Atividade Prática – Projeto de Análise de Vulnerabilidades em Redes Wi-Fi

Disciplina: Segurança Cibernética
Formato: Dupla
Ferramentas sugeridas:

- aircrack-ng
- airodump-ng
- aireplay-ng
- nmap
- Wireshark
- reaver (opcional)
- wpscan (caso o roteador tenha painel web)

Objetivo

O aluno deverá executar todas as etapas de um projeto prático para detectar e documentar vulnerabilidades em redes Wi-Fi. O projeto deverá incluir análise técnica, execução prática e proposição de mitigação. Os alunos aplicarão conhecimentos de mapeamento de redes, análise de riscos, tipos de ataques (DoS, força bruta, spoofing, etc.) e aplicação de boas práticas de segurança.

Estrutura da Atividade

Etapa 1: Planejamento (em sala)

Tópicos trabalhados:

- Avaliação do ambiente de teste autorizado (rede laboratorial ou roteador vulnerável preparado pelo professor)
- Identificação dos ativos da rede: BSSID, ESSID, tipo de criptografia, canal, nível de sinal

Ferramenta recomendada:

- airodump-ng com placa em modo monitor

Etapa 2: Mapeamento e Coleta

Objetivo: Executar mapeamento de rede com coleta passiva e identificação de alvos com potenciais vulnerabilidades.
Itens a coletar:

- SSID, BSSID, canal, tipo de segurança (WEP/WPA/WPA2)

- Verificar redes com WPS habilitado
- Estações conectadas (clientes)

Ferramentas:

- airodump-ng, wash, nmap (para host scan de possíveis clientes)

Etapa 3: Teste prático

Ações possíveis:
Escolher 1 ou 2 abordagens abaixo com autorização do professor:

- Captura de handshake WPA/WPA2
    - airodump-ng + aireplay-ng + aircrack-ng
- Ataque DoS de desautenticação (testar proteção IEEE 802.11w)
    - aireplay-ng -0
- Tentativa de força bruta via aircrack-ng com wordlist reduzida
- Ataque WPS PIN brute-force (se autorizado e com WPS ativado)
    - reaver

Etapa 4: Documentação e Relatório

Itens obrigatórios no relatório:

1. **Descrição da rede analisada:** tipo de criptografia, vulnerabilidades observadas
2. **Metodologia aplicada:** fases seguidas, ferramentas utilizadas
3. **Capturas e evidências:** prints ou logs dos comandos
4. **Resultado da análise:** se houve obtenção de handshakes, sucesso/falha em ataques
5. **Recomendações de segurança:** desativar WPS, uso de WPA3, filtragem de MAC, ocultação de SSID, atualização de firmware
6. **Referência à CID (Confidencialidade, Integridade, Disponibilidade):** quais princípios são mais afetados

Entrega

- Entrega do relatório completo em PDF até o próximo encontro.
- O relatório deve conter identificação do aluno/grupo, ambiente de testes, ferramentas usadas, resultados, prints e recomendações.

Observações

- **É proibido realizar testes fora do ambiente autorizado.**
- **O foco da atividade é educacional e ético.**

- Os testes deverão ser conduzidos com placas compatíveis com modo monitor e injeção de pacotes.