International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1392-1401

Design And Development Of Intrusiondetection And Prevention System For Lan Based Networks

G.S.Anandha Mala[1], M. Deepika[2], B. Dharani[3], K.M. Keerthika[4]

[1]Professor, Department of Computer Science and Engineering, Easwari Engineering College, Chennai-89.
[2,3,4]Under graduate Student, Department of Computer Science and Engineering, Easwari Engineering College, Chennai-89.

Abstract

Nowadays, Internet and network technology have been growing rapidly, people are shifting towards the new technologies for various reasons. Although the growing technologies make life easier, one of the greatestproblemsof using those technologies is providing security against cyberattacks, security breaches and data leakages. Networks are more prone to the attacks because of vulnerabilities. Since, there are many techniques available nowadays for providing maximum security to networks. While considering the growth of network security many students are willing to build their career in networking and this could be possible while learning practically. So, we present a network based "Intrusion Detection and Prevention System (IDPS) for LAN based networks", which can efficiently detect many types of well-known network attacks and can immediately prevent the network system from the unauthorized access by providing security.Our approach is simple and efficient and can be implemented with some available opensource application such as GNS 3, Snort, Nmap, Wireshark, and Cisco Packet Tracer. The implementation of IDPS is done by using Rule based algorithm with Snort-rules and test for various simulated LAN based networks. This system will be the efficient and affordable learning platform for students to learn practically about network security.

Keywords--Cyber Attacks, Vulnerabilities, Security, Rules, LAN, Learning Platform.

1. INTRODUCTION

Cyber Security brings new challenges and opportunities for the hackers and the network security professionals. These challenges refer to the increased rate of cyber-crime. Since, we need to concentrate more on security of the networks and the new challenges created by the cyber criminals. Although we have many technologies to provide maximum security for the existing challenges, the real time security is still on research. So, the main contribution of the paper is to provide maximum security for the LAN networks and also an effective platform for students who learn network security in practical way. Network security is designed to protect the usability and integrity of any network. It includes both hardware and software technologies to target a variety of threats. It stops them from entering or spreading on network. IDPS is a software technology for detecting and preventing network threats. This system includes both intrusion detection and prevention system for protecting networks from security breaches. This system acts as a security layer between LAN network and the internet while sharing the data packets. This layer of protection will have certain user-defined rules to allow the packets inside and outside the network. If the packets arriving at the layer is a mismatch according to the rules defined then the layer authenticates the administrator regarding the threat.And the intrusion prevention system also recognises the threat simultaneously and provides protection for the network by some methods such as dropping the malicious packets,blocking traffic from the source address, resetting the connection of the network.

The process of the system states, when the unauthorized packets enter or leave the network the IDPS works as a security layer between the protected network and internet.

This will detect and prevent the networks from the attacks which may jeopardize the network function.The modules developed in this system includes Network Simulation Module, Intrusion Detection Configuration Module, Intrusion Prevention Configuration Module.

ISSN: 2233-7857IJFGCN

So, this system is proposed inorder to protect the networks both internally and externally, and also to support students for learning the methodologies practically and efficiently.

