XIV CICTED
CONGRESSO INTERNACIONAL DE CIÊNCIA, TECNOLOGIA E DESENVOLVIMENTO

ATAQUES DE NEGAÇÃO DE SERVIÇO E SUA EFETIVIDADE NOS TEMPOS MODERNOS

ODS (9)

Guilherme de Almeida Mormito (Universidade de Taubaté)
Alison de Oliveira Moraes (Universidade de Taubaté)
Moisés José dos Santos Freitas (Universidade de Taubaté)

Ataques *Distributed Denial of Service* (DDoS) representam uma crescente ameaça na era digital, causando enormes prejuízos para empresas e instituições. Este tipo de ataque tem como principal objetivo sobrecarregar os recursos de um alvo, sejam servidores, redes ou aplicações, causando indisponibilidade ou afetando parcialmente as funcionalidades do serviço, prejudicando o acesso de usuários legítimos. A interrupção de um serviço não só acarreta em prejuízos financeiros, mas também causa danos diretos à reputação do alvo, pois todas as empresas dependentes de um serviço são afetadas com a queda do mesmo. Os ataques em questão podem atingir uma escala ainda maior quando o alvo é um serviço essencial, por exemplo: companhias de água, companhias de luz, sistemas da área de finanças, sistemas da área de saúde, sistemas de segurança e sistemas governamentais. O objetivo desta pesquisa é desenvolver uma ferramenta em Python, que seja capaz de simular e executar diferentes métodos de ataque de negação de serviço, utilizando bibliotecas de manipulação e envio de pacotes de rede, como Scapy e *Requests*. Após a realização dos ataques, os dados referentes ao uso de processamento do servidor serão coletados para análise e discussão da efetividade de cada método. Estudo de caso e pesquisa experimental são as principais metodologias para o desenvolvimento deste trabalho, analisando o funcionamento de métodos famosos de ataque a fim de melhorar o código desenvolvido e realizando ataques em ambientes virtuais isolados. Outra importante metodologia que permitiu um grande avanço no trabalho foi a pesquisa bibliográfica, possibilitando um maior aprofundamento técnico e consequentemente permitindo um desenvolvimento mais preciso das ferramentas. Espera-se que a ferramenta permita simular cenários de ataque, auxiliando na robustez de redes e criação de mecanismos de defesa. Atualmente este trabalho se encontra em fase de desenvolvimento, mas apresenta resultados significativos, contando com três modelos de ataque (SYN *Flood*, UDP *Flood* e HTTP *Flood*), parametrização da potência do ataque, e medições quantitativas dos impactos de cada modelo no desempenho do servidor alvo.

Palavras-chave: *Denial of Service*, *Distributed Denial of Service*, DoS, DDoS.