



Teste de Invasão em Redes sem Fio



Descrição e objetivos do tutorial:

Passar um sólido conhecimento sobre a tecnologia envolvida, abordando as principais vulnerabilidades e ameaças que afetam a segurança em redes sem fio. Serão apresentadas técnicas e ferramentas utilizadas por atacantes, assim como maneiras de se defender das mesmas.

Público-Alvo:

Profissionais responsáveis por projetar e implementar redes sem fio seguras, assim como avaliar a segurança e mitigar eventuais vulnerabilidades em redes deste tipo.

Mini-currículo do instrutor: Rafael Soares Ferreira

Analista de segurança das empresas **Clavis Segurança da Informação** e **Green Hat Segurança da Informação**, atuando principalmente nas áreas de análise forense computacional, detecção e resposta a incidentes de segurança, testes de invasão e auditorias de redes, aplicações e sistemas. Foi Diretor da equipe de Resposta a Incidentes e Auditorias do Grupo de Resposta a Incidentes de Segurança do DCC/UFRJ até fevereiro de 2009. Já ministrou cursos e palestras relacionadas à Segurança da Informação em diversos eventos, entre eles: EnCSIRTs - Encontro de CSIRTs Acadêmicos, Fórum de Software Livre do Rio de Janeiro, Ultra Maratona How To de Software Livre, FLISOL, SegInfo entre outros. Na Academia Clavis é instrutor dos seguintes cursos: Fundamentos da Segurança Computacional, Segurança em Redes sem fio, Teste de Invasão e Análise Forense Computacional.

Ementa

1. Redes sem fio: Conceitos e Funcionamento

2. Tipos de ameaças

- 2.1. Captura de tráfego
- 2.2. Senha/Configuração padrão
- 2.3. Negação de serviço (DoS)
- 2.4. Configurações inseguras
- 2.5. Vulnerabilidades em protocolos
- 2.6. Equipamentos sem fio em ambientes cabeados



- 2.7. Mapeamento de ambientes
- 2.8. Wardriving

3. Mecanismos de segurança

- 3.1. Endereçamento MAC
- 3.2. Wired Equivalent Privacy (WEP)
- 3.3. Wi-fi Protected Access (WPA)
- 3.4. Autenticação

4. Técnicas e ferramentas de auditoria

- 4.1. Análise do ambiente
- 4.2. Ferramentas
- 4.3. Escuta de tráfego
- 4.4. Endereçamento MAC
- 4.5. Ataques MITM (man-in-the-middle)
- 4.6. Quebra de chaves WEP
- 4.7. Quebra de chave WPA
- 4.8. Negação de serviço (DoS)

Pré-requisitos

Conhecimentos básicos de tcp/ip;
Conhecimentos básicos de sistemas GNU-Linux;