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

ARP Poisoning Attack com Man-in-the-middle

Objetivo

O objetivo geral do trabalho é desenvolver uma aplicação usando *sockets* raw que possa ser utilizada para estudar o protocolo ARP e demonstrar um ataque do tipo *ARP poisoning* combinado com *man-in-the-middle*. Esse tipo de ataque consiste em enviar pacotes ARP de modo a modificar a tabela ARP de um computador alvo e permitir o redirecionamento de tráfego de rede para um computador intermediário. Esse ataque, quando combinado com a técnica de *man-in-the-middle*, permitir a interceptação de todo o tráfego entre um computador alvo e o gateway da rede. Os objetivos específicos incluem:

- o desenvolvimento de uma aplicação usando sockets raw;
- estudo do funcionamento do protocolo ARP;
- estudo dos problemas de segurança relacionados ao protocolo ARP.

Descrição

O trabalho será dividido em três etapas:

1) Modificar os programas de raw socket Ethernet utilizados na aula para imprimir todos os campos do protocolo ARP formatados para facilitar o seu entendimento (isto é, o programa de funcionar como um sniffer de rede). Esta etapa do trabalho é importante para entender o funcionamento do protocolo ARP e descobrir automaticamente as informações necessárias na etapa seguinte.
2) Modificar os programas para realizar envio e recebimento de pacotes do tipo ARP e implementar o ataque do tipo ARP poisoning. Os campos do pacote ARP devem ser montados na forma de um vetor de bytes e enviados via raw socket. É expressamente proibido utilizar códigos prontos para a montagem e/ou envio destes pacotes (isso é importante, pois um dos objetivos do trabalho é compreender o funcionamento desse protocolo). O programa criado deve receber como parâmetro apenas o nome da interface Ethernet local e o endereço IP do alvo. O restante das informações (ex: endereço MAC do alvo, endereço IP do roteador e endereço MAC do roteador) devem ser descobertas automaticamente.
3) Demonstrar o funcionamento do ataque de ARP poisoning em combinação com a técnica de man-in-the-middle através do redirecionamento de tráfego HTTP (Web). Mais informações no material de apoio anexo.

Tudo deve ser documentado na forma de um relatório. Este relatório deve primeiramente descrever o funcionamento do protocolo ARP (utilize capturas de telas da etapa (1) do trabalho para facilitar a explicação) e, então, descrever como foi explorado o problema de segurança usando digramas, trechos de códigos e/ou capturas de tela. Esse relatório deverá ser entregue juntamente com o código fonte utilizado.

Resultados e Entrega

Grupos: Individual ou em dupla.
Entrega: Upload na sala de entrega do Moodle de um arquivo zipado com o seguinte padrão T1_NomeAluno1NomeAluno2.zip e contendo:

1. Relatório
2. Código da implementação

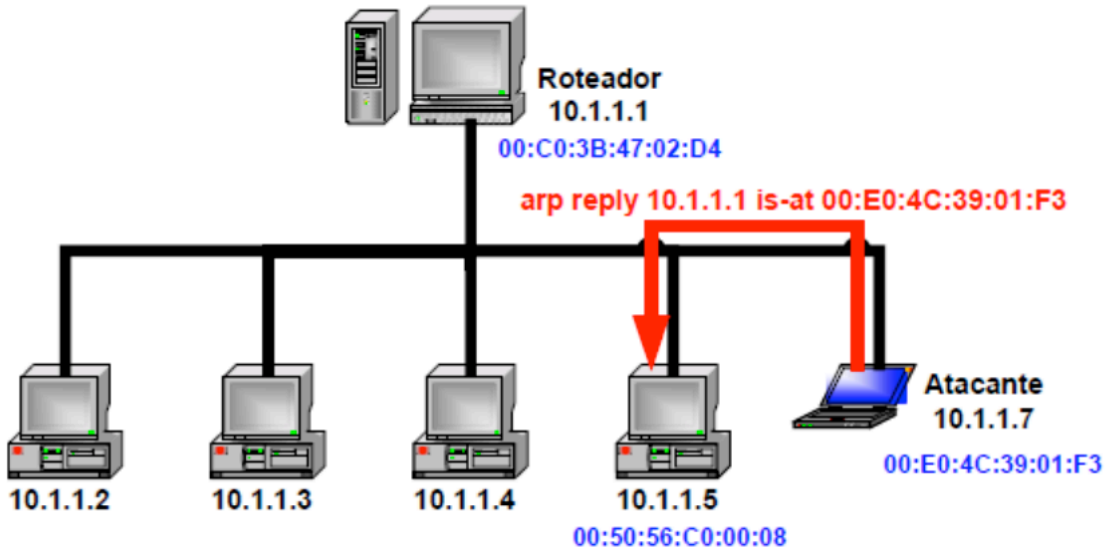
Data Entrega: 12/09/2016 até as 17:30.
Data Apresentação: 12/09/2016 durante a aula (a ordem das apresentações será defina pela ordem de entregas pelo Moodle).

