



ARP Poisoning Attack

Objetivo

O objetivo geral do trabalho é desenvolver uma aplicação usando *sockets raw* que possa ser utilizada para demonstrar um ataque do tipo ARP poisoning. 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 pode ser combinado com a técnica de man-in-the-middle para, por exemplo, permitir a interceptação de todo o tráfego entre um computador alvo e o gateway da rede. Os objetivos específicos incluem:

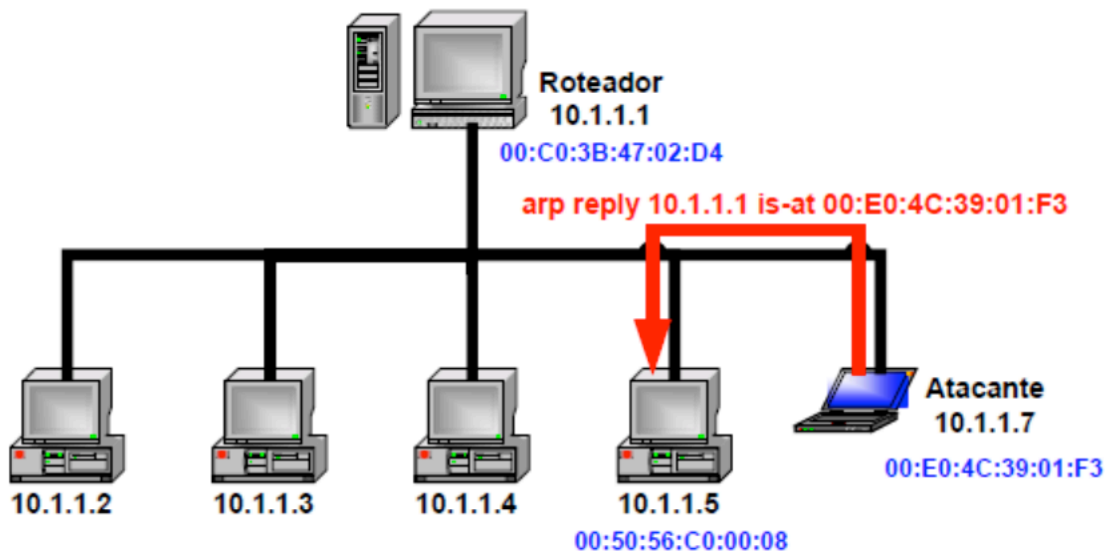
- o desenvolvimento de uma aplicação usando sockets raw;
- estudo dos problemas de segurança relacionados ao protocolo ARP.

Descrição

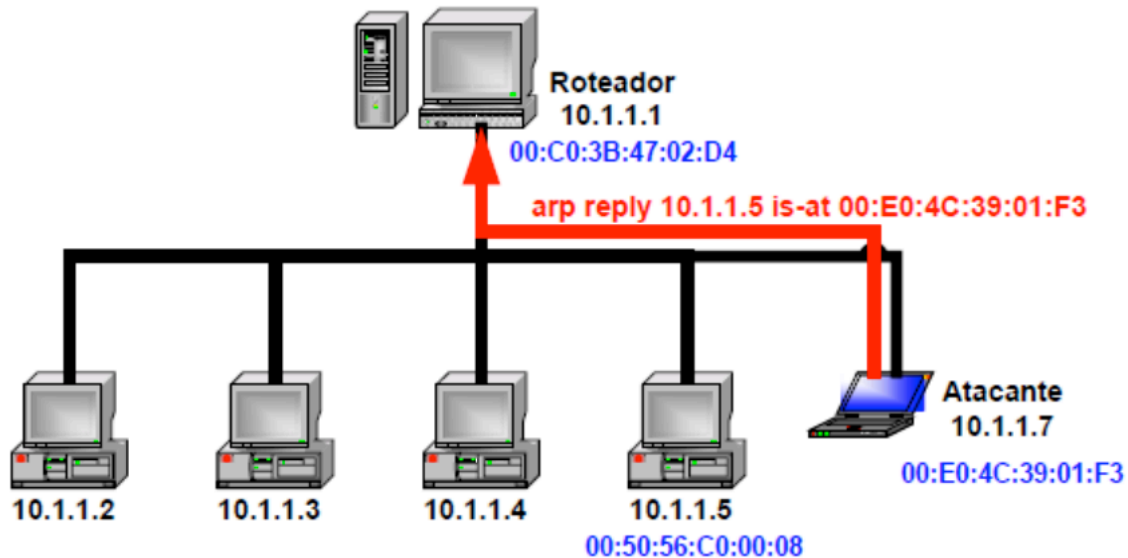
ARP Spoofing Básico

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.

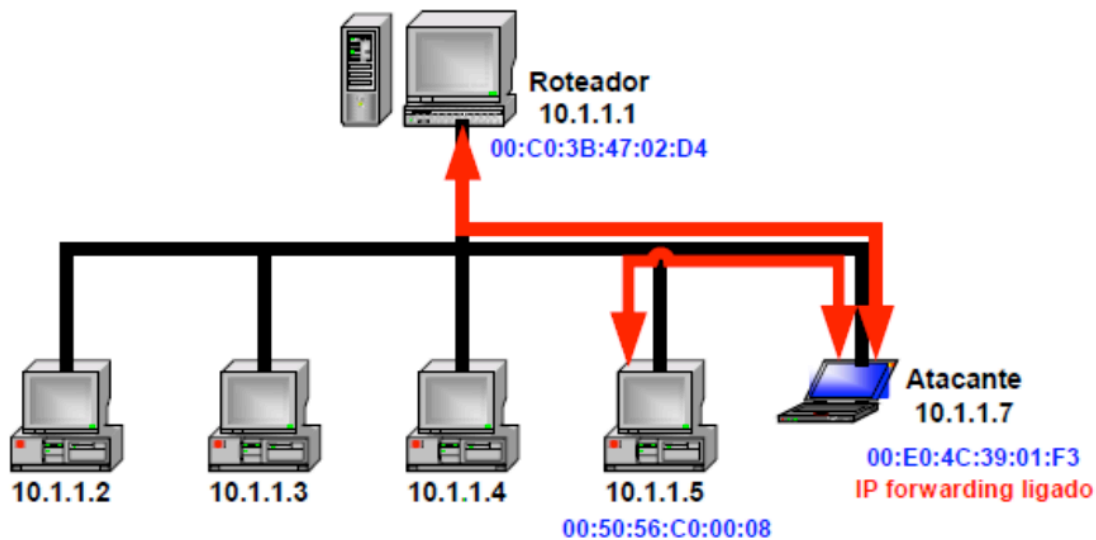
Passo 1:



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 endereço o 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).

Resultados e Entrega

Grupos: Individual ou em dupla.

Entrega: Arquivo zipado com o nome do aluno, contendo:

1. Relatório descrevendo a implementação (*upload* no Moodle)
2. Código da implementação (*upload* no Moodle)

Data Entrega: 14/09/2015.

Material de apoio

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
```

Substitua 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.