Title:
Everything You Always Wanted To Know About Intrusion Detection Systems

Word Count:
601

Summary:

An Intrusion Detection System (IDS) employs a combination of hardware and software products to analyze network traffic. The software analyzes and checks known patterns of traffic and ferrets out activity it suspects as malicious. A sophisticated IDS can even automatically terminate a connection and send an alert to the admin the minute it detects suspicious activity.

An IDS is employed mainly by companies to detect various malicious types of behavior, primarily through the...

Keywords:
GoToMyPC, GoToMeeting

Article Body:
An Intrusion Detection System (IDS) employs a combination of hardware and software products to analyze network traffic. The software analyzes and checks known patterns of traffic and ferrets out activity it suspects as malicious. A sophisticated IDS can even automatically terminate a connection and send an alert to the admin the minute it detects suspicious activity.

An IDS is employed mainly by companies to detect various malicious types of behavior, primarily through the Internet, that can place their networked computers at grave risk. It detects any kind of attack on network systems or on software, as well as unofficial and unauthorized logins and access to critical documents.

Intrusion detection schemes fall into one of the following categories: Anomaly IDS – these systems look for behavior and traffic that is not regular. Misuse IDS – these scout for Internet behavior that matches a known attack scenario the characteristics of which are already stored in the IDS; these are compared with real-time system behavior.

There is another type of IDS called network-based intrusion detection system (NIDS). These systems monitor packets of data on the network and scout for malicious activity. Such a system can monitor several computers on a network at one time, and this sets them apart from other types of IDS, which can usually monitor only one computer at a time.

So, Who's Trying to Break Into The Company's Network?

You will be surprised to learn that a company's computers are more at risk from its employees than from outside hackers! Corporate America thrives in an extremely competitive environment, and competitors will pay top Dollar if they can lay their hands on critical data. Also, employees are job-hopping all the time or setting up their own ventures, so if they can get their hands on valuable data free of charge, it will do them a lot of good - and the company a lot of harm.

How Do Intruders Attack the System?

The easiest method of breaking into a system by an insider is to gain physical access to a system. In companies, it is very difficult to stop employees from gaining access to a computer system located anywhere in the office.

Also, the employee wanting to break into a system may already be computer-savvy and may know how to hack into systems. All he has to do is employ the usual tricks of the hacking trade to gain access into any system on the office network.

Finally, sophisticated hackers who are operating from a remote location can also break into a company's network. Such remote hacking methods are tough to detect and complex to fight.

How Do I get An IDS?

Developers affiliated with the open-source movement have built a few IDSs that are available free of cost. Here are their details:

AIDE (Advanced Intrusion Detection Environment) is a free replacement for Tripwire - a semi-free IDS. AIDE is an efficient IDS and new as well as old users of Tripwire must try it out.

File System Saint (FSS) is another open-source IDS that is available for download at http://insecure.dk/. FSS too works like Tripwire - it is lightweight, is developed in Perl language, and works on any platform that runs Perl.

Snort is yet another open-source IDS that started off small but has matured considerably. It detects intrusions into a network based on rules, combining benefits of signature, protocol and anomaly-based inspection methods. You can get snort here: http://www.snort.org/

Commercial IDS

If you want Commercial Intrusion Detection Systems, then you must consider Tripwire or Polycenter Security Intrusion Detector - both these IDSs have garnered a formidable reputation in the market.