Material de apoio

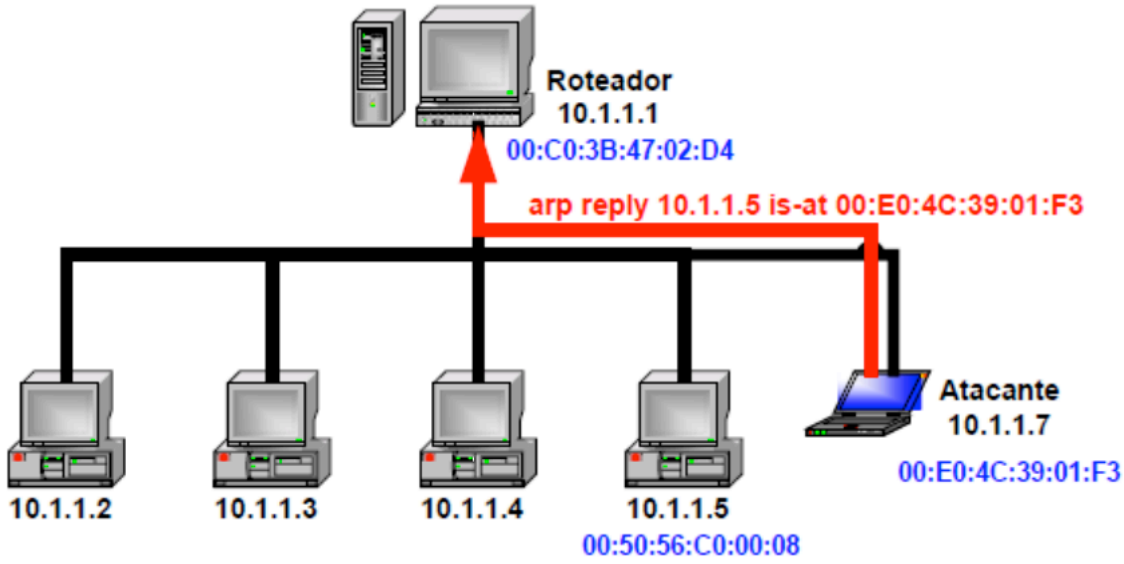
ARP Spoofing Básico

Enviar pacotes ARP reply não solicitados para os computadores alvo para modificar suas tabelas ARP locais. Utilize o programa Wireshark para acompanhar o funcionamento do ataque em cada fase. Veja o exemplo abaixo.

