EXPERIENCE 9 – ADVANCED INTRUSION DETECTION

Student #: 100811212
Student Name: Ben Cendana

Contents

1.0: Introduction

This final experience documents the last foundational paper, Next-generation Intrusion Detection Expert System (NIDES) by Debra Anderson, Thane Frivold and Alfonso Valdes.

The primary aim of this paper was to describe an anomaly based intrusion detection system called (NIDES) derived for the US Navy. Unlike other anomaly based intrusion detection systems this system has a remarkably low false positive rate of 1.3% making it more reliable and potentially able to replace the more popularly used signature based intrusion detection systems.

For this experience we will document how (NIDES) works to help us better understand how to implement and model a better anomaly based system.

2.0: Next-generation Intrusion Detection Expert System (NIDES) Architecture

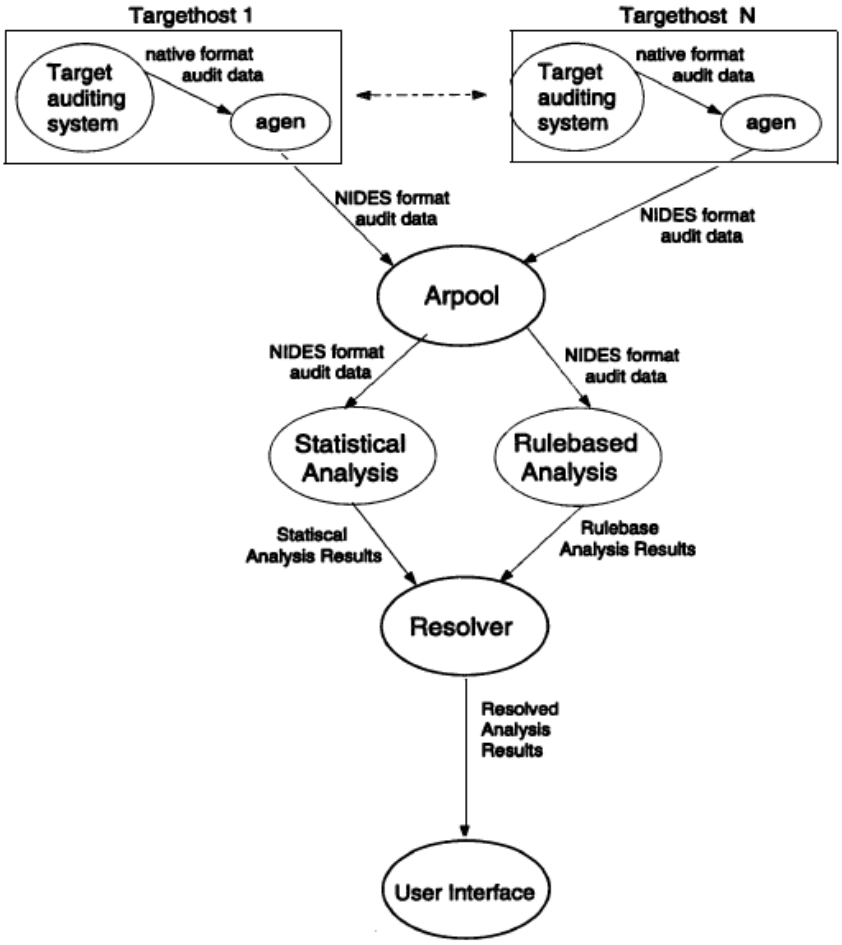

Figure 1: The NIDES Architecture

The main architecture of NIDES is described in Figure 1 and the system is composed of several components, these are the:

1. Host.
2. Agend.
3. Persistent storage.
4. Arpool.
5. Agen.
6. Statistical analysis.
7. Rulebased analysis.
8. Resolver.
9. Archiver.
10. Batch analysis.
11. User interface.

The advantage of setting up an IDS using this model is it allows for real time monitoring as well as limiting the number of false positives.

2.1: The NIDES Host

At the top of Figure 1 is the Targethost 1 and Targethost n both of which represent the workstations of individual users performing some kind of task. Data is then collected on the users system and converted into some kind of audit.

2.2: The Agen Process

The agen process runs on the NIDES host, its primary purpose is to take the audited data and convert it into audit files that are readable only by NIDES.

2.3: The Arpool Process

In Figure 1 there are two hosts Targethost 1 and Targethost n, this is a simplified example since there can be multiple hosts running on an NIDES system. Thus the sole purpose of the Arpool process is to collect all the converted audit files from all the hosts through the Agen process and make it into one big audit file for analysis.

2.4: Statistical Analysis and Rulebased Analysis

The entire intrusion detection system is built on the statistical and rule based analysis, both of which keep track of observed patterns of user behavior. After receiving audit data from the arpool process it is passed through statistical and rule based analysis.

The statistical analysis will maintain statistical profiles of each of the users and will remove old data to help the NIDES system learn and adapt to the users usage habit.

The rule based analysis component is composed of rules that govern known vulnerabilities within the system. This is to prevent an attacker from trying new exploits on the system, if the user behavior

matches any of these rules then an attack attempt must be taking place and the system should be alerted.

2.5: The Resolver

As previously mentioned the NIDES system has a low false positive rate of 1.3% this is do in part to the resolver which filters the alerts. In a typical intrusion detection system there can be up to hundreds or even thousands of alerts leading to a high false positive. However in most cases the majority of these alerts tend to be redundant, as such the resolver attempts to group redundant alerts together which increases the accuracy of the system.

2.6: The Archiver

The archiver saves and stores old audit files and alerts.

2.7: The Batch Analysis

The batch analysis allows the security officer to implement and test new statistical and rule based analysis without effecting the current functions of the IDS.

2.8: The User Interface

The user interface allows the security officer to run any of the processes and interact with the system.

3.0: Future Additions

One of the most import aspects of any system is the ability for it to keep up to date to new potential threats, as mentioned new components can added using the batch analysis.

3.1: Rule Base Additions

Spoofing is a potential addition that could be added to the rulebase analysis, the risk is IPs that were previously authenticated might be exploited by an attacker. To remediate these risks the rulebase could be used to alert unusually IP behavior.

4.0: Conclusion

In conclusion what sets the NIDES system apart from other intrusion detection systems are the batch analysis and resolver.

The batch analysis allows the security officer to try, test and implement new features to insure that the IDS can react and update to new threats.

The resolver is also a big leap as it reduces 100 similar alerts into 1 big alert this in turn helps to reduce the number of false positives.

Therefore these are two features that should be implemented with every intrusion detection system.