An Efficient Working of Network-Based Intrusion Detection System (NIDS)

Dr. Abid Hussain
Assistant Professor, School of Computer Applications
Career Point University, Kota, Rajasthan

Abstract- *Computer networks have added new dimensions to the global communication. But intrusions and misuses have always threatened the secured data communication over networks. Consequently, network security has come into issue. Now-a-days intrusion detection systems play an important role in security infrastructures. Intrusions typically start with intruders infiltrating a network through a vulnerable host and after that approaching for further malicious attacks. The techniques used for intrusion detection have their particular limitations [1].Any of the intrusion detection systems proposed so far is not completely flawless. The host based systems as well as the network based systems have their own limitations. For detecting the network attacks and monitoring network, in this paper, here we present NIDS which is used to monitor and analyze network traffic to protect a system from network-based threats.*

Keywords- IDS, HIDS, NIDS, IP, DOS, Network Security, NIPS, Network Traffic, Host, Server.

I. INTRODUCTION

A "network intrusion detection system (NIDS)" monitors traffic on a network looking for suspicious activity, which could be an attack or unauthorized activity. A large NIDS server can be set up on a backbone network, to monitor all traffic; or smaller systems can be set up to monitor traffic for a particular server, switch, gateway, or router. In addition to monitoring incoming and outgoing network traffic, a NIDS server can also scan system files looking for unauthorized activity and to maintain data and file integrity. The NIDS server can also detect changes in the server core components [2].

In addition to traffic monitoring, a NIDS server can also scan server log files and look for suspicious traffic or usage patterns that match a typical network compromise or a remote hacking attempt. The NIDS also works with other systems, like a firewall, to help better protect against known attack sources (e.g., a suspected attacker IP address). NIDS play an important role in the world of network security. They help prevent the consequences caused by undetected intrusions on the network.

II. ARCHITECTURE OF NIDS

In this section, we explain how NIDS are deployed in a given network [3].In order to maintain clarity, we consider a NIDS as a black box (in next section we discuss the architecture of NIDS in greater detail), and list the popular configurations and locations, where they are deployed to tap into the network links and detect security violations.

2.1 Early Warning Mode

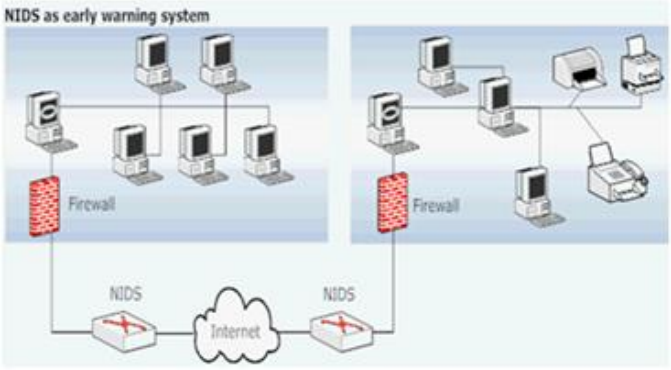

Figure 1: A NIDS as an early detection system.

In such a mode of operation, NIDS are employed outside the perimeter of the firewall (shown in Figure 1). Thus, all traffic entering the host and/or the local/enterprise network is scanned by the NIDS. The key benefit of such configuration is that the NIDS remains at a single locating tapping at a high speed link and can potentially serve a large number of hosts. Thus, the management and update of the signatures and keeping the configurations up-to-date are much easier. A drawback is that the attacks initiated by the hosts within the firewall perimeter will go undetected. Also, notice that in such architecture, it is possible that the NIDS will raise an alarm while the firewall will block the traffic, thereby effectively rendering the alarm a false one.

2.2 Internal Deployments

In such mode of operation, a NIDS is deployed such that it monitors the traffic that traverses any given link within the network, thereby providing an increased security (shown

in Figure 2). Thus the NIDS is deployed near the switching nodes within the local network, and near the access routers at the network boundary. In such configurations, the NIDS will no longer monitor the traffic that has been blocked by the firewall, which will lead to a much reduced false alarm rates. A drawback however is that there will be multiple instances of NIDS, and it will become tedious to keep all of them up-to-date in say a large enterprise network. Such configurations are popular in ecommerce back end networks, consisting of web and mail servers and database and storage servers, as an increased security is desirable there. It also aids in keeping an infected server to infect the others within the network.

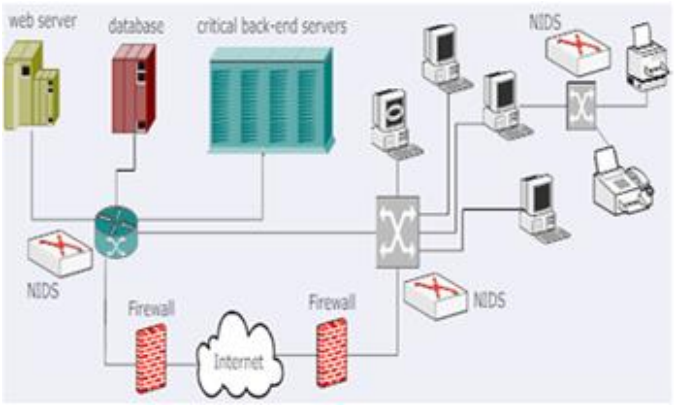

Figure 2: NIDS in complete deployment mode.

