World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:04, 2017

Analysis and Design Modeling for Next Generation Network Intrusion Detection and Prevention System

Authors : Nareshkumar Harale, B. B. Meshram

Abstract : The continued exponential growth of successful cyber intrusions against today's businesses has made it abundantly clear that traditional perimeter security measures are no longer adequate and effective. We evolved the network trust architecture from trust-untrust to Zero-Trust, With Zero Trust, essential security capabilities are deployed in a way that provides policy enforcement and protection for all users, devices, applications, data resources, and the communications traffic between them, regardless of their location. Information exchange over the Internet, in spite of inclusion of advanced security controls, is always under innovative, inventive and prone to cyberattacks. TCP/IP protocol stack, the adapted standard for communication over network, suffers from inherent design vulnerabilities such as communication and session management protocols, routing protocols and security protocols are the major cause of major attacks. With the explosion of cyber security threats, such as viruses, worms, rootkits, malwares, Denial of Service attacks, accomplishing efficient and effective intrusion detection and prevention is become crucial and challenging too. In this paper, we propose a design and analysis model for next generation network intrusion detection and protection system as part of layered security strategy. The proposed system design provides intrusion detection for wide range of attacks with layered architecture and framework. The proposed network intrusion classification framework deals with cyberattacks on standard TCP/IP protocol, routing protocols and security protocols. It thereby forms the basis for detection of attack classes and applies signature based matching for known cyberattacks and data mining based machine learning approaches for unknown cyberattacks. Our proposed implemented software can effectively detect attacks even when malicious connections are hidden within normal events. The unsupervised learning algorithm applied to network audit data trails results in unknown intrusion detection. Association rule mining algorithms generate new rules from collected audit trail data resulting in increased intrusion prevention though integrated firewall systems. Intrusion response mechanisms can be initiated in real-time thereby minimizing the impact of network intrusions. Finally, we have shown that our approach can be validated and how the analysis results can be used for detecting and protection from the new network anomalies.

Keywords : network intrusion detection, network intrusion prevention, association rule mining, system analysis and design
Conference Title : ICCCNS 2017 : International Conference on Computer Communications and Networks Security
Conference Location : Zurich, Switzerland
Conference Dates : April 20-21, 2017