International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

Network Monitor To Detect and Classify The Type of The Attack

Femilda Josephin J S, Rutuja Matey, Shreya Singh

Abstract*: This paper implements the security in computer networks. There is a quick increase in the number of networks and the insufficiency of the security leads to the muddle. This project concentrates on the security issues in the broadcast networks. We codify different types of network attacks that are possible. Our basic goal is to show the various types of attacks and then classify them to remove from the network and to determine all the security violations possible. Our project is similar to the intrusion detection in the systems based on the host. The network attacks are simulated and it shows how the monitor is able to detect attacks. Also we aim to remove those attacks simultaneously as soon as it is detected.

***Index Terms*: Attacks, Encryption, Local Area Network, Network Security Monitor, Security, Wide Area Network.**

I. INTRODUCTION

Networking is a connection between the different systems to communicate with each other. It is very important to have a secured network to assure that the data that is sent is not received/hacked by anyone else. Network Security Monitor is developed to know what are the different possible attacks can be used which can damage the network and it also helps to remove it. The security breaches are the illegal access to the data, services and application using the undisclosed security system. It is completely dependent on the nature whether it is high or low risked according to the event. In any organization, the breaches are detected and removed
Network security monitor is one of the most important
Systems because of the growth in the network in different fields like academics, businesses and other research organizations. All of this are connected to the outside environment via the wide area networks. The attacks such as eavesdropping, accessing others information, using others system, giving incorrect information in the files and to pile the information which results in the inefficient capacity of the network [5]. The attacks that we are going to discuss is brute force attack which is one of the very common attack to access other's data using the trial and error method. The second is DDos which is also commonly used for the hacking of the popular sites to temporarily or permanently damage it. The third attack is Black Hole attack which denies to send the packets to the desired destination. To prevent all this attacks, it was very important to have the proper encryption of the data to send from one place to another or to upload it in the safer environment. But due to the insufficiency of the encryption techniques to protect the information because of the pirated key or the misuse of the legal users, here we handle the problem from a different point.

The literature survey for the monitor is given in the section II. The basic system model is given in the section III. The security measures and the attacks shown is given in the section IV.

In this paper a network monitor which is able to monitor the current network activity is developed. If there is any doubtful act or any security violations, the monitor is able to detect the attacker and take security measures accordingly.

II. RELATED WORK

In [1] the authors have suggested the objective framework, which should be shielded from attacks , comprises of various host PCs (counting gadgets like document and name servers, printers, etc.) and a LAN which handles the association between the hosts. The LAN is accepted to utilize a communicate source, like Ethernet, and all bundles that through the LAN are transmitted, are conceivably accessible to all gadgets associated to the system. The LAN is additionally considered physically secure, as in an aggressor (gatecrasher) won't have the capacity to specifically get to the system equipment, for example, the associating medium (link) and the interfaces of the system at every host. The LAN is associated with the real world by means of at least one portals. The Intrusion Detection frameworks are programming based frameworks that monitor PC client conduct review information (and other PC framework occasions) with a specific end goal to identify and signal potential external harmful acts and unseemly utilization of a PC framework[6]. These location frameworks can be utilized to help distinguish potential outside culprits, inside misusers (who surpass or manhandle benefits), and disguising programs (Trojan steeds). Culprits may try to get to or control information (for criminal or non-criminal purposes), presenting malware (counting yet not restricted to infections, worms, and Trojan steeds), or inquiring about a framework for a future attack. The digital assault on digital physical data foundation is generally one-sided toward the charge and control of physical framework.[2,9] It has been an intentional reception of epistemological defenselessness. This helplessness selection is because of the poor propensities for data utilization, and in addition long standing, to this point unexploited purposes of disappointment now completely presented to hacking. Most associations need exact danger discovery and educated hazard administration abilities[4,5].

Manuscript published on 28 February 2019.
***Correspondence Author(s)
Femilda Josephin J S, Department of Software Engineering, SRM Institute of Science and Technology, Chennai, India.
Rutuja Matey, Department of Software Engineering, SRM Institute of Science and Technology, Chennai, India.
Shreya Singh, Department of Software Engineering, SRM Institute of Science and Technology, Chennai, India.

