International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2023; 4(2): 12-19
Received: 08-05-2021
Accepted: 21-06-2021

Mohammad Anwar Hossain
Department of CSE World University of Bangladesh, Dhaka, Bangladesh

Md. Sabbir Hossain
Department of CSE World University of Bangladesh, Dhaka, Bangladesh

Rezaul Karim
Department of CSE World University of Bangladesh, Dhaka, Bangladesh

Corresponding Author:
Mohammad Anwar Hossain
Department of CSE World University of Bangladesh, Dhaka, Bangladesh

Comprehensive architectural network design based on intrusion detection system

Mohammad Anwar Hossain, Md. Sabbir Hossain and Rezaul Karim

DOI: https://doi.org/10.33545/2707661X.2023.v4.i2a.66

Abstract
Cyber-threats on the internet abound and include ransom ware, malware, viruses, and phishing scams. Protecting against these risks, which have the potential to cause data breaches, financial losses, and reputational harm to a company, requires the implementation of network security measures. Financial information, intellectual property, and personal records are just a few examples of the sensitive and private information that many companies handle. Two essential parts of the architecture for network security are intrusion prevention systems (IPS) and intrusion detection systems (IDS). Their responsibilities in detecting and managing possible security risks are complementary. IDS keeps an eye on network activity and instantly detects any suspicious or malevolent activity. It is able to identify possible dangers before they have a chance to do a lot of harm. IPS takes things a step further by actively stopping harmful activity in addition to just detecting it. It is capable of acting quickly to halt an ongoing attack. Because of this, the authors employed IDS create a cost-effective and adaptable data security solution that any type of organization may adopt. The authors used intrusion detection (IDS) to find any unauthorized activity on the system. The unauthorized user was subsequently blocked and prevented from causing further damage to the system via the use of IDS technology.

Keywords: Architectural, comprehensive, intrusion-detection, network, design

1. Introduction
The advent of the Internet has brought about a significant shift in human communication patterns, adding a new level of complexity to interpersonal relationships. This change has not only affected interpersonal communication but also completely changed how businesses interact with their clientele. Businesses and organizations in the modern day mostly depend on Internet access to set up efficient channels for consumer contact. It is now essential for these businesses to guarantee the security and safety of their internet connections due to the possible hazards involved, including the financial stakes. As a result, businesses usually spend a lot of money building strong systems that can fend against outside and unauthorized attacks.

In order to identify possible security threats, an Intrusion Detection and Prevention System (IDPS) continually monitors system activity and network traffic. To find harmful patterns or departures from expected behavior, it employs anomaly detection, signature-based detection, or a mix of both techniques. Through the use of an Intrusion Prevention System (IPS), IDPS may proactively respond to threats by blocking or mitigating ongoing assaults in addition to producing real-time notifications when suspicious behavior is discovered. IDPS improves network security and aids in defending against a variety of cyber-attacks by integrating with other security products and getting frequent updates. This guarantees a proactive and strong defensive system for businesses and their vital data.

A strong and flexible strategy for protecting computer networks is to choose IDS and IPS to improve network security. IDS and IPS provide thorough threat monitoring and blocking capabilities and can identify and stop a variety of cyber threats in real time. This proactive defensive system lowers the danger of zero-day attacks, protects critical data, and minimizes downtime brought on by possible security breaches. These systems' constant upgrades and flexibility ensure that they continue to be successful in the face of changing threats, and their smooth interface with the current infrastructure facilitates deployment and management. In the end, IDS and IPS offer a reliable and affordable way to strengthen network security, giving consumers and businesses alike comfort and a safer online environment.

The goal of the "Comprehensive Architectural Network Design Based on Intrusion Detection System" project is to protect computer networks from malicious activity, cyber threats, and

unauthorized access. Through the use of an Intrusion Detection and Prevention System (IDPS), the project hopes to improve network security, identify threats in real time, safeguard confidential information, and lessen the effects of zero-day assaults. The IDPS ensures compliance with data protection standards and avoids service interruptions by monitoring network traffic, identifying irregularities, and taking preventative action through proactive defensive measures. Additionally, the solution offers useful information for forensic investigation, helping businesses to better understand attack trends and fortify their network defenses. The ultimate goal of this project is to protect sensitive data and reduce possible dangers while fostering a more secure and safe environment for users.

1.1 Objective

The goal of the project is-

- To detect and prevent unauthorized access, intrusions, and malicious activities in a computer network with the help of intrusion detection and prevention system.

2. Literature Review

An essential part of network security is an intrusion detection and prevention system (IDS/IPS), which seeks to identify and stop hostile activity or unauthorized access within a computer network. IDS/IPS systems have undergone a great deal of development and study, with the goals of increasing reaction times, decreasing false positives, and increasing detection accuracy. The IDS/IPS literature covers a range of methodologies, each having advantages and disadvantages, including as anomaly detection, behavior-based analysis, and signature-based detection. To improve IDS/IPS system efficiency, researchers have also looked at machine learning methods including data mining and deep learning. Overall, research efforts to address new threats and enhance the efficacy of these systems in thwarting cyber-attacks are continuing, and the literature emphasizes the critical role that IDS/IPS plays in protecting networks.

