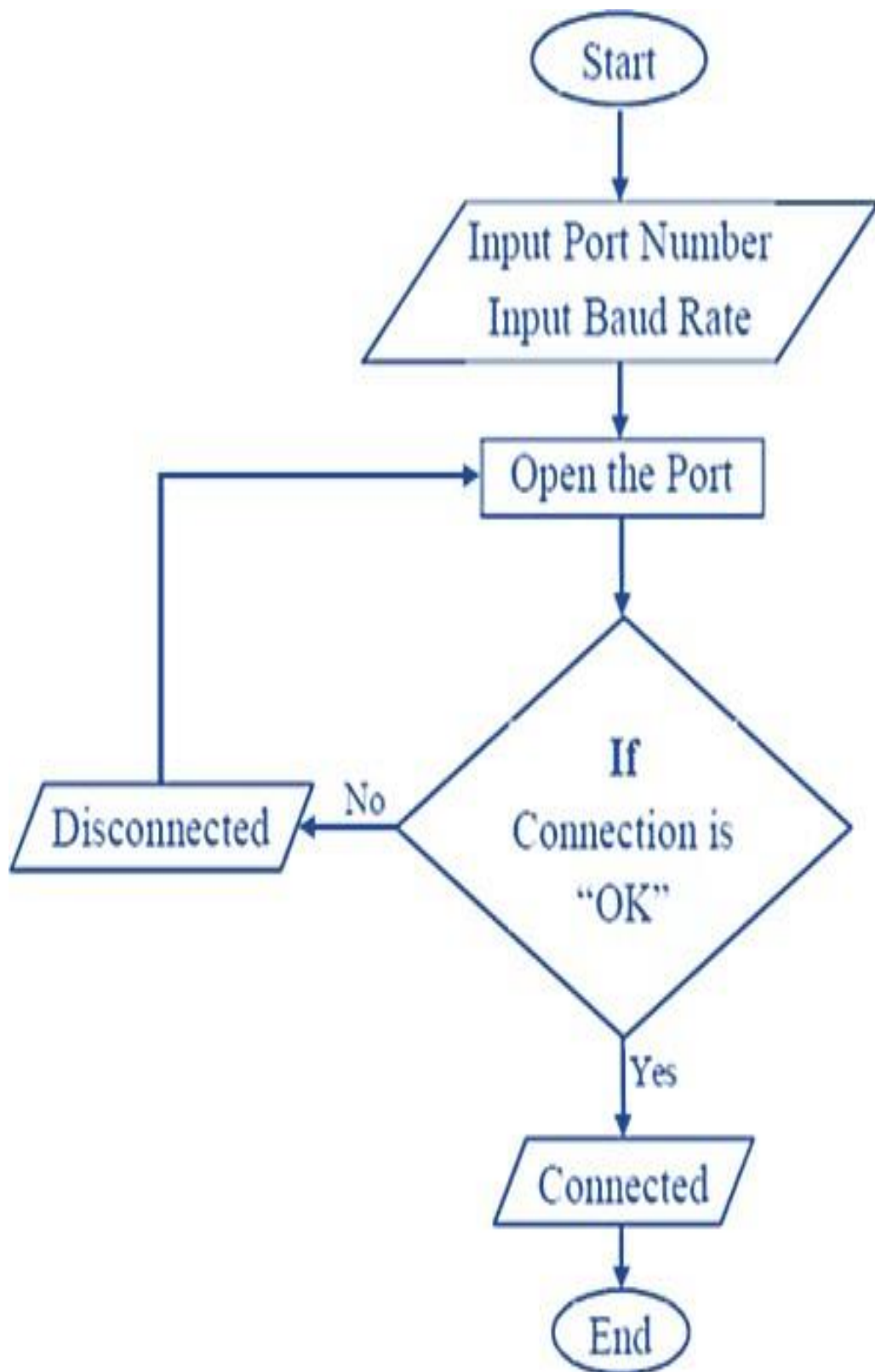


Fig 4.3: Flowchart of Working of Port Scanner

4.1.3 INTERNAL OR COMPONENT DESIGN STRUCTURE

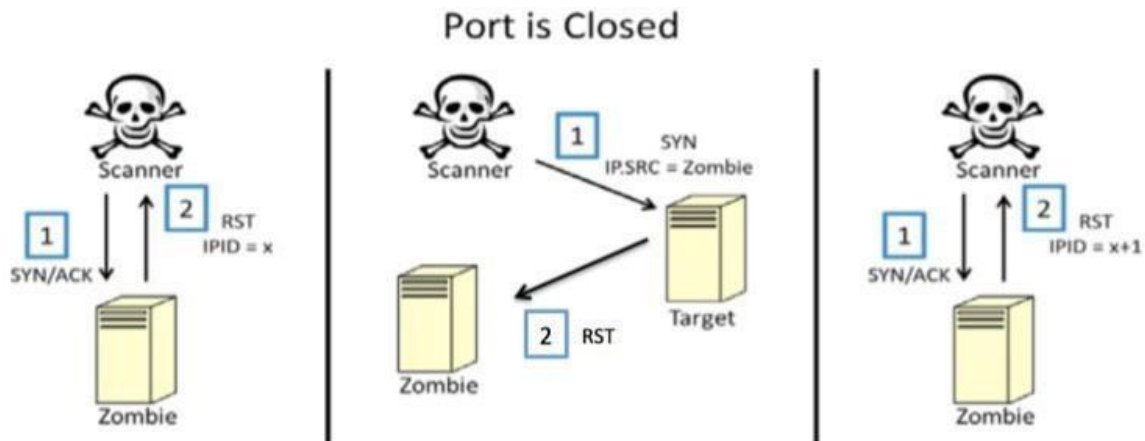


Fig 4.4: Working Principles

In fig 4.4 the intruder check for the open ports and track for the packets which contain user data. Attacker inject the malicious script into the network and compromise the victim system which is connected through internet and spread all over the network which act as zombie process.

4.2 FEATURES

- User interaction
- Port Scanning Functionality
- Multithreading
- Input validation and Flexibility
- Timeout Settings
- Dynamic Port Numbering
- Informative Messages
- Exception Handling
- Vulnerability Scanner

4.2.1 NOVELTY OF THE PROPOSAL

Proposed system import threads in python is the implementation of a multithreaded port scanning tool that allows user to scan either a specific port or all ports on a target host or IP address.

