ATAQUES DE NEGAÇÃO DE SERVIÇO: IMPACTOS, TÉCNICAS E ESTRATÉGIAS DE MITIGAÇÃO

Matheus Vinícius GALICCIOLLI*
José Paulo CODINHOTO**

RESUMO

Introdução: Os ataques de negação de serviço (DoS - Denial of Service), especialmente os distribuídos (DDoS - Distributed Denial of Service), têm como objetivo tornar um website ou serviço online indisponível por meio da sobrecarga de pacotes direcionados ao servidor, geralmente originados de uma rede de botnets (múltiplos computadores infectados). **Objetivo:** Este artigo tem como objetivo analisar o funcionamento dos ataques DoS/DDoS, suas consequências, as principais técnicas ofensivas envolvidas e as formas de monitoramento voltadas à identificação desse tipo de ataque. **Metodologia:** A metodologia utilizada baseou-se em revisão bibliográfica, com levantamento e análise de dados sobre o tema, identificando características relevantes e recorrentes desses ataques. Foram também realizados testes experimentais em ambiente controlado, utilizando ferramentas como hping3 e Slowloris em um servidor Apache executado sobre o Ubuntu Server, com o intuito de observar comportamentos relacionados a alto tráfego, latência e anomalias com o uso de ferramentas como tshark e tcpdump. Todas as etapas foram conduzidas seguindo princípios éticos e de conformidade. **Resultados:** A análise e os testes realizados em ambiente isolado permitiram constatar a elevada eficiência dos ataques contra servidores de pequeno porte. Verificou-se que a sobrecarga de pacotes resulta em rápida indisponibilidade do serviço, evidenciando a vulnerabilidade de sistemas sem camadas adequadas de proteção. Além disso, foi possível identificar padrões de tráfego que podem ser utilizados em processos de monitoramento e detecção, contribuindo para o desenvolvimento de estratégias de mitigação mais eficazes. **Conclusão:** Os ataques DoS/DDoS têm apresentado crescimento constante ao longo do tempo, sendo utilizados de forma cada vez mais eficiente para comprometer a disponibilidade de serviços na internet, principalmente em servidores com ambiente de menor capacidade e infraestruturas vulneráveis. A análise realizada reforça a necessidade da adoção de mecanismos de monitoramento, detecção e mitigação eficazes, a fim de garantir maior resiliência e disponibilidade dos sistemas.

Palavras-chave: ataques; DoS; segurança da informação; monitoramento; mitigação.

* Discente do Curso de Informática para Internet da Etec de Santa Fé do Sul, SP. matheusviniciusgali05@gmail.com
** Orientador, Mestre, Docente do Centro Universitário de Santa Fé do Sul, SP- Unifunec.. codinhoto92@gmail.com