



DHCP Spoofing

Objetivo

Implementar um programa que envia mensagens DHCP para os clientes que solicitam endereços IPv4, para a execução de um ataque do tipo *man-in-the-middle*.

Descrição

Os alunos devem desenvolver um programa em *socket RAW* utilizando o protocolo IPv4 para envio e recepção de pacotes DHCP. **Não serão aceitos trabalhos que apenas instalem e configurem servidores DHCP. É requerida a implementação de um programa capaz de reconhecer as principais mensagens (Discovery e Request) e que seja capaz de enviar mensagens para a configuração dos clientes (Offer e Acknowledgement).** Mensagens do tipo Information e Releasing não precisam ser implementadas.

O ataque, que simula o servidor DHCP, deve identificar os pedidos de endereço dos *hosts* clientes e deve enviar as mensagens necessárias para a configuração do *host*.

O resultado esperado é a execução de um ataque do tipo *man-in-the-middle* através do envio de mensagens DHCP forjadas, de forma a controlar a rota *default* dos *hosts* da rede local e a resolução de endereços no DNS.

O trabalho requer a instalação e configuração de um servidor de DNS para responder as consultas de resolução de nomes. Neste servidor, devem ser configurados alguns endereços de sites conhecidos, mas com endereços IP de outros sites, de forma que o intruso possa controlar a página que o usuário está acessando.

A aplicação deve ter um modo de apresentação na tela das solicitações reconhecidas e respondidas do DHCP e do DNS (no caso de implementação de um programa específico). Além disso, o intruso deve apresentar uma tela que demonstre o controle sobre a roteamento dos pacotes pelo *default gateway* intruso.

Resultados e Entrega

Grupos: até 3 alunos.

Entrega: Upload no Moodle de um arquivo zipado com o nome do(s) aluno(s), contendo:

1. Relatório descrevendo a implementação
2. Código da implementação

Prazo final para entrega: 01/07/2024