Framework for Threat Analysis and AttackModelling of Network Security Protocols

Nachiket Athavale
Smt. KashibaiNavale College of Engineering
Pt. No.1, Kaustubh, Shamsunder Society, Dattawadi, Pune – 411030

Shubham Deshpande
Smt. KashibaiNavale College of Engineering
Isha Garden A 304, Kothrud, Pune - 411038

Jatin Chavan
Smt. KashibaiNavale College of Engineering
Type D 38/06, BARC Colony, Tarapur, Boisar – 401504

Vikash Chaudhary
Smt. KashibaiNavale College of Engineering
Flat no -14, Dangad Garden, Vadgaon (Bk), Pune

ABSTRACT
Nowadays everything is computerized including banking and personal records. Also to boost business profits, businessmen have changed their way of operations from physical way to electronic way, for example Flipkart. But as these developments benefit the developer they also increase the chance of exposing all of customer's personal details to malicious users. Hackers can enter into the system and can steal crucial or sensitive information about other authentic users and in case of banks leads to frauds. Security thus, becomes an important issue for all companies and banks. Intrusion detection systems help such companies by detecting in real time whether an intrusion is carried on or not. Here the authors are developing a signature based intrusion detection system which will scan incoming packets and send a warning message to system administrator. Also the authors are implementing a framework and provide it to all the users so that developing intrusion detection based system similar to the built system. The advantage of using framework is that it can be upgraded and re-defined whenever it is needed.

General Terms
Intrusion Detection System, Framework, DDoS, DoS, network packets, SNORT, database, network security.

Keywords
Framework, Threat analysis, Security, Intrusion Detection System (IDS), Wireshark, Anomaly Detection, MITM, DOS / DDOS, Ip Spoofing, Packet analysis, Attack Detection, Network Based, Host based IDS, Computer security.

1. INTRODUCTION
Computers have revolutionized all sectors and fields of our society. All physical documentation has been replaced with computerized documents. For the convenience of customers banks have offered online banking services, businessmen keep crucial data about their products on computers and online shopping are just some of the examples of the benefits of computers and Internet. But the rise in computerization also gave rise to people becoming skilled in stealing this crucial data for personal or financial reasons. Several measures have been developed to stop this virtual thief from stealing their crucial data. But for administrators to stop attacks they have to know whether an attack is taking place or not. And for that an Intrusion Detection System is necessary.

Now what an Intrusion Detection System will truly do is scan incoming network packets and match them with fixed patterns of well-known attacks to find if an detection has taken place or not. The system will also find IP Address of the attacking individual's device if it is in the network. Different companies have different architectures and set up and might have specific attacks to deal with. So these companies might want to develop their own Intrusion Detection Systems. Taking this thought forward the authors are going to develop a framework, an open source project which might be further developed by anyone however they might wish and for whatever purpose.

So with the rise in computer age, malicious people also started to use their skills to steal crucial data and to counter them a system which detects when an attack occurs and informs network administrator. Also the system will be a framework which can be enhanced and modified according to people's choice.

2. MOTIVATION
With advancements in the technology, most of the tasks that were supposed to be done by humans are now getting done by computers. Such evolution has begun a new era wherein everything is computerized including day-to-day tasks. To boost the performance organizations have changed their way of doing operations from physical way to digitization. Banking systems provides various ways with which a user can communicate with the bank from any remote location. User can transfer, deposit money with just a click.

Also a user can access his confidential information from any location. However this increases the chance of misusing the intellectual data by breaching the security by hackers. With technology evolutions it becomes difficult to maintain user's intellectual information safe as it may be stored at remote locations. So securing such remote storage from hackers becomes an ultimate goal for the organizations. Hackers or attackers can enter into the system and steal the information or can manipulate the sensitive data. Hackers make use of various techniques with which they can enter into the system illegally and achieve their goal. In sensitive areas like banking security is of great importance, because if someone hacks the net-banking passwords then he can do whatever with the account. Security thus becomes the most important issue in such sectors.

