International Research Journal in Global Engineering and Sciences. (IRJGES)
Vol. 1, No. 2, July, 2016 | ISSN : 2456-172X

Cost Benefit Analysis in Intrusion Detection System

[1]S. Saravana Kumar

[1] Assistant Professor, Department of Computer Science, Kristu Jayanti College, Bangalore 560 077.
Email-saravanan.msc16@gmail.com

Abstract: Assessing the cost-benefit tradeoff of a network intrusion detection system requires an understanding of the effectiveness of the system and the cost of its employment. In this paper, we propose a cost-benefit analysis methodology and build a cost model based on an investigation of the cost factors and categories of various intrusions. The model can be used to quantitatively and qualitatively calculate the cost of detecting and responding to an intrusion, and provide necessary advice for determining the tradeoff between costs and benefits.

Keywords: Network intrusion, Cost-benefit analysis, intrusion detection, tradeoff

Abstract

Assessing the cost-benefit tradeoff of a network intrusion detection system requires an understanding of the effectiveness of the system and the cost of its employment. In this paper, we propose a cost-benefit analysis methodology and build a cost model based on an investigation of the cost factors and categories of various intrusions. The model can be used to quantitatively and qualitatively calculate the cost of detecting and responding to an intrusion, and provide necessary advice for determining the tradeoff between costs and benefits.

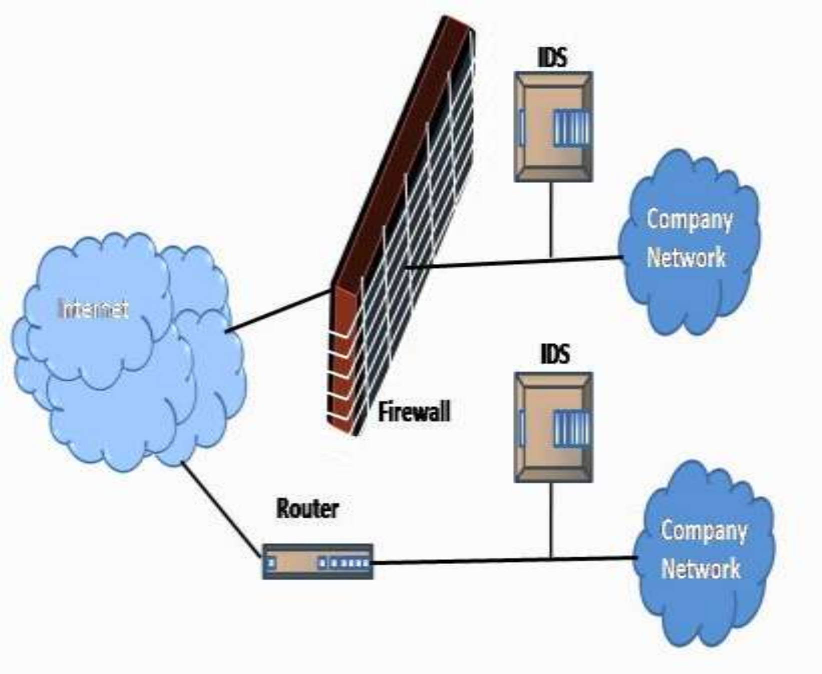
Introduction

An intrusion detection system (IDS) is a device (or application) that monitors network and/or system activities for malicious activities or policy violations.Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.

IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

Internet



IDS Terminology

- Alert/Alarm- A signal suggesting that a system has been or is being attacked.
- True Positive- A legitimate attack which triggers an IDS to produce an alarm.
- False Positive- An event signaling an IDS to produce an alarm when no attack has taken place.
- False Negative- A failure of an IDS to detect an actual attack.
- True Negative- When no attack has taken place and no alarm is raised.
- Noise- Data or interference that can trigger a false positive.
- Alarm filtering- The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.

Types of Intrusion-Detection systems

There are two main types of IDS's: network-based and host-based IDS.

In a **network-based** intrusion-detection system (NIDS), the sensors are located at choke points in network to be monitored, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic.

In a **host**-based system, the sensor usually consists of a software agent, which monitors all activity of the host on which it is installed, including file system, logs and the kernel. Some application-based IDS are also part of this category.

Network intrusion detection system (NIDS)

Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.
Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

Host-based intrusion detection system (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state. An example of a HIDS is OSSEC.
Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected.

Requirements in Traditional Intuition Detection System (TIDS)

In general, an TIDS has the following requirements:

- Detection of known attacks. This is the IDSs basic functionality. An IDS should have the ability to determine the malicious attackers who want to intrude the systems in the past and are likely to occur in the future.

- Real-time/near real-time analysis. An IDS should analyze information sources gathered by the IDS sensor as soon as possible. Before an attacker significantly damages the systems, the IDS can perform the real-time/near real-time analysis.

- Minimal resource. IDSs should use the minimal resource in the systems when monitoring. For example, in HIDSs, the minimal resource could avoid the lack of the systems' recourse. In NIDSs, minimal resource could avoid the IDSs crash by themselves.

