**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**SLP 03**

INTRODUCTION

Your paper should address the following questions related to the topic above.

MOTIVATIONS FOR EVALUATING IDPS

Quantitative evaluations is conducted through the systematic empirical investigation of observable phenomena. With regard to IDPS, a finite amount of data is collected and statistical analysis is conducted to help give useful results for a large array of potential customers (Given, 2008).

Acquisition managers benefit from such information and, in practice, are able to improve the process of system selection. Traditional methods which have proven to be less than optimal are all too often based on the claims of subject matter experts (SMEs) employed by various vendors. Other sources like limited-scope reviews in trade magazines have also proved to be an unreliable source of information (Mell, 2003).

Security analysts, who review the output of IDSs, benefit from such information when seeking to understand and report on various topics related to information security within their organization’s realm of networking concerns – internal or external or both. The likelihood that alerts will be generated when a particular kind of attack is initiated, is an example of such a concern (Goodall et al., 2004).

“R&D program managers need to understand the strengths and weaknesses of currently available systems so that they can effectively focus research efforts on improving systems, and measure their progress” (Mell, 2003).

MEASURABLE IDPS CHARACTERISTICS

This section is a list of a partial set of measurements that can be made on IDSs. Focus is given to those measurements that are not only quantitative, but also relate to accuracy of detection.

COVERAGE

“This measurement determines which attacks an IDS can detect under ideal conditions. For signature-based systems, this would simply consist of counting the number of signatures and mapping them to a standard naming scheme. For non-signature based systems, one would need to determine which attacks out of the set of all known attacks could be detected by a particular methodology” (Mell, 2003).

As the White House shared, in 2009, “cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century" (“Cyberspace Policy Review”, 2009). The large number of cyber-attacks, the number of dimensions that form each attack, their individual goals, the effects of the attacks, and the residual evidence of the attack make measuring the coverages of an IDS difficult, but necessary (Han et al., 2014).

The various cyber-attacks have a culmination of threat areas, located within an organization or external to it. Investigating cybercrimes has revealed that each attack has its own goal; for example, denial of service, penetration, or scanning attacks. The cyber-attacks work against the, software, operating system, or protocol, and they are designed with malicious specificity. They are precise and particular to their intended victim (Han et al., 2014).

Attacks may also be defined by researchers as having the finest level of granularity. This is where each target has a target configuration, like a certain version of a protocol, and a mode of operation that are very specific (Mell, 2003).

Additional struggles with obtaining accurate coverage measurements include obstacles like site-precedence. This is where one site might give a higher level of importance to a particular cyber-attack and another site will not share the same level of concern for such an attack. An E-commerce site, for example, might be very interested in detecting distributed denial of service attacks, whereas a military site might be more interested in surveillance attacks (Stavroulakis et al., 2010).

PROBABILITY OF FALSE ALARMS

“This measurement determines the rate of false positives produced by an IDS in a given environment during a particular time frame. A false positive or false alarm is an alert caused by normal non-malicious background traffic” (Mell, 2003). To determine the rate of false alarms produced by an IDS, in a given environment within a particular timeframe, is resolved by finding the probability of false alarms. Different false alarm rates, however, in different network environments make measuring false alarms difficult. Also, configurable IDSs can be tuned to reduce the false alarm rate and with the diversities involved in host activities and network traffic, it could be difficult to determine the aspects that cause false alarms (Stavroulakis et al., 2010).

PROBABILITY OF DETECTION

This measurement determines the rate of attacks detected correctly by an IDS in a given environment during a particular time frame. The difficulty in measuring the detection rate is that the success of an IDS is largely dependent upon the set of attacks used during the test. Also, the probability of detection varies with the false positive rate, and an IDS can be configured or tuned to favor either the ability to detect attacks or to minimize false positives (see section 3.2 for an explanation of this). One must be careful to use the same configuration during testing for false positives and hit rates. Further, an NIDS can be evaded by stealthy versions of attacks. An NIDS may detect an attack when it is launched in a simple straightforward manner, but not when even simple approaches to stealthiness are used. Techniques used to make attacks stealthy include fragmenting packets, using various types of data encoding, using unusual TCP flags, encrypting attack packets, spreading attacks over multiple network sessions, and launching attacks from multiple sources [3, 4].

RESISTANCE TO ATTACKS DIRECTED AT THE IDS

This measurement demonstrates how resistant an IDS is to an attacker's attempt to disrupt the correct operation of the IDS. Attacks against an IDS may take the form of:

1. Sending a large amount of non-attack traffic with volume exceeding the IDS’s processing capability. With too much traffic to process, an IDS may drop packets and be unable to detect attacks.

2. Sending to the IDS non-attack packets that are specially crafted to trigger many signatures within the IDS, thereby overwhelming the IDS’s human operator with false positives or crashing alert processing or display tools.

3. Sending to the IDS a large number of attack packets intended to distract the IDS’s human operator while the attacker instigates a real attack hidden under the “smokescreen” created by the multitude of other attacks.

