Contra-atacando ataques do tipo Ping Flood

Gabriel Vaz de Souza e Pedro Fratini Chem

[1]Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul
Porto Alegre – RS – Brasil

{gabriel.vaz, pedro.chem}@edu.pucrs.br

Resumo. *Este trabalho apresenta uma técnica de segurança utilizando socket raw para contra-ataque de ataques do tipo ping flood usando técnicas como "IP spoofing"e "Distributed Denial of Service". Seu desenvolvimento é apresentado em detalhes, permitindo uma reprodução do mesmo cenário. Também é apresentada uma simulação do contra-ataque e feita uma análise de seu comportamento, comentando sobre seus respectivos pacotes trafegados.*

1. Introdução

Na área de redes de computadores, aspectos como a segurança dos dados trafegados e a garantia de estabilidade do serviço, são extrema importância para o sistema. Com o avanço da tecnologia, e com ela, o aumento do registro de informações online, observa-se uma crescente necessidade de explorar medidas que enfrentem ataques maliciosos e garantam a segurança de ambientes virtuais.

Este relatório tem como objetivo documentar o processo de desenvolvimento e simulação de um contra-ataque a ataques do tipo ping flood, utilizando uma topologia de rede criada no software "Core Gui". O ataque ping flood trata-se quando um atacante ou agente malicioso envia uma série de comandos pings para uma máquina destino, em um intervalo muito curto de tempo, fazendo com que a máquina alvo sofra instabilidade ao tentar responder todos os comandos pings. Este ataque é conhecido como "Denial of Service"e pode ser escalado a "Distributed Denial of Service"quando temos múltiplas máquinas atacando um mesmo alvo.

O presente relatório está dividido nas seguintes seções: Desenvolvimento, onde é apresentado as características da topologia e logica utilizada; Experimentos, onde é tratado sobre a execução do contra-ataque; Conclusão, que explica os resultados obtidos com os experimentos e discorre de maneira geral sobre o desenvolvimento do trabalho.

2. Desenvolvimento

Para a criação da topologia, foram utilizados 1 roteador, 2 switches e 6 hosts, sendo 1 host identificado como vítima do ataque, 1 como atacante e outros 3 como ajudantes, para auxiliar no contra-ataque. Os endereços de cada máquina foram atribuídos de forma automática. A Figura 1 apresenta a topologia de rede criada.

Para a elaboração do código de contra-ataque ao ping flood, foi tido como maior desafio, identificar quando uma máquina estava de fato realizando um ataque ping flood. Primeiramente é necessário estipular um intervalo de tempo e um limite de mensagens para que possamos diferenciar um ataque ping flood de um comando ping normal. No código desenvolvido, estipulamos um limite de 1 segundo para uma quantidade de 100

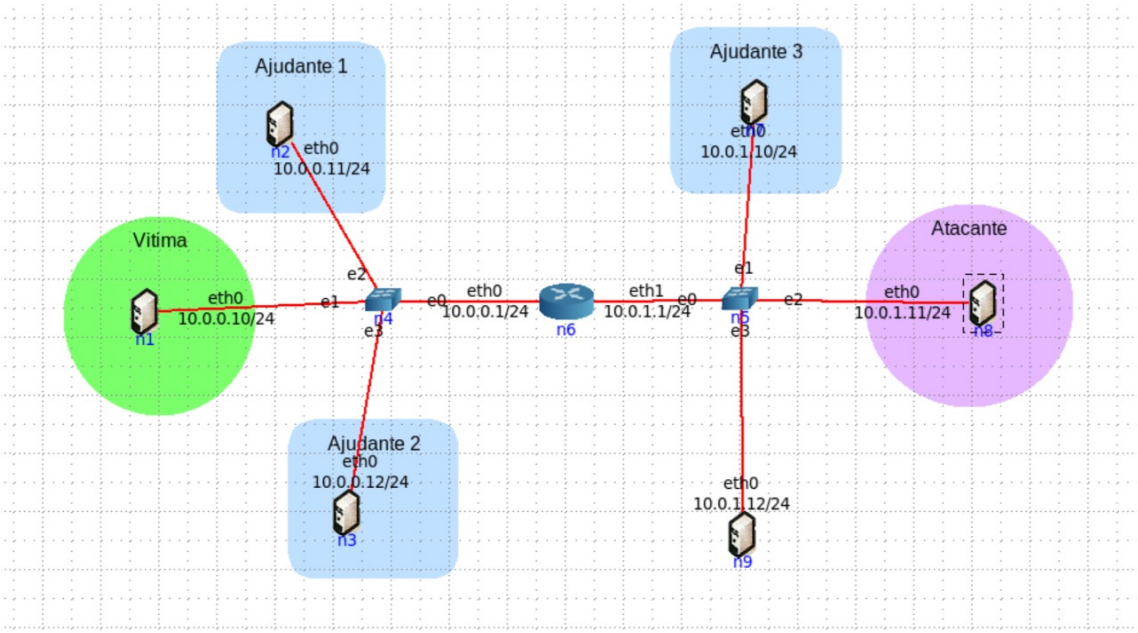

Figura 1. Organização da Rede

comandos ping, ou seja, um envio superior ao de 100 comandos ping em um intervalo de 1 segundo é considerado um ataque ping flood. Para o controle, no código, desta etapa, foi utilizado a estrutura de dados dicionário, onde cada chave corresponde a o endereço IP da máquina que enviou o comando ping e cada valor corresponde a uma fila de tamanho 100. Nesta fila é armazenado o tempo atual do recebimento de cada requisição. Assim, podemos fazer um controle, ao verificar que a fila de um endereço IP está cheia, conferindo se o tempo da requisição da primeira entrada da fila somado a 1 segundo, é maior que o tempo atual, se for, identificamos um ataque ping flood.

