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 um gateway para 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 como também permite a criação de um pacote cru (raw) para envia-lo na rede. 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**

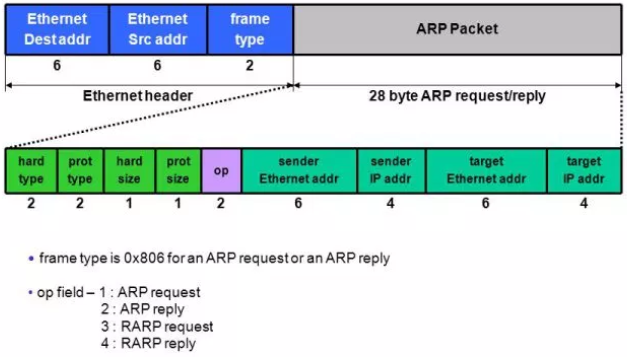
O protocolo ARP (Address Resolution Protocol) é um protocolo de rede utilizado para a resolução de endereços da camada de enlace associado ao endereço da camada de rede que é uma função crítica em redes de múltiplos acessos. O ARP foi definido pela RFC 826.

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.

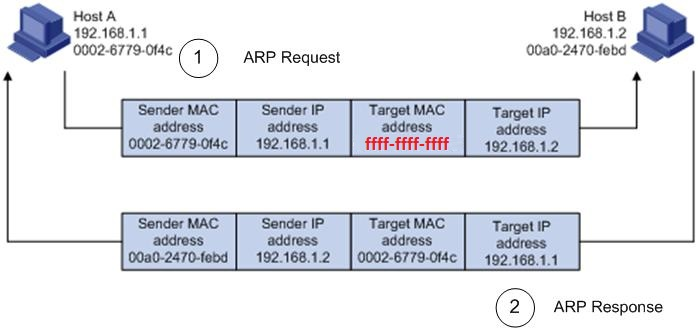
A máquina que corresponde ao endereço IP solicitado, envia uma resposta (ARP Reply) para a máquina solicitante incluindo na mensagem seu endereço de enlace. Assim o host solicitante registra em sua tabela ARP que determinado IP corresponde a determinado endereço de enlace (MAC).

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.

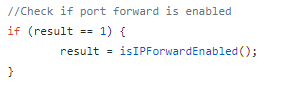
**Man-in-the-middle**

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,

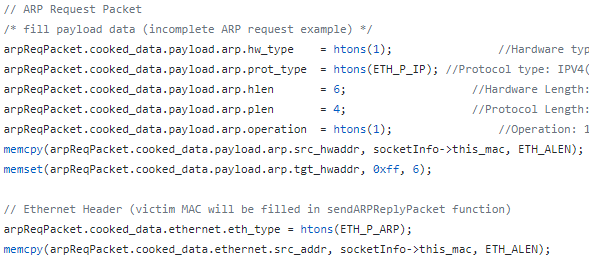


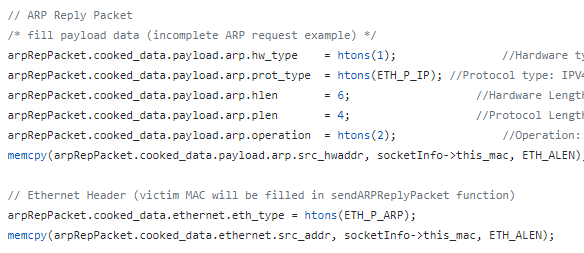
e por fim obtém o MAC address e o IP addres da interface.





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



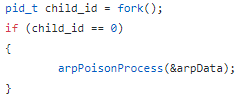


E então inicia o envio de ARP Request para o gateway e para a vítima com o objetivo de descobrir o MAC do gateway e da vítima que até o momento são desconhecidos. Neste mesmo momento o ataque já é iniciado envenenando a tabela ARP de ambos. A tabela ARP do gateway recebe o IP da vítima relacionado ao MAC do atacante e a tabela ARP da vítima recebe o IP do gateway relacionado ao MAC do atacante.

