Título:	DETECÇÃO DE ATAQUES DE FORÇA BRUTA POR MEIO DA ANÁLISE AUTOMATIZADA DE *LOGS* DE AUTENTICAÇÃO		
Autores:	Kaue Müller Prof. Me. Ivan Luis Suptitz		
Área	[ ] Humanas [ ] Sociais Aplicadas [ ] Biológicas e da Saúde [X] Exatas, da Terra e Engenharias	Dimensão:	[X] Ensino [ ] Pesquisa [ ] Extensão [ ] Inovação

Resumo:

A ampliação do uso de serviços digitais e a conexão contínua de sistemas à internet aumentam a exposição a tentativas indevidas de acesso, entre as quais se destacam os ataques de força bruta, caracterizados pela realização repetitiva de tentativas de autenticação com o objetivo de obter credenciais válidas. Nesse contexto, os logs de autenticação constituem uma fonte relevante para o monitoramento de eventos de segurança, pois registram informações sobre tentativas de acesso, falhas e autenticações bem-sucedidas. Este trabalho tem como objetivo desenvolver uma solução computacional para analisar automaticamente logs de autenticação e identificar padrões associados a tentativas de força bruta e acessos não autorizados, utilizando critérios de análise e técnicas de aprendizado de máquina para auxiliar na identificação de comportamentos anômalos. A pesquisa é de natureza aplicada e, quanto aos objetivos, exploratória, combinando a análise qualitativa dos eventos de autenticação com indicadores quantitativos de validação. Para o desenvolvimento da solução, será utilizada como fonte de dados a base pública Comprehensive, Multi-Source Cyber-Security Events, disponibilizada pelo Los Alamos National Laboratory (LANL), com foco nos registros de autenticação. A metodologia contempla o estudo de conceitos relacionados à Segurança da Informação, autenticação, ataques de força bruta, análise de logs e detecção de intrusão, seguido da seleção e preparação dos dados, definição de critérios de detecção, modelagem da solução, investigação de técnicas de aprendizado de máquina para detecção de anomalias, implementação do protótipo e realização de testes e validação. Como vivência e resultado da etapa de desenvolvimento da pesquisa, destaca-se a realização de levantamento bibliográfico e de bibliometria quantitativa nas bases Scopus, IEEE Xplore e SciELO Brasil, permitindo delimitar o tema e identificar trabalhos relacionados à análise de logs de autenticação, detecção de ataques e uso de aprendizado de máquina em segurança. A bibliometria também evidenciou que, embora os termos relacionados à segurança da informação e à detecção de ataques apresentem ampla ocorrência, a combinação específica de registros de autenticação e detecção de ataques possui menor quantidade de publicações, reforçando a especificidade do recorte adotado. A proposta também estabeleceu a base LANL como fonte para a etapa experimental e definiu os procedimentos necessários para a construção e avaliação da solução. Espera-se, com o desenvolvimento da presente solução,

contribuir para a identificação automatizada de comportamentos suspeitos em eventos de autenticação, combinando critérios previamente definidos com uma abordagem de detecção de anomalias baseada em aprendizado de máquina. Como reflexão, a pesquisa busca demonstrar o potencial da análise automatizada de registros de autenticação como apoio às atividades de monitoramento e investigação de incidentes de segurança, contribuindo para a identificação mais ágil de possíveis tentativas de força bruta e acessos não autorizados.

Link do Vídeo:
https://drive.google.com/file/d/1GotWIX1WMyogoQl7_o1v8G1nJAWn2bP3/view?usp=sharing