Ataque Man-in-the-Middle com ICMPv6 Router Advertisement

Gabriel Vaz de Souza, Márcio Góes e Pedro Fratini Chem

[1]Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul
Porto Alegre – RS – Brasil

{gabriel.vaz, marcio.goes, pedro.chem}@edu.pucrs.br

Resumo. *Este trabalho apresenta a implementação de uma técnica de ataque de redes conhecida como Man-in-the-Middle. O programa foi desenvolvido com a linguagem Python, utilizando "Socket raw", manipulando pacotes do tipo "Router Solicitation"e "Router Advertisement". Sua implementação será comentada em detalhes, assim como um exemplo de caso de uso.*

1. Introdução

Na área de redes de computadores, aspectos, como, a confiança dos dados trafegados é de extrema importância para o sistema. Neste trabalho será apresentado um ataque malicioso, em que uma máquina atacante se passa por um roteador e passa a ter acesso a dados sem autorização ou conhecimento por outras máquinas. O ataque em questão é chamado de *man-in-the-middle*, e de modo geral, o atacante altera o endereço do *default gateway* para o endereço da máquina intrusa.

Será apresentado um cenário, desenvolvido em um ambiente virtual, onde é possível identificar o ataque em ação. Para tal, foi criado uma topologia no simulador "CORE emulator"que se assemelha a padrões de redes encontradas no mundo real.

2. Topologia

A topologia construída com a ferramenta Core, contém: 4 *hosts*, 1 roteador principal e 1 *switch*. O *host n5* é identificado como atacante e os demais são vítimas do ataque. Os endereços de cada máquina foram configurados para IPv6. A Figura 1 apresenta a topologia de rede descrita anteriormente.

3. Código

No código elaborado para a realização do ataque *Man-in-the-Middle*, foi criado um "Socket RAW"com o intuito de receber pacotes Ethernet trafegados pela rede. Ao receber o pacote, verifica-se no campo *EtherType* do cabeçalho do protocolo se ele é um pacote do tipo IPv6, ou seja, se o valor nesse campo é '0x86dd', que é referente ao protocolo IPv6.

Uma vez filtrados os pacotes, o próximo passo é a verificação se essa mensagem é do tipo ICMPv6, para isso, é feita uma comparação do valor de *next header* com o valor referente ao protocolo IPv6, utilizando uma constante chamada *IPPROTO_ICMPV6*, disponibilizada pela biblioteca *socket* do python.

Finalizando a etapa de recebimento dos pacotes, deve-se verificar se a mensagem ICMPv6 recebida é do tipo *Router Solicitation*, ou seja, se uma máquina esta solicitando

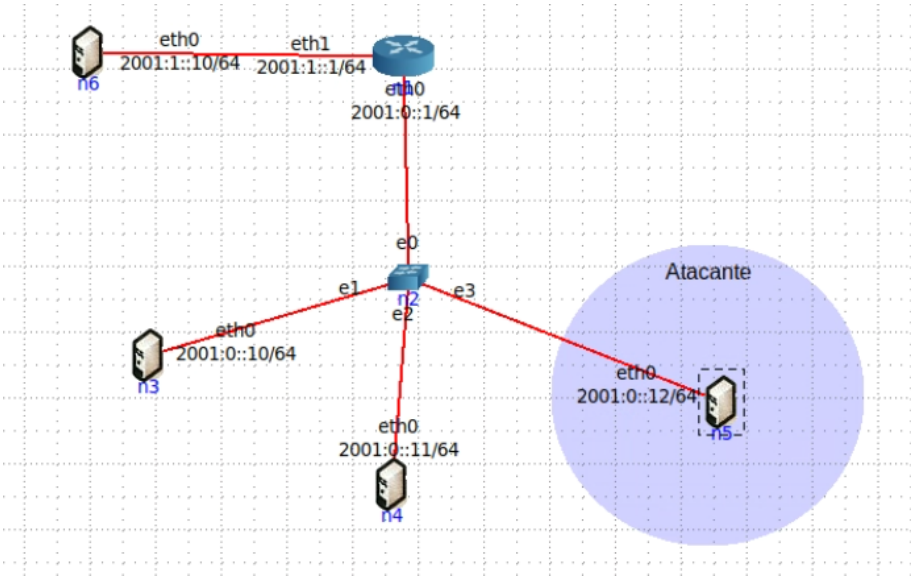

Figura 1. Organização da Rede

um endereço para o roteador. Para isso, é feita uma verificação do campo *icmp type* presente no pacote, caso esse valor seja de 133 é caracterizado como sendo um *Router Solicitation*.

