Trabalho 2
Laboratório de Redes de Computadores

Gustavo Geyer Arrussul Winkler dos Santos, Mateus de Carvalho de Freitas

26 de novembro de 2023

Pontifícia Universidade Católica do Rio Grande do Sul
Escola Politécnica
Ciência da computação
Laboratório de Redes de Computadores

Trabalho 2
Relatório sobre Técnicas de Ataque à Camada de Rede e Detecção com um Sniffer

Gustavo Geyer Arrussul Winkler dos Santos
Mateus de Carvalho de Freitas

PORTO ALEGRE, NOVEMBRO DE 2023

Introdução

Este relatório abordará duas técnicas de ataque à camada de rede - ICMP Flooding e ARP Spoofing. Cada técnica será detalhada quanto ao seu funcionamento, propósito, características e implementação no ambiente Linux.

ICMP Flooding

O que é ICMP Flooding

O ICMP (Internet Control Message Protocol) Flooding é um tipo de ataque de negação de serviço (DoS) que visa sobrecarregar a capacidade de processamento de um host alvo, prejudicando sua capacidade de responder a solicitações legítimas.

Normalmente, mensagens de solicitação de eco e resposta de eco ICMP são usadas para executar ping em um dispositivo de rede a fim de diagnosticar a integridade e a conectividade do dispositivo e a conexão entre o remetente e o dispositivo. Ao inundar o alvo com pacotes de solicitação, a rede é forçada a responder com um número igual de pacotes de resposta. Isso faz com que o alvo se torne inacessível ao tráfego normal.

Outros tipos de ataques de solicitação ICMP podem envolver ferramentas ou códigos personalizados, como hping e scapy. O tráfego de ataque proveniente de vários dispositivos é considerado ataque de negação de serviço distribuída (DDoS) . Nesse tipo de ataque DDoS, os canais de entrada e saída da rede são sobrecarregados, consumindo largura de banda significativa e resultando em negação de serviço.

Como Funciona

O ataque ICMP Flooding envolve o envio massivo de pacotes ICMP de solicitação (ping) para um host de destino. A inundação de solicitações sobrecarrega a capacidade de processamento do host, levando à degradação ou interrupção dos serviços.

Para isso e preciso:

- Para executar um ataque de inundação de Ping, o invasor deve saber o endereço IP do dispositivo destinatário.
- Para um ataque de inundação de Ping bem-sucedido e sustentado, o invasor deve ter mais largura de banda de rede do que a rede alvo. Para tornar viável a sobrecarga de um sistema alvo, os invasores geralmente usam botnets .
- Num ataque de inundação de Ping, o dispositivo destinatário, cujo endereço IP é alvo, é inundado com solicitações de eco ICMP. Existe uma expectativa de que o dispositivo destinatário responda a uma solicitação de eco ICMP.
- Para tornar o dispositivo alvo inacessível e incapaz de responder a solicitações legítimas, o invasor inunda o dispositivo alvo continuamente.

Propósito e Características

O objetivo principal do ICMP Flooding é criar uma condição de congestionamento na rede alvo, impedindo-a de atender a solicitações legítimas. Este ataque é caracterizado pela alta taxa de pacotes ICMP enviados, visando saturar a largura de banda e recursos de processamento.

Funcionamento no Linux

No Linux, o ICMP Flooding pode ser executado usando ferramentas como "hping3"ou "ping". A manipulação de parâmetros, como o intervalo entre os pacotes e o tamanho dos mesmos, permite personalizar o ataque de acordo com os requisitos do invasor.

Teoria por Trás do Ataque

A teoria por trás do ICMP Flooding reside na exploração da capacidade limitada do sistema alvo para processar solicitações ICMP. Ao inundar o host com um grande número de pacotes, a taxa de processamento é excedida, resultando em uma negação de serviço.

Justificação da Escolha

A escolha do ICMP Flooding para este trabalho baseia-se em sua eficácia em prejudicar a disponibilidade de serviços, destacando a importância de proteger contra ataques de negação de serviço.

Como os ataques DDoS de inundação ICMP sobrecarregam as conexões de rede do dispositivo alvo com tráfego falso, as solicitações legítimas são impedidas de passar. Este cenário cria o perigo de DoS ou, no caso de um ataque mais concertado, de DDoS. O que torna esse vetor de ataque volumétrico ainda mais perigoso é que, no passado, os invasores falsificavam um endereço IP falso para mascarar o dispositivo remetente. Mas com os ataques sofisticados de botnets de hoje (especialmente bots baseados em IoT), os invasores nem se preocupam em mascarar o IP do bot. Em vez disso, eles utilizam uma extensa rede de bots não falsificados para sobrecarregar o servidor de destino.

Exemplo de Ataque

Para sobrecarregar outra máquina, basta executar utiliza o utilitário ping para realizar um ataque `ping -f -i 1 <ip_destino>`.

Os parâmetros são os seguintes:

- `-f`: Indica para o ping enviar pacotes com a flag "Don't Fragment"(Não Fragmentar) ativada.
- `-i 1`: Define o intervalo de tempo entre os pacotes de ping como 1 segundo (devido a permissões de máquina tivemos que adiciona-lo.
- `<ip_destino>`: Substitua isso pelo endereço IP do destino desejado para o ataque.