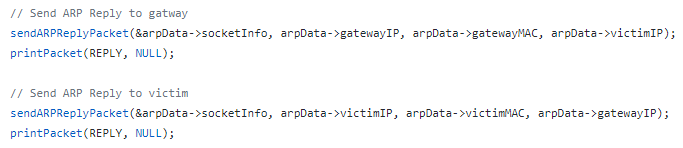




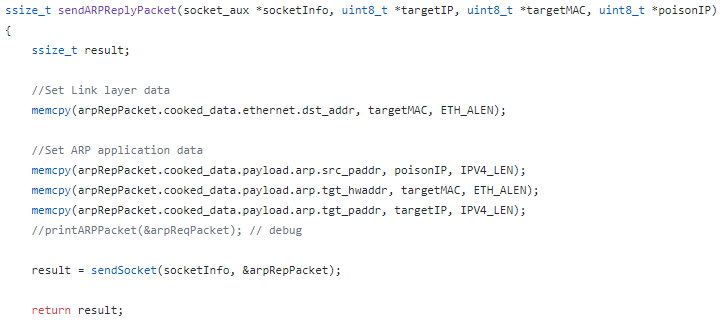
Assim são finalizadas as configurações necessárias para interceptar os pacotes trocados pelo gateway e pela vítima. O atacante já sabe o MAC do gateway e da vítima e também já envenenou as tabelas ARP de ambos. Portanto a aplicação dispara um processo filho para enviar mensagens do tipo ARP Reply periodicamente para o gateway e para a vítima.



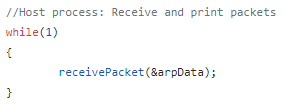
A função *arpPoisonProcess* consiste em chamar a função de envio de ARP Replay na rede.



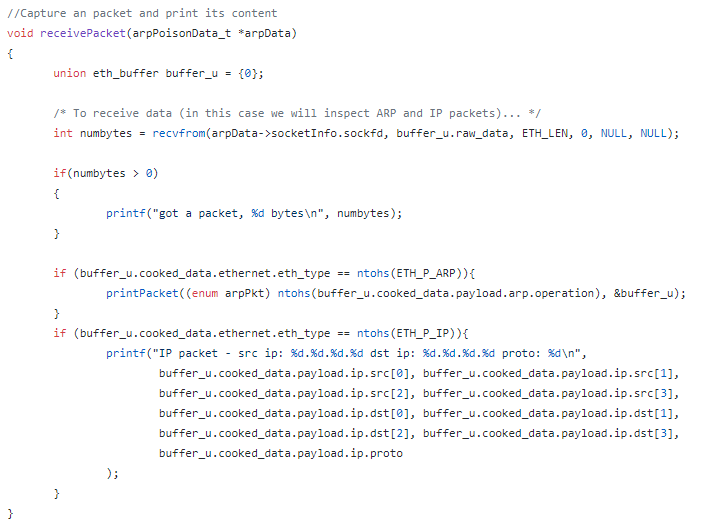
A função *sendARPReplayPacket* faz o envio do pacote ARP Replay, enviando o IP do gateway relacionado com o MAC do atacante quando o envio é para a vítima e relacionando o IP da vítima com o MAC do atacante quando o envio é para o gateway.



Paralelamente o processo pai fica recebendo os pacotes e imprimindo o conteúdo deles.



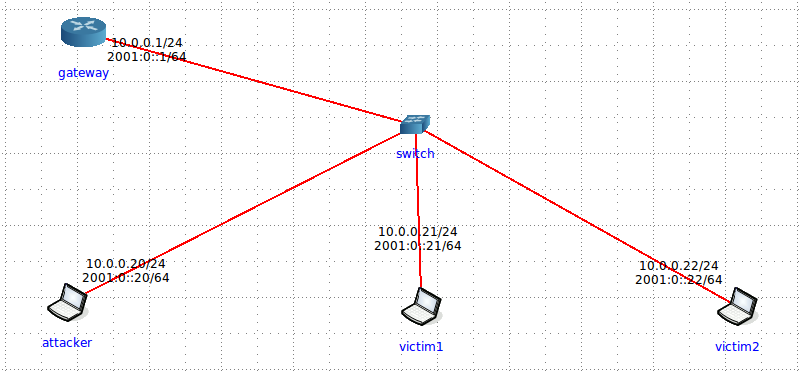
A função *receivePacket* recebe os pacotes direcionados ao atacante e imprime somente pacotes do tipo ARP e IP.



Assim demonstrando o êxito na interceptação de pacotes entre um computador e um gateway e atingindo o objetivo proposto pelo trabalho.

