Abstract

Neural networks are artificial learning systems. For more than two decades, they have help for detecting hostile behaviors in a computer system. This review describes those systems and theirs limits. It defines and gives neural networks characteristics. It also itemizes neural networks which are used in intrusion detection systems. The state of the art on IDS made from neural networks is reviewed. In this paper, we also make a taxonomy and a comparison of neural networks intrusion detection systems. We end this review with a set of remarks and future works that can be done in order to improve the systems that have been presented. This work is the result of a meticulous scan of the literature.

References
2. Ludovic Me, « Méthodes et outils de la détection d'intrusions », Supelec.
3. Guillaume Hiet, « Détection d'instructions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d'informations au sein du système d'exploitation et des applications: mise en œuvre sous Linux pour les programmes java » Université de Rennes, Decembre 2008
5. Nicoleta Minoiu « comparaison entre l'analyse logic et probit et les réseaux de neurones »
6. G. DREYFUS “les réseaux de neurones” Mécanique Industriel et Matériaux, n51, septembre 1998
19. Iftikhar Ahmad & all “Performance Comparison between Backpropagation Algorithms Applied to Intrusion Detection in Computer Network Systems” WSEAS International
Conference on NEURAL NETWORKS, Sofia, Bulgaria, May 2-4, 2008
20. Iftikhar Ahmad && all “Application of Artificial Neural Networks in Detection of Probing Attacks” 2009 IEEE Symposium on Industrial Electronics and Applications(ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia

Index Terms

Computer Science

Networks

Keywords

Intrusion detecting system, NIDS, neural network, MLP