josif 2024
16ª JORNADA CIENTÍFICA E TECNOLÓGICA
13º SIMPÓSIO DE PÓS-GRADUAÇÃO
DO IFSULDEMINAS
ISSN: 2319-0124
REALIZAÇÃO INSTITUTO FEDERAL Sul de Minas Gerais
APOIO CNPq FAPEMIG

DDOS: o ataque e sua defesa

Thiago A. SANTOS[1]; Matheus G. VILAS BOAS [2]; Helder L. PALMIERI CALDAS [3];

RESUMO

Um ataque DDoS (*Distributed Denial of Service*) é uma tentativa maliciosa de sobrecarregar um serviço online, tornando- o inacessível. Este tipo de ataque explora a infraestrutura de rede e os recursos computacionais do alvo, visando comprometer sua disponibilidade e funcionalidade. Basicamente ele é um ataque de estresse ao alvo devido ao alto número de requisições e fluxo de dados em uma rede fazendo com que ela não suporte tal ação e se dê por *offline*, se tornando uma ameaça significativa em todo o mundo devido a sua potência temível de realmente conseguir derrubar o serviço desejado e causar danos muitas vezes irreparáveis as empresas responsáveis por estes serviços. Também podem ser utilizados para ações de golpes subindo outro serviço semelhante falso na rede assim roubando informações ou coletando dinheiro de usuários do serviço verdadeiro de diversas formas distintas.

Palavras-chave:
DDOS; Ataque de Estresse; Negação de Serviço.

1. INTRODUÇÃO

O ataque DOS, considerado mais simples. A técnica de ataque a redes DOS mais antiga e menos desenvolvida do que o DDOS. Segundo desenvolvedores (CLOUDFLARE, 2024) Um ataque de negação de serviço (DoS) é um tipo de ataque cibernético em que um ator malicioso tem por objetivo tornar um computador ou outro dispositivo indisponível para os usuários a que se destinam, interrompendo o funcionamento normal do dispositivo. É um ataque direcional de fluxo de dados de uma máquina a outra: o atacante utiliza o *hardware* de sua máquina para atacar outra sem ajuda de outros computadores.

O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto (KASPERSKY, 2024). Dessa vez, ele é feito por uma rede de computadores que obedecem às ordens de um computador principal. O computador que dá as ordens é o coordenador desta rede e seus zumbis são computadores infectados por algum vírus geralmente executável, assim fazendo com que eles respondam todas as ordens requisitadas, formando assim uma BOTNET, que são redes de dispositivos de computador sequestradas e usadas para realizar vários golpes e ciberataques. O termo "botnet" é formado pela junção das palavras "robot" (robô) e "network" (rede) (KASPERSKY, 2024b).

[1] Discente de Tecnologia em Redes de Computadores, IFSULDEMINAS – *Campus* Inconfidentes. E-mail: thiago.santos.0060@gmail.com

[2] Docente de Tecnologia em Redes de Computadores, IFSULDEMINAS – *Campus* Inconfidentes. E-mail: matheus.vilasboas@ifsuldeminas.edu.br

[3] Docente de Tecnologia em Redes de Computadores, IFSULDEMINAS – *Campus* Inconfidentes. E-mail: helder.caldas@ifsuldeminas.edu.br

2. FUNDAMENTAÇÃO TEÓRICA

O ataque DOS basicamente é um ataque de negação de serviço, sendo assim seu principal objetivo é derrubar um serviço por um tempo indeterminado abrindo brechas para outros tipos de ataques e ações maliciosas. O hacker ataca diretamente utilizando o poder da máquina de ataque para "derrubar" o serviço que é o alvo do fluxo de dados por ele enviado.

Ele ocorre da seguinte maneira: Quando o atacante inicia seu ataque, sua máquina desenvolve pacotes que servirão para "entupir" a rede assim sobrecarregando o dispositivo alvo fazendo que o mesmo saia fora do ar por causa desse estresse provocado por meio do fluxo de pacotes. Esta técnica era muito utilizada, mas com o aumento da capacidade de processamento dos dispositivos de redes, tem caído em desuso, devido a falta de eficiência de que a máquina atacante realmente consiga derrubar um servidor robusto e preparado, além de ser uma técnica antiga.