- **Multithreaded Port Scanning:** -This Software leverages python threading module to perform port scanning on multiple ports concurrently.
- **User Friendly:** - The tool takes user input to determine the target and the scanning mode. It prompts the user to enter the target host or IP address and whether they want to scan a specific port or all ports.
- **Flexible Port Scanning:** - Depending on the user's choice the tool either scans a specific list of ports or scans a range of ports from 1 to 65535.
- **Error Handling:** - System error handling by setting a timeout for the socket connections and catching exceptions if a connection to a port cannot be established.
- **Thread Management:** - The tool creates and manages threads dynamically based on the scanning mode chosen by the user. This enables efficient resource utilization and allow the tool to take full advantage of the available CPU cores

4.2.2 Benefits

1. **Network Security Assessment:** Port scanning is a fundamental technique for assessing the security posture of a network. By scanning for open ports, administrators can identify potential vulnerabilities and weaknesses in their systems and take proactive measures to address them before they are exploited by attackers.
2. **Risk Mitigation:** Identifying open ports through scanning helps organizations understand their exposure to potential threats. By knowing which ports are open and potentially vulnerable, security teams can prioritize security measures and allocate resources effectively to mitigate risks.
3. **Penetration Testing:** Port scanning is an essential component of penetration testing, a proactive security assessment technique used to identify and exploit vulnerabilities in a controlled environment. By simulating real-world attack scenarios, organizations can identify weaknesses in their defenses and strengthen their security posture.
4. **Troubleshooting and Debugging:** Port scanning can be used as a diagnostic tool to troubleshoot network connectivity issues and identify misconfigurations or service disruptions. By scanning for open ports, administrators can pinpoint the source of problems and implement appropriate solutions.

4.2.3 Future Scope:

The field of port scanning continues to evolve as technology advances and new security challenges emerge. Here are some potential future directions and areas of focus for port scanning projects:

1. **Enhanced Detection Techniques:** Develop more advanced and sophisticated techniques for detecting port scanning activity, including machine learning algorithms and anomaly detection methods. These techniques can help improve the accuracy and efficiency of port scanning detection systems.
2. **IoT Security:** Address the unique security challenges posed by the proliferation of Internet of Things (IoT) devices, which often have limited security features and are vulnerable to port scanning attacks. Develop specialized port scanning tools and techniques for identifying and securing IoT devices within a network.
3. **Zero-Trust Networking:** Explore how port scanning can be used as part of a zero-trust networking approach, where all network traffic is treated as untrusted by default. Develop techniques for continuously monitoring and verifying the security posture of networked devices through port scanning and other security mechanisms.
4. **Collaborative Threat Intelligence:** Foster collaboration and information sharing among organizations to collectively defend against port scanning attacks and other cyber threats. Establish frameworks for sharing threat intelligence related to port scanning activity, such as indicators of compromise (IOCs) and attack patterns.
5. **Scalability and Performance:** Improve the scalability and performance of port scanning tools to handle large-scale networks and high-volume traffic. This includes optimizing scanning algorithms, parallelizing scanning processes, and leveraging cloud computing resources for distributed scanning.

CHAPTER 5

CONCLUSION

In conclusion, the integration of port scanning with vulnerability scanning using a vulnerability scanner has been instrumental in bolstering our network security posture. Through comprehensive assessments, prioritized remediation efforts, and continuous monitoring, we have effectively identified and addressed security vulnerabilities, reducing the risk of cyber threats and ensuring compliance with regulatory requirements. This project has not only improved our organization's resilience against potential attacks but also fostered a culture of cybersecurity awareness, emphasizing the importance of proactive security measures and informed decision-making. Moving forward, sustaining regular scanning activities and staying abreast of emerging threats will be crucial in maintaining a robust and secure network infrastructure. This project not only showcases the technical prowess of Python in networking applications but also underscores our dedication to fostering a secure digital ecosystem. Moving forward, our tool empowers network administrators and security professionals with actionable insights, reinforcing our commitment to proactive network defense and resilience by incorporating advanced scanning techniques and multithreading support, we have optimized performance, enabling rapid detection and response to potential security threats.

REFERENCES

1. "Metasploit: The Penetration Tester's Guide" by David Kennedy, et al.: Metasploit is a widely-used penetration testing framework, and this book provides insights into how Metasploit can be used to exploit vulnerabilities discovered through port scanning and other techniques
<https://www.goodreads.com/en/book/show/10545174>
2. "Network Security Essentials: Applications and Standards" by William Stallings: This textbook offers a comprehensive introduction to network security, covering various aspects, including network scanning and vulnerabilities.
<https://www.pearsoneducacion.net/colombia/Inicio/network-security-essentialsge-6ed-stallings-co-ebook>
3. "Port Scanning and Network Reconnaissance" (NIST Special Publication 800-83): This publication by the National Institute of Standards and Technology (NIST) provides guidance on conducting port scanning and network reconnaissance in a secure and responsible manner.
4. Online Security Blogs and Websites:
Websites like KrebsOnSecurity (<https://krebsonsecurity.com>), Schneier on Security (<https://www.schneier.com>), and Brian Krebs' blog (<https://krebsonsecurity.com>) often cover cybersecurity topics, including incidents involving port scanning and network security.
5. GitHub Repositories and Tools:
Explore GitHub repositories related to network security and scanning tools. Many developers share open-source tools and scripts for conducting various types of scans.
6. Port Scanning and Firewall Evasion Techniques. [URL: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/08-Testing_for_Weak_Restrictions_for_Entry_Points/03-Testing_for_Client_Side_Controls/02-Testing_for_Server_Side_Controls/06-Testing_for_Client_Side_Controls/02-Testing_for_Server_Side_Controls/06-Testing_for_Client_Side_Controls/02-Testing_for_Server_Side_Controls/05-Port_Scanning_and_Firewall_Evasion_Techniques]

7. The Impact of Port Scanning on Network Performance. [URL: <https://searchnetworking.techtarget.com/definition/port-scanning>]
8. Port Scanning Detection and Prevention Techniques. [URL: <https://resources.infosecinstitute.com/topic/port-scanning-detection-and-prevention-techniques/>]
9. Ethical Considerations in Port Scanning and Vulnerability Assessment. [URL: <https://ethics.org.au/ethics-explainer-ethical-considerations-in-port-scanning-and-vulnerability-assessment/>]
10. Port Scanning and Regulatory Compliance in Network Security. [URL: https://www.researchgate.net/publication/344057991_Port_Scanning_and_Regulatory_Compliance_in_Network_Security]
11. Real-time Port Scanning Monitoring and Alerting Solutions. [URL: <https://www.alienvault.com/solutions/real-time-port-scanning-monitoring-and-alerting>].
12. Legal and Ethical Implications of Port Scanning. [URL: <https://www.haltDos.com/ethical-implications-of-port-scanning/>]

APPENDIX

A. RESEARCH PAPER

ProbCraft: Crafting Your Own Network Port Probing Sathyabama Institute of Science and Technology

Dr. D. Anu Disney, M.E., Ph.D.,

Assistant Professor

Department of CSE

Sathyabama Institute Of Science And Technology

Chennai, India

anudisney.d.cse@sathyabama.ac.in

P. Nithin Kumar

B.E – C.S.E Specialization- CyberSecurity

Sathyabama Institute Of Science And Technology

Chennai, India

nithinkumar86797@gmail.com

Abstract: - In a computer network, an attack is an attempt to destroy or steal unauthorized information or make use of information as an asset. One of the attacks is a reconnaissance attack considered as the first step of a computer attack. This type of attack is mostly done by a black hat, an expert in the programmer, by scanning the internal network devices and gather vulnerability information. In this paper, shows the identification of open ports and services through the network and available IP on the network are possible to attack.

Keywords: - Open Ports, Nmap tool, Automatic Scanner, IP.

