CENTRO PAULA SOUZA GOVERNO DO ESTADO DE SÃO PAULO

Professor:	**Disciplina:**
Aluno:	**Número:**
Data:	**Conceito:**

Auditoria de Logs de Acesso e Detecção de Ataque de Força Bruta

Fundamentos de Auditoria de Softwares

Análise de Logs e Detecção de Ataque de Força Bruta

Para acessar os Scripts e logs:

https://github.com/RRZamboni/FAS2025

O objetivo é simular o papel de um auditor de segurança, utilizando a análise de logs para identificar, documentar e propor ações de mitigação contra um Ataque de Força Bruta.

O trabalho consiste em duas etapas:

1. Execução do Script: Rodar o código de análise de logs para gerar o relatório simulado.
2. Análise Crítica: Responder às perguntas-chave de auditoria baseadas nos dados do relatório.

1: Geração e Análise do Relatório - DataSet

1. Geração do Relatório:

- Execute o script fornecido em alguma IDE do JAVA e garanta que o relatório de saída seja gerado com sucesso. Ou use o Arquivo relatório.log
- Anexe a cópia do relatório gerado ao envio final do seu trabalho.

2. Análise Estatística e de Origem:

Com base no Relatório gerado, responda com cálculos e referências ao relatório:

1. Taxa de Falhas e Gravidade: Calcule a proporção percentual de eventos ERROR em relação ao Total de linhas no log. O que este número sugere sobre o ambiente?

Fórmula: Total de linhasTotal ERROR×100%

2. Identificação da Ameaça Principal: Qual usuário apresenta o maior número de falhas e qual evidência específica (nome do usuário, IP ou dado da rajada simulada) confirma o ataque de Força Bruta contra ele?

3. Análise de Origem: Qual endereço IP está associado ao maior volume total de atividades (tentativas INFO e falhas ERROR)? Qual a relação provável entre este IP e o alvo principal?

3. Ações de Auditoria e Contramedidas:

1. Ação Imediata do Auditor: Proponha a ação imediata e urgente a ser tomada para conter o incidente com base nos dados do usuário mais visado e do IP de origem. Justifique sua escolha com base no princípio de contenção de risco.

2. Recomendação de Segurança (Controle Preventivo): Qual controle de segurança (*além do simples bloqueio de IP*) deve ser implementado no sistema para mitigar futuros ataques de Força Bruta que visam múltiplas contas em um curto espaço de tempo?

2: Redação do Relatório Conclusivo de Auditoria

Escreva uma breve conclusão comtemplando os tópicos abaixo:

1. Introdução e Objetivo

- Apresente o contexto (Auditoria de Logs de Acesso) e o objetivo do relatório (Identificação e Análise de Ataque de Força Bruta).
- Mencione os dados analisados (o log e suas estatísticas gerais: Total de linhas e a % de ERROR calculada).

2. Análise de Risco e o Papel do Log

- Descreva o Risco/Impacto que o ataque representa para o sistema e os usuários (ex: sequestro de conta, perda de dados).
- Enfatize a importância do Log como Prova e Ferramenta de Rastreabilidade para a auditoria.

4. Recomendações e Plano de Ação – Conclusão

- Plano de Contenção Imediato: Reafirme a ação urgente proposta (bloqueio de IP/conta).

- Controles Preventivos, Mecanismos, Antiforça, Bruta, Monitoramento.