JINCE 2013
VIII JORNADA DE INICIAÇÃO CIENTÍFICA DO IF SERTÃO-PE
II JORNADA DE TRABALHOS DE EXTENSÃO
Local: Salgueiro/PE

MINERAÇÃO DE DADOS APLICADA A AUDITORIA DE SEGURANÇA EM REDES

Francisco de Assis de Lima Gama[1]; Mayla Raianna da Silva Moraes[2]; Gilvaneide Francisca Gomes [3]

[1] Bolsista PIBICJr - IF SERTÃO - PE, estudante do curso Técnico em Informática - IF SERTÃO - PE
[2] Mestrando em Ciência da Computação – Cin - UFPE, Orientador PIBICJr Docente no Curso Técnico em Informática – IF SERTÃO - PE
[3] Bolsista PIBIT - IF SERTÃO -PE, estudante de graduação do curso Gestão em Tecnologia da Informação - IF SERTÃO - PE

RESUMO

Ao tratar de redes de computadores é inevitável não pensar nas possíveis vulnerabilidades que estas podem apresentar em relação aos seus pilares básicos, no que diz respeito aos dados e informações que nelas percorrem, que são: a disponibilidade, integridade e privacidade dos dados. É imprescindível que haja uma forma de tentar garantir a auditoria da segurança nas redes de forma eficaz para que esses princípios sejam mantidos sob quaisquer circunstâncias, mantendo a rede livre de intrusões e ataques cibernéticos. A metodologia abrange um processo de descoberta de conhecimento em banco de dados, de forma a produzir conhecimento (informações relevantes) a partir de etapas de seleção, pré-processamento, utilizando para isso algoritmos de detecção de anomalias no tráfego dos dados, automatizando a análise dos alertas gerado pelo NIDS (Sistemas de Detecção de Intrusão) e a construção de um classificador que é a rede Neural Artificial Multilayer Perceptron (Múltiplas Camadas de Neurônio) que será "treinada" para minerar (filtrar) os dados importantes, permitindo saber quais as máquinas que possuem comportamentos incomuns dentro de uma rede, tornando mais rápida à possibilidade de uma intervenção e resolução do problema. O estudo possibilitou observar na pratica como os classificadores e suas combinações funcionam para automatizar a Auditoria de Segurança em Redes, apontando computadores suspeitos a estarem infectados. Os desvios padrões obtidos nos 30 experimentos mostraram que mesmo os classificadores que tiveram desempenho ruim, tem comportamento estável, possibilitando que a aplicação gere alertas ao auditor.

Palavras-chave: redes, computadores, dados.