Gabriel Mazurco Ribeiro RA: 1611014

Lucas Bueno RA: 142441

Escreva um ensaio sobre ataques de amplificação (amplification attacks), ou seja, ataques que usam um servidor (vítima) para gerar mais dados que os recebidos do atacante original. Tais ataques são arquitetados de tal forma que não retornam os dados ao atacante, mas a outra vítima, com a intenção de causar Dos.

Um ataque reflexivo distribuído de negação de serviço (DRDoS) é uma variação do ataque distribuído de negação de serviço (DDoS) que se utiliza de serviços UDP acessíveis publicamente, bem como de fatores de amplificação de largura de banda, para sobrecarregar o sistema atacado com tráfego UDP.

Recentemente, certos protocolos UDP foram notados por apresentarem respostas a certos comandos muito mais longas do que as requisições iniciais. Onde antes os atacantes eram limitados linearmente pelo número de pacotes enviados diretamente ao alvo para conduzir o ataque DoS, agora um único pacote pode gerar dezenas ou centenas de vezes mais largura de banda em sua resposta. Isto é chamado de ataque de amplificação, e quando combinado com um ataque reflexivo de negação de serviço em larga escala, torna-se relativamente fácil conduzir um ataque distribuído de negação de serviço.

Não é fácil detectar um ataque DRDoS pois devido ao uso de vários e confiáveis servidores que provêm serviços UDP. Para a vítima, meios tradicionais de mitigação de ataques DoS podem ser usadas. Administradores de rede de um destes serviços exploráveis, devem buscar por respostas demasiadas grandes para um IP específico. Isso pode indicar que o atacante está usando seu serviço em um ataque DRDoS.

Para reduzir a efetividade da amplificação primeiro devemos fazer com que os provedores de serviço de internet rejeitem qualquer trafego UDP com endereços forjados. Esta alteração pode reduzir substancialmente o potencial da maioria dos ataques do tipo DDoS. Dessa forma, recomendamos fortemente a todos os administradores de redes a executar a filtragem de pacotes de entrada na rede, se possível. Note que isso não irá

proteger explicitamente um provedor de serviços UDP de ser explorado em um DRDoS, já que todos os provedores devem usar esta filtragem para eliminar a ameaça completamente.