Por sua vez, o ataque DDOS é uma evolução do método listado acima tendo as mesmas características mas com uma principal diferença que o torna muito mais eficaz e perigoso fazendo com que ele seja amplamente utilizado nos dias atuais. Sua principal diferença é a utilização de computação distribuída.

O BYOB é um software para a realização de um ataque DDOS. Ele é um software de controle de redes BOTNET que será a rede que obedecerá as ações dadas pelo computador coordenador na mesma. Este software gerencia todos os computadores zumbis (subordinados às ordens do coordenador) pertencentes a rede de ataque. Estes computadores zumbis são muitas vezes infectados através de programas executáveis adquiridos em sites não confiáveis, golpes, e-mail e diversas outras maneiras. Uma vez executado, o computador se torna um escravo de uma rede cedendo seu processamento para a realização de uma ação definida pelo computador administrador.

Uma vez com esta rede pronta e conhecendo o alvo desejado, é realizado um ataque de fluxo de dados intenso ao alvo fazendo com que seu processamento aumente a níveis indesejáveis e que o mesmo acabe *offline* por conta do estresse que ele tentou processar. Desta forma, quando o serviço está fora do ar, o ataque se torna bem sucedido e abre espaço para outros ataques ou golpes virtuais. O PFsense é um sistema de *firewall* gratuito com inúmeras funções que será utilizado para interceptar o ataque com um de seus recursos, sendo descrito segundo a referência, é uma solução de Firewall largamente adotada e uma das mais robustas entre as opções Open Source que substitui com sucesso – na maioria das necessidades - os principais firewall comerciais existentes no mercado como CheckPoint, Sonicwall, Juniper, entre outros (4LINUX, 2024).

Já o IPS - Um sistema de prevenção de intrusão (IPS) monitora o tráfego da rede em buscade possíveis ameaças e as bloqueia automaticamente, alertando a equipe de segurança, terminando conexões perigosas, removendo conteúdo malicioso ou acionando outros dispositivos de segurança (IBM, 2024), assim sendo um protocolo de rede que visa buscar formas de mitigar ataques de forma automáticas utilizando um banco de assinaturas conhecidas de ataques e as comparando com o pacotes da rede em que ele está implementado.

3. MATERIAL E MÉTODOS

Neste trabalho foram utilizados os seguintes equipamentos: 3 computadores sendo um para ser o administrador da rede de ataque, um para ser um zumbi e o outro para receber o ataque. Eles foram gerenciados por uma RB750 da Mikrotik, que é basicamente um switch gerenciável em menor tamanho com apenas 5 portas fast ethernet e utilizando o sistema RouterOS proprietário da Mikrotik, todos interligados por cabo de rede. Os computadores serão descritos em mais detalhes a seguir:

Computador 1: Administrador. Foi utilizado um notebook Acer com BYOB instalado sendo ele o "centro" de toda a rede boot que será composta por outro computador boot e também responsável por gerar os executáveis de infecção e assim poder realizar o ataque.

Computador 2: BOT. Para este computador foi utilizado apenas seu sistema operacional instalado para ceder seu hardware de escravo para o ataque. Apenas o executável foi utilizado para conectar este computador a rede de bots.

Computador 3: Servidor de página web com firewall, IPS e IDS embutidos. Já este PC foi instalado o mesmo sistema operacional Linux e adicionado uma página web que pode ser acessada pela rede para que sofra o ataque desejado.

Foi utilizado o Mikrotik RB750. Este basicamente é um mini switch da mikrotik capaz de realizar todas as configurações que um switch maior faz e tendo 5 portas de rede para conexão dos 3 computadores do projeto. Ele foi responsável por interligar os computadores utilizando o mínimo de configurações possíveis e criar a rede de comunicação entre eles.