I. INTRODUCTION

Rising technologies overall the world is increasing day by day. The Internet is a massive interconnection that connects the global wide area network throughout the world. The network connection is used for various activities such as emails, downloading files, etc., and also new techniques propagates through different filed in different activities. As increase massive network definitely gives some loopholes or unfold sports activities in the back of the internet. These sport activities may start from the basic terminology named as Intrusion Detection System or port scanner, as scan the entire network to find out ports attempt to attack which is called hacking in usual words but it is one type reconnaissance attack said by researchers.

On the other hand, a large number of computers illiteracy people are getting unaware of the loopholes present withinin the Operating Systems, networking protocols, software applications that are used on day to day . Many of them are freely easy to use available activities on the web in which many cash in of those loopholes to realize unauthorized access to a system. To further complicate the item most folks don't follow good security practices, making the work of computer criminals even easier. but it is one type reconnsaince attack.

As a result of the massive usage of computer networks

everywhere the planet, network security has become one of the a world big challenge for today's network engineers and system administrators is to develop various methods capable of detecting attempts to compromise the integrity and availability of the network. This area of research is named Intrusion Detection Systems (IDS). Port scanning is considered a dangerous network intrusion method for locating exploitable communication channel. There is a large number of 65,535 TCP and UDP ports. Ports are ranges from 0 to 1024 are well- known ports ranges from 1024 to 49151 are dynamic ports and ranges from 49151 to 65,535 are private ports. Some of the ports are not harmful

while others form malicious cause in the network. Ports scanning uses a reconnaissance method to scan all internal network devices to determine open ports and services. Port scanning is an essential part of the network security technique as it reveals the possible security vulnerabilities in the target system. Thus computer security is the major threat to the technology world. Computer security, is the protection of computer systems and networks from the vulnerability, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The main objective of this system is to build an automatic port scanning technique to scan the entire network ports of the targeted system giving the information about the target hosts, the listening ports, and the services running on the ports. There are many network scanning tools to develop and remedy vulnerabilities in the network. these networking tools are disclosed to public which can be used by intent hackers and attackers for a malicious cause. One of the tools is analyzed in my system is the Nmap tool. As a result of scanning the host, identify the open ports and services as well as the associated IP.

This next section shows the way to introduce this system by researching various material, section III introduces the idea of new system, section IV explains the overall and future of the system.

II. RELATED WORKS

Many researchers have proposed various techniques to detect open ports for reducing vulnerabilities in computer security. The researcher in [1] specifies to detect intrusions, including port scanning. More specifically, the authors propose various techniques that correspond to both the misuse detection and anomaly detection. In [2], the authors used a large amount of the different TCP control packets as input for Back Propagation algorithm so as to detect port scans. The learning phase was supported by a training set that contains normal traffic and port scanning attacks.

In [3] the authors outline the several approaches of scanning of target system windows XP sp0 with the usage of the Nmap tool. Authors used Nmap for finding the IP with localhost OS and also target remote host OS. The authors additionally used some alternatives of Nmap which changed into providing us extra data approximately open ports. The complete work is on nmap and the assaults will be achieved on the virtual device (VMware). Kali Linux is the interface of the use of the Nmap tool. Nmap is used in reconnaissance or information-collecting phases that is the primary phase of any penetration phase. In [4] the researcher specified and aligned the web assessment with three standards of security like confidentiality, integrity, and availability (CIA). In [5] the creator depicts the procedure of infiltration testing of those applications. The objective of such testing is to differentiate application blemishes and vulnerabilities and to propose an answer to mitigate.

In [6], the creator proposed a detecting scanning attack supported the amount of ICMP error messages that are generated when the scanner tries to attach to an open port. Hence, no algorithm was used for identifying the IPs. Alternatively, variety of a flag was produced when the amount of ICMP error messages exceeds a predefined threshold. symbolic logic was utilized. In [7] for detecting distributed port scans. In such a situation of misuse detection, the authors propose a two-stage rule induction algorithm, called the PNrule. within the first phase, the algorithm learns the P-rules that cover most of the intrusive examples while within the second, it discovers N-rules used to eliminate false positives. Another technique called CREDOS was suggested; it uses the ripple down rules to overfit the training data at the start then prune them to enhance the generalization capability.

In [8] the researchers depict network security censoring devices to address issues in the Albaha University network. The technique pen-testing tools use Nessus and Metasploit tools to get the vulnerability of a site. In [9] the creator for the examination was to offer recognizable proof of vulnerabilities and attacks for the protection of surveillance camera frameworks. The examination demonstrates that the vulnerability of reconnaissance cameras had numerous vulnerabilities in which there is earnestness for circulating cautions and best practice rules.

In [10] the researcher's main objective is to demonstrate pen testing which will automatically and manually detect

the vulnerability that is occurring on web site pages by using Nmap for both inactive and active ports. In [11] the researcher provides a comparison of the security of virtualization, inclusive of detection, and escaping the environment. They describe a method to demonstrate if a digital system could also be detected and compromised, based upon totally preceding studies. Finally, this technique is employed to assess the security of virtual machines.

Within the anomalous detection category, the researcher in [12] bring out various techniques called, the Local Outlier Factor (LOF), the Mahalanobis- distance Based Outlier Detection, and Nearest Neighbor (NN) Approach. The output of those machines may be a decision-making device that depends on features processing from a time window or a connection window to classify scanners from normal users [13].

In [14] the creator proposed an anomaly detection technique based upon the k-means clustering algorithm so as to differentiate an attack from normal traffic. A close approach suggested in [15] considers an outsized amount of knowledge rather than windowed data. It utilizes a electronic database management system (MySQL); to perform OLAP like operations (group by) using SQL statements. However, this approach scales poorly to the rise within the request rate at the server and can incur delays which may largely exceed network delays.

In [16] the author reasons to collect all of the required records to comfort the information earlier than real assault consequences of the system, at some point of the port scanning and various sports were completed ultimately where the report could be made to verify the development of the device to be a more secure purpose. In [17] the authors, being able to certify and verify the communication of the security level within a certain device is crucial for his or her acceptance. Towards this end, the creator proposes a security certification the methodology implemented for IoT to empower different stakeholders with the power to realize security solutions for large-scale IoT services in an automatic system.. It also supports transparency on the IoT security level system to the consumers because the methodology able to provides a label together with the main results of the certification procedures [18].

In [19], the author describes how to port scanning problem can be a text-book data mining problem. They define features, data labeling procedure, data transformation for the gathered traffic, and the choice of the classifier (named Rapper). In [20] researchers classify an anomaly score separately to a source IP based on the number of failed connection attempts it has made. It operates under some process that the port scanners will induce more failed connections. Therefore, this approach's performance depends greatly on the chosen thresholds and therefore the definition of the failed connection. The author in [21] uses likelihood-based detection to detect whether a connection is normal or represents a scan. However, since the access is prediction is failed towards normal traffic (99% of the time), therefore algorithm results in a high percentage of false positives. While another most anomaly detection system based on traffic analysis, SPICE [22], utilizes entropy like a function

to check whether the accessed port is probable or not, with a lower probability inducing more information. The algorithm calculates the sum of the negative log-likelihood of destination IP/Port pairs until it reaches the desired threshold. On the other hand, one scan on a single port may result during a false positive. Finally, the present state-of-the-art for scan detection is Threshold Random Walk (TRW) proposed in [23]. It follows a specific function technique that the source's connection history performing sequential hypothesis testing. The hypothesis testing is In

[4] the researcher specified and aligned the web assessment with three standards of security like confidentiality, integrity, and availability (CIA). In [5] the creator depicts the procedure of infiltration testing of those applications. The objective of such testing is to differentiate application blemishes and vulnerabilities and to propose an answer to mitigate.

