American Journal of Applied Sciences 2 (6): 1032-1035, 2005
ISSN 1546-9239

Increasing Effectiveness of IDS to Improve Security in Intranet

[1]Umesh Kumar Singh, [2]A.K. Ramani, [3]Narendra S. Chaudhari and [4]Vandana Gupta
[1]MICS, Mahakal Institute of Technology, MIT Campus, Ujjain (MP) -India
[2]Institute of Computer Science and Electronics (ICSE), D.A.V.V., Indore (MP) -India
[3]School of Computer Engineering, Nanyang Technological University (NTU), Singapore
[4]Department of Computer Science, Kalindi College, Delhi University, Delhi-110008, India

Abstract: Today Intrusion Detection Systems (IDS) are becoming one of the most important tools for intranet security. Research regarding Intrusion Detection Systems (IDSs) has become more active with the recent increases in illegal accesses to computer systems. Many researchers focus only on the techniques or mechanisms for detecting intrusions automatically, without considering the security of IDSs themselves. When an intruder attacks and breaks into a system, he or she often deletes system logs and stops auditing processes. Thus, the security of an intrusion detection system is an important aspect of intrusion detection. This study explores the methods for increasing effectiveness in configurations of an IDS for obtaining maximum effects in security in an intranet. We also discuss the hurdles that have blocked successful measurements in this area and present suggestions for improving effectiveness of an IDS.

Key words: Intranet, IDS, Intrusion, Intruder, Security

INTRODUCTION

There is a continuous race between attack and defense technologies as depicted in Fig. 1. With the development of firewalls, intrusion detection and similar techniques, effective attacks are becoming more difficult and short-lived. On the other hand, automated attack tools, widespread scanning, fast dissemination of tools and information via the Internet and the advent of network worms mean that attackers have a greater coverage than ever before.

In the last few years, the use of Intrusion Detection System (IDS) has grown considerably and now becoming one of the most useful tools for intranet security. According to International Data Corp., the projected revenue from IDSs and related services is expected to rise approximately 50% every year[9]. After having enormous growth in investment every year in IDS technology, no comprehensive and scientifically rigorous methodology is available today to test the effectiveness of these systems.

The CSI/FBI Computer Crime and Security Survey [CSI/FBI] shows that a range of security technologies is in wide use in organizational systems. For example, 95% of respondents use firewalls, 98% use anti-virus software, 90% user access controls and 61% use intrusion detection. Similarly, many organizations have come to rely on Internet-based services to conduct business. In the survey, it is noted that 97% of respondents have www sites, 47% using these to conduct electronic commerce, with 23% suffering unauthorized access or misuse. Recent events have demonstrated the weakness of current network security approaches however, with network worms compromising hundreds of thousands of systems in hours.

Smart attackers are generally aware of the presence of IDS capabilities of a network and may directly attack such systems. An IDS cannot function correctly if the information it receives is corrupted. A more dangerous scenario is where an attacker takes over and impersonates a sensor: No alert will be generated from losing contact and an attacker can then feed arbitrary information to the monitor. While IDS protocols and modules are designed to resist attack, the reports of an IDS are only as good as the information it is fed. IDSs generally depend on seeing all traffic on a network segment or all of the event logs for a host-based IDS. With the current increasing use of network bandwidth, it is becoming impossible for any machine to dependably monitor a network link under heavy load. This implies that some parts of an attack may be missed. A similar problem is the increasing use of switching technology in networks-where an IDS sensor would have to be embedded into the switch hardware in order to ensure that it can inspect all traffic.

In order to recognize attacks, an IDS has to model the effect of an event on the systems it is protecting. Particularly in networking IDS, the heterogeneity of systems monitored may cause problems. In particular, since different systems respond differently to the same events, it becomes impossible for an IDS to accurately predict the effect of any given sequence. This implies that an IDS needs to maintain a detailed state of the network it is guarding (which is clearly infeasible), or make assumptions as to the effect of observed events.