2. LITERATURE SURVEY

This method recognizes weaknesses, reports vindictive exercises, and orders preventive measures to stay aware of the progression of PC related violations utilizing a few reaction strategies. This paper presents a refreshed audit on IDPSs given the way that the latest audit found regarding the matter was done in 2016. It will likewise talk about the utilization of IDPSs to recognize weaknesses in different channels through which information is gotten to on a organization or framework and anticipation systems applied to alleviate against interruption[1]. The paper comprises of the writing overview of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that employments different information mining and scientific strategies calculations for the framework to work progressively. Information mining techniques are proposed for digital investigation on the side of interruption location[2].Thispaper presents the Network Intrusion Detection Framework (NIDS), which utilizes a set-up of information mining procedures to consequently distinguish assaults against PC organizations and frameworks. This paper centres around two explicit commitments: a solo peculiarity location strategy that doles out a score to each organization association that reflects how peculiar the association is, and an affiliation design investigation-based module that sums up those organization associations that are positioned profoundly atypical by the peculiarity location module. Trial results show that our peculiarity location strategies are fruitful in consequently identifying a few interruptions that could not be recognized utilizing well known mark-based devices Besides, given the extremely high volume of associations noticed per unit time, affiliation design-based rundown of novel assaults is very valuable in empowering a security examiner to comprehend and describe arising dangers [3]. This method represents intrusion recognition framework (IDS) is programming that computerizes the interruption discovery measure. An interruption counteraction framework (IPS) is programming that has every one of the capacities of IDS and can stop potential episodes. This paper gives an outline of IDPS advances. It clarifies the key capacities that IDPS advances perform and the discovery procedures that they use. Then, it features the main attributes of every one of the significant classes of IDPS advances. The paper likewise examines different kinds of IDPS security capacities, innovation restrictions and difficulties[4]. Intrusion Detection has gotten the basic part of Information Security and the significance of secure organizations has hugely expanded. Inspite of the fact that the idea of Intrusion Recognition was presented by James Anderson J. P. in the year 1980, it has acquired bunches of significance in the new years in light of the new assaults on the IT foundation. The main objective of this examination is to look at the current writing on different methodologies for Intrusion Discovery specifically Anomaly Detection, to analyse their calculated establishments, to taxonomize the Intrusion Detection System (IDS) and to build up a morphological system for IDS for simple arrangement. In this investigation a nitty gritty overview of IDS from the underlying days, the advancement of IDS, models, segments are introduced [5]. This Survey, regarding various methods and techniques of handling network attacks provides a clear analysis about network based IDPS. Based on the survey, hereby an IDPS system has been proposed in paper that acts as a effective learning platform for network security maintenance in various distributed and complex networks.

ISSN: 2233-7857IJFGCN

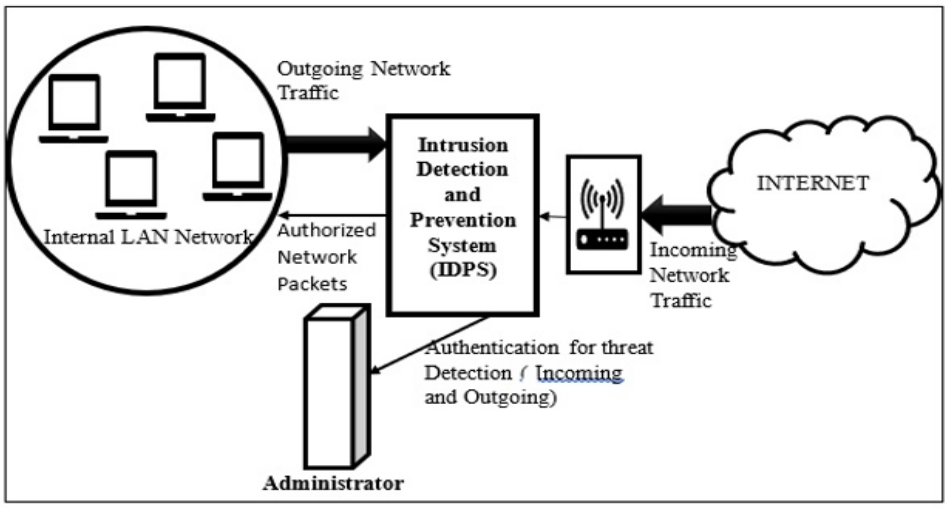

Figure 1: System Architecture of IDP System

3. PROPOSED INTRUSION DETECTION AND PREVENTION SYSTEM

For Students, the practical knowledge about security maintenance is necessary for easy understanding and to gain a clear knowledge about security and also to make learning easier and adventurous for learners. So, we propose an Intrusion Detection and Prevention System(IDPS) as a platform for students to learn network security practically and efficiently by using the open source and affordable applications such as GNS3 which allows the combination of virtual devices to simulate various simple and complex networks. It uses Dynamics emulation software to simulate.

Cisco Packet Tracer with IOS images, this feature simply makes it much easier. Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Snort, it is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect suspicious anomalies.

