Laboratório de Redes de Computadores - Trabalho 1

ARP Poisoning Attack com Man-in-the-middle

Objetivo

O objetivo geral do trabalho é desenvolver uma aplicação usando *raw sockets* 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*, permite a interceptação de todo o tráfego entre um computador alvo e o roteador (*gateway*) da rede. Os objetivos específicos incluem:

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

Descrição

O trabalho será dividido em quatro etapas:

1. Criar uma topologia que consiste de pelo menos 3 PCs / hosts (duas máquinas vítimas e um atacante) e um Ethernet switch no Core Emulator. Essa topologia deve ser usada durante o desenvolvimento do trabalho e servirá para demonstrar a funcionalidade do ataque. As máquinas vítimas são uma estação (PC) e um roteador. Alternativamente, pode-se utilizar as máquinas do laboratório.

2. Modificar o programa fornecido juntamente com o enunciado (arp.tar.gz) para imprimir todos os campos do protocolo ARP formatados, com o objetivo de facilitar o seu entendimento (isto é, funcionar como um *sniffer* de rede). Utilize as funções *htons()* e *ntohs()* para resolver problemas de *endianness*. Adicionalmente, utilize como referência o pacote *sendrecv_ raw.tar.gz* disponibilizado no Material Auxiliar da disciplina.

3. Modificar o programa para realizar envio e recebimento de pacotes do tipo ARP (pode ser necessário o uso da chamada de sistema *fork()* e auxiliares) e implementar o ataque do tipo *ARP poisoning*. Importante: o ataque deve ser implementado em um único programa (executável). Além disso, os campos dos pacotes ARP devem ser montados ou extraídos exclusivamente das estruturas de dados fornecidas, e os pacotes devem ser enviados/recebidos via *raw sockets*. É expressamente proibido utilizar outras estruturas de dados ou códigos prontos para a montagem e/ou envio destes pacotes (isso é importante, pois um dos objetivos do trabalho é compreender o funcionamento do protocolo ARP e formato de frames Ethernet, e para isso será necessário implementar sua versão baseada nas estruturas fornecidas).

4. Demonstrar o funcionamento do ataque de ARP poisoning em combinação com a técnica de *man-in-the-middle* através da interceptação do tráfego de uma máquina alvo (que pode ser emulada no Core Emulator). Para isso, deve ser escolhida alguma aplicação onde haja comunicação entre as máquinas atacadas, e a partir da máquina atacante seja possível interceptar o tráfego. Preferencialmente utilize tráfego não encriptado para que o conteúdo possa ser visto claramente (por exemplo, *telnet* ou alguma página *web*).

Tudo deve ser documentado na forma de um relatório. Este relatório deve primeiramente descrever o funcionamento do protocolo ARP e então, descrever como foi explorado o problema de segurança usando diagramas, trechos de códigos e/ou capturas de tela. Esse relatório deverá ser entregue juntamente com o código fonte desenvolvido e deve ter um tamanho entre 8 e 10 páginas.

