Criando regras no Snort para análise de tráfego de rede

Douglas Fabio da Cruz Junior, Lucas de Araújo Oliveira. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – Campus Barretos. douglasfabio.ifsp@gmail.com

Palavras Chave: Redes, Segurança, Tecnologia.

Introdução

Pode-se retratar a segurança de redes como sendo uma forma de proteger a integridade da informação de modo a evitar o uso incorreto ou indevido de dados tanto intencional como acidentalmente, sejam elas praticadas por pessoas internas ou externas a determinado ambiente.

A vulnerabilidade ou falha de segurança pode estar ligada diretamente a dois fatores: humano e tecnológico, onde falhas simples e na maioria das vezes imperceptíveis abrem caminho para que hackers tenham acesso à informações sigilosas. Vale lembrar que não existe informações que sejam 100% segura, devendo o sistema estar preparado para possíveis ataques virtuais que possam ocorrer[1].

Neste preparo, além das configurações básicas como atualizações dos programas e sistema operacional, pode-se incorporar ferramentas de alertas que informarão caso alguma anomalia aconteça. Tais ferramentas são conhecidas como IDS (Intrusion Detection System) que emitirão alertas ao administrador do sistema.

Objetivos

Identificar e alertar possíveis ameaças virtuais, criando regras que farão a análise de cada pacote de rede para detectar tentativas de invasão ou ataque em um servidor rodando o sistema operacional Linux distribuição Ubuntu [2].

Material e Métodos

A ferramenta que será utilizada é o Snort[3], que trabalha como um IDS ou também NIDS (Network Intrusion Detection System) que tem como objetivo identificar e criar alertas sobre comportamentos anormais dentro do tráfego de uma rede. O Snort se baseia em regras e combina inspeções em protocolos e assinaturas através de um de seus métodos chamado de “Sniffer” (Farejador/Detector), este método irá analisar os pacotes que trafegam na interface de rede do computador e fará a depuração afim de encontrar possíveis tentativas de ataques e invasões.

Outro método em que o Snort é capaz de trabalhar é o método de “Packet Logger” (Registro de pacotes) onde o IDS registra todos os pacotes para posterior consulta ou análise mais detalhada.

Será utilizado o software Oracle Virtual Box[4] para virtualizar 2 máquinas, sendo 1 a máquina com o snort e a outra para realizar os ataques.

Resultados e Discussão

A base de regras disponíveis no Snort permite analisar vários tipos de ataques. Porém, como cada rede executa um sistema ou plataforma específica, pode ocorrer o alerta de vários falsos-positivos, ou seja, o alarme de uma situação que na verdade não aconteceu. Estes alertas são comuns nas mais variadas ferramentas de configuração de rede devido ao grande número de pacotes e situações que não são esperadas pelo sistema de detecção, como por exemplo a instalação de um novo software que utilizará uma porta específica. Nesse exemplo o IDS poderá entender como um ataque. Nestas situações, a experiência do analista confirmará se trata-se de um ataque ou não, tendo autonomia para editar a regra que criou o alarme.

A título de experimento, foi realizado um estudo na estrutura da regra do snort com o objetivo de criar regras próprias.

Toda regra no snort possui um padrão:: alert [tipo de protocolo] [ip origem] [porta origem] -> [ip destino] [porta destino] (“[mensagem do alerta]”; sid: [numero do ID do alerta];.

Nos experimentos iniciais, foi criado uma regra simples apenas para alertar o envio de pacotes icmp:alert icmp 192.168.0.2 255.255.255.0 -> 192.168.01 255.255.255.0 (“Mandando pacotes ping”;sid: 1000001;).

Nos testes seguintes, foi configurado um servidor web apache na porta 80 e inserido uma regra que alertasse caso ocorresse algum acesso web. Tais testes iniciais objetivaram familiarizar-se com a estrutura e funcionamento da ferramenta. A regra ficou da seguinte maneira: alert tcp 192.168.0.2 255.255.255.0 -> 192.168.0.1 80 (“Tentativa de acesso web – porta 80”; sid:1000002;).

Para simular uma situação real, foi escolhido

o ataque de SYN FLOOD, que é uma forma de ataque de negação de serviço (também conhecido como Denial of Service - DoS), onde o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga na camada de transporte. A ferramenta utilizada para realizar este ataque foi o metasploit [5]. Foi inserida uma regra para tentar identificar este tipo de ataque. A figura abaixo ilustra a execução do ataque.