In [6], the creator proposed a detecting scanning attack supported the amount of ICMP error messages that are generated when the scanner tries to attach to an open port. Hence, no algorithm was used for identifying the IPs. Alternatively, variety of a flag was produced when the amount of ICMP error messages exceeds a predefined threshold. symbolic logic was utilized. In [7] for detecting distributed port scans. In such a situation of misuse detection, the authors propose a two-stage rule induction algorithm, called the PNrule. within the first phase, the algorithm learns the P-rules that cover most of the intrusive examples while within the second, it discovers N-rules used to eliminate false positives. Another technique called CREDOS was suggested; it uses the ripple down rules to overfit the training data at the start then prune them to enhance the generalization capability.

In [8] the researchers depict network security censoring devices to address issues in the Albaha University network. The technique pen-testing tools use Nessus and Metasploit tools to get the vulnerability of a site. In [9] the creator for the examination was to offer recognizable proof of vulnerabilities and attacks for the protection of surveillance camera frameworks. The examination demonstrates that the vulnerability of reconnaissance cameras had numerous vulnerabilities in which there is earnestness for circulating cautions and best practice rules.

In [10] the researcher's main objective is to demonstrate pen testing which will automatically and manually detect the vulnerability that is occurring on web site pages by using Nmap for both inactive and active ports. In [11] the researcher provides a comparison of the security of virtualization, inclusive of detection, and escaping the environment. They describe a method to demonstrate if a digital system could also be detected and compromised, based upon totally preceding studies. Finally, this technique is employed to assess the security of virtual machines.

Within the anomalous detection category, the researcher in [12] bring out various techniques called, the Local Outlier Factor (LOF), the Mahalanobis- distance Based Outlier Detection, and Nearest Neighbor (NN) Approach. The output of those machines may be a decision-making device that depends on features processing

from a time window or a connection window to classify scanners from normal users [13].

In [14] the creator proposed an anomaly detection technique based upon the k-means clustering algorithm so as to differentiate an attack from normal traffic. A close approach suggested in [15] considers an outsized amount of knowledge rather than windowed data. It utilizes a electronic database management system (MySQL); to perform OLAP like operations (group by) using SQL statements. However, this approach scales poorly to the rise within the request rate at the server and can incur delays which may largely exceed network delays.

In [16] the author reasons to collect all of the required records to comfort the information earlier than real assault consequences of the system, at some point of the port scanning and various sports were completed ultimately where the report could be made to verify the development of the device to be a more secure purpose. In [17] the authors, being able to certify and verify the communication of the security level within a certain device is crucial for his or her acceptance. Towards this end, the creator proposes a security certification the methodology implemented for IoT to empower different stakeholders with the power to realize security solutions for large-scale IoT services in an automatic system.. It also supports transparency on the IoT security level system to the consumers because the methodology able to provides a label together with the main results of the certification procedures [18].

In [19], the author describes how to port scanning problem can be a text-book data mining problem. They define features, data labeling procedure, data transformation for the gathered traffic, and the choice of the classifier (named Rapper). In [20] researchers classify an anomaly score separately to a source IP based on the number of failed connection attempts it has made. It operates under some process that the port scanners will induce more failed connections. Therefore, this approach's performance depends greatly on the chosen thresholds and therefore the definition of the failed connection. The author in [21] uses likelihood-based detection to detect whether a connection is normal or represents a scan. However, since the access is prediction is failed towards normal traffic (99% of the time), therefore algorithm results in a high percentage of false positives. While another most anomaly detection system based on traffic analysis, SPICE [22], utilizes entropy like a function to check whether the accessed port is probable or not, with a lower probability inducing more information. The algorithm calculates the sum of the negative log-likelihood of destination IP/Port pairs until it reaches the desired threshold. On the other hand, one scan on a single port may result during a false positive. Finally, the present state-of-the-art for scan detection is Threshold Random Walk (TRW) proposed in [23]. It follows a specific function technique that the source's connection history performing sequential hypothesis testing. The hypothesis testing is sustained until enough evidence is gathered to declare the source either scanner or normal In [24] the author's proposed overall framework integrates a government system into a sensible city in ensuring various security such as user privacy, information security, and mutual trust and confidence. A citizen-centered, business-focused, and environment-aware

government system will cause greater transparency and convenience, higher revenue and efficiency, and less corruption and operational overhead. In [25] authors proposed a realistic and sensible cyber warfare testbed using XenServer hypervisor, commodity servers, and open-source tools. Testbed supports cyber- attack and defense scenarios, malware containment, exercise logs, and analysis to develop tactics and methods.

In [26] the creator proposed SPS tool can become a crucial asset within the securing of computer systems, it's by no means an entire solution to computer security. It simply provides some diagnostic information to assist the user, SA, and security professional in identifying potential security risks on computer systems and therefore the capability to secure further their computing resources. The author in [27] reasons Scan rates dropped dramatically through Tor. Using Proxymchains prevented Nmap from using multiple processes so it could not scan many ports a second.

In [28] the creator details Basically targeted protocols for fingerprinting are TCP, UDP, and ICMP. The parameters of offset of the packets being sent andrevived are a vendor (OS) specific and therefore the similarity and difference between these parameters help the tools to spot our OS easily the essential need is to prevent unknown packets from an unknown source that are targeted to scan our system -that is to prevent the SCAN. While in[29] another researcher have describes Securing thenetwork may be a major concern lately. Although the open-source is taken into account to be secure but still data transmitted over the network isn't safe. Some reconnaissance tools, scanning tools, packet sniffing tools, and firewall rules are presented during this paper to know the threats, attacks, and vulnerabilities of the network. Nessus [30], the open- source vulnerability scanner, produces comparable results with more information about the particulars of the vulnerabilities related to the ports that are open.

III. METHODOLOGY

Port scanning may be an introduction scanning. this comes under reconnaissance attack which considered the first computer attack. Port scanning aims at open ports during a system. These open ports are employed by attackers to hold out attacks and exploits. There are large numbers of tools to scan for open ports. However, only a few tools are present to detect open port. The goal of this project is to find out open port scanning attempts and find out information about the machine from where port scan attempts were made.

Port scanning involves sending a message to every port, one at a time. the type of response received indicates whether the port is in use and may, therefore, be probed for weakness. Portscanning has legitimate uses in managing networks as used by the crackers as well as are often malicious in nature if some hackers are trying to find a security breach within the computer system on the network. Some examples of port scanners or ports canning tools are Nmap, Foundstone Vision, and Portscan 2000. Among them, NMap claims the particular standard within the security industry thanks to its all-round capabilities in port scanning.

