# Redes de Computadores II - Trabalho Final

Nicolas Nascimento[1] and Tadeu Marchese[1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul

10 de novembro de 2016

## 1 Introdução

A segurança em redes de computadores é um assunto bastante relevante e é tema de diversas análises. Existem muitas falhas, decorrentes da própria estrutura das redes e os protocolos que operam sobre estas, que podem ser exploradas. A técnica que será implementada aqui é o DCHP Spoofing, onde, através de envio e recebimento de pacotes DHCP, pode-se interceptar pacotes de uma máquina (mas sem prejudicar o tráfego desta).

## 2 Protocolo DHCP

O protocolo DHCP é um protocolo de configuração automática de redes de computadores. Ele possibilita com que uma máquina possa se conectar a uma rede(i.e, obter os diversos parâmetros de um rede, como Gateway Padrão, Mascará de Sub-Rede, etc) de forma independente e sem a necessidade de configuração prévia.

## 3 Funcionamento do Protocolo DHCP

O processo de configuração de uma máquina em uma rede que possui um servidor DCHP funciona através do envio de uma série de pacotes. A seguir são demonstrados os pacotes

- **Discover** - O "host"que deseja se conectar a rede envia este pacote para toda a rede a fim de descobrir se existem servidores DHCP.
- **Offer** - O servidor DHCP envia este pacote em resposta ao Discover, mandando as informações de configuração para a rede local. Este pacote contém, dentre outras coisas, a identificação do servidor.
- **Request** - O "host"envia este pacote de maneira a informar ao servidor DHCP de que ele deve reservar algumas configurações para este "host"

- **Ack** - O servidor DHCP envia este pacote confirmando que as informações solicitadas pelo "host"estão corretas e a configuração finalizou com sucesso.

Abaixo pode-se observar todo o processo através de screenshots do Wireshark, já com o processo de intervenção feito pelo programa desenvolvido acontecendo.

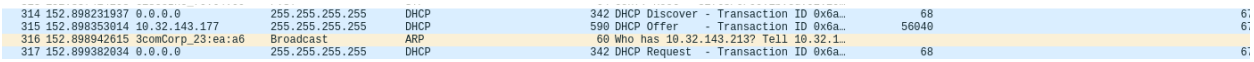


Figura 1 - Sequência de pacotes enviados para a configuração usando DHCP

# 4 Monitoramento do Tráfego HTTP

Esta parte do trabalho objetivava, após a correta implementação da tática de *man-in-the-middle*, obter-se uma lista de endereços que um host visitou. Este processo consistia em obter os pacotes que estivessem sofrendo a interceptação e obter o endereço de navegação e subenderenços e associoar estes a um host. Para esta parte, em específico, obtém-se todos os pacotes HTTP que fossem solicitações do tipo GET e faz-se o *parsing* do texto HTML deste pacotes. Outro aspecto importante desta fatia da implementação era a diferenciação entre os diversos requests que são realizados e fazer-se um acesso. A fim de filtar-se os diversos pacotes, mas ainda assim conseguir manter um registro de navegação, uma metodologia foi seguida. Para os pacotes que o host envia, verifica-se o campo `host` e espera-se pelo pacote de retorno. Com o pacote de retorno em mãos verifica-se o campo `content-type` e, caso este campo conter `html`, salva-se o endereço de navegação, proveniente da primeira linha do comando `GET`.