Chapter 16
Innovative Approach for Improving Intrusion Detection Using Genetic Algorithm with Layered Approach

Aditi Nema
BIRT, India

ABSTRACT

The detection portion of Intrusion Detection System is the most complicated. The IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. In this paper the reduced the features and perform layered architecture for identify various attack (DoS, R2L, U2R, Probe) and show accuracy using SVM with genetic approach.

INTRODUCTION

Intrusion detection systems are the 'burglar alarms' (or rather 'intrusion alarms') of the computer security field. The aim is to defend a system by using a combination of an alarm that sounds whenever the site's security has been compromised, and an entity—most often a site security officer (SSO)—that can respond to the alarm and take the appropriate action, for instance by ousting the intruder, calling on the proper external authorities, and so on. This method should be contrasted with those that aim to strengthen the perimeter surrounding the computer system. We believe that both of these methods should be used, along with others, to increase the chances of mounting a successful defence, relying on the age-old principle of defence in depth.

It should be noted that the intrusion can be one of a number of different types. For example, a user might steal a password and hence the means by which to prove his identity to the computer. We call

DOI: 10.4018/978-1-5225-9866-4.ch016

such a user a masquerader, and the detection of such intruders is an important problem for the field. Other important classes of intruders are people who are legitimate users of the system but who abuse their privileges, and people who use pre-packed exploit scripts, often found on the Internet, to attack the system through a network. This is by no means an exhaustive list, and the classification of threats to computer installations is an active area of research.

Early in the research into such systems two major principles known as anomaly detection and signature detection were arrived at, the former relying on flagging all behavior that is abnormal for an entity, the latter flagging behavior that is close to some previously defined pattern signature of a known intrusion. The problems with the first approach rest in the fact that it does not necessarily detect undesirable behavior, and that the false alarm rates can be high. The problems with the latter approach include its reliance on a well defined security policy, which may be absent, and its inability to detect intrusions that have not yet been made known to the intrusion detection system. It should be noted that to try to bring more stringency to these terms, we use them in a slightly different fashion than previous researchers in the field.

An intrusion detection system consists of an audit data collection agent that collects information about the system being observed. This data is then either stored or processed directly by the detector proper, the output of which is presented to the SSO, who then can take further action, normally beginning with further investigation into the causes of the alarm.

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. As network attacks have increased in number and severity over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. Although firewalls have traditionally been seen, as the “first line of defense” against would be attackers, intrusion detection software is rapidly gaining ground as a novel but effective approach to making your networks more secure. Intrusion detection operates on the principle that any attempt to penetrate your systems can be detected and the operator alerted - rather than actually stopping them. This is based on the assumption that it is virtually impossible to close every potential security; intrusion detection takes a very “real world” viewpoint, emphasizing instead the need to identify attempts at breaking in and to assess the damage they have caused.

Intrusion detection involves determining that some entity, an intruder, has attempted to gain, or worse, has gained unauthorized access to the system.

Intruders are classified into two groups:

- External intruders do not have any authorized access to the system they attack.
- Internal intruders have at least some authorized access to the system. Internal intruders are further subdivided into the following three categories.

Masqueraders are external intruders who have succeeded in gaining access to the system and are acting as an authorized entity.

Legitimate intruders have access to both the system and the data but misuse this access (misfeasors).

Clandestine intruders have or have obtained supervisory (root) control of the system and as such can either operate below the level of auditing or can use the privileges to avoid being audited by stopping, modifying, or erasing the audit records [Anderson80]