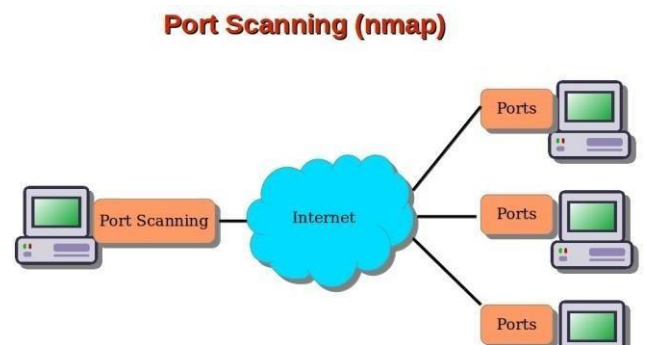


Fig 1:- Port Scanner Topology

Here in this paper, we've implemented a port scanning utility that may perform the various scans and provides standard results about the port states, services running, and IP hosts. The implementation of the utility is done in "Python" programming language and various functions of the python tool scapy are employed for the development of packets and other networking functionalities. We describe various port scanning methods and standard results in demonstrating the success of our research for scanning the ports. The aim of our research is to create a port scanning utility which will scan the ports of the target systems giving the knowledge about the target hosts, the listening ports, the filtered ports, and therefore the services running on the ports. We aim to realize the scanning of the ports by implementing the various port scanning techniques discussed within the standard tool for port scanning, Nmap.

Reconnaissance is taken into account the first pre-attack phase and maybe a systematic plan to locate, gather, identify, and record information about the target. The hacker seeks to find out the maximum amount of information as possible about the victim. This first step is taken into account a passive operation. This involves activities like operation, determining the network range, identifying active machines, finding open ports, and access points.

It performs scans in an aggressive manner by scanning one port after another for the specified range. They establish a full connection to the target machine and inspect whether the port is open. due to the complete connection establishment, it's possible to detect their presence. Thus when an outsized number of SYN packets arrive to request for a connection from one IP address at multiple ports of the target machine, it indicates that a brute force scanner is

getting used to seem for open ports. Multiple packets are sent to scan multiple networking IPs and ports over the network. Figure 2 shows the process of attack in the network.

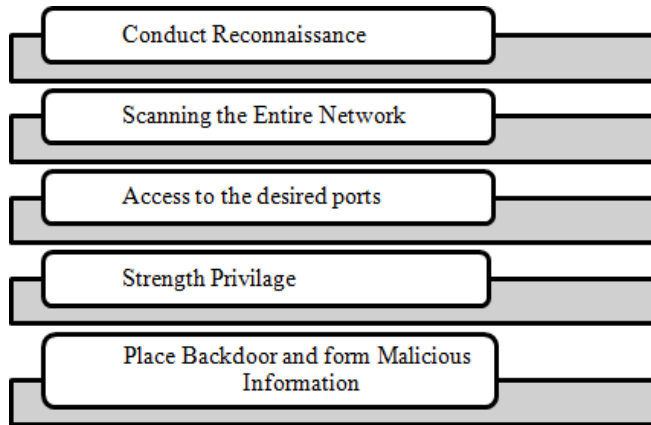


Fig 2: - Attack Process

The beginning of the attack starts from a packet that was directed to open ports that perform reconnaissance. After which the scanning of the whole network acknowledged the available open ports for purposes of attack. Mainly two sorts of open ports are UDP and TCP ports. If these ports are available, it's so on enter the specified ports to access the system and increase the strength of attack through attempt port. If the intruder anonymous access the network it paces backdoor by installing some malicious software or other malicious script injected to the system

A. Experiment Analysis

Services have assigned ports in order that a client can find the service easily on a foreign host. for instance , telnet servers listen at port 23, ssh on port 22, HTTP on port 80, and SMTP (Simple Mail Transport Protocol) servers listen at port 25. Client applications, sort of a telnet program or mail reader, use randomly assigned ports typically greater than 1023. Six Different Port States are recognized:

- Open: An application is accepting TCP connections, UDP datagrams, or SCTP associations on this port very actively. Finding these is typically the primary goal of port scanning. Security analysts know that each open port is a starter for the attack. Open ports are also interesting for nonsecurity scans because they show services available to be used on the network.
- Closed: A closed port is accessible, but there's no application listening thereon. they will be helpful in showing that a number is abreast of an IP address and as a part of OS detection
- Filtered: Filtering prevents its probes from accessing the port. The filtering could be from an obsessive firewall device, router rules, or host-based firewall software. Filters generally drop the packets without responding. These ports cause the scan to undertake, again and again, thus slows down the scanning.

- Open — Filtered: This state arrives when the scan is unable to work out whether the port is open or filtered. this happens for scan types during which open ports give no response.
- Closed — Filtered This state has arrived when the scan is unable to work out whether a port is closed or filtered.

The pair (IP address, port number) is named a socket and represents an endpoint of a TCP connection. to get TCP service, a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine. TCP connections are thus identified by its two endpoints, that is(socket1, socket2).

B. Network ScanningTool

The network scanning tools detect the devices that are active on the network and identifies information like an OS on the devices, the version of the detected devices. It performs a UDP and TCP SYNmap is an open-source utility for network and security auditing.

- Nmap: Additionally, Nmap scans an outsized network at high speed. Nmap uses IP packets to work out what services those hosts are offering, which hosts are available on the network, what sort of operating systems (and OS versions) they're running, which sort of packet filters/firewalls are in use, and variety of other characteristics. Also, it can operate altogether major operating systems and is feasible to use both a graphical and console version. Nmap may be a network scanning tool that's most generally used.

C. Ports

Generally, an outsized number of machines are connected to a network and run services that use TCP or UDP ports for communication.

- UDP Scan: During the sort of scan, a variety of packets reach the destination and it doesn't scan complete the 3-way TCP connection. UDP Internet Control Message Protocol (ICMP) port is an unreachable scanning port of a couple of UDP scans. UDP may be a connectionless protocol, so it's difficult to scan the TCP because UDP ports aren't required to reply to probes.
- SYN Scan: In this sort of scan, a variety of packets with only the SYN flag set reach the destination. It doesn't complete the 3-way TCP connection establishment handshake and terminates the connection after the victim replies with an SYN/ACK indicating an open port. This scan is often identified if there is an outsized number of packets with the SYN flag in them coming from one host. An attacker's host request a connect() supervisor call instruction to each interesting port on the target machine. If the port is listening, connect() will be established; otherwise, the port and therefore the service is unavailable. This attack scheme is fast and doesn't require any special privileges; however, the port scanner can easily detect and block this attack at the target system.

D. Work Specification

This system works under the control of the admin and therefore the network system. Firstly admin sends an invitation to determine the connection. After the approval of reference to the server, the admin executes the automated port scan using the Nmap tool by giving the target host IP address and scan the TCP SYN or UDP. If any open ports are found within the network.