Developing a perfect secured system is not possible, because

- Most of the security systems have some limitations
- Possibility abuses by privileged users inside the organization
- Not all kinds of intrusions are known
- A system cannot detect all types of attacks fully

Therefore there must be a system which will be able to detect any kind of security breach and will ensure security. Quick detection of intrusion can save the intellectual data from being

stolen and can alert the user if any hacker tries to attempt such intrusions.

Hence, the authors are developing an Intrusion Detection system which is capable of detecting any type of intrusion within short time and which alerts the user about the security breaches so that user can prevent any further data loss.

3. RELATED WORK

3.1 Types of Network Attacks

3.1.1 Rogue Access Point

Access point is a device to which other devices connect to form a network and access point also connects private network to internet. All the browsing, downloading of data from internet on our devices goes through the access point. Thus access point has access to all the data sent and received by the devices in a network. Now in huge companies there are multiple access points to service all the devices. An attacker inserts his device like a laptop into the network as an authentic user and makes the laptop an access point. This access point is called Rogue Access Point and it is called rogue because it is not valid access point and it opens up attack possibilities.

Attacker denies access to valid access point, so all the other devices mistakenly connect to attacker's device as an access point. Attacker sends all the requests for data to the valid access point and thus the devices connected to rogue access point do not find any difference in their browsing, while the attacker is reading all the packets travelling through his access point and stealing vital information at the same point. Detection of rogue access point is by using hop count by counting if hop count is increased or not. Also by scanning and comparing MAC addresses rogue access point can be detected.

3.1.2 Packet Sniffing

When packets are sent to any switch or hub, the packets are sent to all the devices connected to the network regardless the true destination of packets. Each packet contain destination device to which the packet was sent. When the same packet reaches all devices in a network, the network interface card inspects the destination of the packet and if it is not the destination the packet is dropped. The device which is intended to be the destination only accepts the packet. Now what happens in packet sniffing is that the device which is sniffing switches on to promiscuous mode like mon0 which does not drop packets even though it is not the intended receiver. Thus using promiscuous mode device can read all packets and their respective data.

Mostly these packet sniffers are used by attackers or intruders who want to steal sensitive information like passwords or generally monitor the traffic in network. Packet capturing results in attackers gaining passwords and hence is considered as an attack. Detection of packet sniffing is done simply by checking the interfaces of each and every device connected to the network. If the devices' interface is a promiscuous mode like mon0 then it would be safe to assume that packet sniffing is being performed at that device.

3.1.3 Man In The Middle Attack (MITM)

Man in the middle attack can intercept communication between two or more systems. Normally client server model uses TCP connections. By using different methodology intruders can split normal TCP connection into two TCP connections wherein one connection is formed between client & the intruder and one TCP connection between the intruder and server. Once the connection is intercepted or placed successfully in between client & server intruder acts as proxy who is able to read and modify the data in intercepted traffic or communication.

MITM attack is very popular due to easy conduction & very effective due to structure of http protocol and data transaction which are ASCII based, so it's possible to read the actual data stream from intercepted traffic. Now a day's most of the website uses https protocol that means HTTP + SSL (secure socket layer) but intruders can mitigate or bypass the SSL connection and force the transaction to pass through normal HTTP protocol.

Detection of MITM: To perform MITM intruder spoof mac address of server to communicate with client & spoof client'sMAC address to communicate with client. This way an ARP packet traverses in network. The network traffic can be captured using Wireshark to detect the source of ARP poisoning attack. The idea is to use this filter :arp.duplicate-address-frame , this way the authors can detect ARP poising.

3.1.4 Denial of Service (DoS)

Denial of service attack is used to make service unavailable for legitimate users. if a service receives very large number of packets or requests it may cause disruption of service for legitimate users . In the same way by exploiting vulnerability of service it may also cause disruption of service.

