Abstract

An intrusion detection system is a computer-based information system designed to collect information about malicious activities in a set of targeted IT resources, analyze the information, and respond according to a predefined security policy. The most common computer intrusion detection systems detect signatures of known attacks by searching for attack-specific keywords in network traffic. Intrusion-detection systems aim at detecting attacks against computer systems and networks or in general, against information systems. This strategy is mainly focus on to detect intrusion in multitier web applications. Multitier web application include two ends that is front end as well as back end of the applications. The front end include web server which can responsible to run the application and gives that output to back end i. e. file server. This strategy is useful to identify the intrusion at both front end and back end of web application.

References

- "Common Vulnerabilities and Exposures," http://www.cve.mitre.org,
Using Container Architecture to Detect Intrusion for Multitier Web Application

2011.

Index Terms

Computer Science Security

Keywords

Intrusion Detection System Multitier Architecture Pattern Mapping