Ao identificar o ataque, são montadas, através da biblioteca “socket”, requisições ICMP e enviadas para as máquinas conhecidas da rede, exceto pela máquina atacante. Ao montar a requisição, é realizado a técnica de IP spoofing,, ao alterar o endereço IP da máquina vítima pela atacante, para que as máquinas que recebem estas requisições respondam a requisição ICMP para o atacante, sobrecarregando-o.

As partes do código de controle de recebimento de requisições ICMP e envio já estavam disponíveis, e foram reaproveitadas com leves mudanças. Uma das mudanças, de maior importância, foi a adição de uma verificação para não processar requisições ICMP com endereço IP destino diferente do IP da máquina host. Esta adição é necessária, pois a máquina vítima passou a realizar IP spoofing, de modo que pacotes com endereços alterados passem a circular por sua rede.

3. Experimentos

Para realização dos experimentos, foi utilizado o software ”Core Gui”, que permite a simulação de múltiplas máquinas em um ambiente controlado. Para a elaboração do software foi utilizado a biblioteca socket da linguagem “Python”, possibilitando a análise e envio de pacotes pela rede.

Após realizada a configuração da topologia no Core Gui, e implementado o código

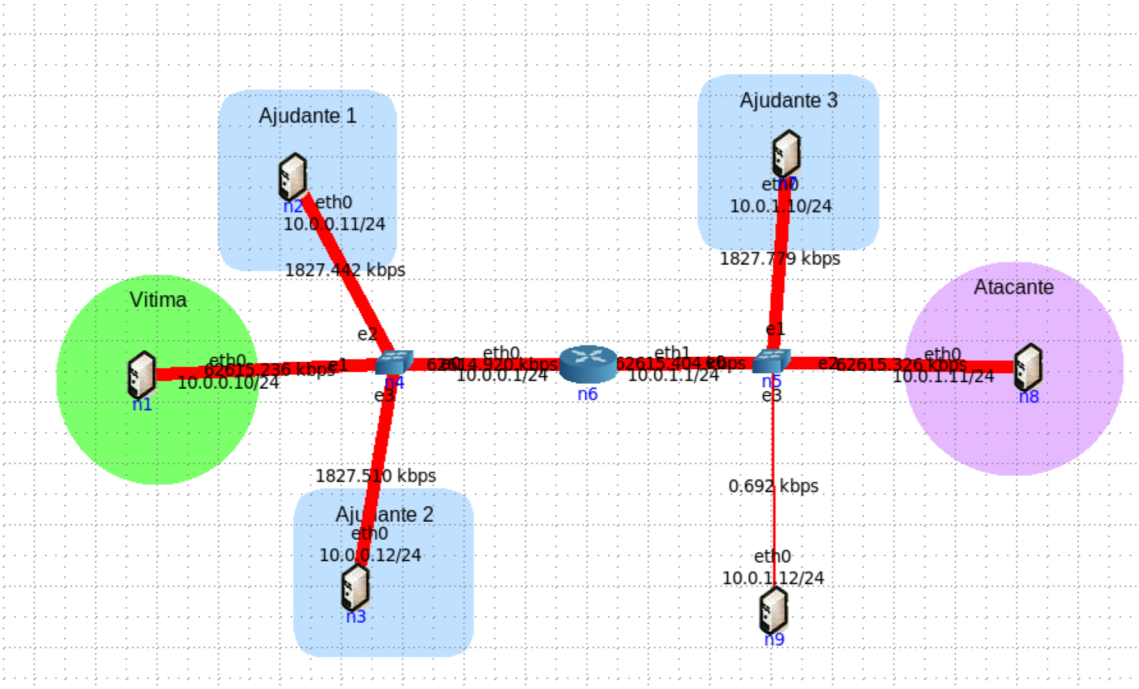

Figura 2. Organização da Rede

para execução na linguagem Python, foram realizados alguns testes de ataque e contra-ataque no ambiente simulado. A Figura 2 ilustra a realização de um dos testes. Para sua implementação, primeiramente, foi-se executado o código criado "PingFloodCounterAttack.py". Após, foi executado o comando ping nas máquinas "Ajudante 1", "Ajudante 2"e "Ajudante 3"com a máquina "Vítima"como destino, esta etapa é necessária para que a vítima tenha conhecimento das outras máquinas. E finalmente, foi executado um comando ping flood na máquina "Atacante"tendo a máquina Vitima como destino.

Foi observado, conforme esperado, que a máquina vítima, ao receber um volume alto de tráfego do atacante, passa a enviar um volume alto de tráfego para suas máquinas ajudantes, que por sua vez, encaminham o tráfego para o atacante. Podemos concluir que a máquina vítima, de fato, estava contra-atacando o ping flood ao realizar outro ping flood em suas máquinas ajudantes, se passando pela máquina atacante.

4. Conclusão

Finalizada as etapas de desenvolvimento e experimentos, obtivemos exito em nosso objetivo de realizar o contra-ataque a ataques do tipo ping flood. Também foi possível perceber na prática a importância e a eficácia da técnica, além de expandirmos nosso conhecimento sobre técnicas de ataque e contra-ataque em redes.