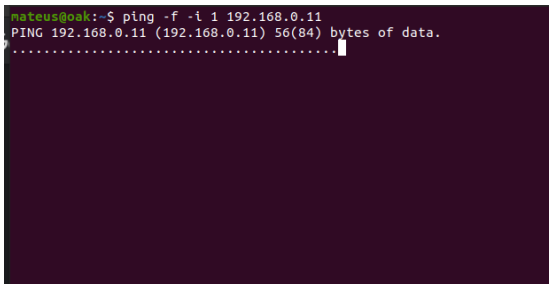

Figura 1 – Comando executado em uma maquina linux

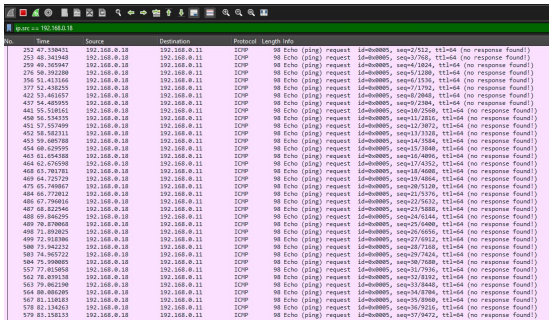

Figura 2 – Monitoramento via Wireshark

ARP Spoofing

O que é ARP Spoofing

ARP Spoofing é uma técnica na qual um invasor envia falsas mensagens ARP (Address Resolution Protocol) para associar seu endereço MAC a um endereço IP legítimo, permitindo assim a interceptação do tráfego destinado a esse endereço.

Como Funciona

Ao enviar falsas mensagens ARP, o atacante consegue enganar outros dispositivos na rede, fazendo com que eles associem o endereço IP do alvo ao seu próprio endereço MAC. Isso permite a interceptação de pacotes destinados ao dispositivo alvo.

Propósito e Características

ARP Spoofing é frequentemente utilizado para realizar ataques de ”Man-in-the-Middle”, nos quais o invasor pode interceptar, modificar ou redirecionar o tráfego entre dois dispositivos sem o conhecimento deles.

Funcionamento no Linux

Ferramentas como ”arpspoof”e ”ettercap”podem ser usadas para realizar ARP Spoofing no ambiente Linux, permitindo que o invasor manipule a tabela ARP para alcançar seus objetivos.

Teoria por Trás do Ataque

A teoria subjacente ao ARP Spoofing reside na vulnerabilidade do protocolo ARP, que não possui mecanismos robustos de autenticação. Isso permite a um invasor enganar os dispositivos na rede sobre as associações entre endereços IP e MAC.

Justificação da Escolha

A escolha do ARP Spoofing destaca a importância de proteger contra ataques de interceptação de tráfego, uma vez que esta técnica permite ao invasor monitorar ou modificar comunicações na rede.

Exemplo de Ataque

Neste exemplo usamos a ferramenta chamada arpspoof, que faz parte de um conjunto chamado dsniff. O dsniff pacote contém vários programas que podem ser usados para lançar ataques MITM.

A arpspoof é uma ferramenta antiga, mas ainda funciona e, por ser tão simples, então para realizarmos o ataque basta usar os comandos:

- arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]: Executando o arpspoof, diremos ao ponto de acesso que o endereço IP do cliente possui nosso endereço MAC, então, basicamente, informaremos ao ponto de acesso que somos o cliente alvo:

- arpspoof -i [Network Interface Name] -t [Router IP] [Victim IP] : Em outro terminal vamos executar o arpspoof novamente e, em vez de dizer ao ponto de acesso que somos o cliente alvo, vamos dizer ao cliente que somos o ponto de acesso, então vamos apenas inverter os IPs. Portanto, ao executar o comando anterior, enganaremos o cliente e o ponto de acesso e deixaremos os pacotes fluírem pelo nosso dispositivo.

Assim que fizermos o ataque, veremos que o endereço MAC do ponto de acesso alvo foi alterado. Nas capturas de tela a seguir, podemos ver que o endereço MAC do ponto de acesso foi alterado de c0-ff-d4-91-49-df para 10-f0-05-87-19-32 , que é o endereço MAC da máquina Kali.

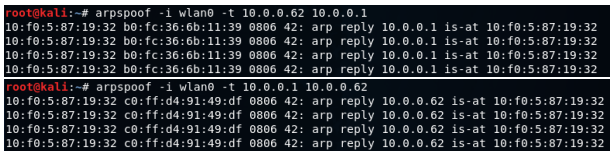

Figura 3 – Executando o ataque

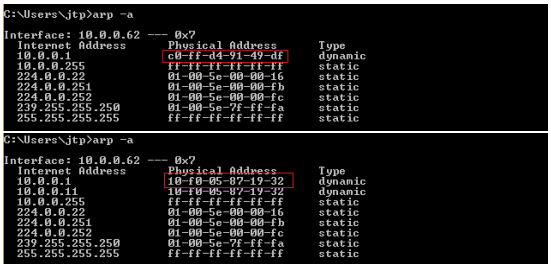

Figura 4 – Antes e depois do ataque

Conclusão

Este relatório fornece uma visão detalhada das técnicas de ataque ICMP Flooding e ARP Spoofing. A compreensão dessas ameaças é crucial para implementar medidas eficazes de segurança de rede. A Parte 2 deste trabalho aborda a nossa implementação de um sniffer de rede simples que faz detecção desses ataques.