2.3 NIDS within Every Host (like an anti-virus)

In such configurations, every host has an inbuilt NIDS attached to all of its network interfaces. In a way, such architecture is similar to an anti-virus running on the host; however its key benefit is that the NIDS is decoupled from the host operating system, thus it can be separately managed by the network administrator through a central location. Nevertheless, the management can become complex when the network is large containing several host computers. It has been argued that such structures can lead to difficulty in implementation of the NIDS algorithms as a single instance of NIDS will remain unaware of the traffic traversing through the other links; thus attacks such a Distributed Denial of Service (DDoS) might go undetected. Another disadvantage arises due to the extensive use of devices such as access gateways which dynamically assigns IP addresses to the local hosts. Due to the limited local scope of these IP addresses, it sometimes becomes difficult for the host based NIDS to effectively trace the route of the packet, which affects its detection mechanism and capability.

With the description of the above 3 popular NIDS deployment configurations, we proceed to the NIDS architecture and the algorithms that are used to implement NIDS. NIDS has traditionally been designed with two popular techniques: a signature based detection and a relatively advanced implementation called anomaly based detection. We begin with the description of the signature based design.

III. COMPONENTS OF NETWORK INTRUSION DETECTION SYSTEM

A NIDS is consist of several components which are used to detect intrusions such as a malicious activity, computer attack and/or computer misuse, spread of a virus, etc, and alerting the proper individuals upon detection. A NIDS has following major components [4]:

- **Alert: Message** generated from the analyzer indicating an interesting event has occurred.
- **Analyzer:** Processes data collected from one or more sensors and looks for suspicious activity.
- **Data Source:** Raw data being analyzed-log files, audit logs, system logs, network traffic, etc.
- **Event:** Indication that suspicious activity may have occurred (can trigger an Alert or notification),If confirmed, Event becomes an incident.
- **Manager:** Intrusion Detection System(IDS) console-used to manage the system.
- **Notification:** Process by which the operator is alerted to an Event or Incident.
- **Operator:**User,Admin,etc.,responsible for IDS
- **Sensor:** Primary data collection point for the IDS and Device driver on a system or a separate physical attached to the network to collect data.

IV. STRENGTH AND LIMITATIONS OF NIDS

NIDS today have become extremely valuable in enhancing the security of the networks and end hosts; they however have a number of key drawbacks. In the deployment of NIDS, it therefore is important for the network administrator to be aware of its strengths and limitations. In the section we discuss these properties.

4.1 Strength of NIDS

- NIDS can perform the following functions to enhance the security.
- Measurements and analysis of typical and atypical user behavior [5]. For example an anomaly based NIDS is capable of detecting high volume traffic flows, flash crowds, load imbalance in the network, sudden changes in demand of a port usage, sudden surge of traffic from/to a specific host, etc [6].

- Detection of known worms, viruses, and exploitation of a known security hole. Signature based NIDS can detect these events with fairly high degree of accuracy. An appropriate signature will also ensure a low false positive probability.
- Some advanced NIDS systems also enable recognitions of patterns of system events that correspond to a known security threat [7].
- Enforcement of the security policies in a given network. For example a NIDS can be configured to block all communication between certain sets of IP addresses and or ports. A NIDS can also be used to enforce network wide access controls.
- Anomaly based NIDS can also recognize, with a certain false positive probability, new attacks and abnormal patterns in the network traffic, whose signatures are not yet generated. This will alert the network administrator early, and potentially reduce the damage caused by the new attack.

4.2 Limitations of NIDS

- **A mere Workaround:** A number of researchers have argued that a NIDS is more or a less a workaround for the flaws and weak or missing security mechanisms in an operating system, an application, and/or a protocol [8].
- **False Positives:** NIDS comes with a bane, i.e. false positives. A false positive is an event when a NIDS falsely raises a security threat alarm for harmless traffic. Signatures can be tuned precisely to reduce such false positives, however fine signatures create a significant performance bottleneck, which is the next limitation of NIDS. Current Anomaly based algorithms lead to even higher false positives[9].
- **Performance issues:** Current signature based NIDS systems use regular expressions signatures which creates a significant performance bottleneck. In order to reduce false positives long signatures are required which further reduces the performance. The data throughput of current NIDS systems is limited to a few gigabit per second.
- **Encryption:** The ultimate threat to the very existence of the signature based NIDS systems is the increasing use of data encryption. Everybody dreams to encrypt their data before transmission. Once the packet payloads are encrypted, the existing signatures will become completely useless in identifying the anomalous and harmful traffic.
- **New and sophisticated attacks:** Commercial NIDS which are signature based are unable to detect new attacks whose signatures are not yet devised. Anomaly based NIDS can detect such attacks but due to the limitations of the current anomaly detection algorithms, an intelligent attacker can always develop attacks that remain undetected.
- **Human intervention:** Almost all NIDS systems require a constant human supervision, which slows down the detection and the associated actions. Some recent systems such as Network Intrusion Prevention Systems (NIPS) can automatically take pre-programmed actions but these are limited only to the well known attacks.
- **Evasion of signatures:** A number of researchers have argued that it is not difficult for an attacker to evade a signature. Additionally there has been an increase in polymorphic worms which can automatically change their propagation characteristics thereby effectively changing their signatures [10]. Such worms also pose a critical threat to the current NIDS.

