Curso: Bacharelado em Sistemas de Informação
Período: 6º
Dupla: Paulo Prado e Sara Luiz de Farias
Disciplina: Segurança da Informação

Análise e Mitigação de Vulnerabilidades em Ambiente de Laboratório Acadêmico

Novembro - 2025

SUMÁRIO

1. Introdução

A segurança da informação é um pilar fundamental para instituições educacionais, onde dados sensíveis de alunos, professores e pesquisa são processados diariamente. O incidente ocorrido no laboratório de informática da universidade, envolvendo um acesso não autorizado via protocolo SSH e subsequente manipulação de recursos institucionais, destaca vulnerabilidades críticas em ambientes acadêmicos. Esse evento não apenas expôs falhas técnicas, mas também implicações éticas, legais e organizacionais, reforçando a necessidade de uma abordagem holística para mitigar riscos cibernéticos.

Este trabalho, desenvolvido como parte da disciplina de Segurança da Informação, adota uma perspectiva consultiva em segurança, atuando como uma equipe especializada para diagnosticar o incidente e propor soluções robustas. O objetivo principal é analisar o cenário fornecido, explorar vulnerabilidades adicionais (como redes não segmentadas, permissões excessivas, falta de rastreabilidade, pontos de rede expostos e engenharia social via pretexting) e demonstrar ataques simulados, seguidos de técnicas de hardening para fortalecimento dos sistemas.

O relatório está estruturado em seções claras: análise de vulnerabilidades e vetores de ataque, análise forense digital e resposta a incidentes, avaliação de riscos e impactos, além de propostas práticas de políticas e conscientização. A demonstração em sala incluirá simulações éticas em máquinas virtuais isoladas, assegurando conformidade com princípios éticos e legais. Ao final, o trabalho contribui para a cultura de segurança institucional, reduzindo a probabilidade de recorrências e promovendo responsabilidade coletiva.

2. Análise de Vulnerabilidades e Vetores de Ataque

2.1 Identificação de Vulnerabilidades

Foram identificadas as seguintes vulnerabilidades no ambiente:

- Redes não segmentadas: todos os computadores visíveis entre si;
- Níveis de permissões excessivas: acesso generalizado ao comando sudo su;
- Falta de rastreabilidade: uso de contas compartilhadas;
- Pontos de rede expostos: dispositivos não autorizados facilmente conectados.
- Ataques de engenharia social (pretexting): exploração de confiança e obtenção de credenciais.

2.2 Análise dos vetores de ataque

- Engenharia social: Observação de senha via shoulder surfing;
- Acesso remoto não autorizado: Conexão SSH com credenciais roubadas;
- Manipulação: Uso de privilégios para alterar arquivos (ex.: dados institucionais);
- Vetores adicionais: Escaneamento de rede (Nmap), exploração de permissões (sudo), pretexting para credenciais.

3. Análise Forense e resposta a incidentes

A Análise Forense Digital é um processo sistemático para investigar incidentes de segurança, coletando, preservando e analisando evidências digitais de forma que sejam

admissíveis em contextos legais (ex.: tribunais ou auditorias). A Resposta a Incidentes envolve ações imediatas para conter o dano, mitigar riscos e aprender com o evento. No contexto do incidente no laboratório (acesso não autorizado via SSH e manipulação de dados), essa análise é crucial para identificar culpados, restaurar sistemas e prevenir recorrências.

3.2 Cadeia de custódia

A cadeia de custódia garante a integridade das evidências digitais, provando que não foram alteradas, perdidas ou contaminadas desde a coleta até a apresentação. É essencial para evidências serem aceitas judicialmente, evitando alegações de manipulação. No incidente SSH, isso inclui discos rígidos, logs e capturas de rede.

- Metodologia: Preparação (identificar evidências), Coleta (cópias bit-a-bit), Preservação (armazenamento seguro com hashes), Análise (em ambiente isolado), Apresentação (relatórios assinados).
- Importância: Protege evidências de contaminação; permite reversão de danos.
- Passos no Cenário: Isolar sistema, usar dd para imagem (**sudo dd if=/dev/sda of=image.dd bs=4M**), calcular hash (**sha256sum image.dd**), documentar (data/hora/responsável).
- Ferramentas: dd, FTK Imager, shasum.

3.3 Análise de logs

Logs são registros de eventos do sistema, cruciais para reconstruir o incidente (ex.: quem acessou, quando e como). No caso SSH, analisam-se logs de autenticação, rede e sistema para identificar vetores como brute-force ou engenharia social.

- Logs Cruciais: **/var/log/auth.log (logins SSH)**, **/var/log/syslog (atividades)**, logs de firewall (conexões bloqueadas).
- Comandos para Extração: **grep "sshd" /var/log/auth.log** (filtra SSH); **journalctl --since "2023-10-15"** (horários); **awk** para IPs.
- Ferramentas: Wireshark (tcpdump -w capture.pcap), Autopsy.
- Limitações: Logs podem ser deletados

3.3 Análise de riscos e impactos

- Impacto no Negócio (Instituição):
    - Reputação: Perda de confiança de alunos/pais. Custos: Reparo de sistemas, reestruturação (novas políticas, treinamento).
        - Riscos legais: Violações de LGPD (dados pessoais expostos).
- Impacto Humano:
    - Professor: Quebra de privacidade (dados pessoais manipulados), estresse psicológico, exposição pública.
        - Consequências: Ansiedade, perda de credibilidade.