In this way, the reaction to new data security dangers can be a "security insight" approach with a responsive new arrangements or tenets. A comparative study of arrangement calculations to create a preparation show utilized for misuse discovery was given by the authors in [3]. Positives of the types true and false and negatives of the types true and false were identified.

In [7] the authors have presented research work based on a framework for wireless sensor network security. It is based on the Integrated Technical Reference Model. It is made of three planes: The data plane which is used for the data processing side of the system, the control plane which is used to set the aim and control the system and the behavior plane which is a path for the feedback. This face of the I-TRM revolves around fundamental security issues checking key foundation, secret, confirmation, security, additionally, secure guiding.

The participation of endeavors can be analyzed under two situations[4]. In the main situation, there is a degree of trust between the included accomplices who can participate what's more, trade information specifically without the intercession of intervening element. In the other situation, there isn't enough trust amongst accomplices and for this situation, an approved outsider has to be set up to guarantee the trading of information and in addition control and observing of collaboration between accomplices. It is important for the people working on network to know about the securities related to it as the number of hackers are increasing. The network needs more effective methods to create awareness on the WLAN risks. The vulnerability of the network has revealed that it can misuse the network. It should be encrypted so that the network traffic and the other activities should not create a problem in the communication. The analysis should be done by using different security measures.

III. PROPOSED ARCHITECTURE

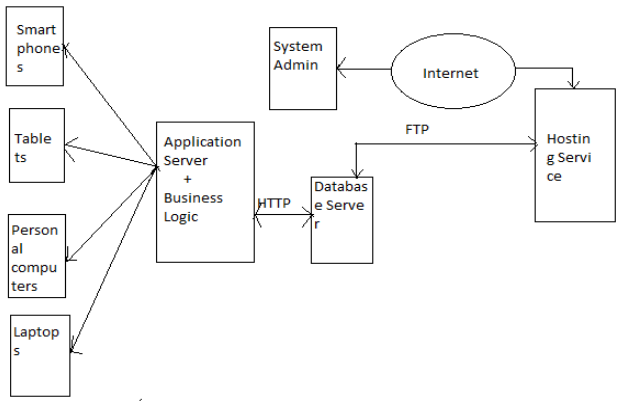

Fig 1. System Architecture

In this, the target system is the one on which the protection is applied, which consists of a number of host computers and a LAN (Local Area Network) through which it is connected. It is the main distribution system of the network. Here we consider the LAN to be secured and the attack that is going to happen is from the outside world i.e WAN (Wide Area Network). The intruder's approach can be given as to capture any less secure host and then use his trust to set the attack on the main target.

In this way, the basic mechanism of the system is given and the attack is simulated. Fig 1. shows the architecture of the proposed system.

IV. SECURITY MEASURES

A.IP blocker

It is a type of security measure that blocks a connection between a group of Ip addresses. This is usually done to protect our system from the harmful sites and hosts. This method is generally applied by companies to block intrusion and to limit the number of sites that can be visited by employees. It is also implemented by schools and other academic organizations to protect the data and records. In this project, we are blocking the ip addresses that are not appropriate for the network to make the network more secure.

B .Honeypot

Honeypot is a type of system that is used to trap the hackers and track their hacking methods. Honeynet is formed by setting multiple honeypots over the network. It is very easy to employ and the information gathered through honeypot is precious to study the hacker's intention. So, in this way, we will be applying the honeypot over the network to know about the hacker, track their behavior and block them using security tools.

C .Encryption-Decryption

This is the basic methodology of sending the data from one side to the other so that the data is secured while travelling from one place to another and it is done by using specific public and private keys. In this project, we are using the encryption-decryption so that the data will be converted into the cipher text to transfer and then to plaintext after received.

V. ATTACKS IMPLEMENTED

A. Brute Force attack

This is a trial and error method in which the attacker tries to obtain the information such as passwords, files, personal identification number. In this attack, an automated software is used to generate a large number of guesses. It can be used by the criminals to crack the data or by the security experts to test any system's security. In this project, we have showed that only three chances are given to the user to access any uploaded file. If it exceeds more than three, then it is considered as the attacker and a pin is sent to the corresponding email id to recover the access to the account.

