Trabalho Final de LabRedes
Sniffer de rede
Gabriel Tabajara, Lucas Dellatorre e Giovani Schenato.

1) ICMP Flooding

O ICMP Flooding é um tipo de ataque de negação de serviço (DoS - Denial of Service) que usa o comando ping de maneira maliciosa para sobrecarregar um sistema alvo com um grande volume de requisições de ping. Este ataque visa esgotar os recursos do sistema alvo, como largura de banda, CPU ou memória, tornando-o incapaz de responder a solicitações legítimas.

Exemplo de ataque:

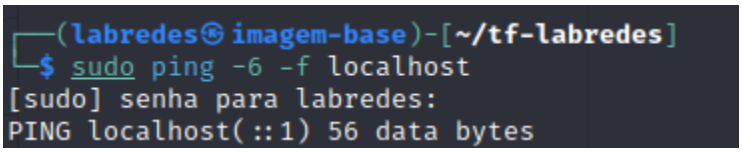

Figura 1: envio de pacotes ICMPv6 na rede

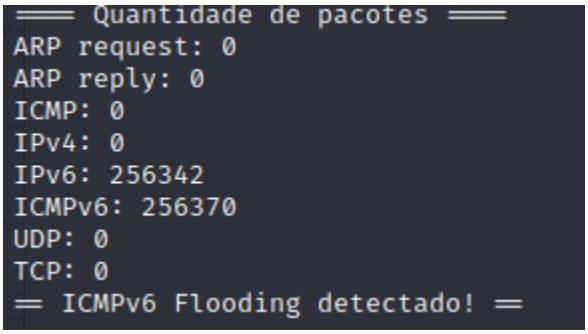

Figura 2: detecção de ataque pelo sniffer

Nota-se que há um grande volume de pacotes chegando na rede em um curto período de tempo, logo para o sniffer isso se enquadra como um ataque de ICMP Flooding.

2) ARP Spoofing

O utilitário *arpspoof* é uma ferramenta de manipulação de ARP (Address Resolution Protocol) que faz parte da suíte de ferramentas de software chamada dsniff. O ARP é um protocolo usado para associar endereços IP a endereços MAC (Media Access Control) em uma rede local.

O arpspoof funciona explorando a vulnerabilidade no ARP, que é um protocolo sem autenticação, permitindo a associação entre endereços IP e endereços MAC. Esse utilitário

permite que um atacante redirecione o tráfego de rede de um dispositivo para outro, executando um ataque conhecido como ARP spoofing ou ARP poisoning.

O atacante primeiro identifica os endereços IP dos dispositivos na mesma rede local e envia pacotes falsificados para as máquinas na rede, informando a elas que o endereço MAC associado a um determinado IP mudou. Isso faz com que as máquinas atualizem suas tabelas ARP, associando o endereço MAC do atacante ao endereço IP legítimo de um dispositivo alvo específico. Uma vez que a tabela ARP de uma máquina foi manipulada, o tráfego destinado a essa máquina é redirecionado para o atacante.

Exemplo de ataque:

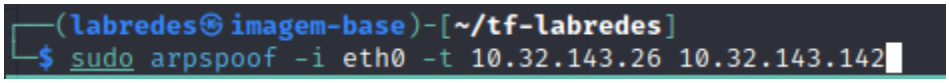

Figura 3: comando de interceptação (arpspoof) realizado na máquina do atacante

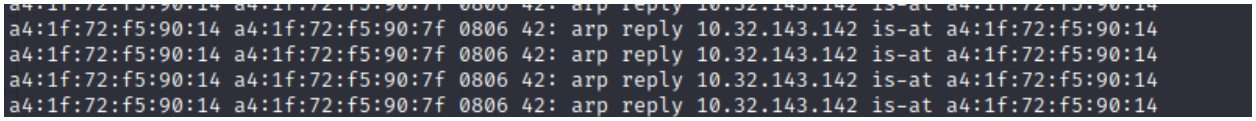

Figura 4: saída do comando de monitoramento

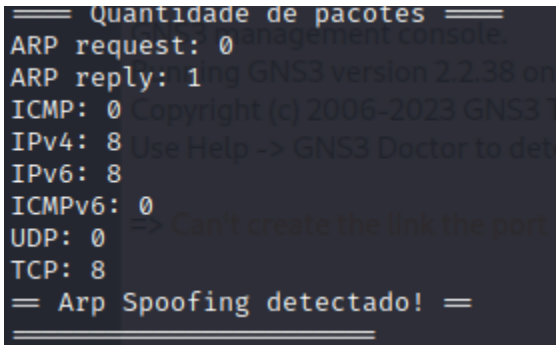

Figura 5: detecção realizada pelo sniffer de rede

```
=== Quantidade de pacotes ===
ARP request: 0
ARP reply: 0
ICMP: 0
IPv4: 0
IPv6: 256342
ICMPv6: 256370
UDP: 0
TCP: 0
= ICMPv6 Flooding detectado! =
```

```
┌──(labredes㉿imagem-base)-[~/tf-labredes]
└─$ sudo ping -6 -f localhost
[sudo] senha para labredes:
PING localhost(::1) 56 data bytes
```