V. ROLE OF THE NETWORK INTRUSION DETCTION SYSTEM

A NIDS can detect attacks, and anomalous conditions, additionally they can also provide a number of key information which can be used to identify the nature of attack, its origin and propagation characteristics. First and foremost, most NIDS often reports the location of the attacker or hacker (from where the attack has been triggered). However, the location is commonly expressed as an IP address, which is not reliable information, as the smart attackers often change the IP address in the attack packets, which is called IP address spoofing [4].

The key to determine the importance of the source IP address reported by the NIDS is to classify the attack and then determine if the attack requires the reply messages to be seen or not. In attacks where reply packets are required, IP source address spoofing can not be done. In attacks such as a one way DoS flooding attack, the attacker need not examine the reply, and can easily spoof its address. However, Modern NIDS can also report the route that the attack packets have taken. The route information contains key pieces that can be used to trace the hacker in spite of the source address spoofing. A large variety of attacks such as scanning attacks and penetration attacks, etc requires the attacker to examine the reply messages, in which case tracing them becomes much easier.

VI. FUTURE OF NETWORK INTRUSION DETECTION SYSTEM

One of the key challenges with NIDS has traditionally been performance. Most NIDS employ deep packet inspection which limits the performance. However we have seen that a wide variety of high performance algorithms have been proposed recently, which enhances the performance. Current systems can easily scale to multi gigabit throughputs, and in future performance is likely to become less of an issue.

With the mounting security concerns, the future of IDS is surely promising; however it is important for the above model to emerge. Host machines need to aid the central NIDS component in looking for the behavior (network or system) that is malicious or abnormal. Current well known schemes such as signature based detection can be used here. Additionally, these clients can efficiently run sophisticated anomaly detection algorithms, as data rates over there will be relatively low.

The key challenge then remains in devising the algorithms that can detect anomalies with a fairly high degree of confidence. Although this is an active research topic, it still is questionable when such algorithms will be devised that can be used in a commercial setting. There is another aspect that requires attention in the future - standards concerning the NIDS reporting. In the immediate future, an NIDS protocol will be established and a standardized reporting format will become a requirement. A number of other standardization will likely occur once NIDS mechanisms become better understood and well implemented.

VII. CONCLUSION

In this survey paper, we describe the design and architecture of a NIDS and its configurations, strength and limitations in which they are employed in the network. Specifically we focus on two important models of NIDS: early warning mode and complete deployment mode based. We thoroughly investigate their components and roles. Finally we discuss the future trends in this space, where we argue that a more distributed version of NIDS is on the horizon and that the NIDS mechanisms need to be standardized.

REFERENCES

[1] Subramanian, M.: Network Management Principles and Practices. Addison-Wesley (November 2008)

[2] Northcut, S: Network Intrusion Detection, an Analyst's Handbook. Copyright 1999 by New Riders Publishing, ISBN 0-7357-0868-1.

[3] Dhawal Thakker, Choosing the right intrusion detection system, 2003.

[4] B. Mukherjee et al., "Network intrusion detection", IEEE Network, vol.8,no.3,pp.26–41,1994

[5] C. Estan, S. Savage, and G. Varghese, "Automatically Inferring Patterns of Resource Consumption in Network Traffic," In ACM SIGCOMM, Karlsruhe, August 2003.

[6] Rebecca Bace and Peter Mell, "NIST Special Publication on Intrusion Detection Systems," 16 August 2001. csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

[7] Open Source Host-based intrusion detection system, 2007. http://www.ossec.net/

[8] S. Kumar et al., "Algorithms to accelerate multiple regular expressions matching for deep packet inspection," Proc. ACM SIGCOMM, 2005.

[9] A. Lakhina, et al., "Mining Anomalies Using Traffic Feature Distributions," Proc. ACM SIGCOMM 2005.

[10] G. Varghese, A. Fingethut, and F. Bonomi, "Detecting Evasion Attacks at High Speeds without Reassembly," Proc. ACM SIGCOMM, 2006