DOS attack can be generated from single source. This way it's easy to detect the DOS attack on network by capturing packets on network. If packet contains same length size & same destination & same source of too many packets then it can be said that DOS attack has happened by source_ip.

3.1.5 Distributed Denial of Service (DDoS)

DDOS is a type of dos attack where attacks can be generated from multiple sources this may cause disruption or unavailability of service for legitimate users. This type of attack is not easy to detect because of traffic generated from multiple sources. In some cases where legitimate users are constantly trying to access a service or file in such scenarios it's also a type of DDOS but unintentional DDOS. For example, crashing of exam results server. Detection of DDOS can be identified by capturing packets & if packet contains same destination_ip, same Protocol or same length occurring in too many packets, then it can alert admin that DDOS happened within a span. [1]

3.1.6 DNS Spoofing

DNS spoofing is type of MITM attack where attacker force user to navigate fake website disguised to look like a real one, with the intention of diverting traffic or stealing credential of the users. DNS resolve domain name to respective domain IP address that is used to communicating nodes on the internet.

DNS spoofing is done by replacing domain IP to the controlled IP that means whenever a user or victim visit a website it will redirected to fake one. Detection of DNS spoofing is very easy if intruders only spoofed one Domain but if attacker uses all the domain which users want to visit that DNS should spoofed to redirect to fake one this may be little high to detect . For detection simply check the DNS if DNS contains some LOCAL IP or public IP that not the real IP then it can be said that DNS spoofing is happening.

3.2 Intrusion Detection System

The main goal of Intrusion Detection Systems (IDS) is to identify threats and intrusion attacks and alert concerned

authorities. Intrusion Detection Systems (IDS) are strong at matching known pattern so hostile activity against databases of past attacks. An IDS is very effective at identifying attacks which are known, but less efficient in identifying new threats. [2]

IDS Types:

1. Host Based

2. Network Based

3. Application Protocol Based

Application based IDS will check the effective behaviour and event of the protocol. The system or agent is placed between a process and group of servers that monitors and analyses the application protocol between devices.

3.2.1 Implementation Types

3.2.1.1 Signature based detection method

First is a Signature-based detection method where the intrusion is detected by using predefined rules or user defined rules. The rules will determine pattern of the packet that need to be detecting. If the incoming packets match with the pre-defined pattern, then admin will be alerted regarding the intrusion. The collection of these signatures composes a knowledge base to find if a known pattern is matched and alert is generated. [2]

3.2.1.2 Anomaly detection method

Second approach is anomaly detection method where the system will learn the normal and anomaly packet capturing and it detects intrusion of a modified attack or unknown attack. This approach requires use of some type of artificial intelligence element where the system can learn the normal pattern of the packet traffic and make detection of intrusion if the behavior of the packet is changed. [2]

3.3 Approaches So Far

3.3.1 Log File Monitoring

Another scope in the study is, it focus on system log file monitoring where log file of host system are analyzed from time to time to detect intrusion. The content of the log file will be compared to IDS rules or pattern that is predefined. File system monitor can check files on a large number of different characteristics such as owner, size and other different file characteristics. [2]

3.3.2 SNORT

SNORT is open source software which is both an intrusion detection and intrusion prevention system. It has the ability to perform real time packet analysis and logging for Internet Protocol based networks. It can detect intrusions like buffer overflows, CGI attacks, OS finger printing attempts and many other types of attacks. [3]

3.3.3 Outlier Detection Approach

Outlier Detection Approach uses SNORT [3] to capture packets and sends those packets to detection system which computes distance between extracted features and trained model, where trained model consists of big datasets. In this approach the normal data from packets are nearby whereas outliers are very much away from normal data. A Neighbourhood Outlier Factor (NOF) is used to find rare data which is very exceptional compared to normal data. [4]

3.3.4 Neural Networks based Approach

Here neural networks are trained with datasets where the system or neural networks learn about different attacking patterns. Then the system is fed with live packet capturing which is provided with any sniffer. The system with the help of neural network identifies whether intrusion has taken place or not. [5]

