MAPEAMENTO DE CONJUNTOS DE DADOS CONTENDO ATAQUES DDOS

Ana Caroline Bonatto[1], Matheus Zuchi Balbinot, Jucian Kauê Decezare, Alison Fracasso Savi, Anna Patrícia Borges, Willyan Paproski Bueno, Heitor Scalco Neto, Mateus Pelloso[2]

Os ataques cibernéticos, especialmente ataques distribuídos de negação de serviço, ou popularmente conhecidos como ataques DDoS, estão em constante evolução, tanto em sua incidência quanto no aprimoramento dos métodos utilizados. Por esse motivo está se tornando cada vez mais desafiador detectar e prevenir esses ataques. O principal objetivo de um ataque DDoS é provocar a instabilidade ou ainda a completa interrupção de serviços disponíveis na Internet para seus usuários legítimos. Em um cenário onde uma falha pode afetar a credibilidade de algumas organizações e gerar prejuízos significativos, o estudo e aprendizado sobre esses ataques se faz crucial. Para auxiliar nesses estudos, pesquisadores e empresas monitoram o tráfego da rede a fim de capturar os dados e armazená-los nos chamados conjuntos de dados. Dessa forma, diversos pesquisadores ao redor do globo buscam compreender mais sobre esse evento. Dentre os principais aspectos considerados estão: como identificar, como minimizar ou prevenir tais ataques. Assim sendo, este projeto está organizado em tarefas com a finalidade de compreender a dinâmica do comportamento da rede de dados quando sob ataque. Para tal, foram identificados traços de fluxos de redes que contém registros de ataques DDoS. Esses registros são disponibilizados por instituições como universidades e/ou empresas de forma pública. A seleção dos conjuntos de dados ocorreu com base em uma ampla e extensa pesquisa de artigos relacionados ao tema, observado assim os conjuntos mais discutidos pelos pesquisadores da área. A partir dessa identificação, os fluxos estão em fase de análise exploratória em que serão visualizadas as características de cada um dos conjuntos de dados. Diante disso, serão identificados extensão, quantidade e tamanho de pacotes, timezone, data e horário de início e fim do fluxo, taxa de transmissão de pacotes, informações referentes à captura e ao formato do registro dos dados. Além disso, os dados relativos aos tipos de ataques contidos nos conjuntos de dados serão identificados em etapa posterior, conforme previsto no projeto. Essa fase contempla a identificação dos vetores e respectivas abordagens utilizadas pelos invasores, bem como a visualização das fases do ataque, como por exemplo, o momento da sobrecarga da rede. Dessa forma, as informações obtidas serão compiladas, com o intuito de, posteriormente, fazer a sumarização dos conjuntos de dados, e esta, disponibilizada por meio da elaboração de relatórios, resumos e/ou artigos científicos. Assim, o projeto contribui para comunidade acadêmica e para a sociedade, buscando apresentar as características, o funcionamento e as técnicas utilizadas pelos atacantes. A exposição desse conhecimento permite que organizações possam detectar, mitigar ou prevenir potenciais prejuízos resultantes de ataques DDoS. Este projeto conta com suporte institucional e financeiro do Instituto Federal Catarinense campus Concórdia, por meio do edital de pesquisa registrado sob o número 19/2021.

Palavras-chave: Ataques, Cibersegurança, DDoS, Redes de Computadores.

[1] Autor para correspondência: anacaroline.bonattto@gmail.com
[2] Orientador