Avaliação de desempenho de uma ferramenta de detecção de intrusão

Thales Nicolai Tavares[1], Renato Preigschadt de Azevedo[1]

[1]Colégio Técnico Industrial de Santa Maria – Universidade Federal de Santa Maria (UFSM)
Cep 97.105-900 – Santa Maria – RS – Brasil

{tavares,renato}@redes.ufsm.br

Abstract. *This article presents tests performed in an intrusion detection tool in order to assess their effectiveness with different types of attacks. The tool under study is the SELKS and was developed by Stamus Networks and aims to identify the attacks at the time of his execution, because it has a set of tools able to monitor packets that travel over the network.*

Resumo. *O presente artigo apresenta testes realizados em uma ferramenta de detecção de intrusão com o intuito de avaliar sua eficiência com diferentes tipos de ataques. A ferramenta em estudo é a SELKS a qual foi desenvolvida pela Stamus Networks e tem como objetivo identificar os ataques no momento de sua execução, pois ele possui um conjunto de ferramentas capaz de monitorar os pacotes que trafegam na rede.*

1. Introdução

Durante os últimos anos podemos notar que a rede mundial de computadores vem crescendo de forma muito rápida, e devido a este crescimento temos muitos serviços e aplicações que utilizamos no nosso dia-a-dia funcionando através da internet. Em virtude a essa expansão, temos que nos preocupar com a segurança, pois a quantidade de ataques a sistemas de computadores vem crescendo diariamente.

Este trabalho apresenta resultados de estudos realizados com a ferramenta SELKS, onde foi analisado o comportamento mediante os ataques. Para a análise da ferramenta foi utilizado arquivos PCAPs de tráfegos de redes disponibilizados pela NETRESEC, que é um fornecedor independente de software com foco na área de segurança de rede e a ferramenta hping3, que é um software para realizar testes de vulnerabilidades.

2. Objetivo

O objetivo principal deste artigo é mostrar o estudo realizado sobre o desempenho da ferramenta de detecção de intrusão SELKS, onde foram utilizados tráfegos de redes disponibilizados pela NETRESEC, bem como os resultados das detecções ocorridas.

Para a análise da ferramenta, foram utilizados arquivos PCAPs de tráfego de rede disponibilizados pela NETRESEC. Também foi realizado um ataque de negação de serviço, o qual ocorre quando um dispositivo envia uma grande quantidade de requisições de um dispositivo para outro, não permitindo a comunicação legítima.

3. Desenvolvimento

Nos últimos anos, uma tecnologia tem se mostrado uma grande aliada dos administradores de segurança. São os Sistemas de Detecção de Intrusão (IDS - Intrusion Detection System), que possuem por objetivo tentar reconhecer um comportamento ou uma ação intrusiva para alertar um administrador ou automaticamente disparar contramedidas. [Laureano 2003]

Sistemas detectores de intrusão em redes de computadores são utilizados para permitir a monitoração do tráfego de dados de uma rede de computadores ou um segmento de rede. A análise é realizada em dados coletados da rede ou em base de dados disponíveis ao IDS. [Murini 2013]

A ferramenta em estudo é a SELKS (Figura 1), que está disponível em http://www.stamus-networks.com, produto desenvolvido pela Stamus Networks que tem por objetivo identificar os ataques no momento de sua execução, pois ele possui um conjunto de ferramentas capaz de monitorar os pacotes que trafegam na rede. Sendo assim, é realizada uma análise comparando o tipo de tráfego da rede com uma base de dados que a ferramenta já possui. Esta base de dados é atualizada periodicamente, sendo possível detectar novos ataques.

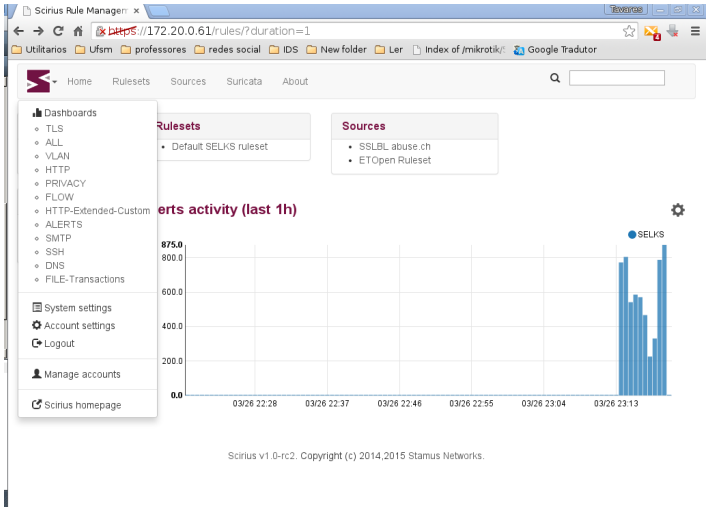

Figura 14. Tela inicial SELKS

Para a instalação da ferramenta foi necessário um ambiente virtual, onde foi utilizada uma máquina para a instalação do SELKS e uma segunda máquina virtual com o sistema operacional Linux, a qual foi utilizada para injetar tráfegos de rede através dos arquivos PCAP. Os arquivos PCAPS são tráfegos de rede coletados em um arquivo, o qual irá analisá-los posteriormente, preferencialmente em uma máquina diferente daquela da qual o tráfego foi coletado. Os arquivos PCAPS que foram utilizados nos experimentos são disponibilizados na página http://www.netresec.com da NETRESEC.

