Analysis of Network Based Intrusion Detection System

Praveen Dutt

Research Scholar, Sai Nath University, Ranchi, Jharkhand

Abstract - The current generation of centralized network intrusion detection systems (NIDS) has various limitations on their performance and effectiveness. In this article, we argue that intrusion detection analysis should be distributed to network node IDS (NNIDS) running in hardware on the end hosts.

Keywords: Network, Intrusion Detection Analysis

----------♦----------

INTRODUCTION

The current generation of network intrusion detection systems (NIDS) has several limitations on their performance and effectiveness. Many of these limits arise from some inherent problems with the traditional placement of the NIDS sensors within the network infrastructure. Sensors are typically positioned at the aggregation points between the internal and external networks and monitor traffic for a large number of internal hosts. However, there may be other external entry points that go unmonitored, such as dial-up and wide-area wireless (cellular) data connections at the end hosts. Also, a sensor at the gateway typically does not monitor traffic between internal hosts, so it cannot detect internal attacks.

REVIEW OF LITERATURE -

Intrusion Detection Systems help information systems prepare for, and deal with attacks. They accomplish this by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems. Intrusion detection system

- Monitoring and analysis of user and system activity.
- Auditing of system configurations and vulnerabilities.
- Assessing the integrity of critical system and data files.
- Statistical analysis of activity patterns based on the matching to known attacks.
- Abnormal activity analysis, Operating system audit [1].

A system intrusion is any attempt to attack a system and compromise its security aspects such as integrity, confidentiality, or availability. Intrusion Detection Systems (IDS) are implemented to detect an intrusion when it occurs and on detection they should trigger appropriate recovery measures [2]. IDS monitor all traffic as it passes through a network, analyze it, reconstruct sessions and detect predefined patterns of attack or abnormal behaviors that could be caused by system attacks.

In the past few years, several interesting algorithms and techniques have been proposed for multi-pattern matching in the context of network intrusion detection. The hardware-based techniques make use of commodity search technologies such as TCAM [3] or reconfigurable logic/FPGAs [6][14][3][12] Some of the FPGA based techniques make use of the on-chip logic resources to compile patterns into parallel state-machines or combinatorial logic. Although very fast, these techniques are known to exhaust most of the chip resources with just a few thousand patterns and require bigger and expensive chips. Therefore, scalability with pattern set size is the primary concern with purely FPGA based approaches.

INTRUSION DETECTION USING PROTOCOL ANOMALIES

Protocol anomaly detection, which is sometimes called protocol analysis, is the ability to analyze packet flows (the uni-directional communication between two systems) to identify irregularities in the generally accepted Internet rules of communication. These rules are defined by open-protocols and published standards (RFC's), as well as vendor-defined specifications for communication between networked devices. The objective is to implement an intrusion detection mechanism that identifies traffic that doesn't meet specifications or violates the relevant standards. Once an irregularity is identified, it can be used to make network security decisions. This is very effective in detecting suspicious activity, such as a buffer-overflow attack.

INTRUSION DETECTION USING BACKDOOR DETECTION

We have discussed how to detect attacks that violate a protocol (protocol anomaly detection) and attacks that are well known and characterized (signature detection), but we need to understand how to detect attacks that are unknown that don't violate a protocol, such as a Trojan or Worm. These attacks install and open up a backdoor on a network resource. This backdoor lays dormant until the attacker activates it and takes control over the resource. This is accomplished through a series of interactions, where the attacker sends commands and the resource obliges. Because there is no attack pattern and no protocol being violated, another method is needed to detect this interactive traffic.

CONCLUSION:

In this article we analyzed that Network-based intrusion prevention systems rely on signatures to recognize malicious traffic. The quality of a signature is directly correlated to the IDS's ability to identify all instances of the attack without mistakes.

Intrusion detection solutions generally implement only a single intrusion detection mechanism, accounting for a lot of false positives and missed attacks. In addition, they are passive, so they cannot stop an attack, and are notoriously difficult to manage [9].

REFERENCES:

[1] Sans institute infosec reading room, Understanding Intrusion Detection System, Internet, sans institude, 1 to 9, and 2001.

[2] E. Biermann, E. Cloete and L. M. Venter. "A comparison of Intrusion Detection systems", Computers & Security, Volume 20, Issue 8, 1 December

[3] F. Yu, R. Katz, and T. V. Lakshman. Gigabit rate packet pattern-matching using TCAM. In IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, Oct. 2004.

[4] C. R. Clark and D. E. Schimmel. Scalable multi-pattern matching on high-speed networks. In IEEE Symposium on Field-Programmable Custom Computing Machines, (FCCM), Napa, CA, Apr. 2004.

[5] Y. Sugawara, M. Inaba, and K. Hiraki. Over 10 Gbps string matching mechanism for multi-stream packet scanning systems. In Field Programmable Logic and Application: 14th International Conference, FPL, Antwerp, Belgium, Aug. 2004. Springer-Verlag.

[6] Z. K. Baker and V. K. Prasanna. Time and area efficient pattern matching on FPGAs. In Proceeding of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays, pages 223–232. ACM Press, 2004.

[7] I. Sourdis and D. Pnevmatikatos. Pre-decoded CAMs for efficient and high-speed NIDS pattern matching. In IEEE Symposium on FieldProgrammable Custom Computing Machines, (FCCM), Napa, CA, Apr. 2004.

[8] Sarang Dharmapurikar, and John Lockwood, "Fast and Scalable Pattern Matching for Network Intrusion Detection Systems" Oct- 2006

[9] Sarah Sorensen "Intrusion Detection and Prevention "Protecting Your Network from Attacks, Juniper Networks