Atividade Prática: Introdução à Segurança da Informação

Objetivo

Aplicar na prática os conceitos de:

- **Princípios da Segurança da Informação (CID – Confidencialidade, Integridade, Disponibilidade)**
- **Ciclo de Vida da Informação**
- **Identificação de Vulnerabilidades e Ameaças**
- **Utilização de Ferramentas de Segurança: Nmap e Nikto**
- **Reconhecimento e Exploração Controlada de Vulnerabilidades**
- **Avaliação da Confidencialidade, Integridade e Disponibilidade**

Cronograma

- **Início da atividade:** 19h40
- **Finalização:** 21h30

Ferramentas utilizadas

- **Nmap** – Mapeamento de portas e serviços vulneráveis.
- **Nikto** – Scanner de vulnerabilidades em servidores web.

Atividade Prática

Fase 1: Levantamento e Reconhecimento (19h40 às 20h00)

- Realizar um mapeamento completo de uma máquina-alvo fornecida em laboratório ou simulada via VM.
- Utilizar o **Nmap** para:
    - Detectar portas abertas;
    - Identificar sistemas operacionais (se possível);
    - Listar serviços rodando e suas versões.

Comandos sugeridos:

bash
CopiarEditar
nmap -sV -O -A <IP-alvo>

Entregáveis:

- Print ou relatório da varredura do Nmap.

- Análise inicial: identificar possíveis vulnerabilidades ligadas aos serviços detectados.

Fase 2: Análise de Vulnerabilidades Web (20h00 às 20h40)

- Utilizar o **Nikto** para escanear o servidor web detectado no Nmap (caso exista serviço HTTP).
- Identificar vulnerabilidades web básicas:
    - Cabeçalhos inseguros;
    - Páginas administrativas expostas;
    - Falta de SSL/TLS ou configurações incorretas;
    - Scripts vulneráveis conhecidos.

Comando sugerido:

bash
CopiarEditar
nikto -h http://<IP-alvo>

Entregáveis:

- Relatório de vulnerabilidades do Nikto (captura de tela ou relatório salvo).
- Descrição de **2 vulnerabilidades** identificadas no scan.

Fase 3: Análise de Ameaças e Aplicação dos Princípios de Segurança (20h40 às 21h10)

- Com base nos serviços e vulnerabilidades encontrados:
    - Classificar os riscos quanto à **Confidencialidade**, **Integridade** e **Disponibilidade**;
    - Associar as ameaças a possíveis vulnerabilidades exploráveis;
    - Explicar qual **controle** seria aplicável (exemplo: firewall, atualização de sistema, senhas fortes, criptografia).

Entregáveis:

- Matriz de ameaças × vulnerabilidades × princípios do CID afetados.

Fase 4: Relatório de Segurança (21h10 às 21h30)

- Montar um relatório resumido contendo:
    - Mapa de rede detectado;
    - Vulnerabilidades detectadas;
    - Correlações com os princípios de segurança (CID);
    - Propostas de medidas de segurança para correção dos problemas.

Modelo de Relatório:

1. Introdução
2. Resultados do Nmap
3. Resultados do Nikto
4. Vulnerabilidades encontradas
5. Relação com CID (Confidencialidade, Integridade, Disponibilidade)
6. Controles sugeridos
7. Conclusão

Observações Importantes

- Esta atividade simula um **Pentest Ético**.
- As análises e varreduras devem ser realizadas **somente** no ambiente autorizado.
- Aplicação de **Boas Práticas de Segurança** discutidas em aula (como criptografia, backup, controle de acesso).
- Lembre-se: **toda descoberta de vulnerabilidade deve ser seguida de uma proposta de mitigação**, conforme aprendido no estudo da ISO/IEC 27001 e 27002.