IDENTIFICAÇÃO DE CONJUNTOS DE DADOS COM ATAQUES DDoS ROTULADOS: VETORES DE ATAQUE E VULNERABILIDADES DOS PROTOCOLOS

Julia Cristina Moreira da Silva, Alison Fracasso Savi, Anna Patrícia Borges, Camila Soares Borges, Guilherme Lisboa Rebellatto, Vítor Magro Krüger, Mateus Pelloso

Modalidade: Projeto de pesquisa
Área temática: Ciências Exatas e da Terra

RESUMO

Em virtude da contínua expansão e das características abertas da Internet, profissionais da área de segurança cibernética, singularmente administradores de redes, desenvolvedores e pesquisadores, demandam conhecer e reconhecer as técnicas utilizadas por atacantes, que promovem a exploração de vulnerabilidades na rede com a finalidade de tornar indisponíveis os serviços de Internet aos usuários legítimos. Esse ataque, é conhecido como DDoS (Ataque Distribuído de Negação de Serviços). O DDoS tem como principais alvos os enlaces de comunicação, servidores e serviços de rede. Entre as técnicas mais conhecidas estão a falsificação (spoofing) de pacotes e inundação (flooding) requisições. Essas estratégias, têm como finalidade causar o retardo no processamento e consequente esgotamento dos recursos disponíveis, como memória, processamento e banda de rede. A ocorrência de ataques DDoS está em crescimento constante e, por isso, se faz necessário compreender os vetores de ataques utilizados, bem como as ferramentas aplicadas para implementá-los. Com base nesse conhecimento, torna-se possível evitar ou mitigar as consequências resultantes de tal ataque. Dessa forma, proporcionar maior disponibilidade dos serviços de Internet aos seus usuários legítimos. Os ataques DDoS baseados em falsificação de pacotes ou inundação de requisições, somente são possíveis de serem realizados devido às características abertas dos protocolos de redes de computadores. Os protocolos foram implementados com a finalidade de proporcionar interoperação e comunicação entre componentes de redes de diferentes fabricantes por meio da padronização. Ao mesmo tempo que é uma característica necessária para a expansão da Internet, também é a principal vulnerabilidade. Dessa forma, é necessário mostrar os protocolos associados às suas respectivas características e vulnerabilidades. Assim, esse estudo identificou os vetores de ataque DDoS mais evidentes e utilizados na Internet, sendo eles principalmente vulnerabilidades inerentes aos protocolos de redes das camadas de transporte e aplicação, assim como suas variantes, a exemplo do TCP, TCP ACK, TCP SYN, TCP SYN-ACK, TCP RST e TCP SYN-PUSH, UDP, HTTP, NTP, DNS e ICMP. Além disso, foram identificados também scripts e ferramentas de ataque, tais como T-50, PentMenu, Hping, LOIC, TFN2K, Golden Eye, Slowloris e XerXes. Os scripts e ferramentas de ataque identificadas foram testadas em ambiente controlado, utilizando máquinas virtuais com os sistemas operacional Linux e

Windows. Os experimentos realizados com as ferramentas e scripts evidenciaram as principais características e dinâmica de funcionamento das mesmas durante a execução de um ataque nesse ambiente simulado. Durante esse experimento prático foram identificados os tipos de ataque que cada uma das ferramentas implementa, as plataformas compatíveis, bem como respectivas interfaces de operação. Esta pesquisa identificou inúmeros vetores de ataques e respectivas características, associado às ferramentas que os implementa, além da dinâmica e funcionamento das mesmas. Dessa forma, em trabalhos futuros, as próximas etapas desta pesquisa, utilizará um recorte dos vetores ataques mais evidentes na Internet. Estes serão analisados com mais especificidade com a finalidade de identificar detalhes das características de adulterações internas aos pacotes de dados no fluxo de dados da rede. Tais características são conhecidas como flags e são identificáveis em ataques DDoS baseados no vetor TCP. Para tal, serão realizados novos testes em um ambiente de redes físico ou virtual, isolado da Internet. Este experimento proporcionará a visualização do comportamento da rede associado a análise das consequências desses ataques quando direcionados a alvos reais (enlaces, servidores e/ou serviços) específicos. Assim sendo, será possível avaliar o impacto causado pela sobrecarga no fluxo da rede bem como apontar técnicas e ferramentas de mitigação e prevenção desses ataques.

Palavras-Chave: Ataques, DDoS, Internet, Redes de Computadores, Segurança.