Table 1.Literature Survey with summary, advantages and limitations

Sr. No	Paper Title	Description	Advantages and Limitations
1	Development of host based Intrusion detection system for Log files. (IEEE ISBEIA)	Develop intrusion detection system using signature based detection to detect intrusions and store them in log files. Only applicable for Windows XP.	Advantage - Easy to implement, host based system. Performs packet matching with known attacks. Limitation – Applicable to host based systems only.
2	HSNORT: A Hybrid Intrusion Detection System using Artificial Intelligence with Snort. (IJCTA May-June 2013)	This paper has used SNORT to detect the intrusions, which consist of snort rules that are matched against the suspicious packets to detect the intrusion.	Advantage - It is a combination of Host and Network based Intrusion detection. Limitation – Delay caused due to excess rules.
3	DDoS Attacks Impact on Network Traffic and its Detection approach. (IJCA Vol. 40 2012)	Statistical based approach to analyze distribution of network traffic to identify DDOS/DOS attacks,.	Advantage - Uses anomaly finding method to detect low intensity DDoS attacks. Limitation – Generates false positives and false negatives.

4	Intrusion Detection System – A Study (IJSPTM Vol. 4 2015)	The main objective of this paper is to provide a complete study about the definition of intrusion detection and everything related to it.	Advantage – Introduction to basic concepts of Intrusion Detection System. Limitation – Only serves as introduction without going deep into implementation.
5	Bro: A System for Detecting Network Intruders in Real-Time. (7th USENIX Security Symposium 1998)	Bro is a system which passively monitors incoming packets and detects intrusions. Uses event engine that reduces kernel altered network traffic and policy script interpreter.	Advantage - Uses Bro language i.e specialized python script interpreter. Limitation – Rate of packet capturing is less than incoming packets.
6	Intrusion Detection System (IDS): Anomaly Detection using Outlier detection approach (ICCC-2015)	Intrusion detection System using outlier analysis to find the Neighbourhood Outlier Factor (NOF).	Advantage - Exceptional data from packets appear as outliers as well. Limitation – High false alarm rate during learning.
7	A Neural Network Based System for Intrusion Detection and Attack Classificatio n (IIT, Guwahati)	An Artificial Neural Network based model which has less computational overhead, while having high performance. The system performance is comparable to other models.	Advantage - Performance comparable to SVM and C4.5 but better than Naive Bayes. Limitation – Significant time taken by system to learn about new attack patterns.

4. PROPOSED WORK

4.1 Framework in IDS

Security is an important concern in every field of life. All of the companies which provide services to its customers are under the threat of security breach. So an Intrusion Detection System is used by many companies to alert the concerned authorities that an intrusion has taken place. Many different approaches have been taken under consideration while developing Intrusion Detection Systems like Artificial Intelligence, Machine Learning, and Outlier Analysis. But the problem is that the se software's start losing its importance when new attacks are observed. Hence some functionality should be provided to the owner so that he/her can change the system according to his/her will.

This paper focuses on integrating Framework into an Intrusion Detection System where developers will have a choice to addor modify modules related to detection in accordance with. Developers cannot modify the already created framework program.

Hence when the frame work is created the user is able to make additions to the already available software which will enhance it and update it with time. For example, Rogue Access Point is a comparatively new attack which can be detected based on MAC address or by hop count. This type of attack detection can be added to Intrusion Detection System.

4.2 System Architecture

The figure below, Fig 1 describes the system architecture which will be used for implementing the proposed system. It contains three blocks which perform following functions in brief:

- Data Collector – Capture network packets using a sniffer.
- Analyzer – Checks if packets are legitimate or not
- Reactor – Performs respective action based on suspicious packets such as alerting network administrator.

