Integrando o SNORT em uma rede OpenFlow

Hélio Tibagí de Oliveira

Marcelo Galdino

Agenda

- O que é SNORT?
- Descrição do Problema
- Solução Desenvolvida
- Topologia/Arquitetura
- Passo-a-passo
- Próximos Passos

O que é SNORT?

- O Snort é um Software IDS (Intrusion Detection System).
- Atua de maneira parecida com o “Wireshark”, monitorando tudo o que passa pela placa de rede do computador.

- Possui inúmeras configurações para filtrar o que você está querendo encontrar.
- Roda em Windows ou Linux.
- Open Source e bastante popular no segmento.

Descrição do Problema

- Instalar um Software IDS (Intrusion Detection System) em uma rede OpenFlow para que ele forneça subsídios para a tomada de ações de segurança na rede de forma automática.

Fazer com que ele monitore tudo o que trafegar pela rede, sem agir como um proxy e sem penalidades de performace.

e

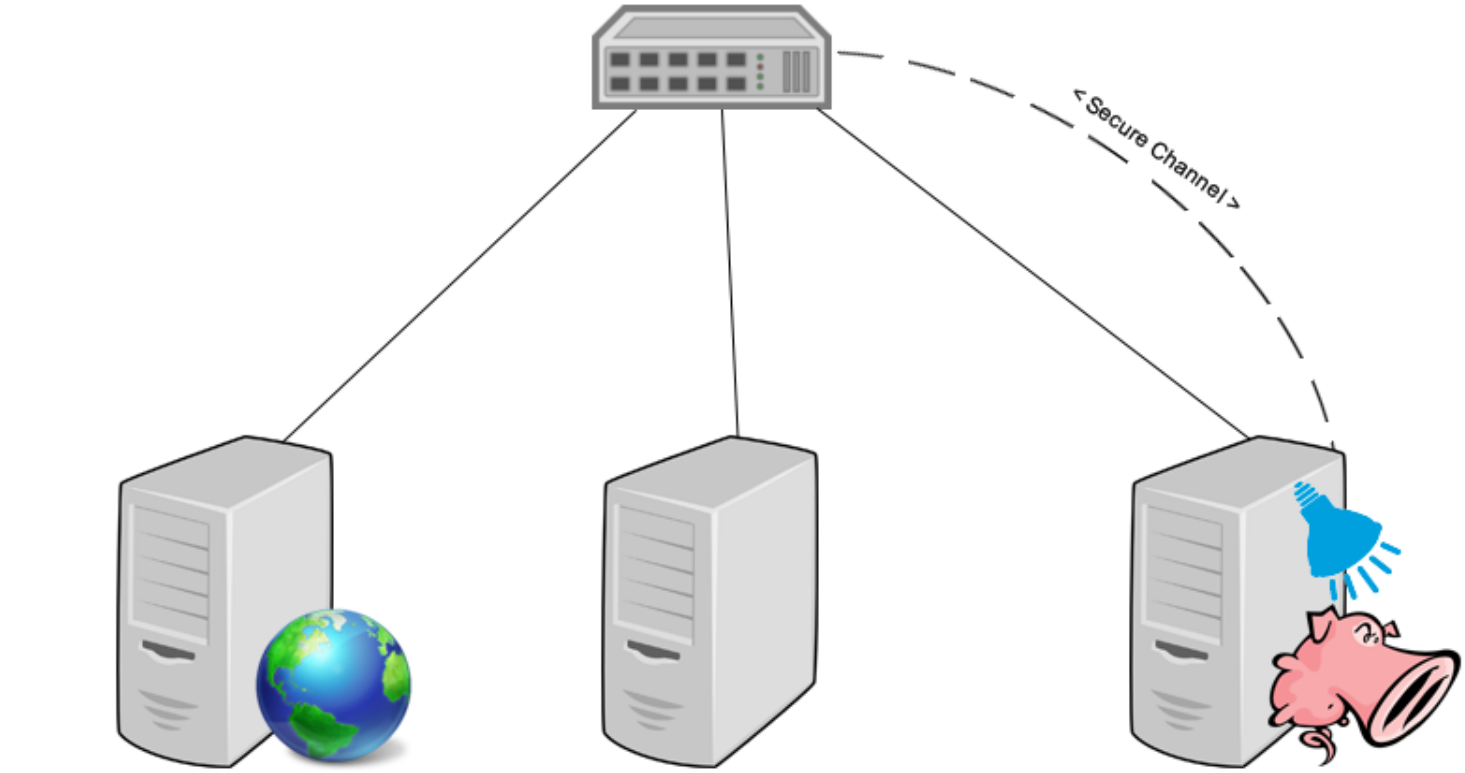
Interpretar os seus alertas e converter isso em ações na rede OpenFlow (alterar rotas, colocar hosts em quarentena e etc...).

