XI MIC - Projeto de Pesquisa - Ciências Exatas e da Terra

# MAPEAMENTO DAS CARACTERÍSTICAS DO PROTOCOLO TCP EXPLORADA POR ATAQUES DDoS

*Vitor Matheus Valandro da Rosa (vitormateusd@gmail.com)*

*Julia Cristina Moreira da Silva (julia.cmoreiras@gmail.com)*

*Vítor Magro Krüger (vitormkruger@outlook.com)*

*Anna Patrícia Borges (annaborges1115@gmail.com)*

*Matheus Zuchi Balbinot (matheusbalbinotzuchi@gmail.com)*

*Jucian Kauê Decezare (Jucian_decezare2015@hotmail.com)*

*Mateus Pelloso (mateus.pelloso@ifc.edu.br)*

Com a expansão e a democratização do acesso à tecnologia nas últimas décadas, a Internet e os serviços de comunicação se tornaram alvos cada vez mais comuns de atividades maliciosas. O número de dispositivos e serviços vulneráveis a ataques cibernéticos cresce de maneira exponencial, graças a ascensão dos meios de comunicação e da rede IoT, sendo necessária a compreensão dos mecanismos e vetores empreendidos nessas violações para tornar as redes mais seguras. Nesse sentido, os Ataques Distribuídos de Negação de Serviços (DDoS), ganharam notoriedade na sociedade devido à agressividade e aos danos causados por esses ataques quando bem sucedidos, assim como pela variabilidade de métodos. Esses ataques podem explorar diversas especificidades e vulnerabilidades dos protocolos de comunicação de rede - em especial do protocolo TCP, atuante na camada de transporte, que é utilizado para a transmissão de informações na internet - com a finalidade de comprometer e/ou interromper os serviços disponibilizados pelo

alvo e intermediários. Inicialmente, a internet foi elaborada para ser funcional e oferecer desempenho no atendimento a necessidade de interconexão entre dispositivos, o que tornou a segurança na sua criação e construção um elemento secundário. Os problemas de segurança envolvendo redes de computadores e a internet só começaram a aparecer significativamente décadas depois, quando era tarde demais para repensar os protocolos que já eram utilizados em larga escala. O principal exemplo é o conjunto de protocolos TCP/IP que assume que todos os usuários conectados não têm nenhuma intenção maliciosa, o que não se reverbera com ênfase quando se analisa o cenário de usuários atual. Dessa forma, essa pesquisa buscou mapear as características do protocolo TCP que são exploradas para a realização de ataques DDoS, devido a sua importância no contexto da intercomunicação e a recorrência com a qual o protocolo é utilizado. Para a obtenção desse conhecimento, foram realizadas, ao longo do ano, pesquisas bibliográficas, em teóricos da ciência da computação com ênfase em redes de computadores, assim como em artigos científicos, junto a experimentos empíricos em ambiente controlado, utilizando máquinas virtuais como Linux e Metasploitable, a fim de consolidar e embasar a base teórica para a diferenciação desses fenômenos tecnológicos. Assim, este estudo foi capaz de identificar três principais variações dos Ataques DDoS TCP: TCP ACK, TCP SYN E TCP SYN-ACK, todos incidentes na etapa de estabelecimento de conexão do protocolo entre duas máquinas, conhecido como Three-Way-Handshake, que visa garantir a inicialização da transmissão de dados. A diferenciação entre os três tipos de ataque ocorreu pela análise de três fatores principais: o alvo, a existência de intermediário (que acarreta na origem do pacote malicioso) e as flags presentes no pacote, a fim de se tornar possível, através da aferição desses parâmetros, a identificação do ataque ocorrido na rede. Ainda assim, existe a necessidade de expandir a pesquisa, identificando novos conjuntos de dados com a finalidade de evidenciar outras características dos ataques DDoS baseados na pilha de protocolos TCP/IP.