- High accuracy. IDSs should make sure the detection is correct and lower the false alarms

Cost Analysis of TIDS

The damage cost (*DCost*), is the cost of damage caused by hackers when IDSs do not work appropriately.
Response cost (*RCost*), means the costs of actions when response components generate alarms, including active (automatic) and passive (manual) responses.

Operational cost (*OpCost*) is the cost of processing and analyzing the activities of events. It is corresponding to the target computing resource.

False Negative cost is the cost of not detecting an attack, but an attack really happened. Therefore, this cost is defined as the damage cost associated with event.

False Positive cost occurs when normal behavior is misidentified as the attack. If RCost is less than DCost, a response will ensue and the response cost must be accounted for as well. If RCost is great or equal than DCost, the minimal cost is that SMs do not responded to this intrusion. Then FP cost is zero.

True Positive cost means the detection cost when attacks really happen.

If Rcost is greater or equal than DCost, the minimal cost is that SMs do not responded to this intrusion, and the loss is DCost. Otherwise, If RCost is less than DCost, an attack is detected and response ensues, some damage may have incurred. TP cost may be defined as Rcost + $Є_1$DCost, here $Є_1$ is the function of the events' progress belongs to interval between 0 and 1.

True Negative is incurred when an IDS correctly decides there are no attacks. This cost is always zero since no attacks happen.

$$CumulativeCost(E) = \sum_{e \in E}(CCost(e) + OpCost(e))$$

$$e \in E(\text{the event set})$$

Roles in Intrusion Detection System with Identification Capability (IDSIC)

In TIDSs, most designers only discuss three roles: hackers, SMs, and DS, but in a large system with high security environment, it always includes system security auditors to perform some tests to keep a check on system vulnerability.

The security auditor (SA) can be defined as a person appointed and authorized to audit whether the security equipments work regularly or not by using the vulnerability testing tools. One of security auditors' main works is to check the security holes or vulnerabilities in the system. Note that in traditional IDSs, they have no abilities to distinguish the security auditors and hackers.
Detection System with Identification Capability (DSIC) is defined as One type of DS that runs the same function of DS. However, it has an extra functionality to distinguish between the roles of hackers and SAs.

In order to distinguish SAs and hackers, we will define the fingerprint first. The fingerprint is some secret information is used to let DSIC distinguish the difference between hackers and SAs.

Cost Analysis in IDSIC

The damage cost (DCost) should be divided into two parts; hackers' and SAs' damage cost.

- The term HDCost(*e*) means the damage cost caused by hackers that may harm to the systems.
- The cost of SAs, SDCost(*e*), is the amount of security testing cost that may damage to the systems.
- The HDCost is much greater than SDCcost since SAs do not want to harm to the system, but hackers do.
- Similarly, the response cost (RCost) will also be separated into two parts: the cost of response generated by hackers (HRCost) and the one created by SAs (SRCost).

- The HRCost will be similar with SRCost since hackers and SAs use the same tools.

False Negative (FN_{IC})

$$FN_{IC} = HDCost(e) + \varepsilon_2 SDCost(e), 0 \le \varepsilon_2 \le 1$$

False Positive (FP_{IC})

$$FP_{IC} = \begin{cases} RCost(e') & \text{if } DCost(e') \ge RCost(e') \\ 0 & \text{if } DCost(e') < RCost(e') \end{cases}$$

$$Cumulative\,Cost(E) = \sum_{e \in E} (ICCost(e) + OpCost(e))$$

- *OpCost*(*e*) is similar in TIDS and IDSIC
- *CCost*(*e*) in TIDS is greater than *ICCost*(*e*) in IDSIC
- IDSIC could have smaller *CumulativeCost*(*E*) than TIDS.

The purpose of the cost-benefit analysis is to periodically review the effectiveness of planned and implemented security controls to determine if they are doing what they are supposed to do, rather than creating additional vulnerabilities. It is used to support the management and control actions.

Conclusion

The research objectives of this paper were quantitative and qualitative analysis of the security risks in a distributed network environment, creation of a cost model, and determination of the cost-benefit tradeoff of a network intrusion detection system.
We propose a new model, IDSIC, based on the auditing point of view and propose the new requirements in IDSIC.
We prove the *CumulativeCost* in TIDS does not reach to minimal cost under the roles of SA exists.

References

[1] R. Summers, Secure Computing, McGraw-Hill, 1997.

[2] C.Pfeleeger, security computing, Prentice-Hall, Inc, 1997.

[3] Cost-Benefit Analysis Guide for NIH IP Project, www.itpolicy.gsa.giv

[4] Dunigan, Hinkel “Intrusion detection and intrusion prevention on a large network, a case study”, 1999.

[5] Lee, Miller, et al. “Toward cost sensitive modeling for intrusion detection”

[6] Proctor, “The Practical Intrusion Detection Handbook”, 2001

[7] Richards, Network Based Intrusion Detection: a review of technologies, 1999

[8] Tites et.al. Information systems Security , 1993

[9] Hummer et.al. “A Cooperative, Collaborative Intrusion Detection System”.

[10] Lunt, A survey of intrusion detection techniques, 1993.