Sandeep Singh (2020) **[1]** has proposed 'Intrusion Detection Systems (Ids) And Intrusion Prevention Systems (IPS) For Network Security'. This research paper discuss to enhance network security and protect against cyber threats with a honeypot system. This mechanism uses a crafted attack target to divert criminals away from legitimate targets. They gather intelligence about the identity, methods and motivations of opponents. IDS monitors network traffic and detects suspicious behavior, while IPS proactively blocks intrusions in real time. These can be implemented as NIDS or HIDS for IDS and as HIPS or NIPS for IPS. Both IDS and IPS use signature-based detection to detect known attack patterns. Understanding the similarities and differences between this system and IDS helps organizations improve network security and defend against cyber threats.

Suman Thapa and Akalanka Mailewa Dissanayaka (2021) [2] has proposed 'The Role of Intrusion Detection/Prevention Systems In Modern Computer Networks'. This research discusses the development of IDS and IPS tools to enhance the security of information systems. IDS detects network intrusions at the host level and preventive measures tools prevent networks. The use of these tools automatically takes countermeasures such as logging off the user from the system, killing the process, shutting down the system, dropping connections, etc. It tracks, monitors and detects unwanted network traffic to solve this problem. This research focuses on IDS and IPS as primary tools for intrusion detection and prevention. Unlike traditional security tools, IDS and IPS provide enhanced security functionality. It explores their functions, work processes and important role in providing strong protection against threats.

Bilal Maqbool Beigh (2020) [3] has proposed "Intrusion Detection and Prevention System". This research developed a signature based IDS packet that compares network and pre-configured predefined attack patterns known as signatures. When A new attack specialist or program is recognized Identify common patterns of this type of attack, which may occur Made in signature. Since this process takes time, there will be a gap between discovered new threats and Applying signatures to IDS to identify threats. During this lag period your ID will be unable to be identified. The study focuses on the strengths, weaknesses and overall effectiveness of IDPS through classification and comparative analysis. Such signatures should be updated as often as they are used potentially.

Vijay Ramalingam and Dr. R. Saminathan (2019) [4] has proposed 'A Novel Survey on Intrusion Detection System and Intrusion Prevention System'. The process starts with a risk assessment to identify network vulnerabilities and threats. A comprehensive security policy with network-wide controls is formulated. Strong access control, authentication, and data encryption are implemented. Intrusion detection and prevention systems (IDPS), firewalls, DDoS protection, logging, and monitoring systems work together for real-time security. Regular vulnerability management, employee training, and incident response planning are crucial. Continuous improvement and staying updated on security trends strengthen defense against network threats.

B. Santos Kumar *et al*. (2020) [5] has proposed 'Intrusion Detection System- Types and Prevention'. This research is a cyber-security practice that creates a secure and isolated environment for running suspicious files or code. Operating in this controlled space, it closely monitors file interactions, network connections, and system changes to detect and prevent malicious activity before it harms the network. Sandbox acts as a gatekeeper and early warning system, filtering potential threats. Fine-tuning sandbox policies and integrating it with the broader security infrastructure enhances its effectiveness. Regular evaluation and improvement make sandboxing a vital part of a comprehensive cybersecurity strategy, strengthening defenses against cyber threats. Educating employees about sandboxing fosters an alert and proactive security culture.

Safana Hyder Abbas *et al*. (2023) [6] has proposed 'Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)'. This research focuses with monitoring and improving system events to detect security breaches or threats in IDS. IDS continuously monitors and analyzes system events to detect potential breaches or threats, generating alerts for suspicious activity. IPS goes further by actively attempting to prevent incidents. It can terminate or block connections associated with malicious network traffic. While IDS is a monitoring system, IPS acts as a control system, intervening to protect the network. This research explains network intrusion, detection, and prevention strategies to address security challenges. The combined use of IDS and IPS forms a robust security infrastructure, ensuring proactive monitoring, identification, and mitigation of threats, safeguarding systems and

networks against cyber-attacks.

3. Methodology

3.1 Methodology

This study offers a thorough method for creating and putting into place a secure network infrastructure for a company. Planning, Requirement Analysis, Network Infrastructure Design, Configurations, Testing and Results are the five steps used in the process, as per the research. For a network environment to be strong and safe, each stage is essential. Network security has grown to be an important worry for businesses in recent years. Our study focuses on developing and putting into place a network architecture that guarantees data integrity, secrecy, and authentication in order to address this problem. The methodical procedure for accomplishing this aim is described in this study.