Solução Desenvolvida

- Um software que vai orquestrar as coisas, sendo uma extensão ao controlador OpenFlow.

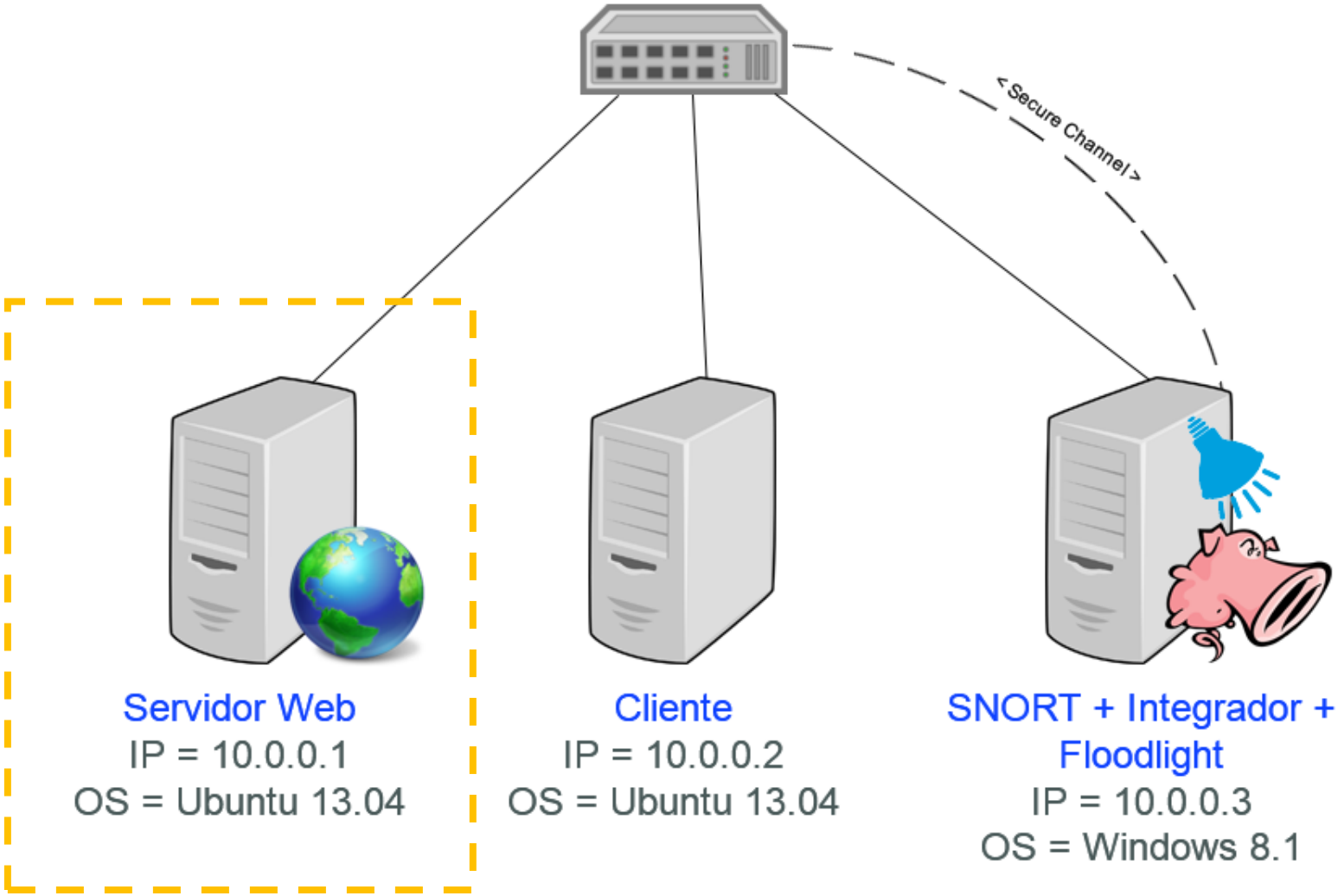
- Construído em C#, e se comunicando com o controlador Floodlight através de suas APIs REST.