Fonte: próprio autor

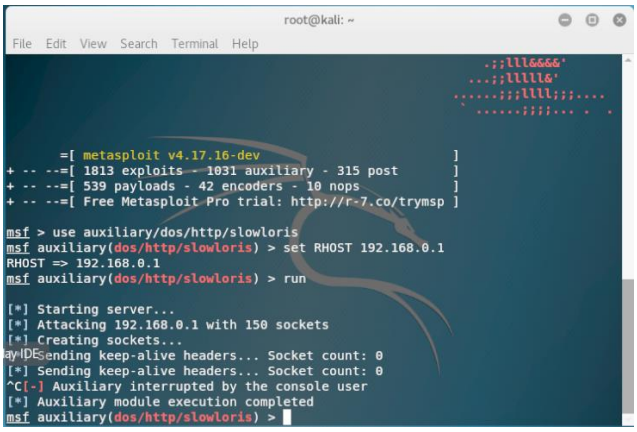

Fig.1 - Execução do metasploit

A ferramenta metasploit é responsável por investigar vulnerabilidades em plataformas, servidores e sistemas operacionais tendo como principal objetivo a execução de códigos maliciosos conhecido como exploits.

Após o início do ataque, pode-se concluir que o snort detectou e apresentou o alerta com a regra criada. A figura 2 apresenta o alerta emetido pelo snort.

Fonte: próprio autor

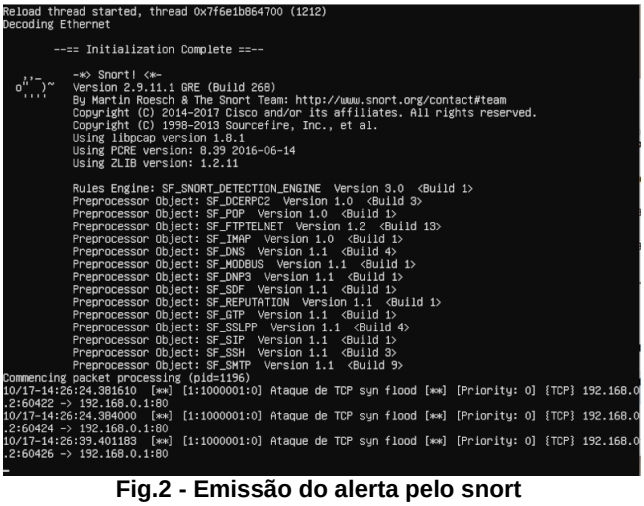

Fig.2 - Emissão do alerta pelo snort

Conclusões

Toda rede, seja de pequeno ou grande porte, deve estar preparada para receber os mais variados tipos de ataques. Uma ferramenta que auxilia o analista é o Snort. Tal ferramenta trabalha como um IDS emitindo alertas caso algo anormal aconteça, por se tratar de uma ferramenta gratuita, de código aberto, sniffer bem como operar tanto como um detector quando para criação de bloqueios e restrições. O snort se mostrou eficiente na análise dos dados e na emissão de alertas. Como trabalho futuro o snort poderia, ao identificar um ataque, chamar uma função do firewall para bloquear o IP que está originando o ataque pois ele possui funções que podem trabalhar em conjunto com um firewall.

Agradecimentos

Gostaria de agradecer primeiramente a Deus pela oportunidade de escrever nesse resumo expandido a experiência e o conhecimento adquirido através do uso de uma tecnologia moderna e eficaz sob orientação de uma pessoa que é um grande exemplo como profissional da área, como ser humano e considerado por mim como grande amigo, Prof. Ms. Lucas de Araújo Oliveira e sob o incentivo de meu pai Douglas Fabio da Cruz à qual dedico esse meu primeiro relato. É com humildade e dedicação e com vontade de aprender que adquirimos cada vez mais conhecimentos, e ao estudar sobre essa ferramenta moderna da tecnologia, pude ter contato com algo totalmente novo em termos de Redes de computadores, pois a segurança na maioria das vezes é pouco lembrada e é onde grandes falhas humanas podem acontecer. O Snort foi um software que me fez enxergar com outros olhos o termo segurança dentro da área de computação.

Bibliografia

[1] Moraes, Alexandre Fernandes de. **Segurança em Redes: fundamentos.** São Paulo: Érica, 2010.

[2]**UBUNTU.** Disponível em: www.ubuntu.com. Acesso em 17 Out/2018.

[3]**SNORT**. Disponível em: https://www.snort.org/. Acesso em: 29 Ago/2018

[4]**ORACLE VIRTUAL BOX**. Disponível em: https://www.virtualbox.org//. Acesso em: 11 Set/2018

[5]**METASPLOIT.** Disponível em: https://www.metasploit.com Acesso em 11 Set/2018