4. Sending to the IDS packets containing data that exploit a vulnerability within the IDS processing algorithms . Such attacks will only be successful if the IDS contains a known coding error that can be exploited by a clever attacker. Fortunately, very few IDSs have had known exploitable buffer overflows or other vulnerabilities.

ABILITY TO HANDLE HIGH BANDWIDTH TRAFFIC

This measurement demonstrates how well an IDS will function when presented with a large volume of traffic. Most network-based IDSs will begin to drop packets as the traffic volume increases, thereby causing the IDS to miss a percentage of the attacks. At a certain threshold, most IDSs will stop detecting 5 any attacks. This measurement is almost identical to the “resistance to denial of service measurement” when the attacker sends a large amount of non-attack traffic to the IDS. The only difference is that this measurement calculates the ability of the IDS to handle particular volumes of normal background traffic.

ABILITY TO CORRELATE EVENTS

This measurement demonstrates how well an IDS correlates attack events. These events may be gathered from IDSs, routers, firewalls, application logs, or a wide variety of other devices. One of the primary goals of this correlation is to identify staged penetration attacks. Currently, IDSs have only limited capabilities in this area.

ABILITY TO DETECT NEVER BEFORE SEEN ATTACKS

This measurement demonstrates how well an IDS can detect attacks that have not occurred before. For commercial systems, it is generally not useful to take this measurement since their signature-based technology can only detect attacks that had occurred previously (with a few exceptions). However, research systems based on anomaly detection or specification-based approaches may be suitable for this type of measurement. Usually systems detecting attacks that had never been detected before produce more false positives than those that do not have this feature.

ABILITY TO IDENTIFY AN ATTACK

This measurement demonstrates how well an IDS can identify the attack that it has detected by labeling each attack with a common name or vulnerability name or by assigning the attack to a category.

ABILITY TO DETERMINE ATTACK SUCCESS

This measurement demonstrates if the IDS can determine the success of attacks from remote sites that give the attacker higher-level privileges on the attacked system. In current network environments, many remote privilege-gaining attacks (or probes) fail and do not damage the system attacked. Many IDSs, however, do not distinguish the failed from the successful attacks. For the same attack, some IDSs can detect the evidence of damages (whether the attack has succeeded) and some IDSs detect only the signature of attack actions (with no indication whether the attack succeeded or not). The ability to determine attack success is essential for the analysis of the attack correlation and the attack scenario; it also greatly simplifies an analyst’s work by distinguishing between more important successful attacks and the usually less damaging failed attacks. Measuring this capability requires the information about failed attacks as well as successful attacks.

CAPACITY VERIFICATION FOR NIDS

The NIDS demands higher-level protocol awareness than other network devices such as switches and routers; it has the ability of inspection into the deeper level of network packets. Therefore, it is important to measure the ability of a NIDS to capture, process and perform at the same level of accuracy under a given network 6 load as it does on a quiescent network. For example, Hall [34] has proposed a test methodology and traffic metrics for standardized capacity benchmarking of NIDS. The NIDS customers can then use the standardized capacity test results for each metric and a profile of their networks to determine if the NIDS is even capable of sustaining inspection of the traffic.

OTHER MEASUREMENTS

There are other measurements, such as ease of use, ease of maintenance, deployments issues, resource requirements, availability and quality of support etc. These measurements are not directly related to the IDS performance but may be more significant in many commercial situations.

1. Examples on some of the current evaluation efforts
2. Challenges in evaluating IDPS

BODY

CONCLUSION

REFERENCES

Cyberspace Policy Review. (2009). Retrieved December 12, 2015, from https://www.whitehouse.gov/assets/documents/Cyberspace\_Policy\_Review\_final.pdf

Given, L. (2008). The Sage encyclopedia of qualitative research methods. Los Angeles, Calif.: Sage Publications.

Goodall, John, Wayne Lutters, and Anita Komlodi. (2004). *The Work Of Intrusion Detection: Rethinking The Role Of Security Analysts*. 1st ed. New York: Proceedings of the Tenth Americas Conference on Information Systems, 2015. Web. 12 Dec. 2015.

Han, C., & Dongre, R. (2014, October 1). Q&A. What Motivates Cyber-Attackers? Retrieved December 12, 2015, from http://timreview.ca/article/838

Mell, P. (2003). *An Overview Of Issues In Testing Intrusion Detection Systems*. 1st ed. Gaithersburg: U.S. Department of Commerce, 2015. Web. 12 Dec. 2015.

Select and Implement an Intrusion Detection and Prevention System. (2015). Retrieved December 12, 2015, from [http://www.infotech.com/workshops/select-and-implement-intrusion-detection- and-prevention-systems](http://www.infotech.com/workshops/select-and-implement-intrusion-detection-%09and-prevention-systems)

Stavroulakis, P., & Stamp, M. (2010). Intrusion Detection Systems. In Handbook of information and communication security (pp. 202-203). Heidelberg: Springer.