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 *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 três etapas:

1. Modificar os programas de *raw socket Ethernet* utilizados na aula 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). Deve-se utilizar as seguintes estruturas:

```c
#define ETH_LEN 1518

struct eth_hdr {
  uint8_t dst_addr[6];
  uint8_t src_addr[6];
  uint16_t eth_type;
};

struct arp_packet {
  uint16_t hw_type;
  uint16_t prot_type;
  uint8_t hlen;
  uint8_t dlen;
  uint16_t operation;
  uint8_t source_hwaddr[6];
  uint8_t source_ip[4];
  uint8_t target_hwaddr[6];
  uint8_t target_ip[4];
};

struct eth_arp_frame {
  struct eth_hdr ethernet;
  struct arp_packet arp;
};

union eth_buffer {
  struct eth_arp_frame eth_arp_data;
  uint8_t raw_data[ETH_LEN];
};
```

2. Modificar os programas para realizar envio e recebimento de pacotes do tipo ARP e implementar o ataque do tipo *ARP poisoning*. 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*. Utilize as funções *htons()* e *ntohs()* para resolver problemas de *endianness*. 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).

3. 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. Para isso, deve ser escolhida alguma

aplicação onde haja comunicação entre a máquina atacada e outra máquina, e a partir da máquina atacante seja possível interceptar o tráfego. Preferencialmente utilize tráfego não encriptado para que o conteúdo possa ser visto claramente.

Tudo deve ser documentado na forma de um relatório. Este relatório deve primeiramente descrever o funcionamento do protocolo ARP (utilize capturas de telas do item (1) 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.

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.

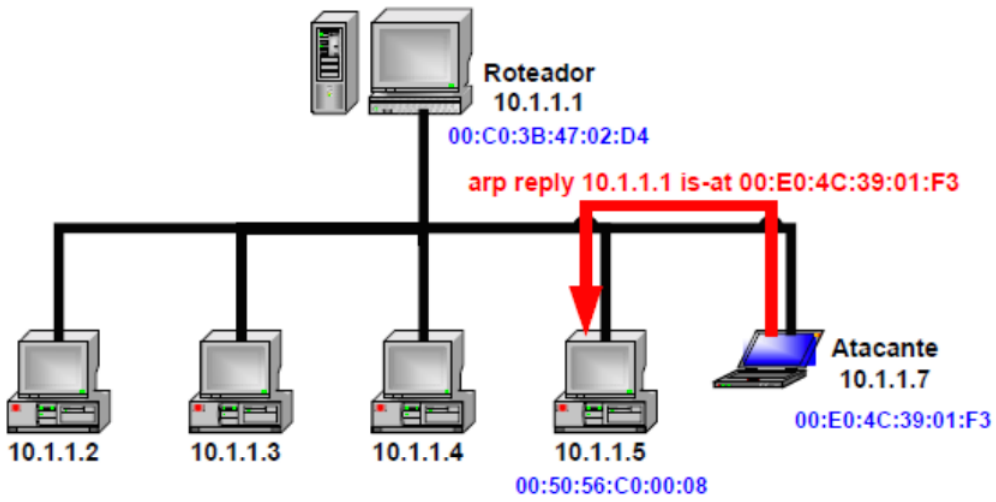

Figura 1: Primeiro passo

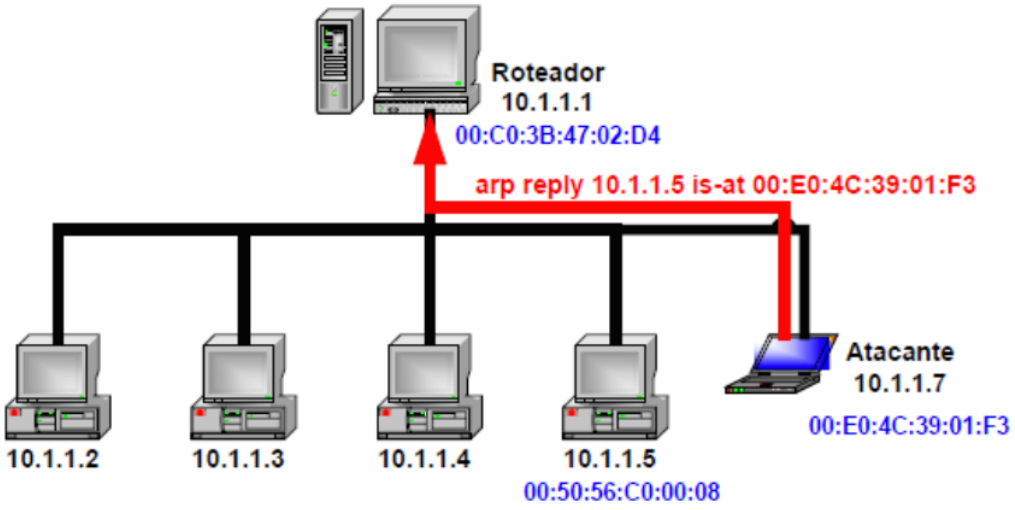

Figura 2: Segundo passo

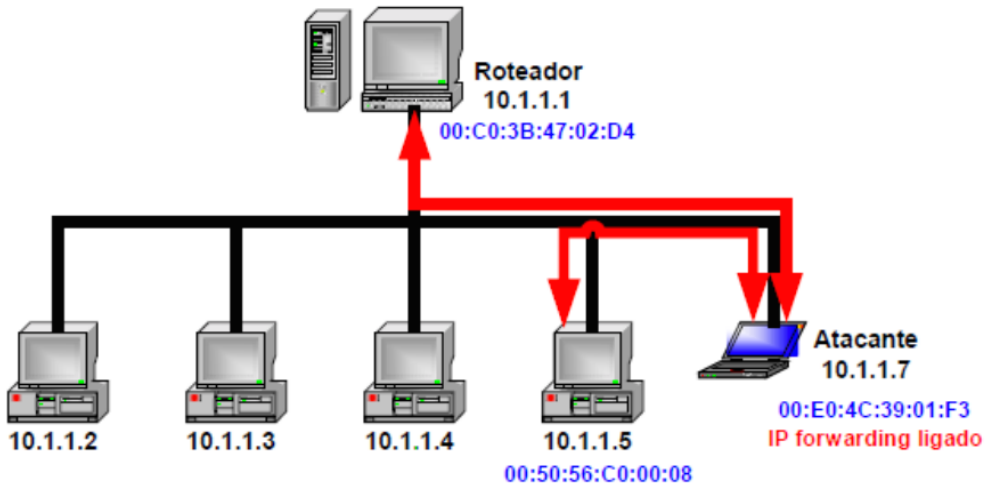

Figura 3: Terceiro passo

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 individualmente. Envie um arquivo compactado (.tar.gz) contendo o código fonte utilizado e um relatório completo descrevendo a aplicação e seu uso para a implementação de um ataque.