Nmap, it is one of the core tools used by network administrators to map their networks. This program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection. This IDPS system has the capability of monitoring both incoming and outgoing network traffic for LAN based networks.

In this proposed system, Security breaches from both internal and external networks are detected and also prevented by using rule based IDPS. It also provides prevention for the network traffic transmitted from the server itself by using the IPS methodology.

ISSN: 2233-7857IJFGCN

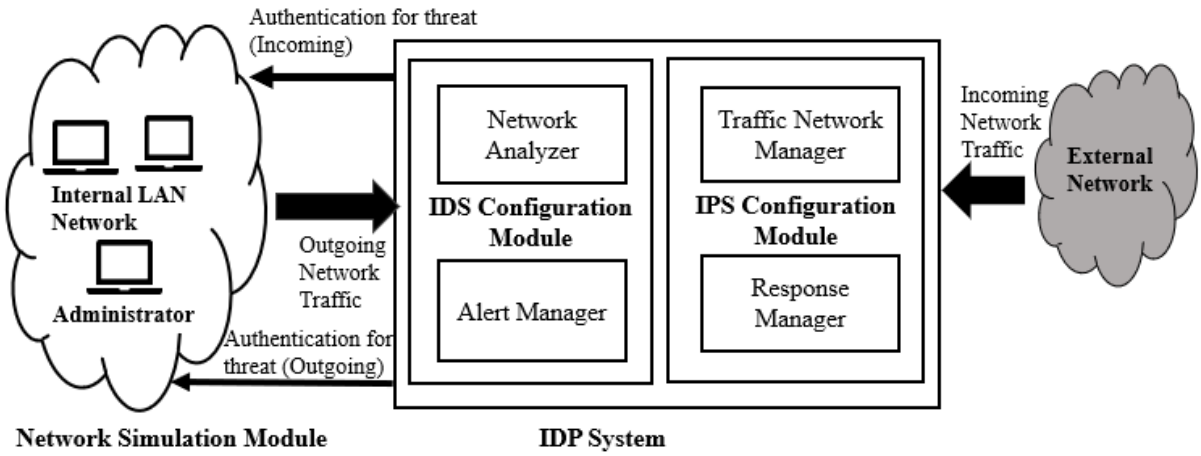

Figure 2: Functional Architecture of IDP System

3.1. LIST OF MODULES

1. Network Simulation Module
2. IDS Configuration Module
3. IPS Configuration Module

3.1.1. MODULE – 1 (NETWORK SIMULATION MODULE)

Network simulation is a technique where a software program models the behavior of a network by calculating the interaction between the different network entities. Graphical Network Simulator-3 (GNS 3). It allows the combination of virtual and real devices, used to simulate complex networks. This module creates a simulated LAN based computer network with various network entities such as routers, switches, links, access points, devices etc., using GNS 3 network simulator.

The GNS3 network simulator is a convenient open source tool for the design and simulation of Cisco-based networks.A Network Simulator virtualizes your hardware enabling it to support the operating system of different networking devices. A good example is GNS3. When you use a router in GNS3, you are running the real device operating system.Network simulators can help you design the desired network on the virtual drawing board and develop network infrastructures, offering several advantages:

- You can design the environment to match your ideas.
- The design can be tested virtually at no great expense before implementation; also, you don't have to implement and maintain a real test network, and no risk is involved.
- Routers can be rolled out with just a few mouse clicks. You can even build a complex network topology with manageable overhead.
- Modelling traffic patterns is easy.

GNS3 supports both emulated and simulated devices. In practice, this means you could run a copy of a physical Cisco IOS router on a virtual, emulated Cisco router. GNS3 simulates router functions such as switch functionality. In practice, you do not run two operating systems in parallel; instead, IOS runs on a GNS3 switch. If you use GNS3 on macOS or Windows, the developers advise you to use the GNS3 VM; you have the choice between a VMware or VirtualBox VM. For performance reasons, the GNS3 developers recommend VMware. Before you can use the VM in the simulation environment, open it within the respective VM environment, and then start GNS3. The program comes up with the setup wizard.