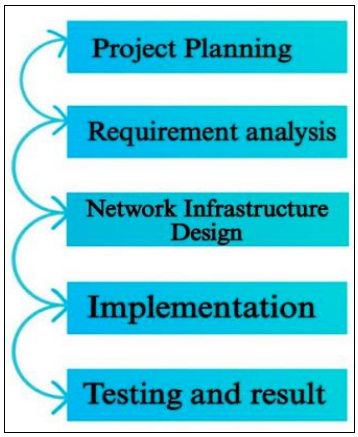

Fig 1: Proposed Project Methodology

3.2 Description of Methodology

There were several phases involved during the development process:

3.2.1 Planning

A sound strategy was the first step towards a successful study. Make a suitable plan for our study initially. We incorporate the study subject and a suitable working procedure in our strategy. In the autumn, we examined the work of several researchers on a related subject. Next, we decide on a suitable and legitimate title for our study. Maximum comparable investigation revealed several restrictions that we have identified. In order to get over these restrictions and maintain the originality of our work, we thus organized the research.

3.2.2 Requirement analysis

Every work has some requirements according to needs. So, our proposed work does require some specific resource.

A. System requirements: - System requirement can be divided into two types.

- Software requirements
- Hardware requirements

Software requirements

- Cisco Packet Tracer

Hardware requirements

- Laptop
- Desktop

B. User Requirements: What the user wants from the system is one of the user needs. The user needs data security, including integrity, confidentiality, and authentication, for this.

3.2.3 Network infrastructure design

Network architecture is based on organizational requirements. It's an unfinished design that explains the entire project. We must grasp the organization's needs and requirements and have a discussion with them about this. Following this, we presented the organization with a design and provided a thorough explanation.

3.2.4 Implementation

The project plan was really carried out throughout the implementation phase. This included carrying out the suggested design as well as delegating responsibilities to team members, keeping an eye on developments, and making any modifications. The authors implemented their approach using a simulation of Cisco packet tracers.

3.2.5 Testing and result

Following implementation, we obtained the outcome that satisfied the needs of the organization. We discovered that the work better provides security than the prior work and satisfies all requirements.

4. Requirement Analysis, Design & Developments

4.1 Requirement Gathering Technique

4.1.1 Stakeholder Identification

Identifying stakeholders is a crucial project requirement strategy when using an intrusion detection system to improve network security. It entails locating and comprehending every person, organization, or other entity that has a stake in or influence over the project's outcome. Stakeholders' wants, expectations, and concerns should be taken into consideration at every stage of the project, which is made easier with accurate stakeholder identification. The primary parties involved in this initiative include IT companies, offices with various divisions, etc.

4.1.2 Stakeholder Interview and Questionnaires

Authors conducted many interviews with different stakeholders, such as partners and users, to obtain their viewpoints on the system. During the interview, the following questions were asked.

- Is using our current system making this easier?
- Which kind of technologies do you employ?
- What kind of security measure or tool did you employ to safeguard our system?
- Is it possible for us to apply distinct policies for each user or department?
- Is it simpler to maintain?
- Has it been updated since our last model?
- Is it possible for us to use this technology to prevent unauthorized outside access to our network?

4.1.3 Legacy System Review

An intrusion detection system's integration with an old legacy network is a difficult process that needs careful thought. The seamless integration of the IDS into the legacy infrastructure is contingent upon several factors, including compatibility evaluation, integration complexity, and policy alignment. While analyzing data flows, analyzing hazards, and determining performance effect are crucial tasks, it's also important to pay attention to compliance and reporting

standards. To further prepare the company for IDS implementation, addressing training needs and doing a cost-benefit analysis are essential. Lastly, in order to verify the system's efficacy and reduce disturbance, extensive testing and piloting are essential. All things considered, adding an intrusion detection system (IDS) to a legacy system is a calculated step that will strengthen network security without sacrificing heritage features.

4.2 Flowchart

Data validation in this module starts when a particular packet is received and processed. Binary files make up the actual data packet file. The relevant result may be returned once the items in the retrieved dictionary list have been matrix-converted and entered into the trained model. In this module, a judgment result is considered normal when the return value is 1, and abnormal when the return value is -1. Additionally, the data will be suppressed in the event of aberrant findings. Any user wishing to access the main branch must first complete the IDS phase. The user will be able to access the main branch if they are authorized; if not, they will be banned.

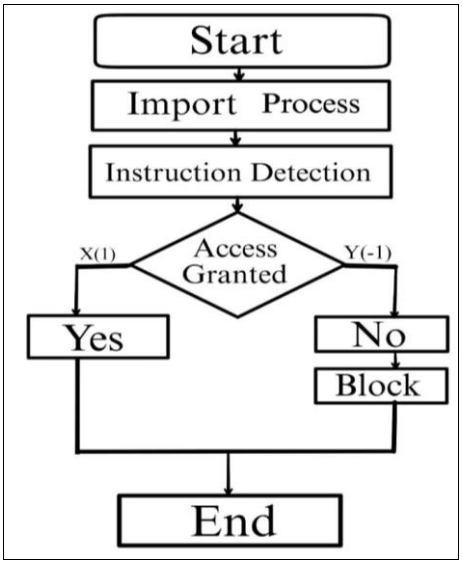

Fig 2: Flowchart of Intrusion Detection System

4.3 Proposed Network Design

Authors installed vital defense measures, such as intrusion detection systems (IDS), to protect their main office branch from any threats coming from sub-branch or hacker network environments. Data travels without interruption when it is transferred from the main branch PC to other PCs or sub-branches. IDS intervenes to intercept and block any suspicious data based on IP addresses when data tries to flow from sub-branches to the main system. We are able to detect intrusion attempts, their originating IP addresses, and timestamps thanks to the security events that are captured in our server's Syslog. Our careful observation of these records contributes to the security of our data.

