Utilizando software livre para implementar serviços de IPS (Intrusion Prevention System) e IDS (Intrusion Detection System) em um cenário virtualizado

João Paulo de Barros[1], André Ricardo Zavan[1], Eduardo Henrique Molina Cruz[1]

[1] Instituto Federal do Paraná (IFPR) – Campus de Paranavaí
CEP 87.706-340 – Paranavaí – PR– Brasil

jpb.ifpr@gmail.com, andre.zavan@ifpr.edu.br, eduardo.cruz@ifpr.edu.br

Segundo [Tanenbaum 2003] desde o início da década de 1990, onde a internet se tornou comercial, houve um crescimento exponencial de dispositivos na rede de dados, através dos grandes avanços das tecnologias em hardware e software, possibilitando cada vez mais a troca de informações entre seus usuários. Além das demandas atuais, novos serviços sempre estão surgindo, com aplicações de inúmeras funcionalidades, como transferências de informações sigilosas e operações financeiras, necessitando uma infraestrutura que garanta a proteção e transmissão segura das informações.

Conforme aponta Morimoto (2011), cada vez mais, as tecnologias de acesso e transmissão de dados são empregadas, o que torna mais complexo manter uma rede segura, já que existem formas inadequadas de se obter informações que poderão ser usadas para prejudicar os processos, tornando-se cada vez mais necessário a proteção das informações que trafegam na rede. Estes incidentes normalmente ocorrem explorando a vulnerabilidade, visando diferentes alvos, tais como, empresas diversas, instituições bancárias, instituições governamentais e usuários domésticos. Para isso, utilizam variadas técnicas, como, negação de serviço, *phishing*, *worms*, *trojans*, *spywares* e *keyloggers*, sendo assim, o uso de um sistema de detecção e prevenção de intrusos tornando-se indispensável em qualquer infraestrutura que se deseja ter uma camada extra de segurança contra ameaças.

Neste sentido até o momento foi possível analisar o estado em que se encontrava os hosts da rede de computadores de um cenário acadêmico num laboratório de informática, bem como a demanda de serviços que necessitam da mesma, através da implementação das regras dos recursos de *firewall e proxy* atrelado a definição de uma política de segurança foi possível observar um ambiente mais claro, sendo possível atingir expectativas de gerenciamento e segurança da rede, além disso através do log gerado do *firewall* observou-se situações relacionadas à segurança da informação na qual compromete a segurança dos *hosts* conectados à rede e o gerenciamento das informações que circulam nela.

Logo, a presente pesquisa tem como objetivo implementar soluções livres para operação dos serviços de *IPS* (Intrusion Prevention System) afim de impedir possíveis incidentes de segurança e o *IDS* (*Intrusion Detection System*) para detectar manipulações de sistemas de computadores indesejadas que ocorrem normalmente através da internet.

Para o desenvolvimento deste trabalho foram estabelecidas algumas metodologias, como o levantamento bibliográfico sobre as áreas e recursos envolvidos neste projeto, abordando questões referentes a redes de computadores, gerenciamento das redes, recursos de *ids*, ips, *firewall*, segurança da informação e política de segurança.

Quanto ao ambiente de aplicação desta solução foi preparado um ambiente virtualizado onde serão implementados um sistema de detecção e prevenção de intrusos (IDS/IPS), chamado *Snort* executando sobre um sobre um sistema operacional baseado em *FreeBSD* (*pfSense*) e implementado no firewall da infraestrutura de redes.

Com o intuito de atingir os objetivos deste trabalho na implementação e configuração de um sistema de detecção de intrusão para analisar sua eficácia nas detecções e prevenção de futuras ameaças proporcionando uma camada extra de segurança para o cenário desenvolvido, tornando possível prevenir e detector diversos métodos de ataques, protegendo assim os hosts internos de uma rede. Espera-se que com os recursos implementados de instrução e detecção seja possível realizar o monitoramento de possíveis ataques, auxiliando e orientando os administrators de redes no tratamento de incidentes de segurança, sendo um dos aspectos deste trabalho a coleta de informações referentes aos tipos mais frequentes de ataque sofrido e os bloqueios que poderão ser efetuadas de forma autônoma com os recursos disponíveis pela solução proposta, prevenindo-se de futuros ataques e outros incidentes de segurança nas quais podem comprometer uma parte ou todo o funcionamento da rede em modo geral.

Referências

MORIMOTO, C. E. (2011) Redes: Guia Prático. Porto Alegre: Sul Editores.

Tanenbaum, A. S. (2003) “Redes de Computadores”, 4. ed. Elsevier, Rio de Janeiro.