ISSN: 2233-7857IJFGCN

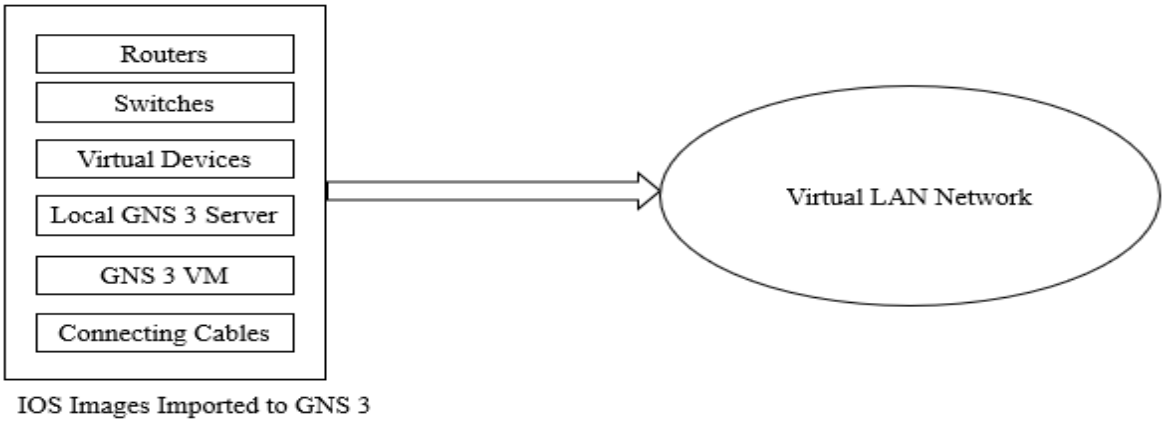

Figure 3: Network Componentsof GNS 3

3.1.2. MODULE – 2 (IDS CONFIGURATION MODULE)

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion Detection system also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications. Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations. An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats.

In this module Intrusion detection system monitors traffic from all devices of both internal and external network. IDS will detect malicious packets as theyenteringthe network and encounters unusual behavior on the network. It performs analysis on the traffic looking for patterns and abnormal behaviors upon which a warning is sent to administrator. This module includes traffic analyzer that monitors traffic for abnormal behaviors and unmatched pattern based on the rules provided for detection of various cyber-attacks. It also consists of an alert manager that sends warning to the administrator about the attacks detected by IDS Configuration Module.