B. DDos

This type of attack is used by the attacker to wreck the popular sites to damage it temporarily or permanently. It uses a number of hosts to flood a server which results a complete crash of the system. This disables the main system and then stops it from operating.

VI. PHASES OF ATTACKS ON NETWORK COMPUTERS

There are different levels in which the attack is done and the post effects are observed. The phases are:

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A. The Preparation Phase

In this phase, the attacker tries to determine how far he can invade the privacy of the system. It can be done by interrupting the system, trying common passwords, attacking the system and weakening it.

The main purpose is not to get detected during the attacks.

B. The Attack Phase

In this phase, the attacker attacks on the services offered by the hosts, networks and the services used by the hosts. It tries to interrupt which can be easily done due to the poor choice of the passwords or because of the bugs in the system which allows the attacker to use the services.

C. Analysis Phase

In this phase, the damage done after the attack is checked and the tools that can be used to remove the problem is used. The network monitor shows us what type of attack it is and what can be used to remove it and make the system more secure for future uses.

VII. RESULTS AND DISCUSSIONS

A. Brute Force Attack

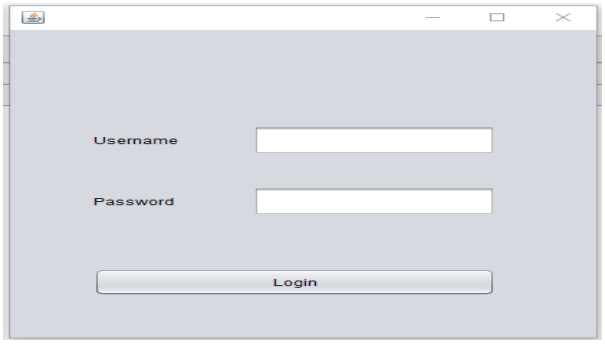

Fig 2. User login page

Fig 2. shows the basic registration and login module where the users get authenticated.

File Handling Module where all the files are to be searched from the files given:

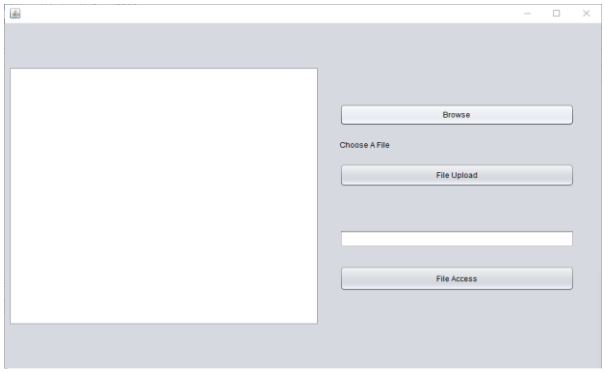

Fig 3. File browsing module

Fig 3. shows the file browsing module in which the file that is to be uploaded is selected. If the attacker logs in and tries to access the file using trial and error method, after the three trials, the hacker(as user) is blocked.

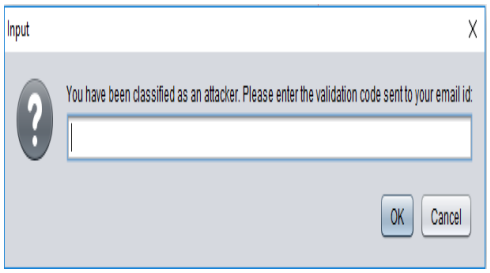

Fig 4. Validation code

As in fig 4. the validation code is sent to the id to check if you are the attacker or not. If you are not the hacker, then after entering the code, you are allowed to log in again otherwise, you are blocked.

