Subject: Detecting Intruders on Your System Is Fun and Easy
Posted by medusha.hanura on Tue, 11 Dec 2007 14:14:34 GMT
View Forum Message <> Reply to Message

Detecting Intruders on Your System Is Fun and Easy

Well, perhaps the title of this chapter is a slightly misleading. Supposedly, becoming an intruder is fun and easy, too. If you want to detect intruders, you should know what type of system resources can be depended on for providing evidence. Should you want to become an intruder, you ought to know how commercial IDSs look for traces of your activity.

Scanners are designed to take a look at your system and to let you know whether you have configuration problems or holes that can be used for attacks. If your system was previously set up in a secure fashion, and an intruder has altered this configuration, a scanner will detect this change (when you run the scan) and notify you of the problem.

System-level intrusion detection tools differ from scanners in a couple of ways. If the IDS runs in real time, it can let you know the instant a compromise has occurred. Also, if the monitor gathers its data by reading an activity stream on the system, it can detect a range of features that a single scanner cannot. For example, scanners will not tell you that someone just entered three bad passwords and exceeded the failed login threshold.

By the time you finish this chapter, you will understand the following:

* How to classify attacks according to how they originate and the threat they pose
* The pros and cons of different data sources that a system monitor can use for decisions
* What system monitors can and cannot detect
* The tradeoffs you may need to make for monitoring your systems in real time
* What it takes to really track someone through a network

As you will soon see, you need to consider a number of issues when trying to build a system-level IDS.

You can see the complate articles at http://www.network.79br.com