Insper

Roteiro 1 – App Reconhecimento do Alvo

Professor Rodolfo Avelino

Objetivo: Desenvolver um aplicativo (CLI ou GUI) que reúna os principais scripts utilizados na fase de reconhecimento de alvo, incluindo o PortScan desenvolvido anteriormente. O aplicativo deve ser modular, permitindo a integração de novas ferramentas futuramente.

Entrega: 28/04/2025

Objetivos de Aprendizagem

- Aprofundar o conhecimento sobre as técnicas de reconhecimento em pentests
- Desenvolver habilidades de programação para integração de ferramentas
- Compreender os diferentes tipos de informações relevantes na fase de reconhecimento
- Implementar boas práticas de desenvolvimento de ferramentas de segurança

Pré-requisitos

- Conhecimento de metodologias de pentest (visto no roteiro anterior)
- Portscan desenvolvido no roteiro 1

Insper

Tarefas e Requisitos

1. Pesquisa e Definição de Ferramentas

Antes de desenvolver, responda às seguintes perguntas (não use IA, apenas fontes técnicas e sua experiência):

Perguntas de Pesquisa:

1. Além do PortScan, quais são as 5 ferramentas mais úteis para reconhecimento em um pentest?
    - Justifique cada escolha com base em casos reais (ex: Shodan para IoT, theHarvester para e-mails).
2. Qual a diferença entre um scanner de portas SYN e um TCP Connect Scan?
    - Explique em qual cenário cada um é mais eficiente.
3. Como um pentester pode evitar ser detectado por sistemas de prevenção de intrusão (IPS) durante o reconhecimento?
    - Liste técnicas e como elas impactam a eficácia do scan.

Insper

2. Desenvolvimento do Aplicativo

O aplicativo deve conter:

- Módulo de PortScan (já desenvolvido no Roteiro 1, mas deve ser integrado).
- Pelo menos mais 4 ferramentas de reconhecimento (ex: WHOIS lookup, DNS enumeration, subdomain scanner, wafw00f, nikto, scan de vulnerabilidades (pode usar o nmap para este), wappalyzer (cli), dirsearch, masscan, sslyze,..).
- Interface amigável (CLI com menus ou GUI simples).
- Documentação básica (como executar e dependências).

Exemplo de fluxo

```
Bem-vindo ao ReconApp!
1. Portscan
2. DNS Lookup
3. Enumeração de Subdomínios
4. Sair
Escolha uma opção:
```

Insper

3. Entrega

Sua entrega final deve incluir:

1. Código-fonte completo do aplicativo (github)
2. Documentação técnica e manual do usuário (entregue no black board junto com os itens a seguir)
3. Relatório contendo:
    - Respostas às questões de pesquisa propostas
    - Descrição da arquitetura e decisões de design
    - Análise das ferramentas integradas
    - Resultado dos testes realizados

Insper

4. Critérios de Avaliação

A avaliação será dividida em três níveis de notas:

1. **Nota 5-6 (Básico)** :
    - O aplicativo funciona parcialmente, mas apresenta bugs ou erros significativos.
    - Apenas o portscan foi implementado corretamente.
    - As respostas às perguntas são superficiais ou incompletas.
    - Falta modularidade e organização no código.
2. **Nota 7-8 (Intermediário)** :
    - O aplicativo funciona bem, com pelo menos duas ferramentas adicionais além do portscan.
    - As respostas às perguntas demonstram compreensão dos conceitos, mas podem carecer de profundidade.
    - A interface é funcional, mas pode ser melhorada.
    - O código é organizado, mas ainda há espaço para otimizações.
3. **Nota 9-10 (Avançado)** :
    - O aplicativo é completo, funcional e robusto, com todas as ferramentas solicitadas implementadas.
    - As respostas às perguntas são detalhadas, demonstrando análise crítica e conhecimento profundo.
    - A interface é intuitiva e os resultados são apresentados de forma clara e organizada.
    - O código é modular, limpo e bem documentado, facilitando futuras melhorias.