Segurança
Experimento N°06
Ataques a Rede Wifi

Disciplina	**Segurança em Redes de Computadores**
Professor:	**Rafael Timóteo de Sousa Júnior**
Monitores:	**Valério Martins (valerioaymoremartins@gmail.com)** **Mariana Stieljes**

1. Introdução:

2. Desenvolvimento teórico

2.1. Discuta os algoritmos de WEP (RC4) e WPA (TKIP).

Solicitamos que pelo menos exponha um pseudocódigo ou a explicação teórica do funcionamento de cada um desses.

- WEP: número de bits e vetores de inicialização. Estender o assunto para WEP2.
- WPA: tem que citar que o produto final não tem correlação com o vetor de inicialização.

2.2. Passos de Ataque a redes WIFI usando o aircrack-ng:

a) (airmon-ng) Descubra o SSID e cheirando pacotes e coletando IVs fracos flutuando no ar

Primeiro temos que operacionalizar o *'sniffer'* dos pacotes de comunicações wifi. Isto é uma tarefa simples e totalmente passiva/discreta, pois esse processo "fica" invisível a quem está sendo interceptado.

Um handshaking do IV irá ocorrer principalmente quando da autorização de login de um usuário no SSID de interesse. Discuta o aimon-ng e qual sua principal funcionalidade (obs.: a discussão é colocar em modo monitor - mon0).

b) (airodump-ng) Captura dos pacotes no modo promíscuo.

Assim, é colocado o tráfego do ar em um arquivo .cap e mostra informação das redes.

c) (aircrack-ng). Quebra chaves WEP e WPA (Busca por Força-bruta).

Qual é o elemento do modelo de segurança wifi que é esperado no pacote para realizar o aircrack-ng. Discuta. Se apontar o pseudocódigo seria interessante.

d) Explique o airdecap-ng

Obs. Trata da decrifragem de arquivos capturados com cifragem WEP ou WPA com a chave conhecida.

e) Explique o aireplay-ng

Obs: Injeção de pacotes (Somente em Linux).