ESTUDO COMPARATIVO DE FRAMEWORKS DE PENTEST: METASPLOIT E SLIVER

Pedro Cézar Silva Ferreira[1]
[1]Escola de Engenharia Elétrica, Mecânica e de Computação,
Universidade Federal de Goiás,Goiânia, Brazil
(pedrocezar@discente.ufg.br)

Resumo: A crescente sofisticação de ameaças cibernéticas tem impulsionado o desenvolvimento e a adoção de frameworks dedicados a testes de penetração (pentest), ferramentas essenciais para a avaliação proativa da segurança de sistemas e redes. Este trabalho propõe um estudo comparativo entre dois frameworks de pentest amplamente utilizados: o Metasploit Framework, consolidado como referência na área há mais de duas décadas, e o Sliver, uma plataforma de comando e controle (C2) de código aberto mais recente, desenvolvida originalmente para operações de red team. A investigação busca analisar sistematicamente as capacidades, limitações e características técnicas de cada framework sob critérios relevantes para operações ofensivas controladas, incluindo geração e gerenciamento de payloads, suporte a protocolos de comunicação, mecanismos de evasão de soluções de segurança, facilidade de uso e extensibilidade. A metodologia adotada combina análise documental com experimentação prática em ambiente isolado, garantindo reprodutibilidade e controle das condições de teste. A motivação do trabalho reside na escassez de comparações rigorosas e atualizadas entre ferramentas de pentest na literatura acadêmica brasileira, especialmente considerando o surgimento de alternativas modernas ao Metasploit. Compreender as diferenças funcionais e operacionais entre essas plataformas é relevante tanto para profissionais de segurança ofensiva quanto para equipes de defesa que buscam antecipar técnicas utilizadas por adversários reais. Espera-se que os resultados orientem a escolha de ferramentas em contextos específicos de avaliação de

segurança e contribuam para a formação técnica na área de cibersegurança.

Palavras-chave: pentest; segurança ofensiva; Metasploit; Sliver; red team.