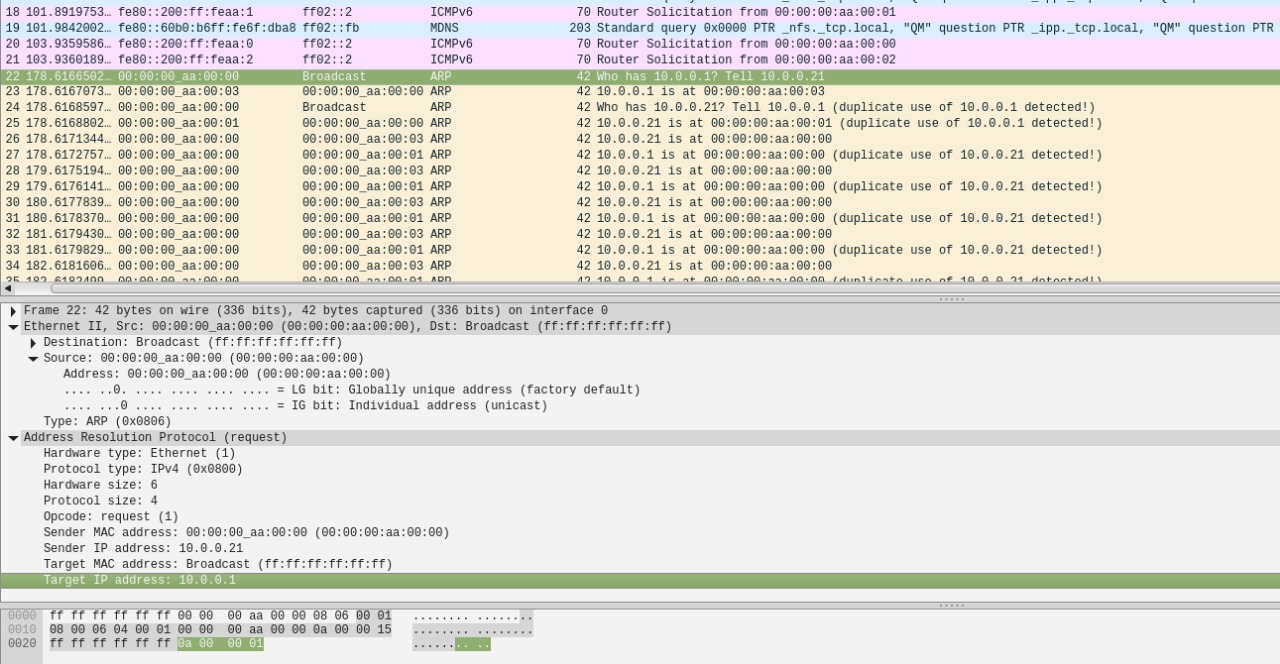
**Resultados**

Topologia utilizada:

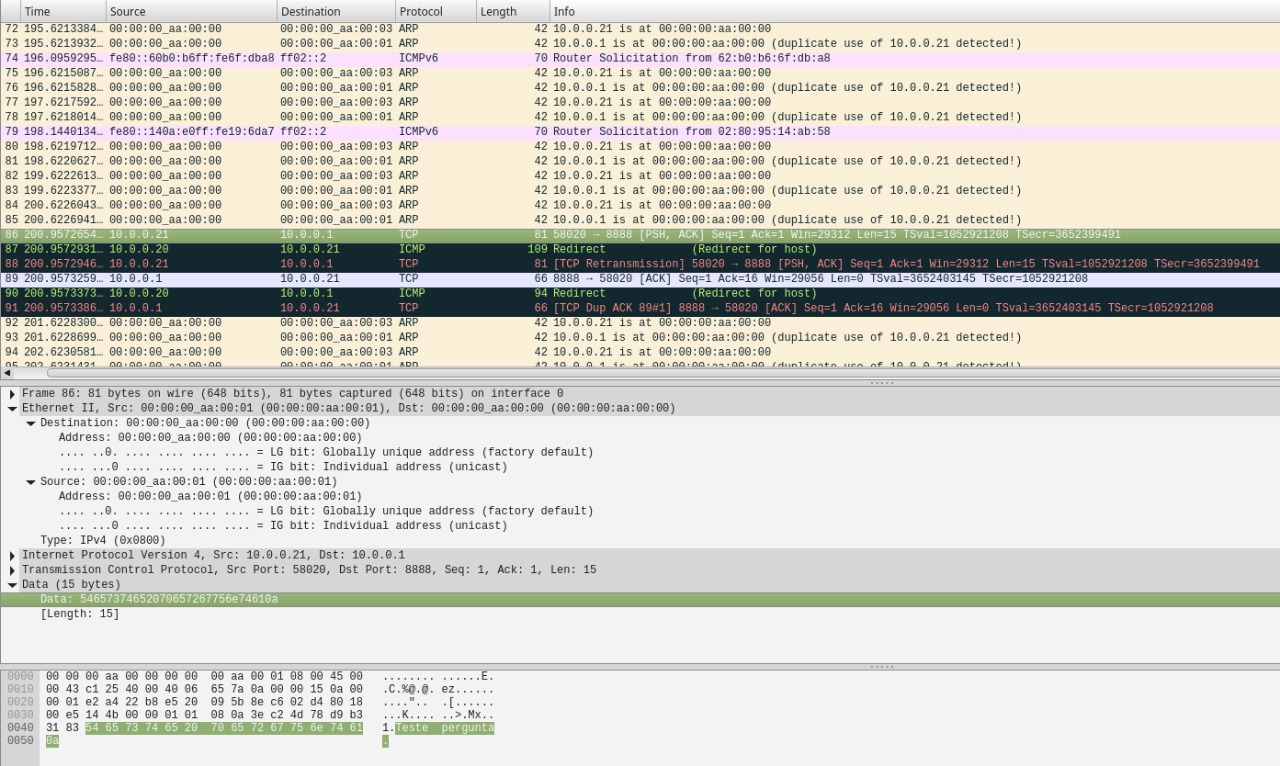


Wireshark aberto na interface do atacante.