ISSN: 2233-7857IJFGCN

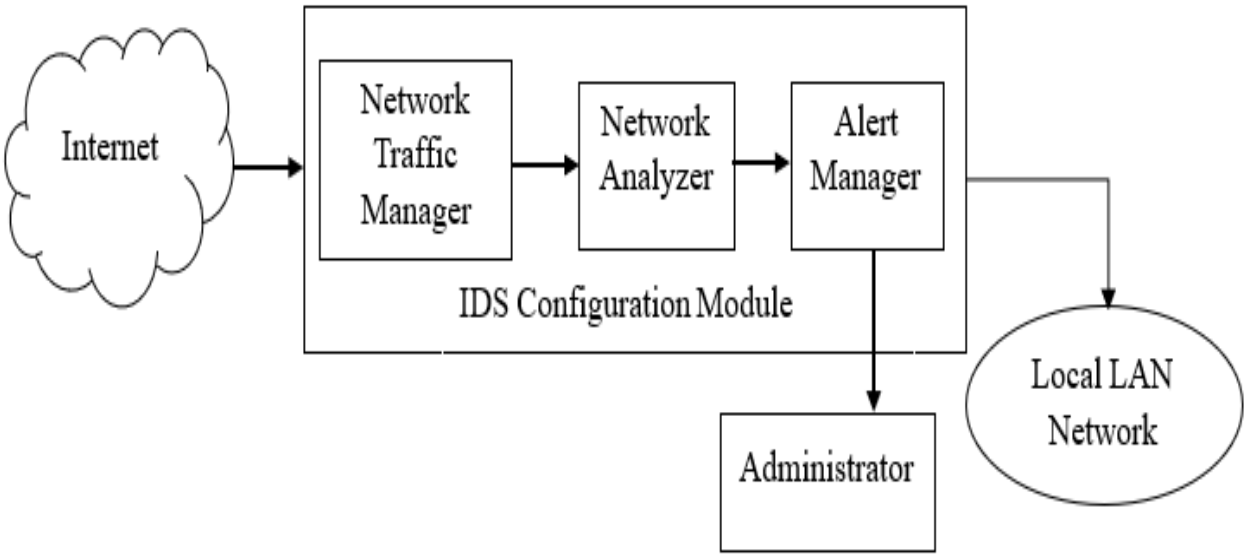

Figure 4: IDS Configuration Module

3.1.3. MODULE – 3 (IPS CONFIGURATION MODULE)

An Intrusion Prevention System (IPS) is a network threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Intrusion prevention systems (IPS) are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and be able to actively prevent or block intrusions that are detected. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.[23] An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.

The IPS configuration module includes response manager that executes the prevention methodology in response to a cyber threat to prevent security breaches.This module also includes network traffic manager which performs the following activities: Dropping the malicious packets, blocking traffic from the source address, Resetting the connection.