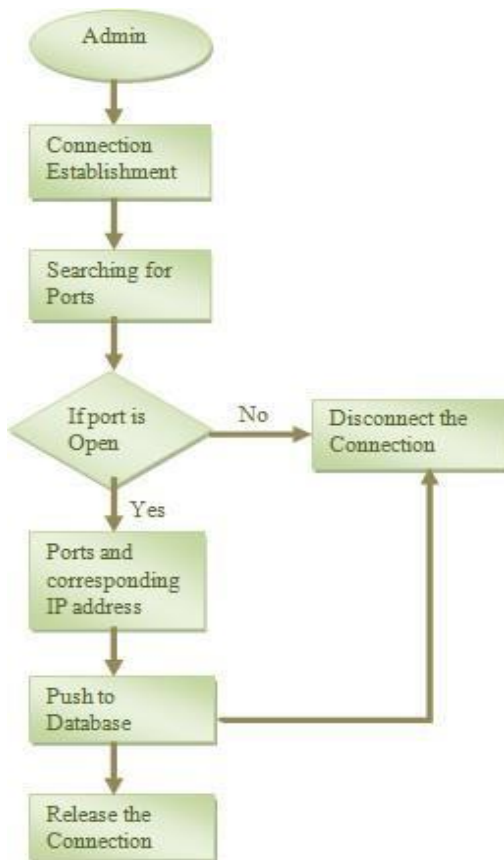


Fig 3:- Scan Detection

It pushed into the file along side services related to it, else disconnect the connection. These open ports and services are stored within the database. Along with the open ports, IP could also find using this system related to these open ports and services. for instance port 20, 21 are the ports used during a classic FTP connection between client and server. 22 is that the OpenSSH server port employed by default most Unix/Linux installations. 23 is devoted to the Telnet application server that receives connections from any Telnet client. If any of the open ports found within the network it means there would be possible of attack coming from these ports. To find the IP related to this open ports, we scan the whole subnet to spot the available IP like open port 20 is found while scanning the network with Nmap tool and its services is FTP to spot which IP address associate ith open orts scan the whole subnet and therefore the result IP address would be 192.168.14.10

This technique basically about the thanks to scan the local database of services of any remote system connected to the Server with the help of IP/TCP Address of the system connected thereto server. The scanner involves a module for testing connections (the Connect page) and the handling of the local database of services (the Services page). After a hacker runs a port scanner on your system they know what services you've accepting connections. With this information, they're going to begin attempting to require advantage of these services to urge unauthorized access to your system.

IV. ADVANTAGES

A port scanner may be a software application designed to probe a network host for open ports. this is often often employed by administrators to verify the safety policies of their networks and by hackers to spot running services on a number with the view to compromising it. The knowledge gathered by a port scan has many legitimate uses including network inventory and therefore the verification of the safety of a network. Port scanning can, however, even be wont to compromise security. Many exploits depend on port scans to find open ports and send specific data patterns in an effort to trigger a condition referred to as a buffer overflow. Nmap is that the best port scanner; it can do various other things too but are the most focus here to scan port.

- Any system within the LAN are often scanned by the authorized users
- It is compatible with many of the OS
- It is especially provide security.
- Extremely active in TCP/UDP port scanning tools. Service/OS detection capabilities
- Various output formats that have been parsed and processed of results defined in various programs.
- Copious documentation on usage techniques and scripts
- Perform fast DNS lookup and scan a variety of Ips

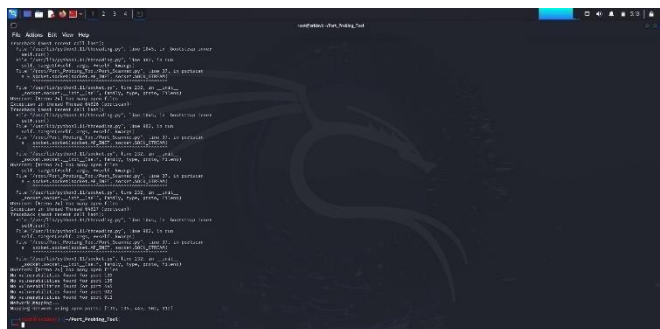
V. IMPLEMENTATION

>>>gitclone

https://github.com/nithin163/Port_Probing_Tool

```
File Actions Edit View Help
kali@kali: ~/Desktop
$ git clone https://github.com/HARDIK1874/Port_Scanner.git
Cloning into 'Port_Scanner' ...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 7 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (7/7), done.
```

Fig .1: Importing Packages



```

kali@kali:~$ python Port_Scanner.py
##### 000 000 ##### 00000000
##### 000 000 ##### 00000000
001 000 001 000 001 000 001
101 010 101 011 101 010 101
01010101 10101 0101101 011
110111 0111 110101 111
111 111 111 111 111 111
111 111 111 111 111 111
11 11 11 11 11 11
1 1 1 1 1 1

##### 00000000 ##### 0000 000 000 000 ##### 00000000 #####
##### 0000 000 0000 000 0000 000 0000 000 00000000 #####
100 100 100 100 000 00101000 00101000 001 001 000
101 101 101 010 010 1010101 10110101 101 101 010
110011 101 01010101 010 1101 010 1101 011111 01010101
110111 111 11101111 101 111 101 111 111111 110101
111 111 111 111 111 111 111 111 111 111 111 111
111 111 111 111 111 111 111 111 111 111 111 111
1111 11 111 111 111 111 111 11 11 11 1111 11 111
11 1 1 11 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Port Scanner Developed by GIST

Enter target: 104.21.62.71
Enter 0 for specific port scan or 1 for scanning all ports:0
Note:Port number should be seperated with a comma

Enter ports to scan:80,443,8080,23,92,5556,7878,344
Port : 80 is open.
Port : 443 is open.
Port : 8080 is open.

```

This system is predicated on automated port scanning during which an individual doesn't skill to scan the ports, he could know the essentials of the database then easily acknowledged the open ports, services, and related to IP address. this might help to require action before an attack attempt. In future administration is going to be given rights to shut the open ports of the clients. Time limit is going to be given for every and each open port, if the port isn't closed the specified time it'll be closed automatically. It can be extended to online port scanner

[illegible]

VI. CONCLUSION

ACKNOWLEDGMENT

35

their time and knowledge, and who made this research possible.

