PRIORITIES IN THE DEPLOYMENT OF NETWORK INTRUSION DETECTION SYSTEMS

Marcin Dobrucki & Teemupekka Virtanen

Nokia & Helsinki University of Technology, Finland.

Abstract: The purpose of this work is to study the priorities in the deployment of network intrusion detection systems (NIDS) in small corporate networks. The goal is to minimize costs while optimizing performance. Despite apparent benefits of automated intrusion detection systems (IDS), they are not widely deployed at this time. Our main research problem is defining key cost areas of NIDS deployment and then developing ways to achieve the required functionality with minimal costs. We present a concept of pre-ids stage, where small, isolated tools are used to target network security problems. The ease of deployment and low maintenance costs help of these tools allow to combat a large part of these problems at a fraction of the costs of a full IDS.

Keywords: Network intrusion detection, optimization and deployment.

1. INTRUSION DETECTION

By intrusion detection, we mean identifying potentially malicious or undesirable activity that may have occurred in a given environment as recorded in an audit trail (Amoroso, 1994) of a security system. Five steps make up this process: capture, analyze, classify, report, and possibly react (Bace, 1999; Heberlein et al., 1991; Lunt et al., 1988; Smaha, 1998) to the event. Our ability to automate the system, and benefit from it is highly dependent on our ability to collect quality data (Ptacek and Newsham, 1998) and our ability to extract useful information from that data.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

2. DEPLOYMENT PRIORITIES

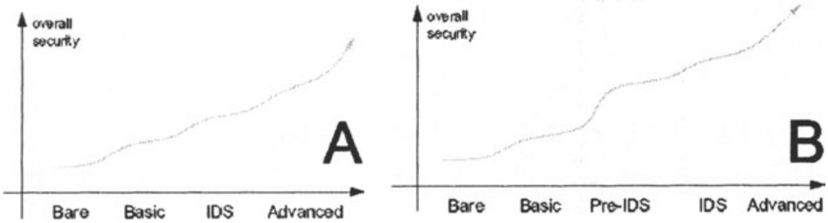

Figure 1. Original (A) and improved (B) security phases in small corporate network

We use the stages in Figure 1A to roughly represent the deployment of security measures in a network infrastructure. The *bare* stage represents computers directly connected to a larger network without any kind of security provisions. We define the *basic* phase when the company implements a firewall (FW), and possibly divides the network into separate zones such as de-militarized zone (DMZ) or extranets. Beyond the basic stage, companies begin to look for active defenses. This typically involves active monitoring of network traffic (NIDS), or host-based IDS, or both. Whereas the gap between the bare and basic functionalities is quite simple to close, the deployment of an IDS is a large and difficult project. Beyond the IDS phase we have defined an Advanced stage, where anything from large data-mining IDS systems to verified platforms can be found.

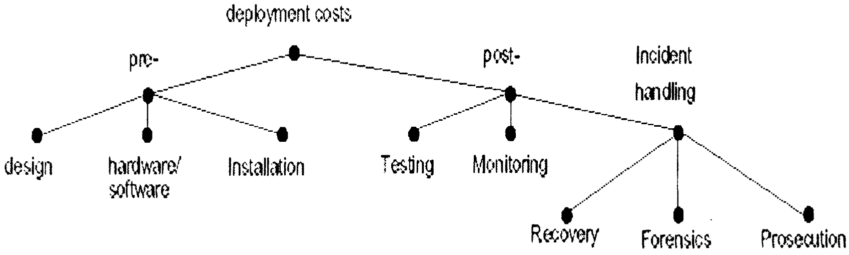

Figure 2. Costs layout for intrusion detection system deployment

In Figure 2 we present different cost areas and divide them into two parts: the pre- and post- deployment expenses. On the *pre-deployment* branch, we accumulate costs such as system evaluation, selection, software purchases, and system installations. At the *post-deployment* branch, we look at costs of actually running the IDS. Deployment of IDS for PR value is wasteful, and hence we should aim towards some return on investment

(ROI) from our system. The gain can vary from minimizing damage inflicted by the intrusions, to providing evidence which can be used in courts to seek compensation from the attackers (Berinato, 2002). In most cases we have studied, however, use of IDS is limited to helping track down and patch problems. If the IDS is expensive to deploy and maintain, this results in low ROI.