ISSN: 2233-7857IJFGCN

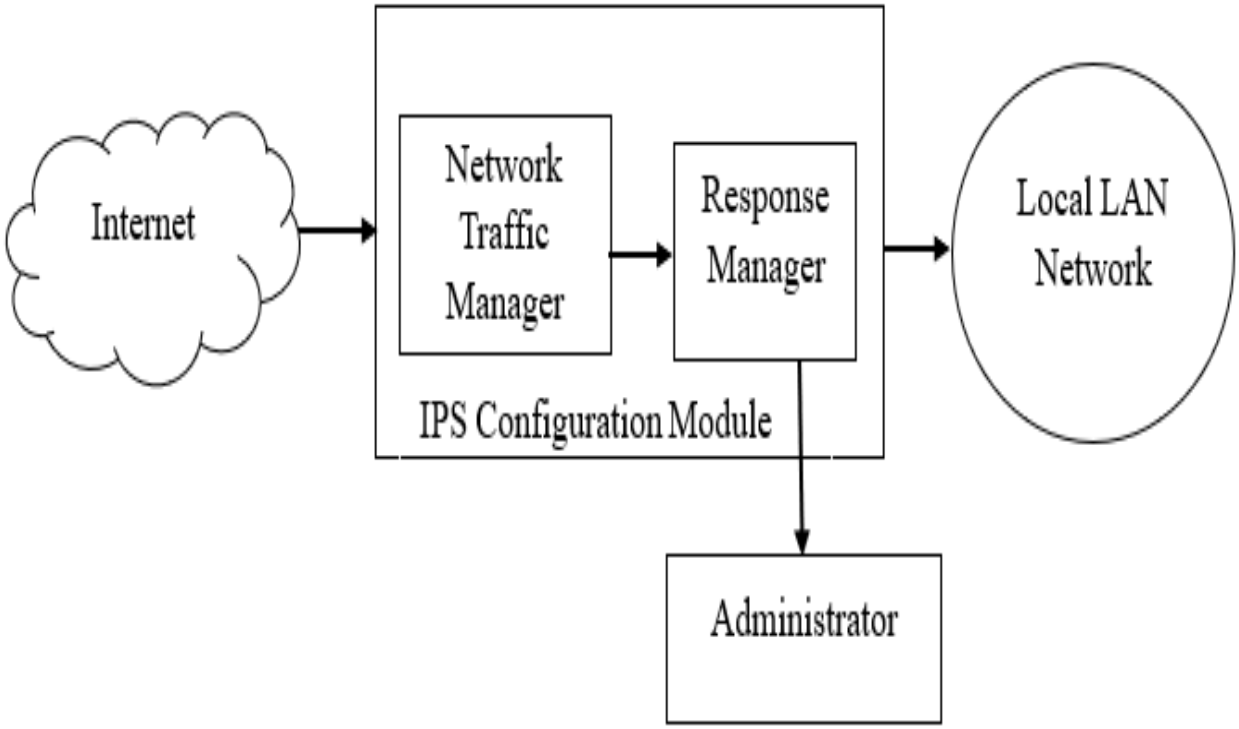

Figure 5: IPS Configuration Module

4. WORKING OF IDPS SYSTEM

4.1. NETWORK SIMULATION

In this module, we would develop virtually simulated network using GNS 3. This is to experience the state and monitor the networks while attackers flood the target system with
connection requests from spoofed source. Here in the given networkdiagram, we have an internal network which contains few systems, connected to a switch connected to a web server. The Internal network is connected by a Cisco 3725, router's hypervisor run on 127.0.0.1:7200, console is on port 2101, aux is on 2501, Fast Ethernet 010 is connected to attacker Fast Ethernet 010 Fast Ethernet is connected to switch sw1 port 1.

The switch is further connected to systems in the Lan. We assume that the attacker attacks from outside the internal network and tries to flood the target system by flood of ICMP messages. Large number and different large size ICMP packets are being send to the victim. This all is being tested and simulated using GNS3which provides graphical user interface to simulate complex networks while being as close as possible from the way real network and devices perform.

ISSN: 2233-7857IJFGCN

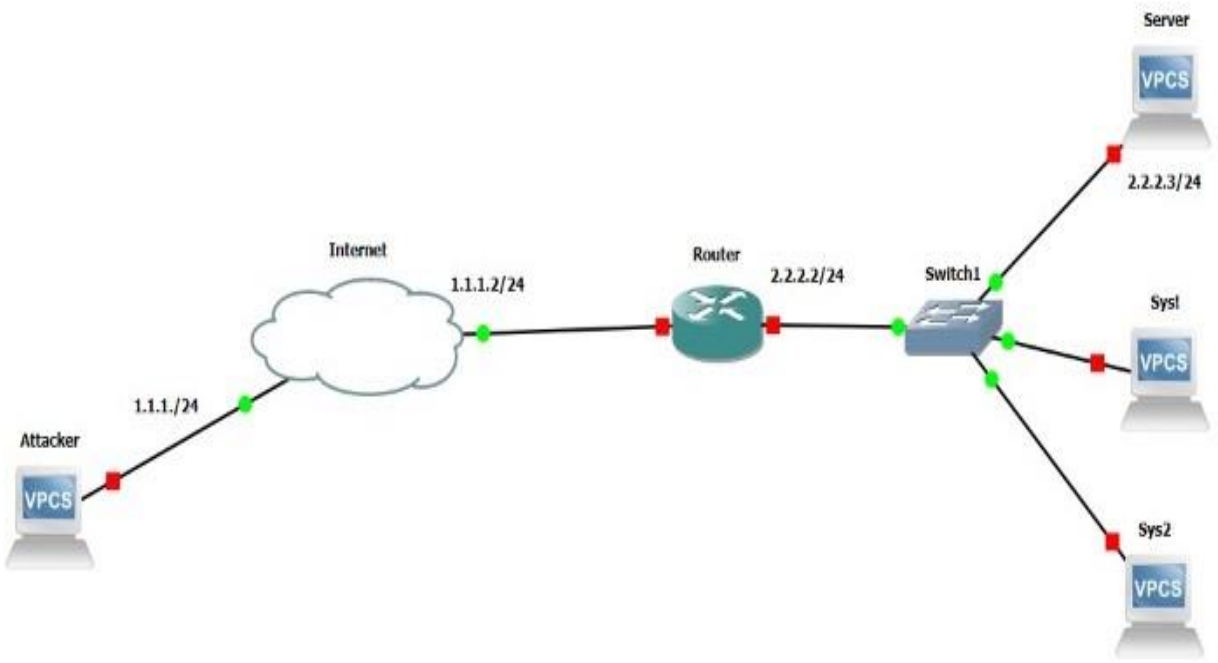

Figure 6: Local LAN Network

4.2. IDS CONFIGURATION

Network Intrusion Detection Configuration Module operates at the network level and monitor traffic from all devices going in and out of the network. NIDS performs analysis on the traffic looking for patterns and abnormal behaviours upon which a warning is sent. In ethical hacking, if a port scanner is performed on a network secured by an IDS, it is flagged, and it is investigated further. A warning is also flagged if the NIDS detects a change in the predetermined conditions such as the standard packet size as well as the standard traffic load.
An example of this is NIDS detects abnormal packet behaviour in application protocol verification.

