Controle da segurança de sistemas com log de honeypots e ferramentas para auxiliar na interatividade e visualização

Pamela Moura Gonçalves[1], Roben Castagna Lunardi[1*]

Orientador(a)*

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Restinga. Porto Alegre, RS.

Os honeypots simulam um sistema com vulnerabilidade na rede para atrair e detectar atividades maliciosas, possibilitando a análise de arquivos de logs, que podem variar entre os diferentes tipos de serviços e seus respectivos objetivos. Em geral, o log é de difícil visualização e contém um grande volume de dados, o que faz com que alguns eventos acabem passando despercebidos. Esses eventos podem ser inofensivos, como também podem envolver um atacante, que conseguindo acessar o sistema real, pode gerar diversos problemas na integridade do ambiente. O propósito deste trabalho é demonstrar que honeypots podem ajudar no gerenciamento de dispositivos se for corretamente monitorado. Além da sua efetividade ser potencializada com ferramentas integradas, com objetivo de ter identificações mais claras, como dashboards para visualização e análise facilitada dos logs, dentre outras funcionalidades que podem ser adicionadas. Para começar o desenvolvimento da pesquisa, foram selecionados honeypots obtidos a partir de um projeto de honeynet chamado t-pot, que foi adicionado em uma máquina virtual. Dentro dele, há ferramentas auxiliares, como o Kibana para visualização em dashboards, e o Elastic Stack com Logstash e Elasticsearch, para tratamento dos dados e envio. Para realizar os testes de intrusão e obter logs, foi utilizado o sistema Kali Linux, que possui ferramentas para PENTEST. Foram utilizadas principalmente: o nmap, para varreduras e detecção de versões de aplicações instaladas; o metasploit, para abertura de comunicação com serviços específicos, verificação de vulnerabilidade e fazer ataque de força bruta ou via wordlist; Hydra, John the Ripper e Ncrack, que também foram utilizados para ataques. A partir destes métodos, foram obtidos logs no Kibana, onde foi possível visualizar diferentes tipos de gráficos e fazer gestão do que era mais importante, podendo ser selecionado algo específico e mostrar tudo que está relacionado, desde um IP até um serviço. Desta forma, esta pesquisa contribui para auxiliar na escolha de Honeypots através da comparação das visualizações dos dados após os testes de intrusão.

Palavras-chave: Honeypots; PENTEST; Logs.