Relatório Técnico - Pentest Simulado em DVWA

Informações do Projeto

Autor: Seu Nome
Data: 16/04/2025
Ambiente: Lab Virtual
Alvo: DVWA
Objetivo: Simular exploração de vulnerabilidades web

1. Reconhecimento

IP do alvo: 192.168.0.100
Scanner de portas: nmap -sV -p- 192.168.0.100
Serviços encontrados:
- HTTP 80 (Apache)
- MySQL 3306

2. Enumeração

- Fuzzing de diretórios com dirb
- Login padrão testado com sucesso: admin:password
- Vulnerabilidade detectada: SQL Injection

3. Exploração

Ferramenta: sqlmap
Comando:
sqlmap -u "http://192.168.0.100/login.php" --data="user=admin&pass=123" --dump
Dump de tabela 'users' com 5 registros

4. Pós-Exploração

- Acesso à conta administrativa
- Coleta de informações sensíveis (simulado)
- Verificação de logs de auditoria

5. Recomendações

- Implementar validação de entrada (Prepared Statements)
- Atualizar DVWA para versão mais recente
- Restringir acesso ao banco de dados

6. Sumário Executivo

Um teste de invasão controlado foi conduzido no ambiente DVWA com o objetivo de identificar vulnerabilidade