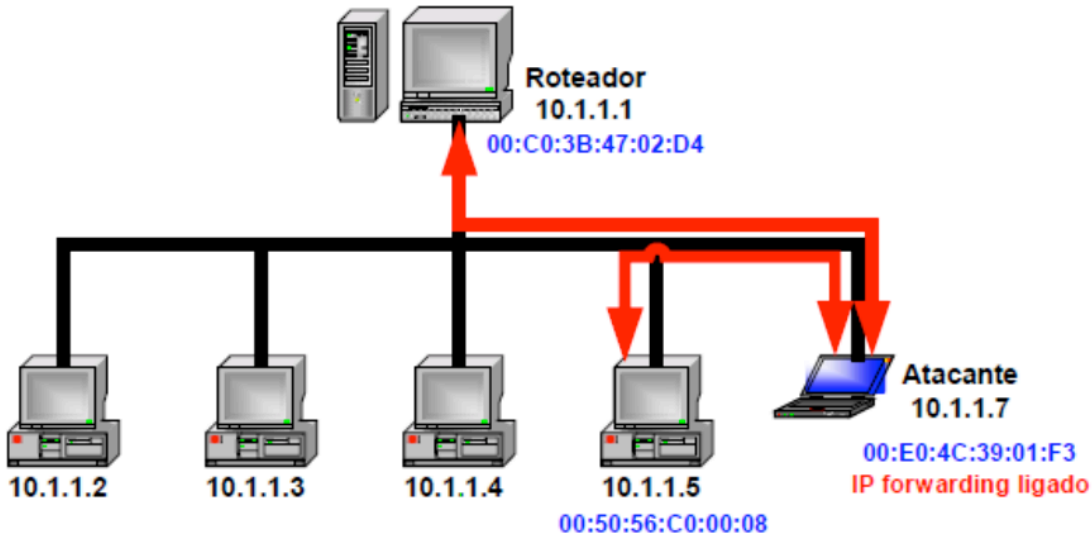
Passo 1:



Passo 2:



Resultado:



Alguns sistemas operacionais como Windows 7 (ou superiores) irão ignorar mensagens ARP reply não solicitadas e realizar uma nova consulta ARP para confirmar o endereço físico de um computador. Neste caso, um método alternativo é enviar uma mensagem ARP request para o computador alvo usando endereços de IP/MAC de origem modificados.

Para que o sistema operacional não corrija a tabela ARP com as informações verdadeiras envias pelos computadores da rede, é necessário manter o envio constante de mensagens ARP modificadas (por exemplo, a cada 1 segundo).

Verificação do funcionamento

Para verificar se o ataque funcionou, visualize as tabelas ARP de cada computador antes e depois do ataque e verifique se as mesmas foram alteradas com sucesso. O comando para verificar a tabela ARP no Linux é:

```
arp –n
```

Adicionalmente, é possível utilizar o programa Wireshark para acompanhar o envio/recebimento de mensagens ARP em cada computador.

Encaminhamento de pacotes

Por padrão, o Linux descarta pacotes que são destinados a outros computadores. Desta forma, para implementar um ataque do tipo man-in-the-middle, é necessário habilitar a funcionalidade de encaminhamento de pacotes do kernel do Linux (IP Forwarding). Isso fará com que o tráfego entre o computador alvo e o roteador não seja interrompido durante o ataque.

Para habilitar a funcionalidade de IP Forwarding, execute o seguinte comando no Linux:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Redirecionamento de tráfego HTTP

Uma maneira de testar o funcionamento do ataque é forçar que todo o tráfego HTTP seja redirecionado para um servidor específico (ex: servidor local). Para isso, é possível utilizar o iptables para configurar NAT (Network Address Translation) e aplicar regras redirecionamento para a porta 80. Execute os seguintes comandos no Linux:

```
iptables –t nat --flush
iptables --zero
iptables –A FORWARD --in-interface eth0 –j ACCEPT
iptables –t nat --append POSTROUTING --out-interface eth0 –j
MASQUERADE
iptables –t nat –A PREROUTING –p tcp --dport 80 --jump DNAT --
to-destination 10.1.1.7
```

Substituía o endereço de IP 10.1.1.7 pelo endereço da máquina atacante ou outra qualquer que execute o um servidor Web. Para instalar um servidor Web na máquina atacante, execute os seguintes comandos no Linux:

apt-get install apache2
echo “Esse eh o site falso!” > /var/www/html/index.html

Assim, quando a máquina alvo tentar acessar um site qualquer na Internet, será redirecionada para esse servidor.

Desafio: modifique o exemplo acima para redirecionar o tráfego apenas de um site específico, como por exemplo www.facebook.com.