Network Security through Signature-Based Intrusion Detection Systems: A Comprehensive Approach

Grace Samantha Nolan, (M.Phil).,

Assistant Professor, Department of Computer Science, Kensington Green College of Arts and Science, London, UK

Abstract— **A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action. NIDS is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. Intrusion detection is an important technology in business sector as well as the research area. It inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. A signature based IDS will survey the packets on the network and compare them against a database of signatures or attributes from known attackers. In this system the attack log displays the list of attacks to the administrator for Unauthorized action. This system works as an alert device in the event of attacks directed towards an entire network. In This Paper we will discuss about the detection and Prevention of Network and the Business world prevent from the unauthorized access.**

Keywords— Network Intrusion Detection System, Online matching algorithm, Signature Based IDS

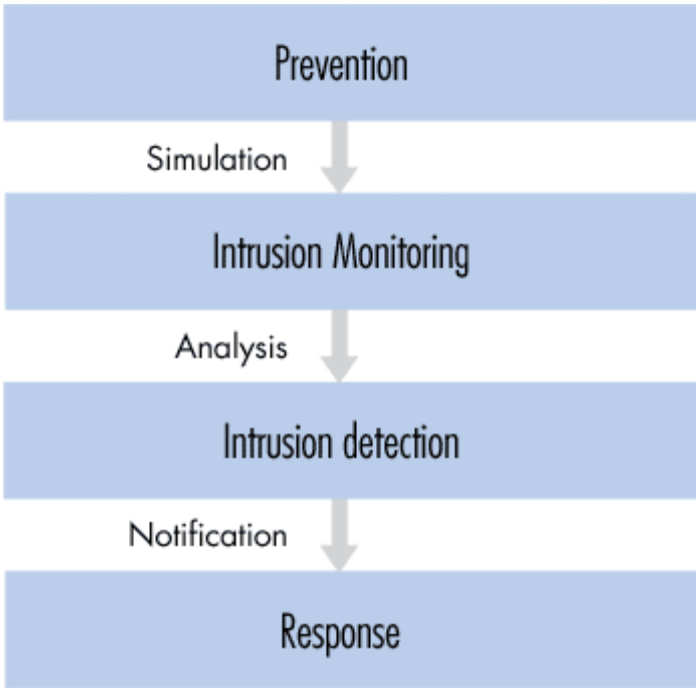
I. INTRODUCTION

The emerging changes in network technology network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of intruder and secures the networks. Main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can prevent and possibly react to the intruder. This provides the proper monitoring and secure the data from the network traffic and detect attacks by observing various network activities

With the emerging growth of network-based services and sensitive information on networks, network security is plays a vital role in the

technologies. that detect attacks by observing various network activities and follow the intruder by using the Signature Based IDS.

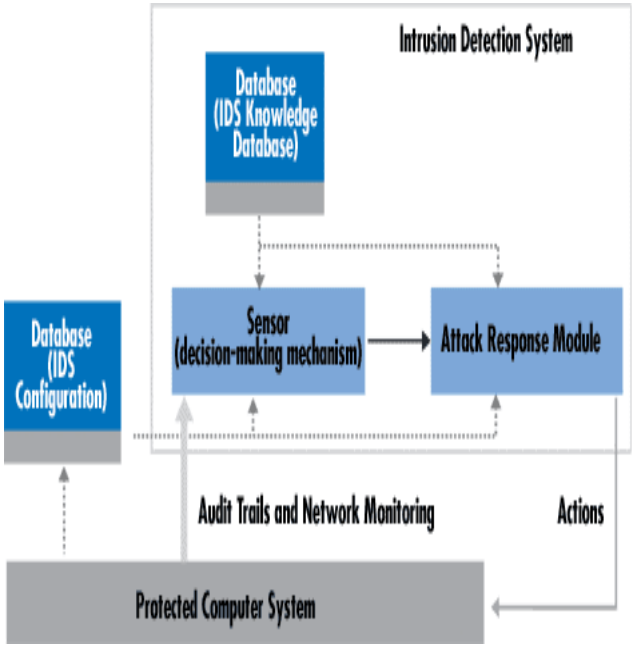
II. STRUCTURE AND ARCHITECTURE OF INTRUSION DETECTION SYSTEMS



A Network Intrusion Detection System [NIDS] is detector system which is mainly used for detecting the intruder from the unauthorized access.

This process finds that whether the data has hacked by the intruder. It simulates the intrusion then It monitors the intrusion whether the data has been hacked. If the data has been hacked then the network sends the notification to the source that the data is in the dangerous stage.

