Os riscos para segurança ao utilizar honeypots com repositórios com falta de atualização

Fabiano Silva Santos[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.

Honeypot é uma ferramenta que serve de isca ou armadilha para atrair usuários maliciosos. Os sistemas que são emulados por um honeypot apresentam um agrupamento de informações com vulnerabilidades que são implementadas de forma proposital pelos administradores da rede. Dessa forma, os demais hosts, servidores e serviços da organização ficam seguros, uma vez que os honeypots emulam um programa com falhas e coletam a forma como o atacante se comporta ao tentar invadir o sistema. A documentação é um elemento necessário para que se desenvolva estratégias de cibersegurança, principalmente quando o assunto trata de honeypots. Entretanto, uma documentação e códigos desatualizados podem comprometer a eficiência das ferramentas e representar diversos riscos para a integridade dos dados de uma organização. Dentre as principais consequências da desatualização de honeypots, pode-se citar exposição à vulnerabilidades já conhecidas pela comunidade de segurança. Quando um repositório de honeypots não está atualizado para refletir as últimas ameaças e atualizações de segurança, os honeypots podem acabar se tornando suscetíveis a ataques que poderiam ser facilmente evitados ou até mesmo ignorados pelos atacantes. Tais como configurações erradas, falhas e práticas obsoletas. Pode-se citar como exemplo o honeypot Dionaea, sendo este um sistema de baixa interação capaz de capturar uma ampla gama de malwares para análise de forma posterior. Entretanto, através de uma avaliação de PENTEST com a ferramenta nmap, é possível identificar que o serviço de honeypot está rodando em um determinada porta. Desta forma, o atacante facilmente descobre que trata-se do honeypot. Este tipo de falha jamais deve acontecer em um cenário onde o foco é atrair o atacante e fazê-lo acreditar que está a invadir um sistema de organização, não uma isca falsa. Podemos citar outros honeypots que também estão com documentação e códigos desatualizados. Por exemplo, o Honeyd, um honeypot de baixa interação que é responsável por criar hosts virtuais em uma rede e cada um desses hosts executar um serviço de forma arbitrária. Além deste, pode-se citar o Kippo, honeypot SSH de interação média projetado para registrar ataques de força bruta, e o mais importante, a interação shell executada pelo invasor. Portanto, medidas devem ser tomadas para que códigos e documentação utilizados por equipes de cibersegurança estejam sempre em constante atualização. Uma vez que vivemos em um cenário onde a evolução tecnológica se torna cada vez mais constante, os métodos utilizados por um usuário malicioso também evoluem. Vale destacar, que assim como as organizações devem implementar processos rigorosos para garantir que os demais sistemas estejam atualizados e com correções de segurança implementadas, o mesmo vale para honeypots. Por fim, este trabalho, ao avaliar diferentes honeypots, identificou muitos que estão desatualizados e podem apresentar riscos para a segurança da organização.

Palavras-chave: Honeypot; Atualização; Segurança.