Pontifícia Universidade Católica do Rio Grande do Sul
Faculdade de Informática
Laboratório de Redes de Computadores

Roteiro – Aula #3

Objetivo

Utilizar *sniffers* de rede para capturar tráfego e identificar a estrutura de pacotes Ethernet, ARP, IP e ICMP.

Descrição

1. Utilizando o *tcpdump* analise o conteúdo de pacotes Ethernet, ARP e IP. Capture o tráfego e identifique os campos que compões o frame de cada protocolo, bem como as informações contidas neles.

2. Usando o comando *ping* e sua opção de variação de TTL, envie pacotes, iniciando o TTL em 1, para uma máquina na sua rede e para uma máquina fora da sua redes local. Aumente o TTL para cada envio de pacote. Monitore o tráfego e verifique quais mensagens são geradas, quais são os endereços de origem e destino destas máquinas, e analise o que este tráfego significa.

3. Usando o comando *ping* varie o tamanho do pacote a ser enviado e monitore o tráfego para analisar as mensagens geradas e as informações de fragmentação contidas no pacote IP.

4. Usando o comando *ping* gere solicitações para:

   a. Uma máquina ativa na sua rede local;
   b. Uma máquina ativa na rede da PUC;
   c. Uma máquina ativa fora da rede da PUC.

   Verifique as informações recebidas e identifique o que ocorre quanto ao tipo de mensagens e seu conteúdo e os tempos de resposta.
   Repita o exercício utilizando máquinas que não estão ativas para as letras (a, b e c).

5. Usando o comando *telnet* verifique o que ocorre quando você envia um pacote para uma porta que não está ativa. Utilize como máquina destino qualquer máquina da sua rede.

6. Usando o Ethereal verifique a ocorrência de ICMP *flooding*. Para gerar o *flooding* utilize o comando *ping* com a opção *–f*.

Resultados e Entrega

Grupos: O exercício deverá ser realizado individualmente.

Entrega: Relatório contendo o resultado dos exercícios.

Data Entrega: 29/04/2006