B. HoneyPot

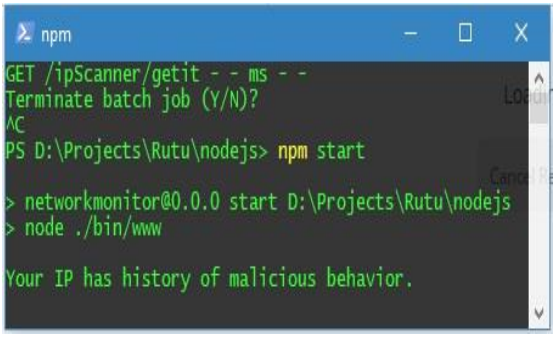

Fig 5. Detection of Honey Pot

The honeypot is used to track the intentions of the hacker. If the IP address contains harmful data that is sent by the hacker, then it is blocked using the security tools. Fig 5. shows the presence of Honey Pot.

C. IP Blocker

If the IP that is used contains malicious sites, then it is blocked by the IP Blocker.

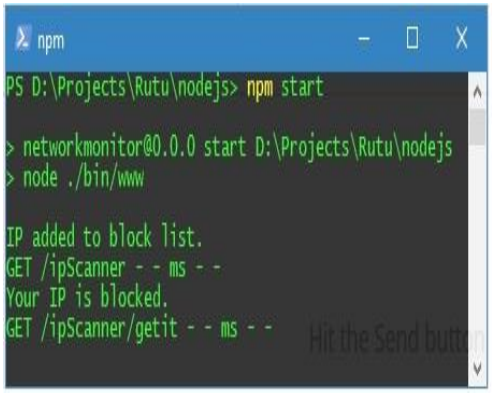

Fig 6. IP Blocker

D. DDos

If the attacker tries to flood the system and to stop it from operating, then the IP's are blocked by the security tools.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

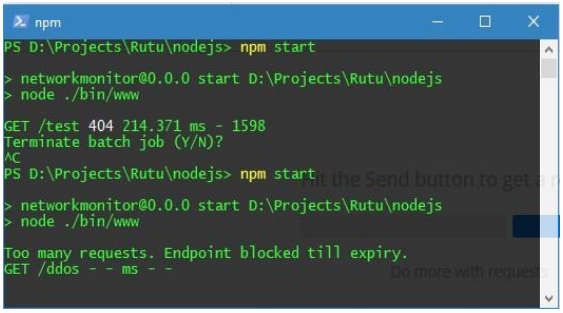

Fig 7. Identification of DDoS Attack

Fig 6 and 7 discusses about the avoidance of IP blocker and DDos attack respectively.

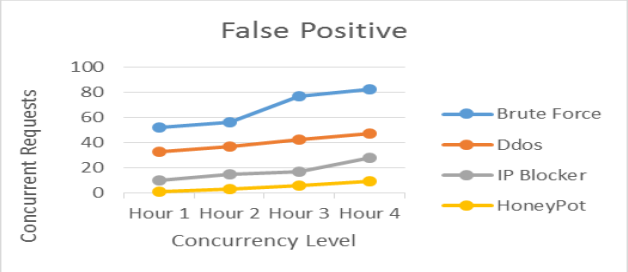

Fig 8. False positive

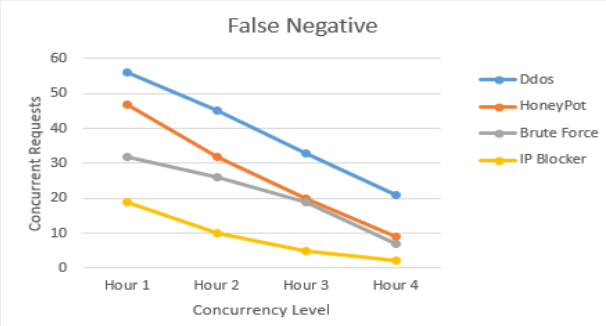

Fig 9. False Negative

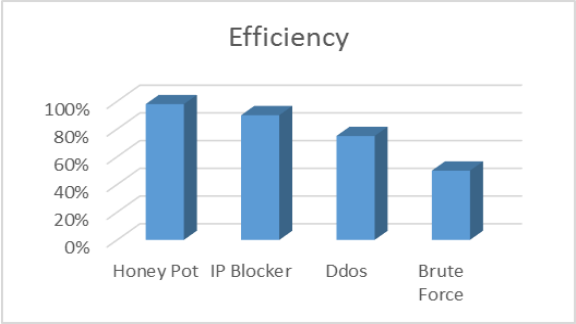

Fig 10. Comparison of efficiency of attack blockers

Fig 8. shows the concurrency level of the requests sent on hourly basis and it is compared to the other attacks. As it is shown that the Brute Force attack has high range of false positive attacks detection while the HoneyPot has low range as it checks the behaviour of the attacker and then blocks it while Brute Force can be handled by trial and error method.