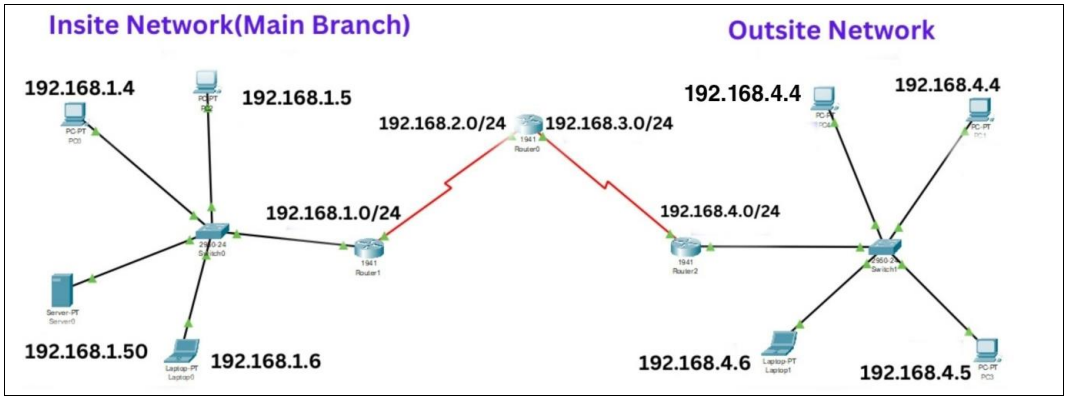

Fig 3: Proposed Network Design

5. Project Description

5.1 Implementation of Proposed Network System

Here, the authors used the Cisco packet tracer simulation to create the suggested network infrastructure. From our main office branch, we may communicate with sub branches or the hacker network here. Data from our main branch office must be shielded from hacker networks and sub branches. We employed an intrusion detection system to do this. Data sent from the main branch PC will be delivered to the sub branch or another computer; however, when data is sent from the sub branch PC to the main branch, our intrusion detection system (IDS) will identify the data first and prevent it from entering our main system through IP. That we are aware of through the server's Syslog, and we believe that someone else is attempting to compromise our system. We will also be aware of the IP and time at which they attempted to hack. We can keep our data safe by being watchful.