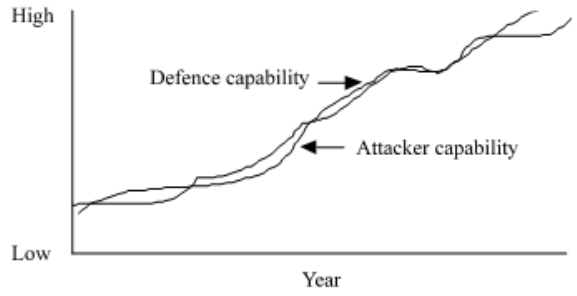

Fig. 1: The Race between Security and Attack

The end result is that it becomes possible to have effective attacks being obscured from IDS systems-again, leading to false positives and false negatives.

MOTIVATION AND OBSERVATIONS

Reviewing the intrusion detection system testing and benchmarking literature, it becomes clear that present approaches to testing are inadequate. A large number of unrelated tests, such as[3, 6, 14] can be brought into use. Most of these tests assess susceptibility to a single weakness or single weakness area. We do not believe that there is ever going to be a comprehensive test nor a single methodology that would examine an intrusion detection system for every attack, verify its abilities and identify all its weaknesses. This in essence would categorically solve the problem of intrusion detection. However, it is possible to improve on the existing practices employed in the field.

As noted, a wide variety of security tools and mechanisms are currently available. This begs the question: Why is there a need for active security? In order to answer this, let us consider the 1999 CSI/FBI Computer Crime and Security Survey[2]. The survey was conducted over 521 US companies from a range of industry sectors, with sizes ranging from under 100 employees to over 10,000. These companies had a variety of security structures in place, as shown in Table 1.

In spite of these measures, 61% of these companies reported experiencing unauthorized use of their computer systems. Twenty percent did not know if their systems had been abused. While 30% of organizations reported outside penetration of their systems, 55% reported insider abuse. Many of the organizations were unable to quantify their losses due to intrusions. It is notable that 94% of those organizations have web sites (29% offering electronic commerce via these sites). Again, figures on the abuse of these sites are startling: 18% report abuse-while 30% do not know. Clearly conventional, static security mechanisms such as firewalls are incapable of offering complete protection. Active Security mechanisms such as Intrusion Detection should have a place in any secure network.

Table 1: Security Measures in Place

Access Control	89%
Biometrics	8%
Encrypted login/sessions	44%
Firewalls	88%
Physical Security	88%
Intrusion Detection	40%

This part of our research study will cover the configuration of IDSs and in this section we are trying to find what elements of an IDS configuration that gives the most value of security, efficiency and low costs. This may help security organizations dealing better with IDS systems in both a secure and economical point of view. Using known benchmarking techniques there will be possible to find out if there are important elements in a configuration that are crucial to get a desired security and efficiency of an IDS, so that this can result in a better understanding of what makes a better configuration of an IDS.

RELATED WORK

On[7] Maxion and Tan cover anomaly IDSs, but this is not the kind of IDSs covered in this study. But the interest of this study lies in the fact that it presents a benchmarking method that can be used or in worst case enlightens aspects of benchmarking principles of IDSs. In[12] Ranum summarizes experiences from the work that has been done with benchmarking IDSs. This study presents useful information about which methods that have proven to be successful and warns of common pitfalls. In addition it presents a scientific approach on how to configure an IDS and design a test. Schaelicke *et al.*[13] introduces a technique of measuring the effectiveness of a Network IDS (NIDS). This study has a technical view and concentrates on hardware and performance. This aspect is also important when benchmarking IDSs. Puketza *et al.* In[11] presents a method for testing intrusion detection systems. This work may be used in creating test suits for IDSs. It describes which elements that are important in a test situation.

Our own earlier work on the Intranet security which mainly concentrated on enhancing the existing firewall for protecting intranet against various malicious attack advocates the use of IDS. In[15] we proposed integration of IDS in existing firewall configuration. Such integration along-with increase in effectiveness in IDS configuration will provide more appropriate effects for securing resources and information on an intranet.

OBJECTIVE

Implementing systems for intrusion detection is an important part of the strategy for securing information over an intranet, especially in organizations where it is

critical for the information security that no unauthorized gain access to these information systems.