3. SECURITY PRIOR TO INTRUSION DETECTION

The costs and difficulties of IDS deployment lead to a question if there is some more cost-efficient way to improve network security? We introduce an idea of pre-ids phase (as shown in Figure 1B), a set of improvements which are designed to mitigate most of the common problems related to network intrusions. We assume that there is a proper FW and the network has been structured to isolate functionality and create zones (Sanchez, 2000). Recent studies have shown that up to about 70-80% of corporate security problems originate from within the companies. (Raili, 2002) Some of the typical events of interest which we would like to detect are: 1. Address spoofing, are there any packets on our network with interesting looking source address? 2.Are there any new bindings between IP addresses and MAC addresses? 3. Has any of our computers put any of their interfaces in promiscuous mode? 4. Has any of our computers started sending or receiving more traffic than usual? 5. Has any of our computers started to listen on a port which was previously closed?

Inside perimeter defenses, the false positive rate for detected spoofs is very low, because under normal circumstances, no legitimate action should require spoofing of any kind. This allows us to deploy a miniature tool, such as ARPWatch for instance, to monitor changes in address bindings on our network. Promiscous mode detection is more difficult, however it provides a clear indication of suspicious activity (Graham, 2000). Most currently utilized operating systems require administrative rights to put network interfaces into promiscous mode. Hence detection of an unknown promiscous interface should be treated as an intrusion. After a certain period of utilization, patterns of systems behaviour and network utilization should be possible to establish (focus.ids, 2002). Detection of new service ports, or abnormal traffic patterns for any trusted host should hence be viewed as suspicious. Typically such checks can be incorporated into network monitoring tools supplemented by periodic network or vulnerability scans. It might appear unclear at first why deploying a number of small, fairly limited tools might yield more benefits than deploying one solid IDS system. However, referring back to Figure 2, we can identify a number of costsaving factors on both the pre- and post- deployment branches. At the *pre* stage, we almost completely eliminate the initial expenses associated with deploying IDS. The tools reviewed for this paper were evaluated within a few short hours, and their deployment was almost instaneous. They have also provided reliable information on the main events of interest mentioned above. The savings at the post stage relate mostly to limiting the responsibility of the system administrators to monitor and maintain yet another surveillance system, when a number of them have already been put into use.

4. CONCLUSIONS

The application of a pre-ids technique is limited to certain type of environments however, it can yield positive results. The deployment of a full-scale IDS can be expensive, and although the initial costs can be kept low, a proper maintenance of the system will be costly. We have identified the common events of interest which constitute the majority of issues that a typical IDS deals with. We have then provided a cost-effective solution to combating them through the use of small, dedicated, easily deployable tools.

REFERENCES

Amoroso, E. (1994). Fundamentals of Computer Security Technology. Prentice Hall, Englewood Cliffs, NJ.

Bace, R. (1999). An intro to intrusion detection assessment. Technical report, Infidel Inc.

Berinato, S. (2002). Finally, a real return on security spending. CIO Magazine. http://www.cio.com/archive/021502/security content.html.

focus.ids (2002). Focus-ids: Statistical anomaly analysis. http://www.securityfocus.com.

Graham, R. (2000). Sniffing faq, v.0.3.3. http://www.robertgraham.com/pubs/sniffing-faq.html.

Heberlein, L., Levitt, K., and Mukherjee, B. (1991). A method to detect intrusive activity in a networked environment. In Proceedings of the 14th National Computer Security Conference. Washington DC.

Lunt, T., Jagannathan, R., Lee, R., Listgarten, S., Edwards, D., and Ford, J. (1988). Ides: The enhanced prototype, a real-time intrusion-detection expert system. Technical report, SRI International.

Ptacek, T. H. and Newsham, T. N. (1998). Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical report, "N/A", Suite 330, 1201 5th Street S.W, Calgary, Alberta, Canada, T2R-0Y6.

Raili, S. (2002). Tietoturvan syydetään raha heikoin tuloksin. ITViikko, (6).

Sanchez, S. C. (2000). Ids "zone" theory diagram. http://infosec.gungadin.com. referred 2.1.2002.

Smaha, S. (1998). Haystack: An intrusion detection system. In Proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference. IEEE. Orlando, Florida.