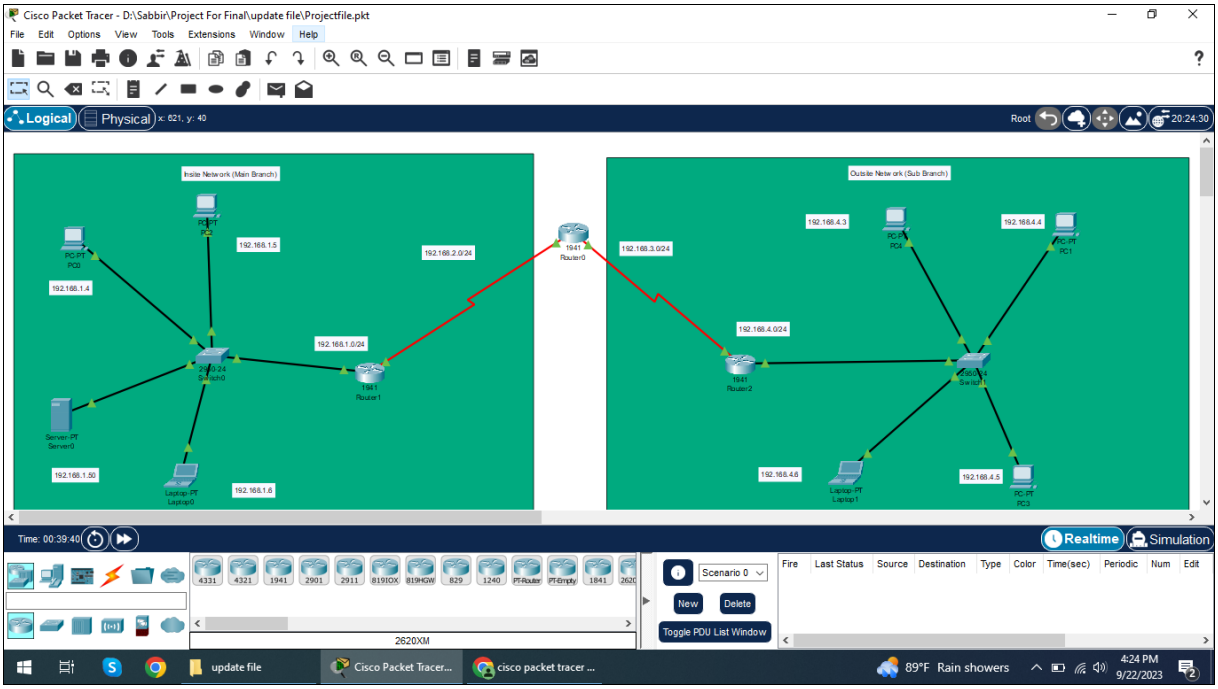

Fig 4: Implementation of Proposed System in CISCO Packet Tracer

5.2 Inside Networks (PC)

Inside Networks (PC): The internal main office branch computer is the primary storage location for a wide range of our vital functional data and information. It is a virtual gold mine of essential resources that are essential to the operation of our company. The main goal of our entire endeavor is to protect this priceless archive. Our steadfast dedication to this project is seen by the extensive and diverse tactics we have painstakingly implemented to strengthen our digital defenses. Our unwavering commitment to safeguarding the confidentiality and integrity of our data is demonstrated by our use of state-of-the-art technology, stringent security procedures, ongoing oversight, and a watchful organizational culture. These measures help to preserve the cornerstones of our operational excellence and strategic choices.

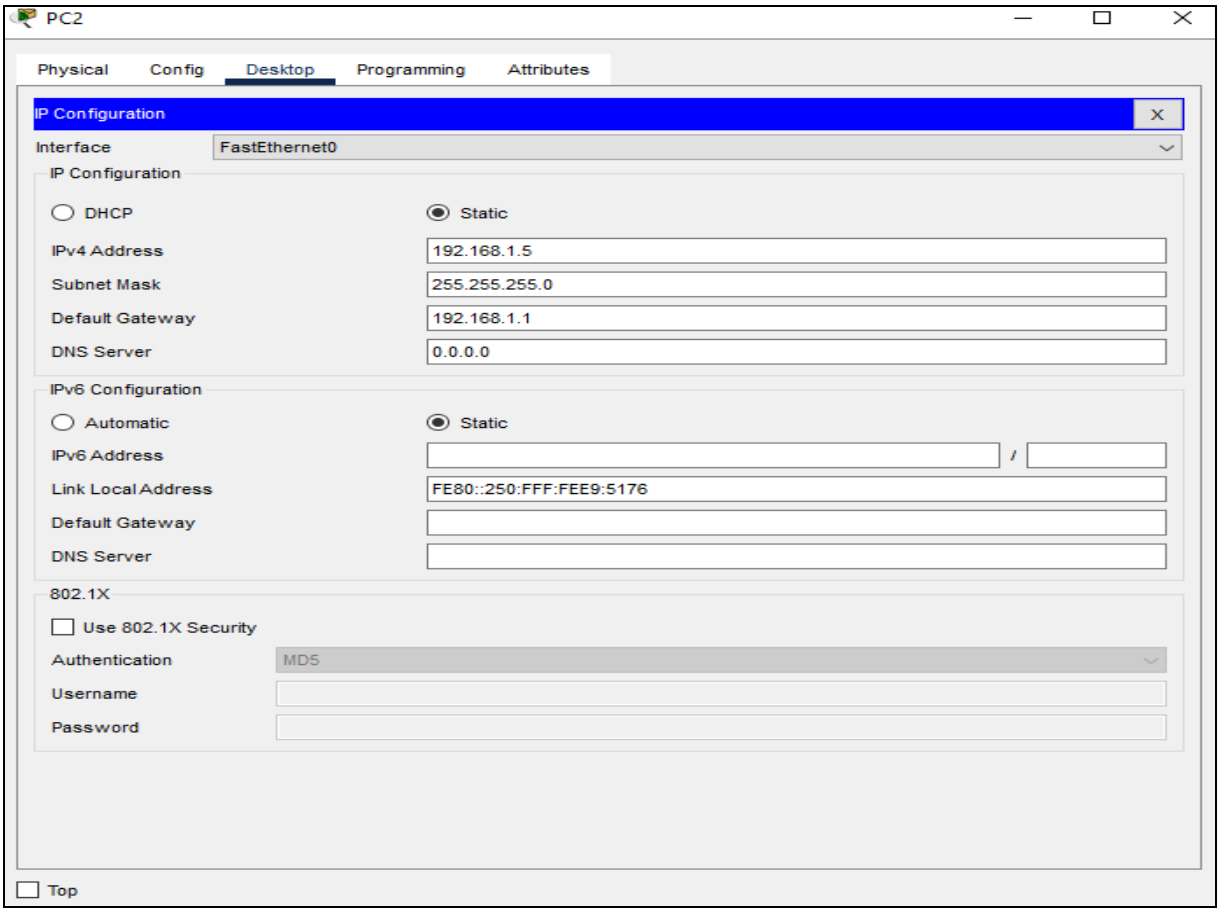

Fig 5: Inside Networks (PC)

5.3 Inside Communication

Inside Our Computer Pinging: The data packet, which was painstakingly assembled and processed, has been sent from the main branch computer (main branch), which serves as our operations' nerve center, to the subsidiary sub-branch, which is outside of our building. It has done so quickly and without error. This accomplishment confirms our commitment to maintaining a strong and connected network infrastructure that supports our organizational success. It also represents the pinnacle of our technical expertise and dedication to ensuring the smooth flow of information between our core operations and remote extensions.

