Introdução e Ataque DoS ao NDP

Objetivo:

*Este trabalho tem como objetivo explorar e demonstrar um ataque de Negação de Serviço (DoS) direcionado ao **Neighbor Discovery Protocol (NDP)** no contexto do **IPv6**, abordando tanto sua introdução quanto sua implementação prática. O ataque explora vulnerabilidades no processo de **Detecção de Endereço Duplicado (DAD)**, um mecanismo essencial para a configuração automática de endereços IPv6. Ao comprometer esse processo, o ataque impede que dispositivos obtenham **endereços IPv6 válidos**, causando uma negação de serviço e impactando toda a rede.*

*Além disso, serão analisadas as consequências desse tipo de ataque, seu impacto na comunicação da rede e possíveis **mecanismos de mitigação** para proteger infraestruturas contra essa vulnerabilidade. A proposta inclui uma abordagem teórica sobre o funcionamento do **NDP**, sua importância no IPv6, e a demonstração prática do ataque, destacando métodos de detecção e defesa contra essa ameaça.*

Autor: Enzo Arrue Juan Fuso

Faculdade: Fatec São Caetano do Sul

Curso: Segurança da Informação

Introdução

O ataque de Negação de Serviço (DoS) é uma técnica maliciosa utilizada para tornar um sistema, rede ou serviço de computador indisponível para os usuários legítimos, afetando negativamente sua funcionalidade e acessibilidade. O ataque pode ser direcionado a um único serviço ou a toda uma rede, e seu principal objetivo é interromper a operação normal, causando frustração e prejuízos aos usuários e administradores.

Esse tipo de ataque é frequentemente realizado por meio do envio de uma quantidade excessiva de solicitações a um servidor ou dispositivo de rede, sobrecarregando seus recursos e, eventualmente, fazendo com que ele falhe ou seja incapaz de responder a novas requisições. No contexto específico deste experimento, estamos focando em um ataque de DoS que explora vulnerabilidades no protocolo IPv6, especialmente no processo de Detecção de Endereço Duplicado (DAD).

O processo DAD é uma etapa crucial no IPv6, utilizada para garantir que cada dispositivo conectado a uma rede tenha um endereço único. Quando um novo dispositivo tenta se conectar, ele envia mensagens para verificar se o endereço desejado já está em uso. Um atacante pode se aproveitar desse processo, enviando respostas fraudulentas para as solicitações de DAD, fazendo com que o dispositivo acredite que o endereço já está ocupado. Como resultado, o dispositivo não consegue obter um endereço IPv6 válido e, portanto, não consegue se conectar à rede.

O impacto desse ataque pode ser significativo. Dispositivos que não conseguem se conectar podem ser incapazes de acessar recursos essenciais da rede, como servidores, serviços de armazenamento e outros dispositivos de comunicação. Isso pode afetar uma ampla gama de usuários e serviços, resultando em uma interrupção generalizada da comunicação. Além disso, esse tipo de ataque pode ser

particularmente difícil de detectar e mitigar, pois envolve a manipulação de protocolos fundamentais da rede que normalmente operam em segundo plano.

Em resumo, o ataque DoS representa uma ameaça grave à disponibilidade e confiabilidade dos serviços de rede, especialmente em ambientes onde o IPv6 está em uso. A compreensão das vulnerabilidades associadas a esse ataque é essencial para o desenvolvimento de estratégias de defesa eficazes, permitindo que os administradores de rede implementem medidas preventivas e reativas adequadas para proteger suas infraestruturas de comunicação.

Softwares/Ferramentas Utilizados:

Wireshark, VirtualBox (Ambiente disponibilizado já configurado acessar link: https://ipv6.br/pagina/livro-ipv6/ e seguir as orientações abaixo), THC-IPv6 no CORE

Metodologia

A seguir, está descrito o passo a passo do experimento realizado para demonstrar o ataque DoS utilizando a ferramenta THC-IPv6 no CORE:

1. ***Inicialização da Topologia de Rede:***

   Abra o arquivo `3-01-DoS-NA.imn` no CORE, representando uma topologia com três nós (n1Host, n2Host, e n3Faker).

   Inicialize a simulação e verifique as configurações IPv6 nos nós. Eles usarão apenas endereços link-local, sem endereços globais, para simular a rede.

2. ***Execução do Ataque:***

No nó n1Host, execute um comando `ping6` para testar a conectividade com o n2Host:

```
ping6 -c 4 -I eth0 fe80::200:ff:feaa:1
```

No nó n3Faker, inicie a coleta de pacotes utilizando uma ferramenta como tcpdump ou Wireshark.

Execute o comando que inicia o ataque DoS:
`dos-new-ip6 eth0`

Esse comando faz com que o n3Faker responda às solicitações do DAD como se todos os endereços já estivessem em uso, bloqueando novas atribuições.

