393 **OTIMIZAÇÃO DE UMA FERRAMENTA BASEADA NA ANÁLISE DE LOGS PARA CLASSIFICAÇÃO, CARACTERIZAÇÃO E CORRELAÇÃO DE EVENTOS.** *Fabiane Cristine Dillenburg, Luciano Paschoal Gaspary (orient.)* (UNISINOS).

O maior contato das organizações com a Internet evidenciou a necessidade destas protegerem suas informações de ataques. Uma medida de proteção adotada é o *firewall*, caracterizado como uma barreira de segurança entre duas redes; sua função é bloquear o tráfego não autorizado oriundo de uma rede a outra; todo e qualquer pacote que entra ou sai é inspecionado, podendo ser aceito ou rejeitado, conforme regras de segurança estabelecidas. Os *firewalls* armazenam todas as tentativas de conexão em um arquivo denominado *log*. Para a gerência de segurança este *log* é rico em informações, pois permite: mensurar e identificar os acessos à rede privada e à externa; acompanhar historicamente o volume de acessos e as aplicações utilizadas; depurar problemas de configuração de regras de filtragem e, sobretudo, reconhecer seqüências de eventos suspeitas que indiquem estratégias utilizadas por invasores para tentar obter acesso indevido a estações e serviços. Apesar da importância desses indicadores, o crescimento da quantidade e da complexidade das informações transitadas diariamente entre as redes torna inviável o controle manual dos arquivos de *log*. Ferramentas foram desenvolvidas objetivando auditar esses *logs*, mas a maioria não permite relacionar eventos e gerar visões históricas. Para solucionar esse problema, nosso grupo de pesquisa desenvolveu uma ferramenta que classifica, caracteriza, armazena históricos, correlaciona e visualiza os eventos do *log* de forma amigável. Entretanto, dado o volume de dados manipulados, o protótipo apresenta limitações quanto ao seu desempenho na exibição da grande quantidade de informações ao usuário, dificultando sua utilização. O presente trabalho compreendeu a identificação e a solução de gargalos existentes na ferramenta. Assim, foram feitas alterações nas estruturas de dados e na manipulação dessas, permitindo a utilização da ferramenta como apoio ao gerente de segurança.