If we could find out what aspects of a configuration of an IDS system that gives the best security and efficiency, it would probably increase the interest in implementing IDS systems. Key elements in a good configuration can help others configuring the IDS with desired effects. Consequently, IDSs may seem more desirable in both security and economic perspectives. More efficient IDS systems detect more attacks and could raise alarms or taking countermeasures to stop attacks as they happen. This may reduce the number of electronic break-ins which leads to: (I). reduced information losses and (ii). reduced costs due to less resources obtained by the IDS.

We discuss a flexible intrusion detection and response framework that is based on active networking technology. Principal findings so far are that active networking proves to be a well suited technology for intrusion detection and response, that the load of intrusion detection can be distributed among multiple systems with this approach and that the overhead stays in acceptable ranges.

METHODS

We identified three factors which are of great importance for intranet security and can be better taken care if an IDS is properly configured and operates in an intranet: (a) security (b) efficiency and (c) cost and resources. To meet at this it is necessary to find out:

* A way to configure an IDS to get optimum values for the variables. What elements in the configuration give great values of the variables. To what extent can these elements be used as guidelines in an IDS configuration.
* How an IDS configuration affects these variables

This can be achieved by using known penetration testing techniques and benchmarking methods with different types of configurations. It is therefore necessary to find out more about:

* Available benchmarking methods
* Important configuration test criteria
* Existing penetration tests used on IDSs

This study of methods based on benchmarking described in[6, 7, 12]. IDSs test can be achieved by using penetration tests. These penetration tests are based on known methods and principles provided in the existing literature. The test must be created as a prototype framework of important test criteria. The criteria will be based on existing literature found in[4, 13, 17] and the factor described in the research question sections. The framework will be used as parameters to a specific penetration test, that will be used to test the IDSs along with their different configurations. The penetration test will be based on ideas and principles found in the literature in[1, 8, 11, 16].

A set of configuration schemes must be created based on how the IDS can be configured. It will most likely be a great number of possible configuration parameters available, so each configuration must have a set of parameters either set “on”, “off” or with a fixed value if available. If possible, this configuration scheme may be ported to different IDSs. This is necessary in order to evaluate and compare results from the benchmarks among different IDSs. The experimental scheme can mainly be performed with two computers, one victim host and one attacking host. The victim will run the IDS with several configurations, based on the configuration scheme. For each configuration, the attacker will run the penetration test and then we can discover which attacks that are detected and which are not. The penetration test should also generate some traffic to discover false-positives, alarms that are not real attacks. The proposed experimental scheme can be classified as a qualitative experimental. It seems that an experiment of this kind will give the most valuable results. The main goal is not to test as many IDSs and configurations as possible to get wide statistical data, but rather to discover some key elements in a configuration that makes the IDS behave in a more desired way. Using the proposed qualitative experimental scheme we will get results provided by the configuration scheme that gives output results of: number of false positives and the number of false negatives.

This can be used to measure the variables security, efficiency and an estimate on costs and use of resources. The rate of false positives and negatives are the results from the penetration test which benchmarks the IDS with a configuration from the configuration scheme. From the various benchmarks of the configurations we get penetration test values that give various results on the three variables mentioned. The configuration that gives the best values, will probably be the best configuration according to the criteria for the penetration tests and the configuration scheme. The results will increase its scientific value if we can prove the elements in the configuration to yield similar results on other IDSs.

From the penetration tests of the different configurations, we will most likely see changes in the number of false positives and false negatives. These changes imply that:

* Security is affected by false negatives. Increase in false negatives means that the target system is more vulnerable to attacks
* Efficiency is affected by false positives and false negatives The criteria for an efficient IDS, are that it has as low rates of false positives and false negatives as possible.
* Costs and use of resources are affected by false positives and also the complexity of configuring the IDS.

False positives generate a lot of extra work that obtains resources. Complex configurations have the same effect on costs and resources. If we find a way, that is important parameters in a configuration that increases security and efficiency, it will ease the configuration of IDS and this will decrease running costs and maintenance of the IDS.