3. ***Verificação de Falha no DAD:***

No n1Host, reinicie a interface de rede para testar o impacto do ataque:

`ip link set eth0 down`

`ip link set eth0 up`

`ip addr show eth0`

`ifconfig eth0`

O resultado esperado é que o n1Host não consiga obter um endereço IPv6 válido, com o comando `ip addr show eth0` retornando o estado "tentative dadfailed".

4. ***Análise dos Pacotes:***

Use o Wireshark para filtrar pacotes ICMPv6 e analise as mensagens NS (Neighbor Solicitation) e NA (Neighbor Advertisement) trocadas. O ataque DoS manipula essas mensagens para enganar o n1Host, fazendo-o acreditar que seu endereço já está em uso.

5. ***Monitoramento com NDPMon:***

No nó n2Host, utilize o NDPMon para monitorar o tráfego da rede e identificar o ataque:
`ndpmon -i eth0 -v`

O NDPMon detectará o ataque de negação de serviço no processo DAD, gerando logs detalhados do evento.

Explicação

Tabela NDP: Pertence à camada 3 **(Rede)**, pelo qual analisa parâmetros como IP e MAC. Cada dispositivo dentro da LAN possui sua própria **Tabela NDP**. Utiliza multicast. Encapsulamento: Pacote IP

Funcionamento Completo (IPv6):

Início da Comunicação: O Computador 1 deseja enviar uma mensagem ao Computador 2, mas não sabe o endereço MAC dele. Ele só tem seu próprio endereço MAC e IP (IPv6).

Consulta NDP (Neighbor Discovery Protocol): O Computador 1 verifica sua tabela NDP e, ao não encontrar o endereço MAC do Computador 2, envia uma mensagem de multicast NDP para a rede, chamada de *Neighbor Solicitation*. Essa mensagem basicamente pergunta: "Quem tem o IP X? Diga seu endereço MAC". Todos os dispositivos na mesma LAN que estão "escutando" essa solicitação de multicast recebem a mensagem.

Router Solicitation e Router Advertisement: Antes mesmo de enviar mensagens diretamente ao Computador 2, o Computador 1 pode precisar descobrir o roteador na rede, caso esteja tentando se comunicar com um dispositivo fora de sua sub-rede local. Ele envia uma mensagem chamada *Router Solicitation* em multicast para os roteadores na rede, pedindo por informações sobre o roteador. O roteador então responde com uma mensagem *Router Advertisement*, informando sua presença e fornecendo detalhes sobre a configuração de rede, como o prefixo da sub-rede e outras informações importantes.

Resposta do Computador 2: O Computador 2, que tem o IP correspondente, responde com seu endereço MAC, utilizando uma mensagem chamada *Neighbor Advertisement*. Essa resposta é enviada diretamente ao Computador 1 (unicast).

Atualização da Tabela NDP: Após receber a resposta, o Computador 1 atualiza sua tabela NDP, aprendendo o endereço MAC do Computador 2. Da mesma forma, o Computador 2 também atualiza sua tabela NDP, adicionando o endereço MAC e IP do Computador 1.

Aprendizado da Tabela CAM pelo Switch: Quando o switch recebe a mensagem de multicast NDP (*Neighbor Solicitation*), ele aprende o endereço MAC de origem do Computador 1 e a porta pela qual a mensagem chegou. Essa informação é

adicionada à tabela CAM do switch. Quando o Computador 2 responde com o *Neighbor Advertisement*, o switch também aprende o endereço MAC do Computador 2 e a porta associada.

Envio da Mensagem: Agora que o Computador 1 já sabe o endereço MAC do Computador 2, ele pode finalmente enviar a mensagem desejada. Para isso, ele encapsula a mensagem em um quadro Ethernet (Camada 2), com o seu próprio endereço MAC como origem e o endereço MAC do Computador 2 como destino. O quadro é então enviado ao switch.

Encaminhamento pelo Switch: O switch verifica sua tabela CAM para descobrir por qual porta ele deve encaminhar o quadro baseado no endereço MAC de destino (do Computador 2). Ele então envia o quadro pela porta correta, direcionando-o ao Computador 2.

Recepção da Mensagem pelo Computador 2: O Computador 2 recebe o quadro Ethernet, verifica se o endereço MAC de destino é o seu, e, se for o caso, remove o encapsulamento. O pacote IP é processado na camada 3 e, finalmente, a mensagem chega à camada 4 para ser processada pela aplicação responsável

Links Complementares:

Denial of Service- *https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/*

Tabela NDC- *https://www.iana.org/assignments/ipv6-nd/ipv6-nd.xhtml*

Tabela CAM-
https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/5244-

Estudo do Protocolo IPv6- *https://www.ietf.org/rfc/rfc2460.txt*

OBS: *Esse ataque foi extraido do seguinte site:*
https://ipv6.br/media/arquivo/ipv6/file/64/livro-lab-ipv6-nicbr.pdf

As explicações e estrutura apresentada neste relatório foram formuladas por mim, Enzo Arrue, todavia o ambiente de ataque foi disponibilizado pela plataforma IPv6.br.