PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

FACULDADE DE ENGENHARIA

LABORATÓRIO DE REDES DE COMPUTADORES

T1 - ARP Poisoning Attack com Man-in-the-middle

Felipe da Silva Angnes

Henrique Correa

Rafael Sperb

Professor: Sérgio Johann Filho

Porto Alegre, 24 de setembro de 2018

**Introdução**

Este trabalho tem como objetivo desenvolver uma aplicação que faz um ataque do tipo ARP poisoning combinado com man-in-the-middle, utilizando raw sockets.

Esta aplicação deve mandar pacotes ARP com o objetivo de modificar a tabela ARP de um computador alvo e permitir o redirecionamento de tráfego de rede para um computador atacante.

**Referencial teórico**

**Sockets Raw**

É um mecanismo que permite o recebimento de pacotes de rede juntamente com seus cabeçalhos. Geralmente o SO entrega somente os dados dos pacotes as aplicações específicas, portanto com Sockets Raw é possível analisar todo o tráfego recebido pela rede.

**Protocolo ARP**

O protocolo ARP (Address Resolution Protocol) é um protocolo de rede utilizado para a resolução de endereços da camada de ethernet em endereços da camada de enlace que é uma função crítica em redes de múltiplos acessos. O ARP foi definido pela RFC 826.

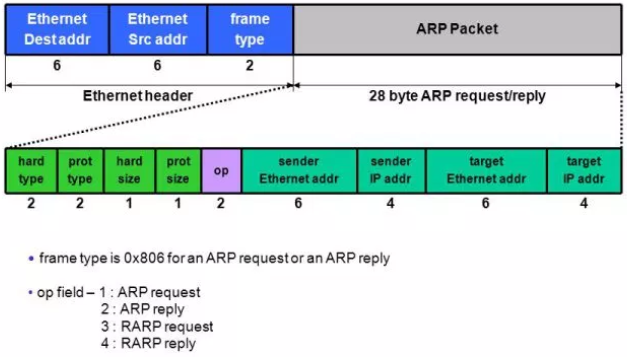
O ARP é utilizado para mapear um endereço de rede(endereço IP) em um endereço físico como um endereço ethernet.

Este procedimento é feito através de uma solicitação(ARP Request), onde o solicitante envia um pacote de solicitação em um formato específico para todas as máquinas da rede LAN(Broadcast) para descobrir se alguma máquina possui o endereço IP correspondente à solicitação.

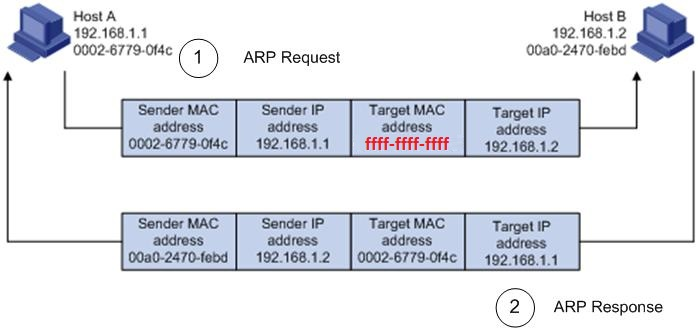
A máquina que corresponde ao endereço IP solicitado, envia uma resposta(ARP Reply) para a máquina solicitante incluindo na mensagem seu endereço físico. Assim o host solicitante registra em sua tabela ARP que determinado IP corresponde a determinado endereço físico(MAC).

Este registro geralmente fica armazenado na tabela ARP por aproximadamente 20 minutos. Após este período uma nova solicitação ARP Request deverá ser feita para identificar novamente o endereço físico do respectivo endereço IP.

**Formato pacote ARP**



**Exemplo ARP Request e ARP Reply(Response)**



**Tabela ARP**

É uma tabela que relaciona endereços IP com endereços MAC.

**ARP Poisoning**

O ataque poisoning consiste em enviar pacotes ARP de modo que modifique a tabela ARP de uma máquina alvo com o objetivo de desviar o tráfego de rede para a máquina atacante.

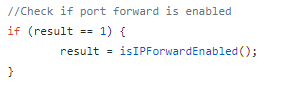
**Man-in-the-middle**

Esta técnica consistem em o atacante re-transmitir o tráfego interceptado. Esta transmissão pode ser com dados alterados, inalterados ou com parte das informações bloqueadas. Como os participantes legítimos da comunicação não sabem se houve alteração ou não na mensagem transmitida e recebida, essa mensagem é vista como válida por ambos. Assim o atacante passa despercebido pelas partes envolvidas.

**Desenvolvimento**

Para a resolução deste problema foi desenvolvido uma aplicação que recebe três parâmetros para iniciar o funcionamento do ataque. O primeiro parâmetro é o nome da interface do atacante, o segundo é o IP do gateway e o terceiro é o IP da vítima.

Antes da criação do socket, é testado se o IP forward está ativado para que o atacante possa encaminhar os pacotes que chegam a ele para a vítima.



Após a confirmação, é iniciado o socket,



configurado para modo promíscuo,

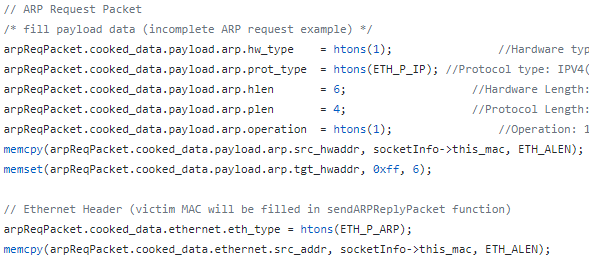


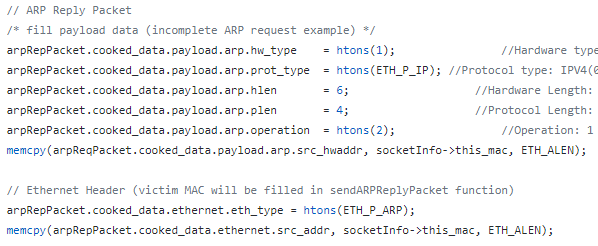
e por fim obtém o MAC address e o IP addres da interface.





Com o êxito das operações anteriores a aplicação inicia a criação do pacote ARP Request e ARP Reply.





E então inicia o envio de ARP Request para o gateway e para a vítima.





**Resultados**

**Conclusão**