MINERAÇÃO DE DADOS APLICADA À SEGURANÇA DE SISTEMAS COMPUTACIONAIS

André Carrilho da Costa (Acadêmico)
Sibelius Lellis Vieira (Orientador)

A constante evolução e popularização da internet são fatores importantes na disseminação da informação manipulada pelos computadores, tendo trazido várias vantagens para o mundo atual, mas paralelamente a esta evolução foi observado o aumento nas formas de ataques às redes e crimes que utilizam este meio de comunicação. Uma das formas de tornar este meio de comunicação mais seguro é a utilização de ferramentas que podem gerar logs (registro de atividades e aplicaçoes) presentes em um sistema e através deste dados coletados pode-se obter conclusoes sobre eventos ocorridos e descobrir possíveis erros ou até mesmo descobrir vestígios de ataques ou intrusoes. Com a utilização de técnicas de data-mining (mineração de dados) aplicadas sobre logs coletados é possível obter estatísticas e padroes de ataques. Estes dados devidamente tratados e analisados podem fornecer aos gerentes do sistema meios de prover melhor segurança, identificando os potenciais problemas do sistema em análise e atuando diretamente na solução destes problemas.

Palavras-Chaves: 1) segurança; 2) mineração de dados; 3) firewall; 4) resposta ativa

Apoio: BIC/PROPE/PUC Goiás