ANÁLISE DE INTEGRAÇÃO DE FERRAMENTAS DE SEGURANÇA

Fernandes Macedo Ribeiro (Acadêmico)
Sibelius Lellis Vieira (Orientador)

A invasão de redes e sistemas ligados à Internet é uma realidade. Para dissuadir os atacantes e invasores de rede pode ser utilizado o honeypot, que atrai a atenção para si e a retira dos sistemas reais em uma rede de computadores. No presente trabalho foi observado que é de grande valor a adoção de honeypots em rede. Apesar dos riscos e vantagens da sua utilização, o ganho é grande se for levando em consideração o uso do honeypot de baixa interatividade. Inicialmente foi montado um ambiente de teste usando o software de virtualização VMware Workstation, onde foi implantado os honeypots e efetuado os testes para verificar se o honeypot pode cumprir o seu papel, que é ser invadido e sondado geralmente por invasores a procura de falhas e configuraçoes mal feitas pelo responsável de uma rede de computadores. Deve-se observar que a utilização de honeypots não substitui as regras de segurança aplicadas em uma rede, sendo apenas uma ferramenta para auxiliar no gerenciamento e melhoramento da segurança da empresa. Além da honeypot, foi observado que devido à quantidade de alertas gerados pelas ferramentas de detecção de intrusão, pode-se utilizar a técnica de data mining para analisar os resultados, e através dos mesmos criar regras relevantes de segurança. Para se obter resultados relevantes foi realizada uma demonstração da aplicação da técnica de classificação usando o algoritmo de indução J48 pertencente ao software WEKA, sobre os dados de entrada. Obteve-se no final uma árvore de decisão que pode ser analisada pelo analista de segurança, para avaliar os resultados obtidos e tomar as melhores decisoes de segurança.

Palavras-Chaves: 1) Data mining; 2) Honeypot; 3) Segurança; 4) log.

Apoio: Voluntário