Mini Project Proposal
Security - Intrusion Detection Systems

Laurent De Wilde
Master of Science in the Applied Computer Science
Vrije Universiteit Brussel

October 31, 2014

Abstract

An Intrusion Detection System or IDS is an automated system for detecting unauthorized access to a computer network. It is a type of security management system for computers and networks. Unauthorized access includes infringement of confidentiality, integrity or availability of information. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Some intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

One can state an IDS is an essential part of a computer network. However, many system administrators tend not to trust intrusion detection systems because they believe this type of software is not very effective. Also, some overpriced intrusion detection solutions are marketed as "the perfect solution to all your problems", while in fact they do not contribute to the security of a computer network.
But one may not forget that the main cause of malfunctioning / failing of intrusion detection software is probably the lack of configuring the software.

That's why I'm so intrigued about this topic: I would like to prove that, if the software is configured properly, an IDS actually does help to improve security of computers and computer networks. Also, since I have a Linux server myself at home, this topic is of great use for myself as well.

Project planning

As soon as my proposal is approved, I would like to start right away by defining and explaining what an Intrusion Detection System actually is. Next, I will compare some of the available solutions and pick one (the best) of those. These two things are part of the theoretical considerations. It should take no longer than a week to complete this part.

After that, for the practical part (the installing and configuring of the software), I will first of all create a virtual network for testing purposes. It will consist of a Linux server running the intrusion detection software and a Windows client to configure the server using SSH and, eventually, testing if the configuration was done properly.

This whole configuring and testing process should take up about six to seven weeks. So when this period is finished, we will be the end of december. By then, I can concentrate on other courses.

Of course, it is difficult to predict exactly what I will do each week, but the above schedule should give a general impression of what I'm planned to do in the coming eight weeks.