4. Proposta de políticas e conscientização

Uma Política de Uso Aceitável (PUA) é um conjunto de regras que estabelece como os recursos de uma organização, como computadores, redes e a internet, podem ser usados de forma legal, segura e apropriada. Ela define atividades permitidas e proibidas, protege os ativos da empresa, previne violações de segurança e minimiza riscos legais e de reputação.

4.1 Estrutura da PUA

- Introdução: Objetivo da política (proteger dados institucionais, garantir conformidade com leis como LGPD e evitar riscos de segurança).
- Escopo: Aplica-se a todos os laboratórios de informática, equipamentos (PCs, servidores, redes) e dados (acadêmicos, pessoais).
- Regras detalhadas:
    - **Acesso a Sistemas:** Acesso autorizado apenas com credenciais pessoais (proibidas contas compartilhadas). Uso obrigatório de autenticação de dois fatores (2FA) para logins remotos (ex.: SSH, VPN).
        - Proibido o compartilhamento de senhas ou o uso de dispositivos não autorizados (ex.: pendrives externos sem aprovação).
    - **Uso de Privilégios de Administrador**: Privilégios de administrador (sudo, root) só para usuários autorizados e com justificativa (ex.: manutenção). Logs obrigatórios para todas as ações administrativas.
        - Proibido o uso excessivo ou compartilhado de privilégios; violações resultam em revogação imediata.
    - **Responsabilidade sobre os Dados:** Usuários são responsáveis por proteger dados pessoais e institucionais (ex.: não armazenar senhas em texto plano). Relatar incidentes imediatamente ao departamento de TI.
        - Proibido o acesso não autorizado a dados de terceiros (ex.: arquivos de alunos/professores). Backup regular obrigatório, com criptografia.
    - Outras Regras: Redes segmentadas (VLANs para isolamento); monitoramento contínuo (logs e alertas)
        - Proibição de engenharia social ou pretexting.
        - Penalidades: Advertência, suspensão ou ação legal.

5. Plano de treinamento de Segurança da Informação para servidores e estudantes

O plano de treinamento visa conscientizar e capacitar usuários, reduzindo riscos humanos (ex.: engenharia social). Deve ser anual, com módulos online (plataforma como Moodle) e presenciais. Avaliação: Quiz final com 80% de acerto mínimo. Duração: 4 horas por grupo.

5.1 Estrutura do plano

- **Objetivos Gerais:** Reduzir incidentes em 50% nos primeiros 6 meses; promover cultura de segurança.
- **Público-Alvo:** Servidores (administrativos), Professores e Alunos.

- **Metodologia:** Módulos interativos (vídeos, quizzes), cenários reais (baseados no incidente SSH), certificação ao final.

5.2 Módulos específicos

- Para Professores (Foco: Proteção de Dados, Senhas e Identificação de Ameaças)

Módulo 1: Proteção de dados (1 hora)	**Módulo 2: Senhas Seguras (1 hora)**	**Módulo 3: Identificação de Ameaças (2 horas)**
Conceitos de LGPD, criptografia. Cenário: Como proteger dados pessoais em PCs de laboratório.	Criação de senhas fortes (mín. 12 caracteres, com símbolos), uso de gerenciadores (ex.: LastPass). Cenário: Evitar senhas previsíveis como no incidente SSH.	Reconhecer phishing, engenharia social, vetores como SSH mal configurado. Cenário: Simulação de ataque pretexting (fingir ser aluno pedindo senha).

- Para alunos (Foco: Ética Digital, Consequências de Ciberataques e Boas Práticas)

Módulo 1: Ética Digital (1 hora)	**Módulo 2: Consequências de Ciberataques (1 hora)**	**Módulo 3: Boas Práticas (2 horas)**
Princípios éticos (não compartilhar credenciais, respeitar privacidade). Cenário: Impacto de acessar dados de professores sem permissão.	Exemplos reais (ex.: vazamento de dados, multas LGPD de R$ 50 milhões). Cenário: Como um ataque SSH pode levar a exposição pública e danos à carreira.	Uso seguro de redes (evitar Wi-Fi públicas), reconhecimento de pretexting, responsabilidade em laboratórios (não conectar dispositivos não autorizados). Cenário: Simulação de hardening pessoal.

- Cronograma: Outubro (treinamento), Novembro (avaliação);
- Avaliação: quizzes interativos;
- Métricas de Sucesso: Taxa de participação (90%), redução de incidentes reportados;
- Certificação ao final.

6. Recursos e Validação Prática

Para validar as vulnerabilidades analisadas (SSH mal configurado, redes não segmentadas, permissões excessivas, falta de rastreabilidade, pontos expostos e engenharia social), acesse o repositório GitHub com códigos e scripts de simulação:

https://github.com/PauloMAPrado/trabalhofinalSegurancaInformacao.git

- -Execute em VMs Ubuntu isoladas (rede interna);
- Siga o README.md para hardening e testes éticos.