Identificado o pacote de solicitação de um endereço por parte de um *host*, então o atacante cria um pacote *Ethernet* com protocolo IPv6 e ICMPv6 do tipo *Router Advertisement* para enviar de volta ao solicitante. Para a construção dessa mensagem, primeiramente montamos a parte do pacote *Ethernet* com o endereço MAC origem e endereço MAC destino.

O próximo passo é criar o pacote IPv6, para isso foi definido os campos de *version* igual a 6 (valor da versão do IPv6), *traffic class = 0*, *flow label = 0*, *payload = 16*, *next header* com o valor da constante *IPPROTO_ICMPV6* (referente ao valor do protocolo ICMPv6), *hop limit = 255* e os endereços IPv6 do atacante e da vítima.

Por fim, é criado o pacote ICMPv6 contendo o *type* 134 (valor referente à mensagem *Router Advertisement*), *code = 0*, *hop limit = 0*, *router lifetime = 0x0708*, *reachable time = 0x01010000*, *retrans timer = 0x00aa0005* e *flags = 0x80*, calculamos o *checksum* da mensagem e enviamos para o destinatário.

4. Experimentos

Para realização dos experimentos, foi utilizado o software ”Core Gui”, o qual permite a simulação de múltiplas máquinas em uma rede controlada. A execução foi realizada com a topologia apresentada na seção 2.

Após inicializada da rede, executamos o programa de ataque na máquina *n5*. Com as demais máquinas executamos o comando *ip link set eth0 down* para desativar as interfaces e o comando *ip link set eth0 up* para ativar a interface, a modo que force as mensagens de *Router Solicitation* na rede. O invasor recebeu os pacotes e retornou pacotes para as máquinas vítimas, podemos observar um exemplo de execução na Figura 2. Porém, as máquinas invasoras não definiram o IPv6 enviado como *default gateway*. Analisando

Figura 2. Demonstração de Execução

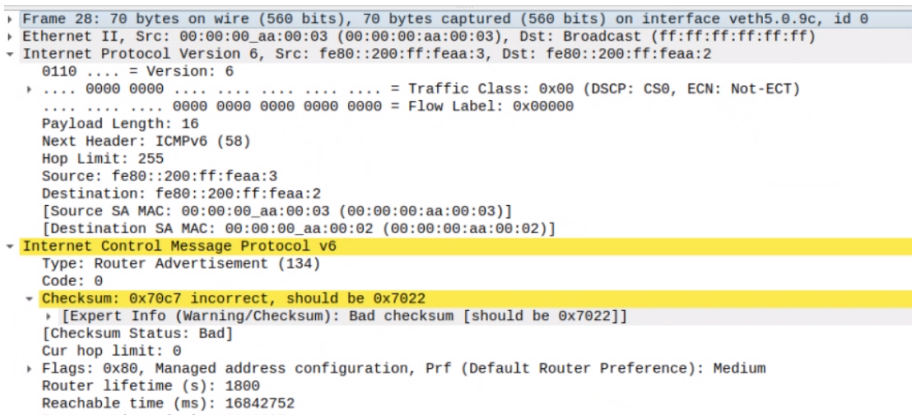

Figura 3. Demonstração de *checksum*

os pacotes pela ferramenta WireShark, foi averiguado que os cálculos de *checksum* do ICMPv6 apresentavam valores errados. Em uma das execuções a mensagem apresentou um valor de 0x70c7, enquanto deveria ser 0x7022, como podemos observar na Figura 3.

5. Conclusão

Finalizada as etapas de desenvolvimento e experimentos, não obtivemos exito completo em nosso objetivo de realizar o ataque *Man-in-the-Middle*. Os pacotes de *Router Advertisement* foram montados e enviados para as vítimas que solicitavam um endereço com *Router Solicitation*, porém o *checksum* apresentou erros. As vítimas receberam a mensagem de ataque, mas não definiram o endereço IPv6 como *default gateway*, por conta do erro apresentado em *checksum*. Também foi possível perceber na prática a importância da segurança em uma rede, para que informações não sejam interceptadas por máquinas invasoras.