Fig 9. shows the DDos has the high range of False Negative attacks while Ip Blocker is given as the low ranged. As it shows that Ip Blocker uses manual data so it is more accurate and has less chances of losing attacker. In this way, the honeypot is more efficient of all while the Brute Force is less secured comparitively as shown in fig 10.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have discussed about the network security needs and how to implement the security measures. The different types of attacks are simulated and are removed to get a secure network. If any suspicious activity is examined which is different from the previous one that are stored in the database, then it is removed using the tools and safety is given to the network. This models gives us the hierarchical approach. So, in this way, it becomes easier to detect the attack and then remove it while going from host to host, then services and then its connections. If the suspicious behavior is seen in the lowest levels, then it is sent to the upper levels. This is the basic method in which the Network Security Monitor works. This paper also shows a model of network attacks in which the form of the attack, the services that are used and the cause of the attack is reflected. The common work done here is that the user gets the gain to the network and then it attempts to decide what the host can offer or try to damage the network. Many attacks are detected in this network security monitor. In future, this project can add more attacks like the password based attacks, identity spoofing, sniffer attack and application layer attack. Also, the security monitor is made more secure by adding more security measures.

REFERENCES

1. L.T.Heberlein, G.V.Dias, K.N.Levitt, B.Mukherjee, J.Wood, D.Wolber," A network security monitor", Proceedings. IEEE computer society symposium on research in security and privacy.10.1109/RISP.1990.63859, 1990
2. Ronald Loui and Will Hope, "Information Warfare Amplified by Cyberwarfare and Hacking the National Knowledge Infrastructure", Dependable, Autonomic and Secure Computing FL, USA, Nov. 2017
3. Abdulrazaq Almutairi and David Parish, "Using classification techniques for creation of predictive intrusion detection model", Internet Technology and Secured Transactions (ICITST),London, UK,Feb.2015.
4. Samiha El Messari, Khalid Bouragba, Mohamed Ouzzif and Mounir Rifi,"Modeling securized cooperation of inter-organizational workflows in a multi-level virtual architecture",Next Generation Networks and Services (NGNS), Casablanca, Morocco, Dec. 2014.
5. Roumen Trifonov, Georgi Tsochev, Galya Pavlova, Radoslav Yoshinov and Slavcho Manolov, "Adaptive Optimization Techniques for Inteligent Network Security", Mathematics and Computers in Sciences and in Industry (MCSI),Corfu, Greece, Aug 2017.
6. Jeffrey R. Yost, "The March of IDES: Early History of Intrusion-Detection Expert Systems", IEEE Annals of the History of Computing, July 2015.
7. Babak D. Beheshti, "A framework for Wireless Sensor Network security", Systems, Applications and Technology Conference (LISAT), NY, USA, June 2016.
8. V. Saravanan and A. Neeraja, "Security issues in computer networks and stegnography", Intelligent Systems and Control (ISCO), Coimbatore, India, March 2013.
9. Abolfazl Zargar, Alireza Nowroozi and Rasool Jalili, "XABA: A zero-knowledge anomaly-based behavioral analysis method to detect insider threats", Information Security and Cryptology (ISCISC), Tehran, Iran, Nov. 2016.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

AUTHORS PROFILE

Femilda Josephin J S is currently working as Associate Professor in Department of Science and Technology, SRM Institute of Science and Technology, Chennai, India. She completed her PhD in Anna University, Chennai during 2015. Her area of interest include computer networks , network security and machine learning. She has published and presented more number of papers in national and international level.

Rutuja Matey is a undergraduate student of SRM Institute of Science and Technology, Chennai, India. Her area of interest is Computer Networking.

Shreya Singh is a undergraduate student of SRM Institute of Science and Technology, Chennai, India. Her area of interest is Computer Networking.