CONCLUSION

Developing configuration schemes and test suites for an IDS are the most critical elements in intranet security because these forms the basis for further work. This work cannot be ignored for long time period. Throughout their history, intrusion detection systems have been configured and designed with different structures and schemes for detection. They started by being host-based[3], later evolved into network-based systems[5] and in the later years they have tended towards a distributed combination of the two[10]. However, during all that evolution, the sources of information used by intrusion detection systems have remained essentially unchanged: audit trail and network traffic. Raising of false alerts is clearly going to lower the effectiveness of the IDS and our priority during the detection phase should be to correlate events from a number of systems to increase both speed and accuracy of detection. An effective way of correlation is to use a signature-based NIDS in combination with a statistical profile.

By studying deployed systems, we have noticed that under limited resources, the usability of signature-based systems decreases with network size. As networks grow, the emphasis is shifted from popular signature-based systems for statistical analysis. Machine automation of response, although cost-effective, has highly limited applications. The burden of incident response is still carried by security administrators. In order to simplify the process and decrease the time needed to analyze alerts and perform recovery, administrators should be equipped with policies, checklists and guidelines allowing them to work methodologically. This is especially crucial if the goal of the incident response is to pursue legal action against the attacker. Finally, intrusion detection systems are not an answer to all network security problems. They require a certain level of maturity and are only effective if monitored and maintained.

REFERENCES

1. Chung, M., Puketza, Olsson and Mukherjee, 1995. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions. Proc. of the 1995 National Information Systems Security Conf. Baltimore, Maryland, pp: 173-183.
2. Computer Security Institute "1999 CSI/FBI Computer Crime and Security Survey, 1999. Computer Security Issues and Trends, Vol: 5.
3. Denning, D.E., 1987. An Intrusion-Detection Model. IEEE Transactions on Software Eng., 13: 222-232.
4. Gene, H. Kim and H. Eugene Spafford, 1994. The design and implementation of Tripwire: A file system integrity checker. In Proc. of the 2nd ACM Conf. Comp. and Communications Security, pp: 18-29.
5. Heberlein, Dias, Levitt, Mukherjee, Wood and Wolber, 1990. A Network Security Monitor. In Proc. of the IEEE Symposium on Res. in Security and Privacy, pp: 296-304.
6. Lippmann, R., Fried, Graf, Haines, Kendall, McClung, D. Weber, S. Webster, Wyschogrod, Cunningham and Zissman, 2000. Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation, IEEE Computer Society Press.
7. Maxion, R. and K. Tan, 2000. Benchmarking Anomaly-Based Detection Systems, In Proc. of the 1st Intl. Conf. on Dependable Systems and Networks.
8. Mell, P., V. Hu, R. Lippmann, J. Haines, M. Zissman, 2003. An Overview of Issues in Testing Intrusion Detection Systems, National Institute of Standards and Technology ITL, Massachusetts Institute of Technology, Lincoln Laboratory.
9. Mukherjee, B., Herberlein and Levitt, 1994. Network intrusion detection. IEEE Network, 8: 26-41.
10. Phillip, A. and Neumann, 1997. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proc. of the 20th National Information Systems Security Conf., pp: 353-365.
11. Puketza, N.J., K. Zhang, M. Chung, B. Mukherjee and R.A. Olsson, 1996. A Methodology for Testing Intrusion Detection Systems, IEEE Transactions on Software Engineering.
12. Ranum, M.J., 2001. Experiences Benchmarking Intrusion Detection Systems. NFR Security Technical publications.
13. Schaelicke, L., T. Slabach, B. Moore and C. Freeland, 2003. Characterizing the Performance of Network Intrusion Detection Sensors. Proc. Of the Sixth Intl. Symposium on Recent Advances in Intrusion Detection.
14. Schneier, B., 1999. The Trojan Horse Race. Communications of the ACM. 42: 128.
15. Singh, U.K., A.K. Ramani and N.S. Chaudhari, 2005. On analysis and design of the enhanced firewall for intranet security. J. Computer Sci., Science publications, New York, USA. 1: 290-296.
16. Song, D., M. Shaffer, Undy and Nidsbench, 1999. A Network Intrusion Detection Test Suite, Recent Advances in Intrusion Detection.
17. Steven, A.H., F. Stephanie and A. Somayaji, 1998. Intrusion detection using sequences of system calls. J. Comp. Security, 6: 151-180.