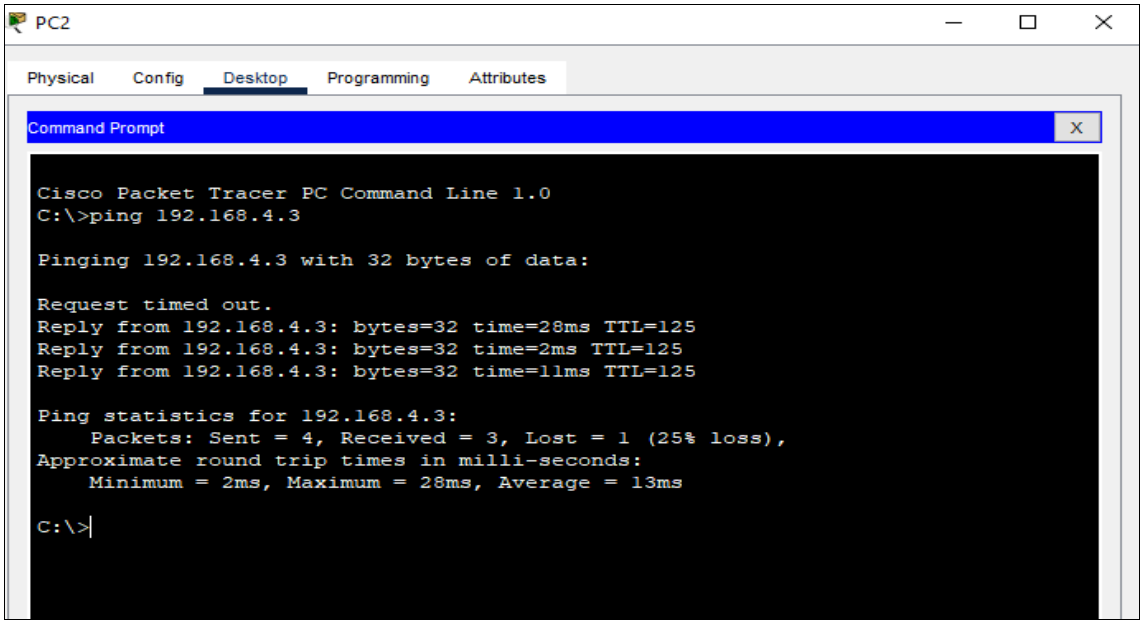

Fig 6: Inside Computer Pinging

5.4 Outside Network (PC)

Outside Network (PC): Staff members of the outside sub branch office or other individuals utilize this computer. This is an attempt by an external PC setup to communicate with the main branch, which is unacceptable.

