MODELING AND ALERTING OF NETWORK ATTACKS BASED ON NETWORK TRAFFIC FLOW PATTERN OBSERVATION

K.Pratheepan

Postgraduate Institute of Science, University of Peradeniya, Peradeniya, Sri Lanka

Vavuniya Campus of the University of Jaffna, Vavuniya, Sri Lanka

Infrastructure based networks are often prone to heavy attacks by intruders and hackers. There have been few successful and many un-success attacks on networks all over the world carried out by intruders and hackers on popular and other networks to crash networks and related services. Network security has become an important issue for all computer networks because of the continuous attempts of attacks on such networks. One recent trend in network security attacks is the increased number of indirect attacks, which influence network traffic negatively, instead of directly entering a system and damaging it.

In this research work, we analyze network attack traffic flow pattern, compare the attack traffic flow patterns of two proxy servers to model and predict network attack traffic flow pattern. For the development of the model to predict network attack patterns, we collect data for a longer period of time, analyze it for statistical properties. From the measured statistical properties our system monitors network access activities and when it observes activities that have the similar statistical properties then it will alert the network manager.

We find that most of the network attack attempts were less than 200 and only few numbers of attacks were more than 200. When an attack pattern is observed our system automatically notifies the IP address of the machine, from which the access is originating, to the network administrator and the administrator could take necessary action to prevent such attacks.

Keywords:

Intrusion Detection System, Firewall, Traffic flow, Pattern observation.