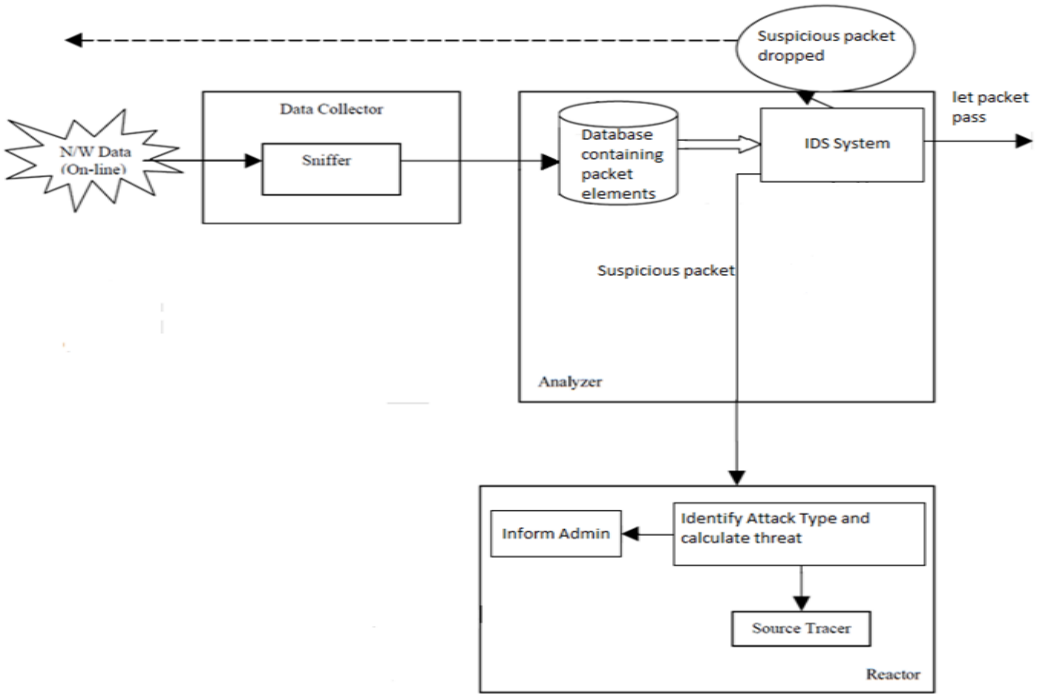

Fig 1: Proposed System Architecture

4.3 In-Program Detection

In various Intrusion Detection Systems the method to implement the detection mechanism is to have two databases. One database stores all the packets captured in real time by a packet sniffer (a tool which captures packets from the network using promiscuous mode). And the other database is used to store fixed rules which have been practically proved to spot any malicious activity taking place. Now all the packets stored in first database are matched or compared with each and every rule available in the second database and if there is any match found then the system will detect an intrusion and take necessary measures to deal with the detected intrusion. Most famous example of this type of implementation is SNORT. The working of these types of systems is shown in diagram. In Fig 2 it is shown that the main system only plays the role of supervisor where it retrieves packets and matches them with rules in second database.

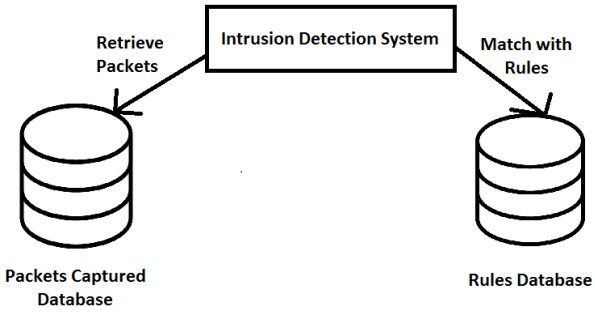

Fig 2:Intrusion Detection System with Rules Database

Now there are two problems with this kind of implementation. The base programming language used by the system is not related to database language, for example JAVA. So all the workings and features of system is developed in one language and a connector is used which connects main system programming language with database language. Example of this connector is JDBC which connects JAVA and MySQL. While retrieving packets and rules from database using connector is possible, it comes at a cost of slight delay. And because the system alerts regarding any intrusion taking place, there should be less delay as much as possible. The system retrieves packets and rules from two databases and compares them for every single packet which results in minute delay.

