

Repositório
Digital
da UFPE

Buscar no repositório



>> Busca avançada

[Home](#) [Navegar](#) [Sobre](#) [Ajuda](#) [Contato](#) [Idioma](#) [0](#)[Entrar](#)

RI UFPE / Teses e Dissertações / Teses e Dissertações defendidas na UFPE / Programa de Pós-Graduação em Ciência da Computação / Dissertações de Mestrado - Ciência da Computação

Use este identificador para citar ou linkar para este item: <https://repositorio.ufpe.br/handle/123456789/27515>

Compartilhe esta página


Título: Log de Eventos: aplicação de um modelo de análise de logs para auditoria de registro de eventos**Autor(es):** SILVA, Luiz Hamilton Roberto da**Palavras-chave:** Ciência da computação; Auditoria de logs**Data do documento:** 14-Jul-2017**Editor:** Universidade Federal de Pernambuco

Abstract: A análise do registro de eventos – conhecido como logs – em equipamentos e sistemas computacionais é útil para a identificação de atacantes, para delinear o modo de ataque e, também, para identificar quais são as falhas que foram exploradas. Há alguns trabalhos e pesquisas que demonstram a vantagem para uma política de segurança da informação em manter os logs de comunicação em redes e sistemas computacionais, focando nas trilhas para auditoria, que é um conjunto de ações onde se inclui: a coleta, o armazenamento e o tratamento dos logs de equipamentos, de aplicações e de sistemas operacionais, dentro de um sistema de computação. A auditoria de eventos atua na coleta de elementos que possam individualizar comportamentos perigosos de usuários, internos ou externos, ou eventos de sistema que possam vir a comprometer o uso aceitável dos recursos computacionais ou a quebra da triade da segurança da informação: a confidencialidade, a integridade e a disponibilidade. Percebe-se que, dentro do modelo de política de segurança adotado nos centros de operação (datacenters) dos Institutos Federais de Educação, em sua imensa maioria, não utilizam o recurso de servidor de logs, ou tão somente atêm-se ao registro de eventos em seus sistemas e hosts, de forma individual e, sem o contexto da centralização e do tratamento dos registros dos eventos. A coleta dos logs, na modalidade loghost centralizado guarda, em um único repositório, os registros de eventos de diversos sistemas, equipamentos e serviços de rede, o que possibilitará uma análise do montante de logs adquiridos e a possibilidade de gerar trilhas de comportamento de usuários, além de permitir o cruzamento de informações conexas à autenticação de usuários. O recurso que permite a comunicação entre as aplicações, os sistemas operacionais e os equipamentos de rede, informando os eventos a serem registrados é o protocolo Syslog (system log), que é um padrão criado pela IETF para a transmissão de mensagens de log em redes IP. O objetivo maior deste trabalho é estabelecer um modelo para a análise e auditoria de logs, com o fim de identificar ações de usuários em uma rede com servidor de autenticação, aplicando a extração de informações úteis para o Gerenciamento da Segurança, elemento este levado a execução via o uso de scripts no formato PS1 (Windows PowerShell), atuando sobre os arquivos de logs dos Eventos de Segurança (Security.evtx) e gerando relatórios dos eventos relativos ao serviço de autenticação (Active Directory). Ressaltando que as funções implementadas pelos scripts não são disponibilizadas nativamente pelos sistemas Windows e, que o ferramental desenvolvido é de grande valor às atividades diárias do Administrador de Redes, concluindo-se que esta pesquisa apresenta um modelo de análise de logs para auditoria de registro de eventos.

URI: <https://repositorio.ufpe.br/handle/123456789/27515>**Aparece nas coleções:** Dissertações de Mestrado - Ciência da Computação

Arquivos associados a este item:

Arquivo	Descrição	Tamanho	Formato
DISSERTAÇÃO Luiz Hamilton Roberto da Silva.pdf		3,07 MB	Adobe PDF

[Visualizar/Abriu](#)

Este arquivo é protegido por direitos autorais

[Ver licença](#)[Mostrar registro completo do item](#)[Recomendar este item](#)[Visualizar estatísticas](#)Este item está licenciada sob uma [Licença Creative Commons](#)

ATTENA - Repositório Digital da UFPE

(81) 2126-8089

attena@ufpe.br

Compartilhe esta página