ARP Spoofing básico

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

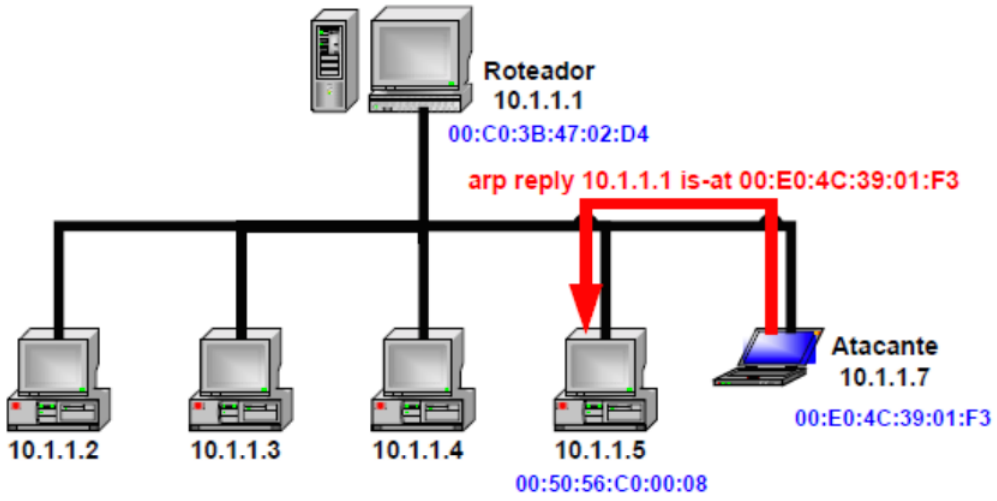

Figura 1: Primeiro passo

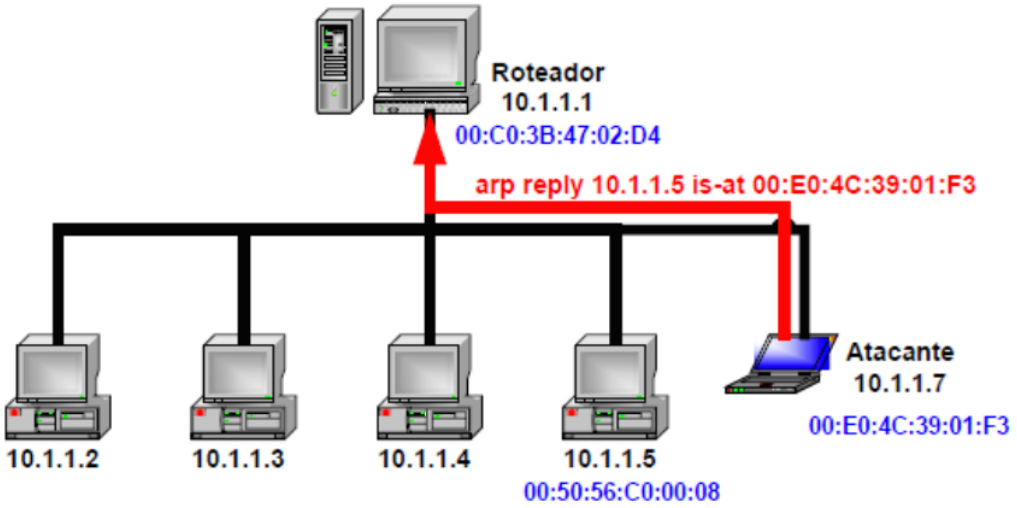

Figura 2: Segundo passo

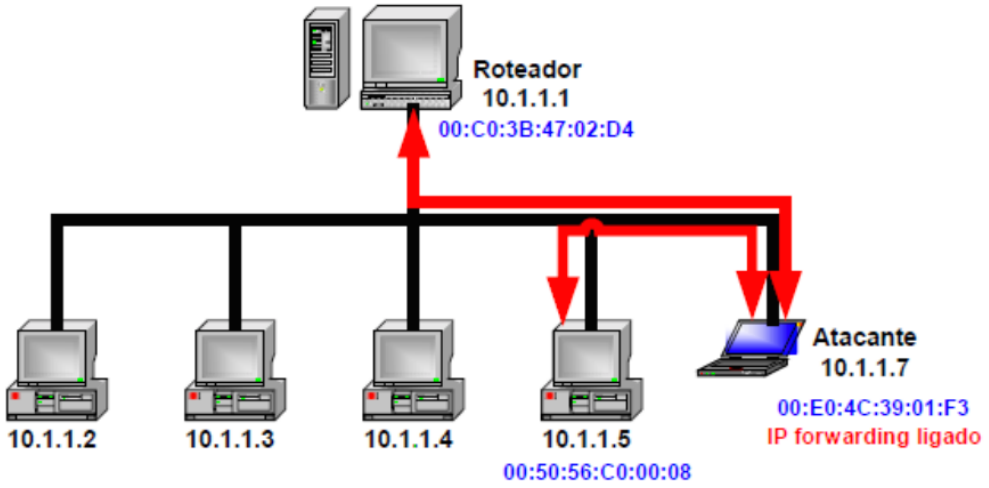

Figura 3: Terceiro passo

Alguns sistemas operacionais podem 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. A máquina atacada irá responder, e também irá popular sua tabela ARP.

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 (a cada 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. É essencial que a comunicação entre as máquinas afetadas pelo ataque seja aparentemente normal, do ponto de vista da aplicação.

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) na máquina atacante. 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
```

Entrega

O trabalho deve ser realizado em duplas ou trios. Envie um arquivo compactado (.tar.gz) contendo o código fonte utilizado e um relatório completo (descrito anteriormente).