So the authors of this paper have come up with a new idea for system implementation which might reduce the delay occurring for database retrieval and matching. Most common and important attacks, for example DoS and DDoS are taken into consideration and the rules are setup within the program only. Hence the packets will be retrieved from the database by the system and each packet will be compared with fixed rules within the system only. Thus the need for a second database containing rules for detection is not required at all. The thought using this type of implementation is delay would probably be reduced as system interacts with only one database. Fig 3 shows working of in-program detection.

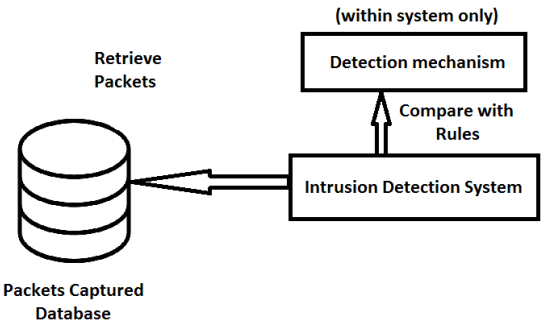

Fig 3:Intrusion Detection System with In-Program Detection

The second problem with rules database is that as days pass new attacks and new patterns are constantly being developed by attackers or intruders to find vulnerabilities in the system. To counter this Intrusion Detection Systems such as SNORT store more and more rules into their Rules Database. Thus the time taken for each packet being compared with so many rules would be considerably large. Taking this effect in consideration the idea of Framework is used by the authors to detect newly observed attacks. Framework provides generic functionality which can be modified later by owner. Also using a framework is relatively easy as framework will call your added functions, so the authors don't have to worry about sequencing. It is a widely considered that Framework and Libraries are similar, but they are widely different. Framework has three main properties and they are as follows:

1. Usually developer calls library functions in his program But for frameworks, it calls developers programs and arranges them accordingly. Hence developer doesn't need Hence developer does not need to bother about calling other functions.

2. Developers can only extend framework functions by modifying them or overriding them.

The second problem with rules database is that as days pass new attacks and new patterns are constantly being developed by attackers or intruders to find vulnerabilities in the system. To counter this Intrusion Detection Systems such as SNORT store more and more rules into their Rules Database. Thus the time taken for each packet being compared with so many rules would be considerably large. Taking this effect in consideration the idea of Framework is used by the authors. The client systems with their specific security needs will develop their own detection mechanisms rather than having rules of each and every possible attack being stored in database. Example is for social networking sites there is a high chance that Brute Force Attacks or DNS High jacking takes place to steal users' passwords. So these companies should develop methods to detect only those types of attacks whose probability of occurring are high.

4.4 Proposed Network Triangulation Approach for Positioning Intruder

Network triangulation uses signal strength to find out the distance among user and other three transmitters.

Spherical Trilateration Algorithm is used which uses parameters of known networks like frequency of network signal, its signal strength, the network MAC – address and real coordinates of access points in the location.

The received signal strength by device used to estimate distance of access point and devices. This method requires minimum three or more access point or packet injector disposed in the building.

The signal strengths of the points decrease exponentially and depend on the distance between transmitter, receiver and the random noise factor. Therefore, this dependency can be considered as a distance function, where the distance is estimated by the signal strength is presented as a circle with a radius around the access point.

The intersection of three access point radiuses provides an area of receiver.

This model can be shown as such equation

$$d1^2 = (x - x1)^2 + (y - y1)^2$$

$$d2^2 = (x - x2)^2 + (y - y2)^2$$

$$d3^2 = (x - x3)^2 + (y - y3)^2$$

where x1,x2,x3,y1,y2,y3 are the coordinates of access points ,d1,d2,d3 is the estimated distances. The solution of these equations gives intersection of different circles which results into an area.

