A Rule based Http Anomaly Classifier

Abstract

Ever since the inception of internet network security has been the prime important area of research for computer scientists. Network security using Honeypot presents a system that pretends to have one or more network vulnerabilities that a blackhat is looking for. Actually it does not have those vulnerabilities; it does so just to deceive the intruder by stealthily monitoring the network. Honeypots are emerging technology and have got lot of attention of late. In this research work, our system uses the advantages of Honeypot for implementing an intrusion detection system. There are two major part of our research work. First is data accumulator and second is data analyzer. For data accumulation, we have used honeypot. We have also used open source tool Honeyd which is available free of cost. Honeyd is a powerful tool which can simulate even complex networks very easily. Second part is data analyzer which analyzes data captured by the Honeyd. This part of the system is basically a java based Intrusion detection system which can work along honeyd system. This is a basic pattern based IDS which uses snort rule base to detect intrusion. It is a feature rich data analyzer which can detect intrusion. Function of the system is quite simple it reads the data logged by the honeypot system and looks for intrusion pattern of rule base into the packets. This analyzer can work in both offline and online mode; in online mode it reads data directly from the network interface card while in offline mode it reads data from binary files (tcpdump) which also gives it an
advantage that it can analyze data from other resources as well.

References

- Niels Provos, "Honeyd: A Virtual Honeypot Daemon", Center for Information Technology Integration University of Michigan.

Index Terms

Computer Science

Web Services

Keywords

Honeypot  Data Capturing Engine  Data Accumulator