Trabalho Prático 2

Disciplima: Segurança e Auditoria em Sistemas

Professor: Erinaldo da Silva Pereira

Tema: Ataques a Sistemas Computacionais

Introdução

Este trabalho prático tem como objetivo demonstrar, de forma controlada e educativa, técnicas comuns de ataques a sistemas computacionais, bem como estratégias de auditoria e resposta a incidentes. Os roteiros propostos possibilitam a simulação de cenários reais em ambientes laboratoriais seguros, permitindo a compreensão aprofundada das vulnerabilidades e defesas.

As práticas seguem uma progressão lógica: reconhecimento, ataque, coleta de credenciais, exploração, captura de tráfego e auditoria pós-invasão. O foco está na análise técnica, aplicação de ferramentas amplamente utilizadas no mercado e na construção de uma mentalidade crítica de defesa.

Etapas do Trabalho

Pesquisa Teórica e Planejamento

- Grupos devem estudar **ao menos três tipos de ataque** reais, ocorridos nos últimos anos (fontes confiáveis).
- Apresentar um **plano de simulação segura** em ambiente virtual.
- Levantamento das ferramentas e alvos utilizados.

Montagem do Ambiente Virtual

- Criar rede virtualizada (com VirtualBox, VMWare, GNS3 ou Docker).
- Configurar máquinas com Linux/Windows simulando cliente, servidor e firewall.

Execução das Simulações

- Realizar **simulações controladas** de ataques escolhidos.
- Registrar todos os passos, saídas e logs.

Detecção, Auditoria e Resposta

- Utilizar ferramentas de monitoramento e auditoria para:
    - Detectar comportamentos anômalos.
    - Coletar evidências (capturas, logs, indicadores de comprometimento).
    - Avaliar tempo de resposta e eficácia das defesas.
    - Simular política de resposta a incidentes.

Relatório Técnico e Apresentação

- O relatório deve conter:
    - Introdução e fundamentação teórica.
    - Metodologia e arquitetura do ambiente.
    - Descrição detalhada dos ataques simulados.
    - Logs e capturas de tela com análise técnica.
    - Estratégias de detecção e auditoria.
    - Propostas de mitigação e melhoria de segurança.
    - Discussão crítica e referências.
- Apresentação final com defesa do trabalho e demonstração das simulações.

Requisitos e Cuidados Éticos

- Todo experimento deve ocorrer em ambiente isolado (laboratório local ou VMs).
- É proibido simular ataques fora do escopo autorizado.
- Utilizar conhecimento apenas para fins educacionais e profissionais.
- Aplicar conceitos de **ética em segurança da informação**.

Critérios de Avaliação

Critério	Peso
Embasamento teórico e plano de simulação	15%
Execução técnica das simulações	20%
Qualidade da auditoria e análise forense	25%
Relevância e profundidade do relatório técnico	25%
Apresentação oral e domínio do conteúdo	15%

Roteiros Técnicos

Roteiro Técnico 1: Ataque de Força Bruta com Hydra
Simulação de tentativa de acesso a um serviço SSH utilizando força bruta com a ferramenta Hydra.

Roteiro Técnico 2: Exploração de Vulnerabilidade em Aplicação Web (DVWA)
Identificação e exploração de falhas comuns em aplicações web como SQL Injection e XSS na plataforma DVWA.

Roteiro Técnico 3: Escaneamento de Portas e Evasão de Firewall com Nmap
Reconhecimento de serviços em uma rede e simulação de evasão de mecanismos de segurança utilizando o Nmap.

Roteiro Técnico 4: Phishing Local com SET (Social Engineering Toolkit)
Captura de credenciais através de site falso criado com o SET, simulando ataques de engenharia social.

Roteiro Técnico 5: Sniffing de Tráfego com Wireshark
Análise de tráfego em rede local e identificação de dados sensíveis transmitidos sem criptografia.

Modelo de Relatório por Roteiro

1. Título do Experimento
2. Objetivo
3. Ferramentas e Ambiente Utilizado
4. Etapas Realizadas
5. Evidências (capturas de tela, logs, etc.)
6. Análise Crítica
7. Medidas de Mitigação
8. Conclusão

Data de Entrega e Apresentação

Deverá ser enviado um vídeo juntamente com o relatório explicando o desenvolvimento do roteiro escolhido. Grupos de no máximo 6 alunos.

O trabalho deverá ser entregue via moodle no dia 25/06/2025.

Referências

- DVWA - Damn Vulnerable Web Application: https://dvwa.co.uk
- OWASP Top 10: https://owasp.org/www-project-top-ten/
- Nmap: https://nmap.org/
- Hydra: https://github.com/vanhauser-thc/thc-hydra
- Social Engineering Toolkit (SET): https://github.com/trustedsec/social-engineer-toolkit
- Wireshark: https://www.wireshark.org/