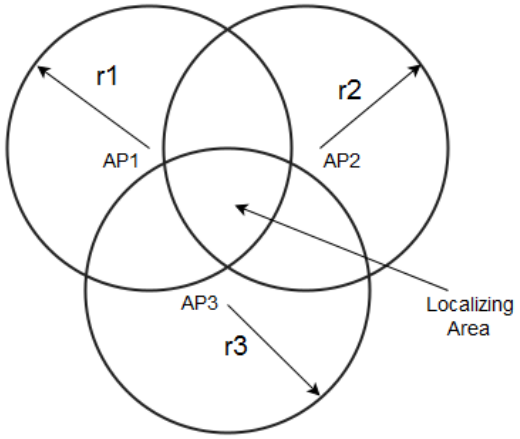

Fig 4: Triangulation Approach for positioning Intruder

5. BENEFITS OF SYSTEM

5.1 Framework

- Using Framework the time and energy required for developing any software is reduced as all the basic functionalities have already been developed and hence only modified part is required to be added by developers.
- The developed Intrusion Detection System can be customized or modified according to native platform and networks. For example, developing Windows based Intrusion Detection System using original system.
- Developer can add new attack patterns to his rules so that new attacks are easily detected.

5.2 Intrusion Detection System

- The system provides complete network visibility to the user. The visibility includes all the devices connected to the network. Also information such as Manufacturer, MAC address and IP address is also visible.
- The system provides layer of defence to the network as it constantly alerts the administrator about any attacks taken place in the system.
- Response capabilities include instructing administrator regarding further steps to be taken if any attack takes place. Also if intruder is identified that device can be disconnected from the network, though this comes at a risk in case of false report.
- Information about any attack that has taken place is stored in log files. Information contains attack type, attacker's IP address. So using these log files can be used by authorities to take any kind of action against the attacker where log files would serve as evidence.

6. LIMITATIONS

6.1 Framework

- Using and developing software's using framework is a tough task as framework is complex and is abstracted from user. Hence user has to spend a lot of time in understanding the working of framework before he can start developing it.
- Framework only plays as an advantage in huge projects. In small projects it is easier to create own separate code instead of learning the workings of framework.

6.2 Intrusion Detection System

- More maintenance is required for the system. Also the system does not replace working of firewall, virus scan and other measures. So additional burden of its maintenance would add up to the existing work.
- When any attack or malicious activities do not take place, but the system alerts user about one then it is called as false positive. False positives tend to reduce user's attention to any alerts.
- The system also misses any attacks that take place due to heavy traffic or any other system problem. This is known as false negatives when system does not alert user even though any attack takes place.
- This system requires experienced staff in network working to operate as many of the features would be understood only by an expert.

7. CONCLUSION

The authors of this paper have discussed several different ways in which the problem of anomaly detection has been formulated and have attempted to provide an overview of various techniques. The system looks for the attack signatures and matches it with the known attack signatures from the database and alerts the admin if match is found otherwise simply let the packet pass. Also the admin is provided with complete visibility of the network which keeps the admin aware of all the activities going on in the network.

In this way successful intrusion detection can be achieved and all the intellectual information of a user can be kept safe in a network. This system not only allows a reader to understand the motivation behind using a particular anomaly detection technique, but also ensures a qualified analysis of various techniques.

7.1 Future Scope

7.1.1 Unknown Attacks

The authors have used Signature Based Intrusion Detection System which matches only the known attack patterns with incoming packets. So only known attacks can be detected. But in-case if any new attack arrives, the system will not be able to detect it. Hence in future some artificial intelligence technique can be developed which will learn new attack types and then will be able to detect them.

7.1.1.1 Security of Intrusion Detection System

It is very much clear that the Intrusion Detection System will secure the network by alerting network administrator who will take further actions. But it is a very crucial point if a malicious attacker attacks the system only which will render intrusion detection system useless. So security of Intrusion Detection System needs to be taken into consideration.