O SELKS é uma distribuição baseada no Debian, composto pelos componentes principais: *Suricata IDPS,* que é um ID/PS motor baseado em regras e que utiliza regras desenvolvidas externamente. Ele monitora o tráfego de rede e fornece alertas para o administrador do sistema quando ocorrem eventos suspeitos; *ElasticSearch,* que é um mecanismo de busca *open source*, desenvolvido sobre o Apache; *Logstash* para centralização de logs; *Kibana,* que é uma plataforma de visualização de dados de código

aberto que permite que você interaja com os seus dados através de gráficos; e o *Scirius* que é a interface web dedicada à gestão do conjunto de regras Suricata.

A ferramenta SELKS pode ser utilizada de duas maneiras, a *live* e a instalável, e fornece um sistema de detecção de intrusão com o Suricata com seu próprio gerenciador de regra e gráfico. Para a os testes, foi utilizado a versão instalável, onde foi usada uma máquina virtual com espaço de disco de 25GB e 4GB de memória.

Como a intenção não é avaliar a eficiência da ferramenta IDS, a segunda máquina virtual foi utilizada para injetar os arquivos PCAPS baixados da NETRESEC, utilizando a ferramenta TCPreplay para a reprodução desses tráfegos.

Outro teste realizado foi no ambiente virtual, formado por uma máquina como servidor web, e outra máquina virtual para realizar um ataque DOS (*Denial of Service*) no servidor web. Um tipo de ataque de negação de serviço ocorre quando um dispositivo envia uma grande quantidade de requisições de um dispositivo para outro, assim não permitindo a comunicação legítima. Para realizar os experimentos foi utilizada a ferramenta hping3, que é um software para realizar testes de vulnerabilidades.

4. Resultados

Após deixar a ferramenta operando sob ataques dos arquivos *PCAP,* e logo em seguida os ataques de *DoS*, nota-se a alteração do gráfico da ferramenta SELKS (Figura 2). Percebe-se que a ferramenta consegue detectar a alteração no tráfego de rede e gera gráficos mostrando que ocorrem ataques contra a rede.

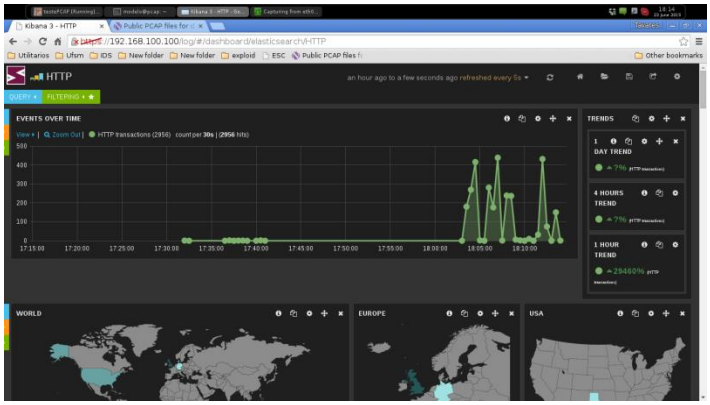

Figura 2. Gráfico de alteração do comportamento da rede

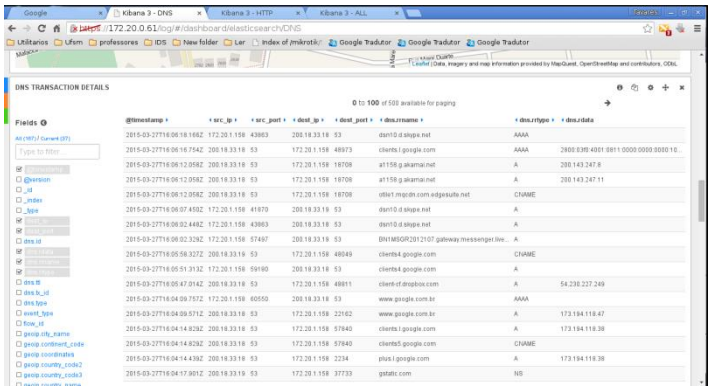

Figura 3. Tabela com endereços de origem e destino

Através da análise dos gráficos e tabelas gerados pela ferramenta de detecção de intrusão ficam evidentes as requisições que originaram o ataque. Nestes gráficos também são apresentados os endereços IPs de origem e destino.

5. Conclusão

Neste trabalho foi mostrada uma alternativa de ferramenta de detecção de intrusão, a SELKS. Foi possível perceber que a ferramenta apresenta um rendimento satisfatório ao detectar ataque no tráfego de rede, pois nos experimentos realizados foram disparadas diferentes formas ataques contra o servidor e analisado o comportamento da ferramenta IDS.

Através da análise dos gráficos gerados pela ferramenta de detecção de intrusão, ficam evidentes as requisições e a mudanças repentinas no tráfego de rede. Sendo assim, é possível concluir que o uso de um sistema de detecção de intrusão é de grande importância para o correto funcionamento de uma rede de computadores.

References

Laureano, M.A.P. (2003) Detecção de intrusão em máquinas virtuais. 5º Simpósio de Segurança em Informática.

Murini, C.T. (2013) Análise de sistema de detecção de intrusão em redes de computadores. 28ºJornada Acadêmica Integrada.