

Network Intrusion Detection by Pattern Recognition (PR)

Ayesha Akter

Brac University,CSE Dept

ayesha.akter2@g.bracu.ac.bd

SHIHAB SHARAR

Brac University,CSE Dept

shihab.sharar@g.bracu.ac.bd

Annajiat Alim Rasel

Brac University,Sr. Lecturer,CSE Dept

annajiat@bracu.ac.bd

September 22, 2021

Abstract

Attacks on Internet service providers take advantage of both known and unknown flaws or faults in system and application software, as well as complicated, unexpected interconnections between software components and network protocols. One of the security fields is network intrusion detection. Intrusion is one of the most important hazards to any data organization, hence PR system applications aid in intrusion detection by recognizing intrusion trends over time. This ensures that security systems will sound an alarm if even the tiniest patterns of intrusion appear on the network. In order to find an attack pattern within network traffic, Intrusion Detection System (IDS) use pattern recognition techniques. This system is based on the cidf architecture. Recognizing that string matching is the bottleneck, our system has enhanced detection engine performance by using an improved approach based on the present Boyer-Moore algorithm. There are numerous studies that use either the kdd-cup 99 or the darpa 1999 datasets to validate the creation of the idss that will be used in this work.

Keywords -Intrusion Detection System, Attack Detection, Boyer Moore Algorithm.