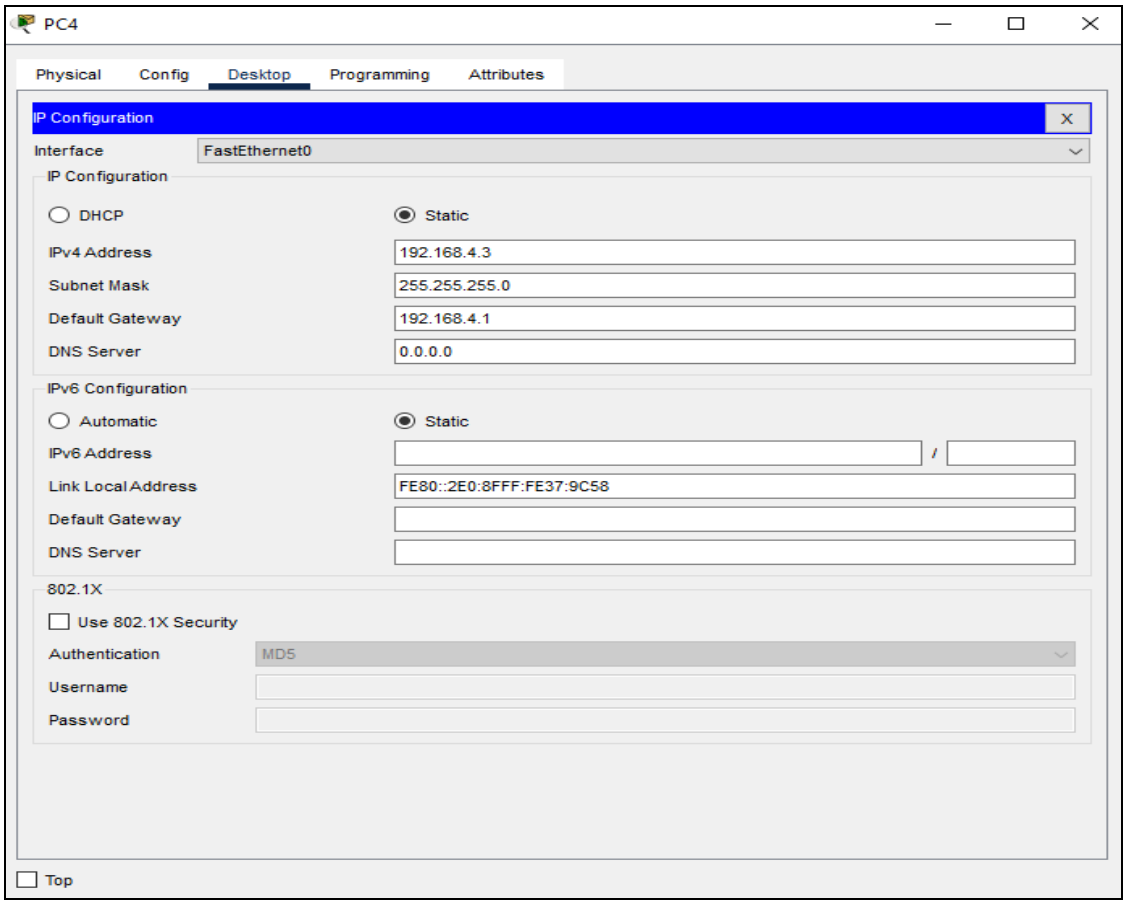

Fig 7: Outside Network (PC)

5.5 Outside/Hacker Communication:

Pinging outside our main branch: Data is not sent from Outside (Sub branch) computer to Inside (Main Branch). (IDS) immediately detects and blocks these data packets using intrusion detection system.

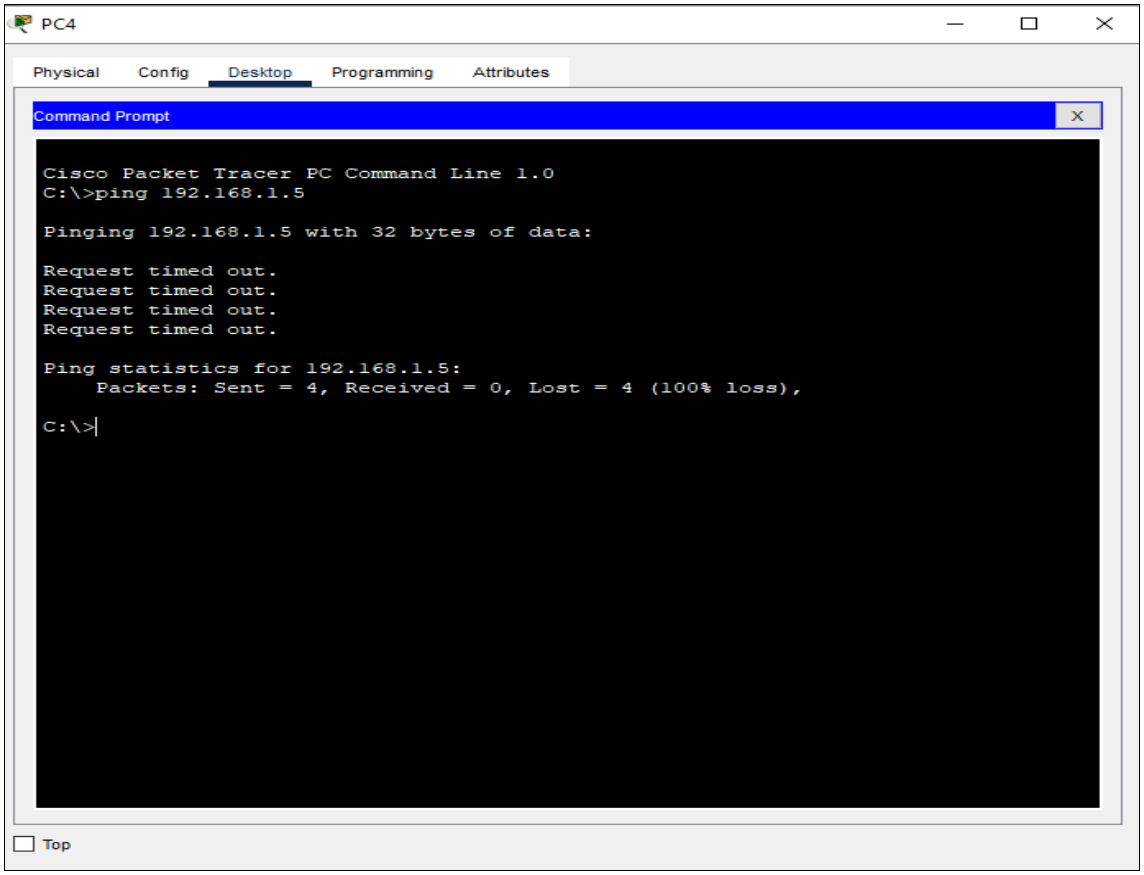

Fig 8: Outside Computer Pinging

5.6 Final Output (Blocked IP):

From the Inside (Main branch) computer to the external network (Sub branch), the data packet has been successfully sent. The Outside (Sub branch) computer does not, however, send data to the Inside (Main Branch) computer. This data packet was quickly identified and stopped by (IDS). Host Name, IP, and Message Block are shown in Server Syslog format.

