POR DENTRO DO ATAQUE: UM ESTUDO DA HONEYPOT COWRIE

VII Encontro de Iniciação Acadêmica

Joao Batista Andrade dos Santos, Alana Martinho dos Santos, Joao Henrique Goncalves Medeiros Correa

Honeypots são ferramentas que funcionam como uma armadilha para os criminosos virtuais, simulando um sistema operacional real com falhas de segurança propositais a fim de coletar informações sobre seus padrões de ataque. O uso dessas ferramentas é de extrema importância, permitindo desenvolver defesas contra os ataques realizados nas honeypots, principalmente os ataques de dia zero. Este trabalho tem como objetivo a instalação, configuração e aprofundamento das funcionalidades de uma honeypot. Especificamente, foi escolhida a honeypot Cowrie, classificada como honeypot de média interação. A ferramente Cowrie visa coletar informações de ataques de força bruta, o mais básico e porta de entrada para os demais ataques, de DDoS (Ataque de negação de serviço) ou de intrusão. Para isso, foram feitas pesquisas sobre a ferramenta Cowrie, na sua própria documentação e também em sites especializados. Como Prova de Conceito, foi realizada a instalação da honeypot em uma máquina virtual, com Sistema Operacional Ubuntu. Além disso, foi testado a invasão da honeypot com o aplicativo “juicessh”, instalado em um smartphone com o Sistema Operacional Android. Posterior aos testes iniciais, foi realizado uma análise dos arquivos e logs que a Honeypot Cowrie disponibiliza. Dessa forma, foi verificado que o ambiente instalado como Prova de Conceito está disponível para uma configuração mais detalhada, voltada para algum ataque específico. Como Trabalhos Futuros, espera-se inserir a honeypot Cowrie com um IP público, a fim de obter informações de possíveis ataques.

Palavras-chave: Honeypot. Cowrie. Ataques.