O sistema operacional escolhido para ser utilizado em todos os computadores foi o Linux Lite devido ao seu baixo uso de memória tanto RAM como ROM pois os computadores não dispunham de tantos recursos. Também foi utilizado o Winbox, que é o programa responsável por abrir as interfaces gráficas da RB virtualizado por um recurso do Linux para instalação e utilização de programas de Windows chamado WINE. Desta forma, foi possível realizar a programação. O sistema de ataque BYOB foi obtido via GitHub, o qual é responsável por gerar executáveis de infecção para computadores zumbis e administrar a rede de bots formada para o ataque.

4. RESULTADOS E DISCUSSÃO

Até o momento foram implementados os 3 computadores citados ao longo do texto - o administrador da BOTNET, o computador zumbi e o servidor WEB que será alvo do ataque. Todos estão utilizando o Sistema Operacional Linux Lite.

O computador administrador está com o software BYOB implementado e funcionando, e o computador zumbi está infectado com o executável que cede seu hardware a rede de bots. O *switch* está configurado com um DHCP para o comunicação de todos os *hosts* e permitindo com que o ataque seja realizado.

O computador servidor está com o site web implementado para que seja alvo de requisição do ataque de rede, mas o *firewall* ainda não foi implementado para "barrar" as requisições dos dois outros computadores.

Espera-se que com o trabalho possa-se esclarecer questões sobre este ataque tão antigo e comum, mas que possui pouco conhecimento por parte da população de como é feito em parte técnica e como prejudica, afeta de forma geral uma rede e principalmente como ela funciona.

5. CONCLUSÃO

O DDOS além de uma técnica maliciosa de ataque, pode ser utilizada para estudos, teste de reação de rede e muito mais. Como é fácil compreender este tipo de ataque, entende-se melhor o seu risco para a Internet e todas as empresas que atuam no mercado, sendo uma das principais formas de abrir portas para outros tipos de técnicas e golpes utilizando o nome de empresas como o que ocorre em sites falsos enquanto o original se encontra *offline*.

De forma geral, o trabalho proposto demonstrou as partes técnicas de um ataque tão comum realizado contra a sociedade, buscando um outro lado de segurança em redes de computadores com as técnicas utilizadas de formas maliciosas para a realização de atos ilegais. Toda a parte de configuração e técnica abordada no artigo busca levar esclarecimento ao leitor de forma simples, até mesmo o ajudando a combater esta técnica.

REFERÊNCIAS

CLOUDFLARE. Cloudflare, 2024. Como evitar ataques DDoS | Métodos e ferramentas. Disponível em:< https://www.cloudflare.com/pt-br/learning/ddos/how-to-prevent-ddos- attacks/#:~:text=Um%20ataque%20de%20nega%C3%A7%C3%A3o%20de,por%20longos%20per%C3%ADo dos%20de%20tempo. > Acesso em: 9 ago. 2024

IBM, Ibm. 2024. SISTEMA DE PREVENÇÃO DE INTRUSÃO. Disponível em:< https://www.ibm.com/br- pt/topics/intrusion-prevention- system#:~:text=Um%20sistema%20de%20preven%C3%A7%C3%A3o%20de%20intrus%C3%A3o% 20(IPS)%20monitora%20o%20tr%C3%A1fego,acionando%20outros%20dispositivos%20de%20segu ran%C3%A7a. > Acesso em: 10 ago. 2024

KASPERSKY. Kaspersky, 2024. O QUE SÃO ATAQUES DE DDOS? Disponível em:< https://www.kaspersky.com.br/resource-center/threats/ddos-attacks > Acesso em: 9 ago. 2024.

KASPERSKY. Kaspersky, 2024. O QUE É BOTNET? Disponível em:< https://www.kaspersky.com.br/resource-center/threats/botnet-attacks > Acesso em: 15 ago. 2024

4LINUX. 4Linux, 2024. O QUE É PFSENSE? Disponível em:< https://4linux.com.br/o-que-e-pfsense/ > Acesso em: 15 ago. 2024