Projeto Integrado de Segurança Cibernética

Tema do Projeto: Simulação de Cenários de Ataque e Defesa em Ambiente Controlado

Objetivo Geral: Proporcionar aos alunos uma experiência prática de planejamento, execução e mitigação de ataques cibernéticos em um ambiente controlado, utilizando ferramentas de código aberto disponíveis nas distribuições Debian e Kali Linux.

Cenários Envolvidos:

- **Atacante:** Equipe responsável por identificar e explorar vulnerabilidades em sistemas e redes simuladas.
- **Defesa:** Equipe encarregada de proteger os sistemas contra possíveis ataques, implementando medidas de segurança e monitoramento.
- **Cliente:** Representa a entidade que possui os aplicações e dados a serem protegidos, fornecendo requisitos e expectativas de segurança.

Ferramentas Sugeridas:

- **Pentest e Invasão:**
  - ✓ **Metasploit Framework:** Plataforma para desenvolvimento e execução de exploits contra máquinas remotas.
  - ✓ **Nmap:** Ferramenta para varredura de redes e descoberta de hosts e serviços.
  - ✓ **Aircrack-ng:** Conjunto de ferramentas para avaliar a segurança de redes sem fio.
- **Proteção:**
  - ✓ **Snort:** Sistema de detecção e prevenção de intrusões em rede.
  - ✓ **iptables:** Ferramenta de filtragem de pacotes e firewall para Linux.
  - ✓ **Fail2ban:** Programa que analisa logs e impede tentativas de intrusão bloqueando endereços IP suspeitos.
- **Documentação:**
  - ✓ **Dradis:** Plataforma de colaboração para relatórios de segurança.
  - ✓ **CherryTree:** Aplicativo de anotações hierárquicas para organização de informações.
  - ✓ **LaTeX:** Sistema de preparação de documentos para criação de relatórios técnicos e científicos.

Aplicações Vulneráveis no Ambiente do Cliente:

Para enriquecer o projeto, serão instaladas no servidor do Cliente as seguintes aplicações vulneráveis:

- **Damn Vulnerable Web Application (DVWA):** Aplicação web intencionalmente vulnerável para prática de testes de penetração.
- **bWAPP:** Aplicação web com diversas vulnerabilidades, projetada para ajudar no aprendizado de segurança web.
- **Ambientes do VulnHub:** Plataforma que fornece máquinas virtuais vulneráveis para prática de segurança cibernética. Link: https://blog.solyd.com.br/hackeavel-passo-a-passo-do-vulnhub/

Cronograma de Entregas:

1. **12/03/2025:** Formação das equipes e definição dos papéis (Atacante, Defesa, Cliente).
2. **19/03/2025:** Entrega do plano de projeto, incluindo objetivos específicos, metodologia e cronograma detalhado.
3. **26/03/2025:** Configuração do ambiente de teste e instalação das aplicações vulneráveis no servidor do Cliente.
4. **02/04/2025:** Entrega do relatório de análise de vulnerabilidades identificadas pela equipe Atacante.
5. **09/04/2025:** Entrega do plano de mitigação e defesa elaborado pela equipe Defesa.
6. **16/04/2025:** Execução dos testes de invasão e defesa no ambiente controlado.
7. **23/04/2025:** Entrega do relatório de incidentes e respostas aplicadas durante os testes.
8. **30/04/2025:** Revisão e aprimoramento das estratégias de ataque e defesa com base nos resultados obtidos.
9. **07/05/2025:** Simulação final integrando todos os componentes do projeto.
10. **14/05/2025:** Preparação da apresentação final e do relatório conclusivo.
11. **21/05/2025:** Apresentação dos resultados e discussão das lições aprendidas.

Desenvolvimento do Trabalho:

- **Preparação do Ambiente:**
  - ✓ **Cliente:** Configurar um servidor Debian ou Kali Linux e instalar as aplicações vulneráveis (DVWA e bWAPP).
  - ✓ **Atacante:** Preparar ferramentas de teste de penetração para identificar e explorar vulnerabilidades nas aplicações do Cliente.
  - ✓ **Defesa:** Implementar medidas de segurança para proteger o servidor do Cliente contra possíveis ataques.
- **Execução das Atividades:**
  - ✓ **Equipe Atacante:** Utilizar ferramentas como Nmap e Metasploit para identificar e explorar vulnerabilidades nas aplicações do Cliente.

- ✓ **Equipe Defesa:** Monitorar atividades suspeitas e aplicar medidas de mitigação para proteger o servidor do Cliente.
- ✓ **Equipe Cliente:** Fornecer requisitos de segurança e avaliar as medidas de proteção implementadas.

- **Documentação:** Registrar todas as etapas do projeto, incluindo configurações, procedimentos executados, resultados obtidos e análises realizadas.
- **Apresentação Final:** Cada equipe apresentará seus resultados, desafios enfrentados, soluções implementadas e lições aprendidas, acompanhados de um relatório conclusivo detalhando todo o processo.

Instalação das Aplicações Vulneráveis:

- **DVWA:**
  - → Clone o repositório oficial do DVWA: git clone https://github.com/digininja/DVWA.git
  - → Instale as dependências necessárias: sudo apt install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php
  - → Configure o banco de dados e ajuste as permissões conforme as instruções do repositório.
- **bWAPP:**
  - → **Baixar o bWAPP:** github.com
    - Acesse o site oficial do bWAPP e faça o download da versão mais recente.
  - → **Preparar o Ambiente:**
    - Atualize o sistema:
    - sudo apt-get update -y
    - Instale o Apache e o MySQL: sudo apt install apache2 mysql-server php php-mysqli php-gd libapache2-mod-php