1 Introduction

Intrusion Detection Systems (IDS) have been around for the last 20 years both in public domain and proprietary. But, still the use of IDS is not that popular in industry. This is not due to lack of systems that capture malicious events, but due to the very nature of incidents that a typical IDS look for. IDS look for incidents in a discrete way but attacks happen within a span of hours, days and years. Many a time, the discrete incidents that an IDS look for are part of normal user activity as well, which lead to false positives and massive alert logs. So there is a need for a system which works on the discrete events that an IDS reports and correlate them and present alerts that belong to a single attack/session/activity together.

2 Problems with the current IDSs

- IDS generates lakhs of alerts per day (in a network like cc@iith)
- Lot of false positives
- Lot of trivial alerts due to the discrete nature of IDS signatures

3 What is needed

A system that
- that correlates the alerts generated by the IDS
- aggregates similar alerts and present them together

4 What we propose to do

- Install SNORT, a public domain IDS in our network (KReSIT or CC)
- Understand the Rules used and Alerts generated by the Signature Based Detection module of SNORT
• Understand/Survey and simulate some attack approaches
• Discretize the attack in terms of the actual network packets that make an attack realize
• Classify the rules based on their similarity in the phase of attack in which such a rule gets matched
• Classify alerts into the categories created by the above classification
• Using Sequential Pattern Mining algorithms, try to correlate alerts/alert-groups

References