ARCHITECTURE



This Architecture represent that IDS follows the intruder by using the IDS knowledge Database. These databases have a set of condition for avoiding the intrusion. Once the Network simulates these conditions then Intrusion Detection System automatically sends the alerts to Source System to prevent from the Network Attacks. The Database Knowledge sensor the Decision making mechanism to analyze the attack of Network. IDS Configuration always Simulate the Protected Computer System.

III. NETWORKING ATTACKS

NIDS is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. Attacks are

A. Eavesdropping

An Attack listener listen the Authentication protocol to capture information which is used to frequent attack.

B. Identity Spoofing

In this attack , the attacker theft the data and the false data to the destination. This makes the falsy data can distribute to the designator

C. Denial-of-Service Attack

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.[5]

D. Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized intruder. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own

E. Reconnaissance

Reconnaissance attack is a kind of information gathering on network system and services. This enables the attacker to discover unstable on the network. [4]

IV. ANALYTICAL STUDY

A.signature based intrusion detection

Signature-based IDSs operate analogously to virus scanners, i.e. by searching a database of signatures for a known identity – or signature – for each specific intrusion event. In signature based IDSs, monitored events are matched against a database of attack signatures to detect intrusions. Signature-based IDS are unable to detect unknown and emerging attacks since signature database has to be manually revised for each new type of intrusion that is discovered.

B. Online Matching Algorithm

In this algorithm , the memory space of the environment can be decreased and increase the speed of the system,

```
   Procedure OnlineMatching(T, H^I, H^II)
   Input: Packet payload T, two preprocessed indexing tables: H^I and H^II
   Output: The matched pattern set of T: P^M, and its corresponding pid PID^M
1  Load the input payload into buffer T;
2  Initialize: P^M ← ∅ ;
3  For each T[t] do
4    If (k←H^I[T[t]].pid) ≠ NULL then P^M←P^M ∪ {p_k} and
       PID^M←PID^M ∪ {k}; /* First-tier matching*/
5    If (k←H^I[T[t]].fid) ≠ NULL && t < |T| then
6      Load data from the external RAM at entry H^I(T[t], T[t+1]) to a local
       buffer LB;
7      While (k← LB.pid) ≠ NULL do
       /* Second-tier matching*/
8        Compare the substring start at T[(t-LB.offset)] with the pattern
           LB.data of length LB.size; /* Assume no fragmentation here*/
9        If the comparison is matched then P^M←P^M ∪ {p_k} and
           PID^M←PID^M ∪ {k};
10       If LB.next ≠ NULL then
11         Load data from the external RAM at entry LB.next to the local
             buffer LB;
12       Else
13         Break;
14 Return;
```

By applying Online matching in the IDS, It stores the History of existing intruder in the Databases. It gives the alert information when the same process is going on the real world environment. Therefore, Online matching Algorithm enables efficient, practical and cost-effective IDSs. [7]

V. CONCLUSION

We conclude this paper by Securing the Network from the intruder by using Signature IDS Algorithm . It successfully captures packets transmitted over the entire network by promiscuous mode of operation and compares the traffic with crafted attack signatures. This IDS Algoirthm not only secure the network it also Reduce the memory Space of the environment. This network captures holds the packets and travel the packets in successful manner which makes the business people can easily communicate with peoples to increase their economic status without hold of unauthorized access.

REFERENCES

[1] B. Mukherjee, T.L. Heberlein, K.N. Levitt, Network intrusion detection, IEEE Network 8 (3), 1994, pages 26-41...

[2] C. Krügel, T. Toth, Distributed Pattern Detection for Intrusion Detection, Conference Proceedings of the Network and Distributed System Security SymposiumNDSS'02,2002,http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/kruege.ps.

[3] Internet Security Systems, Inc., RealSecure,http://www.iss.net/prod/rsds.html, 1997.

Robert Graham, FAQ: Network IntrusionDetectionSystemshttp://www.robertgraham.com/pubs/network-intrusion-detection.html#2.1, last accessed on March 9, 2004

[4] J. Van Ryan, SAIC's Center for Information Security, Technology Releases CMDS Version 3.5, http://www.saic.com/news/may98/news05-15-98.html, 1998.

[5]Vikram Gupta, Srikanth Krishnamurthy,and Michalis Faloutsos. Denial of ServiceAttacks at the MAC Layer in WirelessAd Hoc Networks. In Proceedings of 2002MILCOM Conference , Anaheim, CA, October 2002.

[6]Jump up to: a b www.users.cs.york.ac.uk/~jac/PublishedPapers/AdhocNetsFinal.pdf

[7]http://cial.csie.ncku.edu.tw/presentation/group_pdf/a%20novel%20hierarchical%20matching%20algorithm%20for%20intrusion%20detection%20systems.pdf