Universidade de Brasília – UnB

Departamento de Ciência da Computação - CIC

Disciplina: Tópicos Avançados em Segurança Computacional – 2025/1

Professora: Lorena Borges

Trabalho Prático 02

Detecção de SQL Injection em Ambiente Web Simulado

Objetivo Geral

Desenvolver e implementar um ambiente web vulnerável para realização de simulação de um ataque ou exploração de vulnerabilidade com a técnica de SQL Injection. Deverão ser criadas ferramentas de monitoramento integrado como firewall, sistema de detecção de intrusão, scripts e análises de logs para detecção e resposta a esse tipo de ataque.

Etapas do Projeto

1. **Montagem de Ambiente Virtual Vulnerável**

   Deverá ser criado um ambiente de infraestrutura virtual, isolado, no formato de laboratório, para implantação e execução de testes, com os seguintes recursos mínimos:

   - Implantação e configuração de um ambiente web: website simples com persistência em um servidor de Banco de Dados: NGinx ou Apache, MySQL/MariaDB e PHP.
   - Definição da ferramenta de ataque: escolher um script/toolkit pronto (sqlmap, Burp Suite Community, OWASP ZAP) ou desenvolver próprio.
   - Configuração de um firewall local e de perímetro: iptables ou UFW, PFSense ou Firewall Cloud (ex.: AWS Security Groups).
   - Implantação de um IDS/IPS baseado em assinatura: Snort ou Suricata.
   - Criação de scripts de monitoramento local nos servidores para detecção de anomalias.
   - Coleta, análise e correlação de logs com ferramentas SIEM-like como: Wazuh, ELK ou Splunk.

2. **Resposta a Incidentes e Relatórios**

- Deverá ser simulada uma ação de ataque ou exploração com SQLInjection, demonstrando as etapas de ataque e os resultados bem-sucedidos.
- O projeto deverá conter as detecções realizadas pelas ferramentas e configurações de segurança e respectivas análises dos eventos.
- Deverão ser realizados processos de mitigações que sejam eficientes no bloqueio do ataque simulado.
- Documentação de um processo de resposta a incidentes para a técnica de SQL Injection utilizada. O relatório detalhado deverá constar:
    - Topologia do ambiente.
    - Descrição das ferramentas utilizadas.
    - Scripts desenvolvidos (código comentado).
    - Capturas de tela dos ataques, das detecções e mitigações.
    - Logs dos incidentes.
    - Análise dos eventos.

Orientações:

- O trabalho poderá ser feito em dupla;
- Deverá ser entregue relatório em .pdf, bem formatado (padrão acadêmico);
- A escolha das ferramentas de segurança, plataformas, SO e ambiente virtual de infraestrutura ficará a critério dos grupos (este roteiro contém apenas sugestões);
- Linguagens de programação, web sites e scripts também serão escolhidos de acordo com o propósito de cada grupo;
- As ferramentas utilizadas deverão ser gratuitas e open source;
- O foco principal da avaliação deste trabalho será na identificação de vulnerabilidades e ações de mitigação.