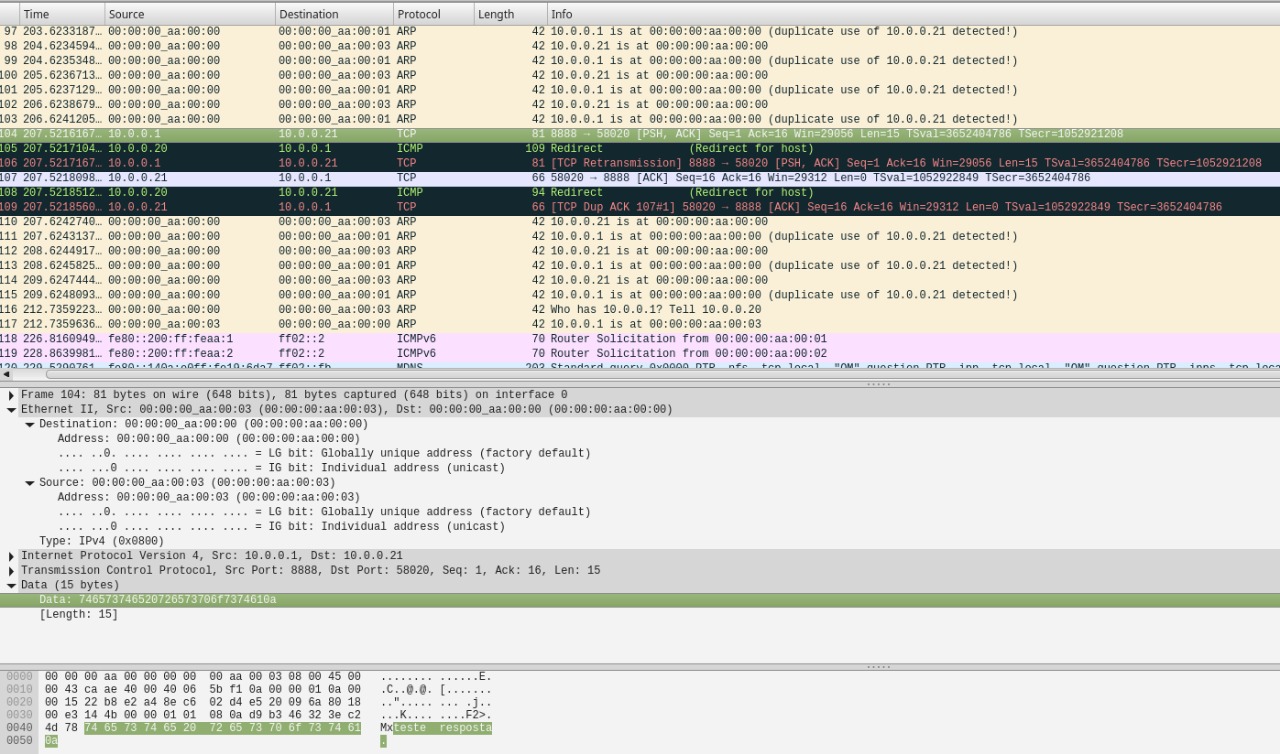
Inicio do ataque: Envio de ARP Request para vítima e gateway



Pergunta da vítima: Vítima faz uma pergunta para o gateway com netcat. Pergunta interceptada pelo atacante e enviada (forward) para o gateway com sucesso



Resposta do gateway: Gateway responde a pergunta com netcat. Atacante intercepta a mensagem e envia (forward) a mensagem para a vítima.



**Conclusão**

Com este trabalho podemos concluir que o protocolo ARP é muito vulnerável. Mesmo nos dias de hoje a vulnerabilidade persistem em IPv4.

Existem algumas soluções que evitam esta vulnerabilidade como por exemplo habilitar MAC binding no switch, entradas estáticas na tabela ARP ou utilizando a ferramenta Arpwatch.

Com relação ao desenvolvimento da aplicação aprendemos meios de consultar informações a respeito dá interface de rede através da chamada de sistema IOCTL e como obter informações de outros nodos da rede e usá-las na aplicação. Também percebemos a eficaz utilização de sockets raw para explorar falhas de segurança na rede.