Some advantages of NIDS include:

- NIDS can be easily introduced into an existing network with minimal disruptions.
- Maybe undetectable by attackers and are mostly immune to direct attacks.

Some notable disadvantages are they at times cannot handle large traffic volumes, and they cannot analyse encrypted data as well as fragmented packets. The algorithms used for the IDS are Signature-Based Detection, Anomaly-Based Detection, Stateful Protocol Analysis.

The types of attacks enhanced by the IDS System includes:

- Active Attacks:
    1. Spoofing
    2. Modification
    3. Wormhole
    4. Fabrication
    5. Denial of services
    6. Sinkhole
    7. Sybil
- Passive Attacks:
    1. Traffic analysis
    2. Eavesdropping
    3. Monitoring

ISSN: 2233-7857IJFGCN

4.3. IPS CONFIGURATION

An intrusion prevention system is an automated network security device used to monitor and respond to potential threats. It will work by actively scanning forwarded network traffic for malicious activities and known attack patterns. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signature database for known attack patterns. An IPS might drop a packet determined to be maliciousand follow up by blocking all future traffic from the attacker's IP address or port.Intrusion prevention systems also perform more complicated observation and analysis, such as watching and reacting to suspicious traffic patterns or packets.

Detection mechanisms can include:

- Address matching
- Generic pattern matching
- TCP connection analysis
- Packet anomaly detection
- Traffic anomaly detection
- TCP/UDP port matching

An IPS will typically record information related to observed events, notify security administrators, and produce reports. To help secure a network, an IPS can automatically receive prevention and security updates inorder to continuously monitor and block emerging Internet threats.

5. RESULT

The final result by implementing this system will provide the following experiences of the networks.

- Network based system which does not require the system to be installed in every node.
- Free from trust problem.
- Free from message spreading difficulties.
- As all the packets of the network are received from the server, the rest of the network does not have to bother with the intrusion.
- The total system is self-sufficient.

6. CONCLUSION

Theproposed IDP System with rule-based algorithm is implemented for the learning platform concentrates on developing tools for detectingattacks and threats against unauthorized computer systems andgiving satisfactory results compared to standardsignature-based tools. This system implementation successfully performs network traffic monitoring tends to have veryhighvolume, dimensionality and heterogeneity with the rule-based algorithm. But there is a need for high performance algorithms that will scale to very large network trafficdata sets between complex networks. This system also provides the prevention and detection mechanism for outgoing traffic specifically. This platform has to be improved in future for real-time intrusion detection for various distributed and complex networks. And this software can be further developed with algorithms for miningdata streams which isnecessary for building real-timeintrusion detection system.Therefore, development of a co-operative anddistributed intrusion detection and prevention system for correlatingsuspicious events among multipleparticipatingnetwork sites to detect coordinated attacks in real time will be oneof the key components to be considered in future development of this platform.

7. REFERENCES

1. NureniAyofe Azeez, Taiwo Mayowa Bada, Sanjay Misra, Adewole Adewumi, Charles Van der Vyver and Ravin Ahuja, 2020, "Intrusion Detection and Prevention Systems: An Updated Review", researchgate.net Publication.
2. Amol Borkar, Akshay Donode, Anjali Kumari, 2017, "A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS)", IEEE 2017, ICICI 2017.
3. Bane Raman Raghunath, Shivsharan Nitin Mahadeo, 2008, "Network Intrusion Detection System (nids)", IEEE 2008, First International Conference on Emerging Trends in Engineering and Technology.