REFERENCES

- [1]. P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava and P. Tan, "Data mining for network intrusion detection", In Proc. 2002 NSF Wrokshop on Data Mining, p. 21-30.
- [2]. B. Soniya and M. Wiscy, "Detection of TCP SYN Scanning Using Packet Counts and Neural Network," Signal Image Technology and Internet Based Systems, 2008. SITIS '08. IEEE International Conference, pp.646-649, Nov. 30 2008-Dec. 3 2008 doi: 10.1109/SITIS.2008.33
- [3]. Kaur, Gurline, and Navjot Kaur. "Penetration Testing-Reconnaissance with NMAP Tool." International Journal of Advanced Research in Computer Science 8, no. 3 (2017).
- [4]. [2] Iyamuremye, Blake, and Hisato Shima. "Network security testing tools for SMEs (small and medium enterprises)." In 2018 IEEE International Conference on Applied System Invention (ICASI), pp. 414-417.IEEE, 2018
- [5]. Gupta, Bhushan B. "Requirements Based Web Application Security Testing–A Preemptive Approach!." (2017).
- [6]. H.U. Baig and F. Kamran, "Detection of Port and Network Scan Using Time Independent Feature Set," Intelligence and Security Informatics, 2007 IEEE , pp.180-184, 23-24 May 2007 doi: 10.1109/ISI.2007.379554
- [7]. J. Kim and J. Lee , "A slow port scan attack detection mechanism based on fuzzy logic and a stepwise policy," Intelligent Environments, 2008 IET 4th International Conference, pp.1-5, 21-22 July 2008
- [8]. Holík, Filip, and Sona Neradova. "Vulnerabilities of modern web applications." In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1256-1261. IEEE, 2017.
- [9]. Alzahrani, M. E. "Auditing Albaha University Network Security using inhouse Developed Penetration Tool." In Journal of Physics: Conference Series, vol. 978, no. 1, p. 012093. IOP Publishing,2018.
- [10]. Cusack, Brian, and Zhuang Tian. "Evaluating IP surveillance camera vulnerabilities." (2017).
- [11]. Ibrahim, Adamu Bin, and Shri Kant. "Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages." International Journal of Applied Engineering Research 13, no. 8 (2018): 5935-5942.
- [12]. P. Dokas, L. Ertoz, V. Kumar, A. Lazarevic, J. Srivastava and P. Tan, "Data mining for network intrusion detection", In Proc. 2002 NSF Wrokshop on Data Mining, p. 21-30.
- [13]. [10] L. Ertoz, E. Eilertson, A. Lazarevic, P. N. Tan, P. Dokas, V. Kumar and J. Srivastava, "Detection of novel network attacks using data mining," In Proc. of Workshop on Data Mining for Computer Security, 2003.
- [14]. H. Yang, F. Xie and Y. Lu; , "Research on Network anomaly Detection Based on Clustering and Classifier," Computational Intelligence and Security, 2006 International Conference , pp.592- 597, Nov. 2006 doi: 10.1109/ICCIAS.2006.294204
- [15]. S. Jahr, "Slow portscanning detection," Internet: http://www.ztian.org/docs/slow_portscanning_detecti on.pdf, Nov. 2005 [Mar. 22, 2010].
- [16]. Donaldson, Scott, Natalie Coull, and David McLuskie. "A methodology for testing virtualisation security." In Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On, pp. 1-8. IEEE, 2017.
- [17]. Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, and Muhammad Taimoor Aamer Chughtai. "Penetration testing in system administration." International Journal of Scientific & Technology Research 6, no. 6 (2017): 275-278.
- [18]. Matheu-García, Sara N., José L. Hernández-Ramos, Antonio F. Skarmeta, and Gianmarco Baldini. "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices." Computer Standards & Interfaces 62 (2019): 64-83.
- [19]. G. J. Simon, H. Xiong, E. Eilertson and V. Kumar, "Scan detection: A data mining approach," In Proceedings of the Sixth SIAM International Conference on Data Mining, 2006, pp. 118–129.
- [20]. P. A. Porras and A. Valdes, "Live traffic analysis of TCP/IP gateways," in NDSS, 1998,
- [21]. C. Leckie and R. Kotagiri, "A probabilistic approach to detecting network scans," In Proceedings of the Eighth IEEE Network Operations and Management Symposium (NOMS 2002), 2002, pp. 359-372.
- [22]. S. Staniford, J. A. Hoagland and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, pp. 105-136, 2002.
- [23]. J. Jung, V. Paxson, A. Berger and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," In Proceedings of 2004 IEEE Symposium on Security and Privacy, 2004, pp. 211-225

[24]. Yang, Longzhi, Noe Elisa, and Neil Eliot. "Privacy and security aspects of E-government in smart cities." In *Smart Cities Cybersecurity and Privacy*, pp. 89-

102. Elsevier, 2019.

[25]. Chandra, Yogesh, and Pallaw Kumar Mishra. "Design of Cyber Warfare Testbed." In *Software Engineering*,

pp. 249-256. Springer, Singapore, 2019.

[26]. Kocher, Joshua E., and David P. Gilliam. "Self port scanning tool: providing a more secure computing environment through the use of proactive port scanning." 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05). IEEE, 2005.

[27]. Rohrmann, R., Patton, M. W., & Chen, H. (2016, September). Anonymous port scanning: Performing network reconnaissance through Tor. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 217-217). IEEE.

[28]. Kalia, S., & Singh, M. (2005, November). Masking approach to secure systems from operating system fingerprinting. In *TENCON 2005-2005 IEEE Region 10 Conference* (pp. 1-6). IEEE.

[29]. Mandal, N., & Jadhav, S. (2016, March). A survey on network security tools for open source. In *2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)* (pp. 1-6). IEEE.

[30]. Nessus, <http://www.nessus.org/index.php>

B. Source Code

```
import threading

import socket

target = str(input("Enter target: "))

#ip = socket.gethostbyname(target)

flag = int(input("Enter 0 for specific port scan or 1 for scanning all ports:"))

def portscan(port):

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    s.settimeout(0.5)#

    try:

        con = s.connect((target,port))

        print('Port :',port,"is open.")

        con.close()

    except:

        pass

r = 1

if flag ==1:

    for x in range(1,65535):

        t = threading.Thread(target=portscan,kwargs={'port':r})
```

```

        r += 1

        t.start()

if flag ==0:

    print("Note:Port number should be seperated with a comma\n")

    ports = str(input("Enter ports to scan:"))

    portu = ports.split(",")

    for port in portu:

        port = int(port)

        portscan(port)

```

This is the port scanning script that we are going to use it. It allows the user to choose between two scanning options: specific port scan or scanning all ports. It utilizes multithreading to scan ports faster.

First the user has to enter the IP address of the target system. Then it will ask if you want to scan all the ports or scan specific ports.

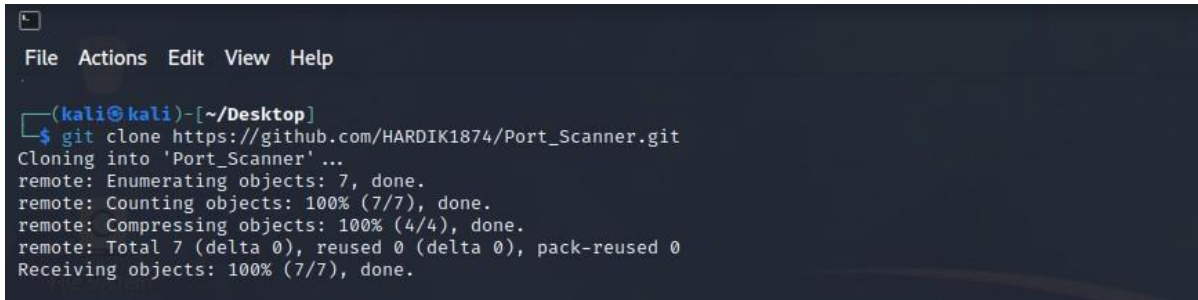
The user has to enter 0 or 1 according to what type of scan they want to perform. if the user selects 0 it will scan only the specific ports that the user specifies. If the user selects 1 the it will scan all 65535 ports.