7.1.1.2 Anomaly detection

A possible future work would be to amalgamate the assumptions made by different multiple techniques regarding the normal and anomalous behaviour into a statistical framework. This system guarantees several promising ways for further research in anomaly detection.

7.1.1.3 Helps in complex systems

Complex systems are another area where anomaly detection is trending more and more applicability. Aircraft system with multiple components could be considered as an example here.

7.1.1.4 Distributed Systems

This system ensures that information present at multiple sites are processed simultaneously and also the information is protected and kept secured. Ultimately, future IDS will definitely be capable of merging all of the independent network components and tools which exist today, into a complete and cooperative system, dedicated to keeping networks stable, safe and secured.

8. ACKNOWLEDGMENTS

We greatly acknowledge the Smt. KashibaiNavale College of Engineering, Pune, Maharashtra for providing basic infrastructure required for this project. We express our deep gratitude to Prof. S. S. Barde for his unending support to carry out this work. We also thank Dr. P. N. Mahalle for giving his suggestions and sharing information to improve this research work.

9. REFERENCES

[1] Bhange, A., Syad, A., & Thakur, S. S. (2012). DDoS Attacks Impact on Network Traffic and its Detection Approach. International Journal of Computer Applications, 40(11), 36-40. doi:10.5120/5011-7332

[2] Ali, F. A., & Len, Y. Y. (2011). Development of host based intrusion detection system for log files. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA). doi:10.1109/isbeia.2011.6088821

[3] Divya, Surender L. (2013) HSNORT: A Hybrid Intrusion Detection System using Artificial Intelligence with Snort. International Journal Computer Technology & Applications, Vol. 4 (3), pp.466-470.

[4] Jabez, J., &Muthukumar, B. (2015). Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach. Procedia Computer Science, 48, 338-346. doi:10.1016/j.procs.2015.04.191

[5] Subba, B., Biswas, S., &Karmakar, S. (2016). A Neural Network based system for Intrusion Detection and attackclassification. 2016 Twenty Second National Conference on Communication (NCC). doi:10.1109/ncc.2016.7561088

[6] Paxson, V. (1999). Bro: a system for detecting network intruders in real-time. Computer Networks, 31(23-24), 2435-2463. doi:10.1016/s1389-1286(99)00112-7

[7] Dubendorfer, T., Wagner, A., &Plattner, B. (n.d.). A Framework for Real-Time Worm Attack Detection and Backbone Monitoring. First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05). doi:10.1109/iwcip.2005.2

[8] Mauro Conti, Nicola Dragoni, Viktor Lesyk. (2009). A Survey of Man In The Middle Attacks. IEEE

Communication Surveys and Tutorials. doi:10.1109/COMST.2016.2548426

[9] Alan Bivens, ChandrikaPalagiri, Rasheda Smith, Boleslaw Szymanski, Mark Embrechts. (2002). Network based Intrusion detection using neural networks. Proc Intelligent Engineering Systems through Artificial Neural Networks.

[10] Honda, S., Unno, Y., Maruhashi, K., Takenaka, M., & Torii, S. (2015). TOPASE: Detection of brute force attacks used disciplined IPs from IDS log. 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). doi:10.1109/inm.2015.7140496

[11] Munz, G., & Carle, G. (2007). Real-time Analysis of Flow Data for Network Attack Detection. 2007 10th IFIP/IEEE International Symposium on Integrated Network Management. doi:10.1109/inm.2007.374774

[12] Mukaddam, A., Elhajj, I., Kayssi, A., &Chehab, A. (2014). IP Spoofing Detection Using Modified Hop Count. 2014 IEEE 28th International Conference on Advanced Information Networking and Applications. doi:10.1109/aina.2014.62

[13] Idris, N., &Shanmugam, B. (n.d.). Artificial Intelligence Techniques Applied to Intrusion Detection. 2005 Annual IEEE India Conference - Indicon. doi:10.1109/indcon.2005.1590122

[14] S. Vijayarani, Maria Sylviaa. S. (2015) Intrusion Detection System – A Study. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.