A aplicação de Honeypots juntamente com Sistemas de Detecção de Intrusão em ambientes corporativos.

The Honeypots application along with Intrusion Detection Systems in Corporate Environments.

Fernando Ortiz Borges[1]
Mario Henrique Akihiko da Costa[2]

Resumo

Este estudo objetivou analisar como o uso de *Honeypots* juntamente com Sistemas de Detecção de Intrusão auxiliam profissionais da área de segurança a implantarem soluções com mais segurança no ambiente corporativo. A finalidade do mesmo é apresentar soluções com técnicas e ferramentas para identificar o comportamento e os métodos utilizados por indivíduos mal-intencionados quando desejam atacarem uma rede de computadores.

Palavras-chave: *Honeypots*; Segurança; Redes de Computadores.

Abstract

This study aimed to examine how the use of Honeypots with Intrusion Detection Systems help security professionals to deploy solutions more securely in the corporate environment. The purpose of it is to present solutions with tools and techniques to identify the behavior and the methods used by malicious individuals when they want to attack a computer network.

Keywords: *Honeypots*; *Security*; *Network*.

INTRODUÇÃO

A confiabilidade na segurança das informações de uma empresa nos dias de hoje tem um valor significativo dentro das organizações. Tecnologias novas surgem no mercado a todo momento, e devido a isso, consigo são trazidas vulnerabilidades e brechas que originam em novos tipos de ataques. Esses ataques são criados e planejados por indivíduos mal-intencionados que desejam se aponderarem desses sistemas sejam por ego ou até mesmo pelo lado financeiro. Esses ataques dificultam a tomada de decisões de administradores de redes, fazendo com que estratégias de defesas sejam mais difíceis de serem adotadas. Nesse contexto, a proposta é apresentar conceitos, definições e ferramentas necessárias para esse tipo de tomada de decisão.

[1]Centro Universitário Filadélfia de Londrina - UniFil
[2]Centro Universitário Filadélfia de Londrina - UniFil

HONEYPOTS E SISTEMAS DE DETECÇÃO DE INTRUSÃO

Honeypots são armadilhas implementadas de maneira propositalmente para atrair indivíduos mal-intencionados que desejam se aponderarem de sistemas e obter acesso não autorizado em determinadas redes de computadores. Eles são implementados para serem comprometidos, e assim administradores de redes poderem fazer uma análise mais precisa nas informações e rastros deixados por esses indivíduos. Sendo assim, é possível traçar medidas de prevenção de segurança.

Como bem nos assegura Wrightson(2014), os *Honeypots* são propositalmente configurados com vulnerabilidades específicas para que o atacante, ou seja, o indivíduo mal-intencionado, seja atraído. Afinal, esse ambiente agora possui vulnerabilidades que são de interesse para o atacante. Esse ambiente preparado, é capaz de fornecer provas de tentativas de ataques, pois foram configurados como armadilhas, e com esse propósito.

Os Sistemas de Detecção de Intrusão, conhecidos como IDS (*Intrusion Detection System*, são sistemas que trabalham monitorando os eventos que ocorrem dentro de uma rede de computadores. Seu principal objetivo é garantir a segurança da rede, onde utilizam meios que são capazes de prevenir e detectar ações e intrusões de indivíduos mal-intencionados que queiram destruir os pilares da Segurança da Informação (Integridade, Confidencialidade ou Disponibilidade).

Conforme destacam Carissimi, Rochol e Granville (2009) os IDS atráves dos logs que são deixados no sistema, conseguem identificar eventos que sejam considerados anormais dentro de uma rede, esses eventos anormais podem ser desde uma tentativa de intrusão por algum indivíduo mal-intencionado, ou até mesmo algum download que esteja aumentando o tráfego da rede. Após essa detecção, alertas são disparados como aviso para os administradores de rede.

METODOLOGIA EXPERIMENTAL

Para execução de um ambiente experimental se viu a necessidade de implementar um *Honeypot* conhecido como *Kippo*. Ele é um *Honeypot* que emula o serviço *SSH* com falhas e é capaz também de criar um sistema de arquivos falso, para o atacante poder se interagir com o sistema, criando arquivos, pastas ou até mesmo

excluindo arquivos do ambiente emulado, com ele também é possível obter todos os *logs* deixados pelo atacante e toda sua interação com o *shell*.

Durante os primeiros dias dessa análise o *Kippo* se mostrou bastante eficiente, conseguindo registrar todos os *logs* deixados pelos atacantes e toda sua interação com o *shell*. Ele também mostrou os *IP´s* provenientes do ataque e de onde eles eram executados.

Com isso foi possível obter detalhes do comportamento dos atacantes e nesse mesmo ambiente instalar e configurar o *OSSEC* para trabalhar em modo agente. Ele é um Sistema de Detecção de Intrusão que trabalha com um sistema de *active-response*, ou seja, para determinados tipos de ataques ele pode tomar medidas de prevenção.

CONCLUSÃO

Neste trabalho foram apresentados os *Honeypots* e os Sistemas de Detecção de Intrusão de uma maneira geral. A simples implementação de ambos pode trazer a tona como indivíduos mal-intencionados se comportam durante o ataque em uma rede de computadores. Sua implementação simples tem como objetivo mostrar para administradores de redes como é possível com recursos computacionais baixos obterem sucesso na implementação de sistemas de segurança.

REFERÊNCIAS

MARCELO, Antonio; ALVES, M. J. P. **Honeypots**: A arte de iludir hackers. Rio de Janeiro: Brasport. 2003.

TYLER, Wrightson. **Segurança de Redes Sem Fio**: Guia do Iniciante. Porto Alegre: Bookman. 2014.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Z. **Redes de Computadores**. Porto Alegre: Bookman, 2009.