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

Trabalho de Redes de Computadores e Laboratório de Redes

Objetivo

Este trabalho tem por objetivo geral implementar um "roteador OSPF" intruso para falsificar rotas nas tabelas dos demais roteadores da topologia do Lab Redes, usando as divulgações do OSPF como um roteador normal. Os objetivos específicos são:

- o desenvolvimento de uma aplicação que implemente o protocolo OSPF sobre IPv4;
- a implementação da comunicação entre processos, utilizando *socket RAW* para envio e recebimento de pacotes;
- a manipulação das estruturas de protocolos (informações do *header* dos protocolos e dos dados da aplicação).

Descrição

O protocolo OSPF implementa o algoritmo *link-state*, realizando divulgações sobre os seus enlaces e o custo dos mesmos aos seus vizinhos. As divulgações são feitas por meio de mensagens chamadas de LSA (*Link State Advertisement*). Para que a divulgação ocorra entre os roteadores vizinhos é preciso que sejam estabelecidas as adjacências, isto é, as relações de vizinhança. Isto ocorre pelo envio de mensagens do tipo *Hello*. Cada roteador cria o mapa da topologia da rede, com as informações recebidas dos vizinhos, e aplica o algoritmo do *Djikstra* para cálculo das rotas. O cálculo resultará na identificação de rotas para popular a tabela de roteamento.

O protocolo OSPF é suscetível ao envio de mensagens LSA mascaradas (*spoofed*) e, portanto, sujeito a ataques e alteração indevida da tabela de roteamento.

Assim sendo, este trabalho visa explorar esta vulnerabilidade pela implementação de uma aplicação que simula um roteador OSPF para envio de mensagens com enlaces falsos. Por exemplo, a aplicação deve divulgar aos seus roteadores vizinhos, que o roteador simulado está diretamente conectado a um enlace com um endereço verdadeiro de outra rede da Internet (por exemplo, endereço de uma rede do Google). Assim, o roteador vítima do ataque, deverá divulgar aos seus vizinhos este enlace, de forma que o tráfego gerado nos outros roteadores será encaminhado ao roteador vítima e finalmente ao roteador simulado, que representa um "buraco negro".

O artigo *Persistent OSPF Attacks*, item 4.1, que descreve o ataque, deve ser lido para o entendimento do mesmo, assim como a RFC 2328 (OSPF).

A aplicação a ser desenvolvida deve ter os seguintes módulos:

- Envio de mensagens OSPF: o envio de mensagens do protocolo OSPF para interação com os demais roteadores, seguindo as regras do protocolo para estabelecimento de adjacências, divulgação da base de dados, divulgação de mensagens de atualização, envio de mensagens de reconhecimento e envio da divulgação por *flooding*;

- Recebimento de mensagens OSPF: o recebimento de mensagens do protocolo OSPF, de acordo com as ações geradas, e a execução da devida ação dado o tipo de datagrama recebido.

Quanto ao tipo de *sockets* a ser utilizado na aplicação para a comunicação entre processos, deve-se observar que:

- A comunicação deve ser implementada com *sockets* RAW, para envio e recebimento das mensagens. Neste caso, devem ser preenchidas as informações dos *headers* de nível de enlace, rede e aplicação, ou, no caso do recebimento, lidas e tratadas por nível.

Quanto às funcionalidades da aplicação, devem ser implementadas:

- Envio de mensagens OSPF;
- Recebimento de mensagens OSPF;
- Apresentação dos pacotes de dados recebidos pelo roteador simulado, que foram roteados para o enlace falso.

Quanto ao ambiente para desenvolvimento, teste e apresentação:

- Deve ser criada uma subrede para o seu trabalho, com a estrutura de roteadores Cisco do Lab Redes. Cada grupo será o administrador de um roteador, com a sua subrede isolada;
- No roteador Cisco deve ser configurado o protocolo OSPF;
- O roteador simulado deve estar na subrede isolada;
- O roteador simulado envia as mensagens para o roteador Cisco;
- O roteador Cisco, se houver sucesso no ataque, deverá divulgar para os vizinhos o enlace falso. Para testar esta condição, será necessário utilizar m segundo roteador Cisco;
- Alternativamente, para testes fora do Lab Redes, poderá ser utilizado o GNS3 ou Core.

Resultados e Entrega

Grupos: 3 alunos