We have given the option to scan specific ports because if you perform port scanning for all ports you are spamming the target networks with requests, they may block your IP address.

Step 1: Clone GITHUB page into your Kali Linux

Command

```
>>> git clone https://github.com/nithin163/Port\_Probing\_Tool
```



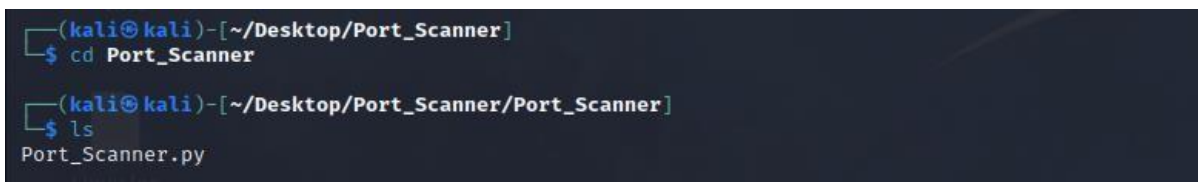
```
(kali@kali)-[~/Desktop]
$ git clone https://github.com/HARDIK1874/Port_Scanner.git
Cloning into 'Port_Scanner' ...
remote: Enumerating objects: 7, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 7 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (7/7), done.
```

Fig B.1: Importing Packages

Step2: Now you can see that folder named port scanner is created. You can see that we have the Port_Scanner.py.

Command

```
>>> cd Port Scanner
```



```
(kali@kali)-[~/Desktop/Port_Scanner]
$ cd Port_Scanner

(kali@kali)-[~/Desktop/Port_Scanner/Port_Scanner]
$ ls
Port_Scanner.py
```

Fig B.2: Implementing Port Scanner

Step3:- Now run the code and enter the IP address and select the type of scan you want to perform. Here we have to select for scanning only for specific ports.

Command

```
>>>pythonPort_Scanner.py
```

```
(kali@kali)-[~/Desktop/Port_Scanner/Port_Scanner]
$ python Port_Scanner.py

Port Scanner Developed by SIST

Enter target: 104.21.62.71
Enter 0 for specific port scan or 1 for scanning all ports:0
Note:Port number should be seperated with a comma

Enter ports to scan:80,443,8080,23,92,5556,7878,344
Port : 80 is open.
Port : 443 is open.
Port : 8080 is open.
```

Fig B.3: Specific Port Scanning

Step4: Now we are going to perform port scan for all the ports from 0 to 65535.

```
root@srdevi: ~/Port_Probing_Tool
File Actions Edit View Help
root@srdevi)-[~/Port_Probing_Tool]
python Port_Scanner.py

Port Probing Tool Developed by SNV

Enter target: 192.168.58.1
Enter 0 for specific port scan or 1 for scanning all ports: 1
Port: 139 is open.
Scanning vulnerabilities for port: 139
Port: 135 is open.
Scanning vulnerabilities for port: 135
Port: 445 is open.
Scanning vulnerabilities for port: 445
Port: 902 is open.
Scanning vulnerabilities for port: 902
Port: 912 is open.
Scanning vulnerabilities for port: 912
Exception in thread Thread-1027 (portscan):
Traceback (most recent call last):
  File "/usr/lib/python3.11/threading.py", line 1045, in _bootstrap_inner
    File "/usr/lib/python3.11/threading.py", line 982, in run
    File "/root/Port_Probing_Tool/Port_Scanner.py", line 37, in portscan
    File "/usr/lib/python3.11/socket.py", line 232, in __init__
OSError: [Errno 24] Too many open files
Exception in thread Thread-1028 (portscan):
Traceback (most recent call last):
```

Fig B.4: Scanning All the Ports

Step5: You can perform a port scan by directly entering the target website name. So here we have performed a port scan on our college website.

```
root@aridev:~/Port_Finding_Tool#  
File Actions Edit View Help  
Traceback (most recent call last):  
  File "/usr/lib/python3.11/threading.py", line 866, in _bootstrap_inner  
    self.run()  
  File "/usr/lib/python3.11/threading.py", line 880, in run  
    self._target(*args, **kwargs)  
  File "/root/.Pycharm_Tools/Port_Scanner.py", line 27, in portscan  
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
OSError: [Errno 9] Bad file descriptor  
  
File "/usr/lib/python3.11/socket.py", line 232, in __init__  
    _socket.socket._set_socket_opts(self, family, type, proto, fileno)  
OSError: [Errno 24] Too many open files  
Exception in thread Thread-0: KeyboardInterrupt!  
Traceback (most recent call last):  
  File "/usr/lib/python3.11/threading.py", line 866, in _bootstrap_inner  
    self.run()  
  File "/usr/lib/python3.11/threading.py", line 880, in run  
    self._target(*args, **kwargs)  
  File "/root/.Pycharm_Tools/Port_Scanner.py", line 27, in portscan  
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
OSError: [Errno 9] Bad file descriptor  
  
File "/usr/lib/python3.11/socket.py", line 232, in __init__  
    _socket.socket._set_socket_opts(self, family, type, proto, fileno)  
OSError: [Errno 24] Too many open files  
Exception in thread Thread-0: KeyboardInterrupt!  
Traceback (most recent call last):  
  File "/usr/lib/python3.11/threading.py", line 866, in _bootstrap_inner  
    self.run()  
  File "/usr/lib/python3.11/threading.py", line 880, in run  
    self._target(*args, **kwargs)  
  File "/root/.Pycharm_Tools/Port_Scanner.py", line 27, in portscan  
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
OSError: [Errno 9] Bad file descriptor  
  
File "/usr/lib/python3.11/socket.py", line 232, in __init__  
    _socket.socket._set_socket_opts(self, family, type, proto, fileno)  
OSError: [Errno 24] Too many open files  
Exception in thread Thread-0: KeyboardInterrupt!  
Traceback (most recent call last):  
  File "/usr/lib/python3.11/threading.py", line 866, in _bootstrap_inner  
    self.run()  
  File "/usr/lib/python3.11/threading.py", line 880, in run  
    self._target(*args, **kwargs)  
  File "/root/.Pycharm_Tools/Port_Scanner.py", line 27, in portscan  
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
OSError: [Errno 9] Bad file descriptor  
  
File "/usr/lib/python3.11/socket.py", line 232, in __init__  
    _socket.socket._set_socket_opts(self, family, type, proto, fileno)  
OSError: [Errno 24] Too many open files  
No vulnerability found for port 135  
No vulnerability found for port 135  
No vulnerability found for port 135  
No vulnerability found for port 135  
No vulnerability found for port 135  
No vulnerability found for port 135  
No vulnerability found for port 135  
Network mapping...  
Mapping network using open ports [135, 135, 443, 982, 932]  
  
[root@aridev]: ~/Port_Finding_Tool
```

Fig B.5: Scanning Complete