ISSN: 2233-7857IJFGCN

4. M.Azhagiri, Dr A.Rajesh, Dr S.Karthik, 2015, "Intrusion Detection and Prevention System : Technologies and Challenges", Researchgate.net publication, International Journal of Applied Engineering Research.
5. D. Ashok Kumar, S. R. Venugopalan, 2017, "Intrusion Detection Systems: A Review", International Journal of Advanced Research in Computer Science.
6. Tomar Kuldeep, Tyagi S.S, 2014, "Enhancing Network Security by ImplementingPreventive Mechanism using GNS3", IEEE 2014, International Conference on ROIT, 2014.
7. Dr.V.Suganthi, P. K. Manoj Kumar, 2018, Intrusion Detection System – A Literature Survey, Nehru E-Journal.
8. D. Selvamani1 and V Selvi, 2018, "A Literature Survey on the Importance of Intrusion Detection System for Wireless Networks", Asian Journal of Computer Science and Technology.
9. Anamika Chauhan, Rajyavardhan Singh and Pratyush Jain, 2020, "A Literature Review: Intrusion Detection Systems in Internet of Things", IOP Publishing, CMVIT 2020.
10. Weiwei Chen, Fangang Kong, 2017, "A Novel Unsupervised Anomaly Detection Approach for Intrusion Detection System", 2017 IEEE 3rd International Conference on Big Data Security on Cloud.
11. Dali, L., Bentajer, A., Abdelmajid, E., Abouelmehdi, K., Elsayed, H., Fatiha, E., & Abderahim, B. (2015). "A survey of intrusion detection system". 2nd World Symposium on Web Applications and Networking doi:10.1109/wswan.2015.7210351.
12. Dorothy.E. Denning, 1987, "An intrusion-detection model". IEEE Transactions Software Engineering, 1987.
13. Bakshi, A., & Dujodwala, Y. B. (2010). "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine". 2010 Second International Conference on Communication Software and Networks. doi:10.1109/iccsn.2010.56.
14. Usha Kiruthika,Thamarai Selvi Somasundaram, S. Kanaga Suba Raja, (2020) 'Lifecycle Model of a Negotiation Agent: A Survey of Automated Negotiation Techniques', Group Decision and Negotiation, ISSN 0926-2644, Volume 29, Issue - 6, pp. 1239–1262. https://doi.org/10.1007/s10726-020-09704-z.
15. M. M. Shurman, R. M. Khrais and A. A. Yateem, "IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS," 2019 International Arab Conference on Information Technology (ACIT), Al Ain, United Arab Emirates, 2019, pp. 252-254, doi: 10.1109/ACIT47987.2019.8991097.
16. Patel, Manish M., and Akshai Aggarwal. "Security attacks in wireless sensor networks: A survey." Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE, 2013
17. P. Gokul Sai Sreeram, Chandra Mohan Reddy Sivappagari, "Development of Industrial Intrusion Detection and Moni-toring Using Internet of Things", International Journal of Technical Research and Applications, 2015.
18. P. Kasinathan, C. Pastrone, M. Spirito, M. Vinkovits, 2013," Denial-of-service detection in 6LoWPAN based Internet of Things, in: Wireless and Mobile Computing, Networking and Communications (WiMob)", 2013 IEEE 9th International Conference on, 2013, pp. 600–607.
19. J. Amaral, L. Oliveira, J. Rodrigues, G. Han, L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks, in: Communications (ICC)", 2014 IEEE International Conference on, 2014, pp. 1796–1801
20. V. Jyothsna, V. V. Rama Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, 2011.
21. Rahim, R., Murugan, S., Priya, S., Magesh, S., & Manikandan, R. Taylor Based Grey Wolf Optimization Algorithm (TGWOA) For Energy Aware Secure Routing Protocol.
22. Efficient Contourlet Transformation Technique for Despeckling of PolarimetricSyntheticApertureRadarImage Robbi Rahim, S. Murugan, R. Manikandan, and AmbeshwarKumarJ. Comput. Theor. Nanosci. 18, 1312–1320 (2021)

ISSN: 2233-7857IJFGCN