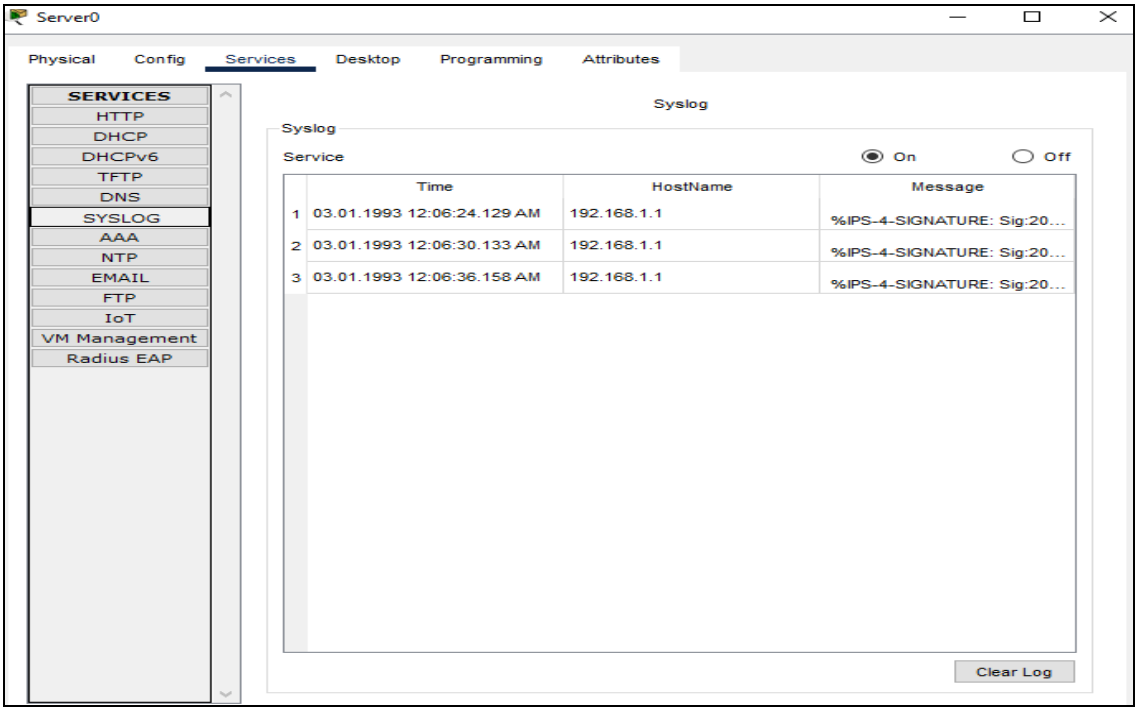

Fig 9: Final Output

6. Conclusion

In the field of network security, this study represents a rock-solid bulwark, offering an indispensable barrier against unseen attacks. Being a strong and powerful instrument, it is a reliable partner for companies, exhibiting unmatched expertise in quickly identifying and blocking illegal access to their network areas. The Intrusion Detection System (IDS) can detect anomalous activity that might indicate security breaches since it is always focused on the nuances of network traffic patterns. When these abnormalities are detected, the alert IDS immediately raises the alarm, informing the observant system administrator and enabling quick action and reaction to minimize possible harm and disturbance. But the IDS's function goes beyond protection; it is a source of insightful information and a driver for improving network efficiency. Because of its many uses, it is a vital component of any organization's security architecture, strengthening the digital landscape and increasing resilience. This research and the IDS it supports serve as a beacon of security in the always changing world of cyber threats, guaranteeing the integrity of digital operations and the ongoing protection of critical data. Its existence secures the basis of the contemporary digital world by strengthening defenses and enabling organizations to adapt and prosper in the face of complex and growing security threats.

7. Acknowledgments

This paper and the research behind it would not have been possible without the exceptional support of our supervisor, Mohammad Anwar Hossain. His enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept our work. Md. Sabbir Hossain and Rezaul Karim, my colleagues at World University of Bangladesh, have also looked over my transcriptions and answered with unfailing patience numerous questions about the Paper. I am grateful to all of those with whom I have had the pleasure to work during this.

8. References

1. Sandeep Singh. ‘Intrusion Detection Systems (Ids) and Intrusion Prevention Systems (IPS) For Network Security’ International Journal of Research in Engineering & Applied Sciences. 2020;3(3):2249-3905.
2. Suman Thapa, Akalanka Mailewa Dissanayaka. ‘The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks’, St. Cloud, MN; c2021. p. 56301.
3. Bilal Maqbool Beigh. Intrusion Detection and Prevention System, ARPN Journal of Science and Technology. 2020;2(7):2225-7217.
4. Ramalingam V, Saminathan R. ‘A Novel Survey on Intrusion Detection System and Intrusion Prevention System’, International Journal of Scientific & Technology Research. 2019;8(12);2277-8616.
5. Santos Kumar B, *et al*. Intrusion Detection System-Types and Prevention, (IJCSIT) International Journal of Computer Science and Information Technologies. 2020;4(1).
6. Safana Hyder Abbas, *et al*. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Global Journal of Engineering and Technology Advances. 2023;14(02):155-158.