Topologia/Arquitetura



Topologia/Arquitetura

Servidor Web



Topologia/Arquitetura
Servidor Web

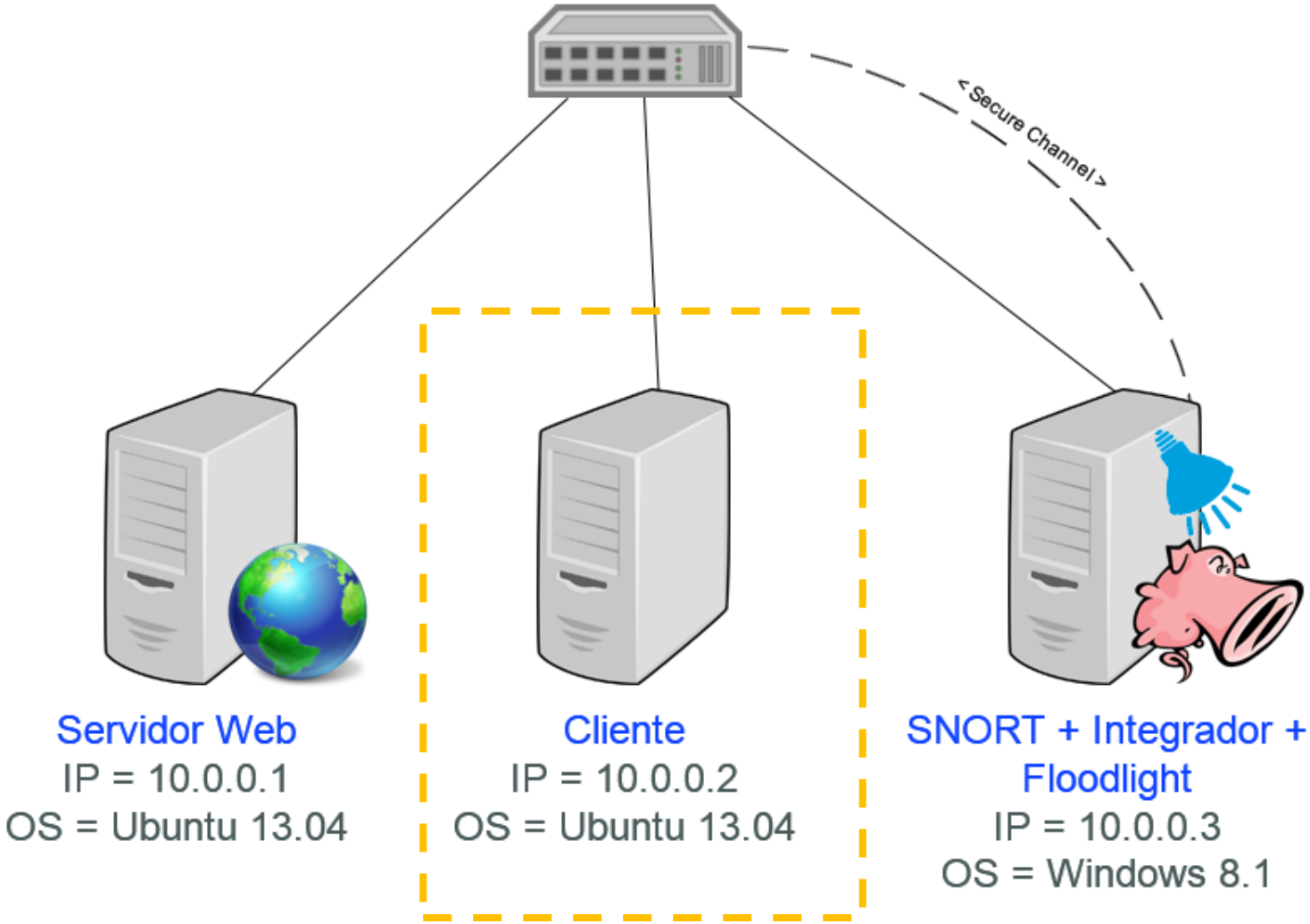
- Um host Linux virtual criado pelo Mininet com o IP 10.0.0.1

- Presente apenas para servir como teste para simular a comunicação com o host Cliente

- Servidor Web simples baseado em Python (vem junto com o Mininet), que somente exibe uma página web que mostra os arquivos do servidor.

Topologia/Arquitetura

Cliente

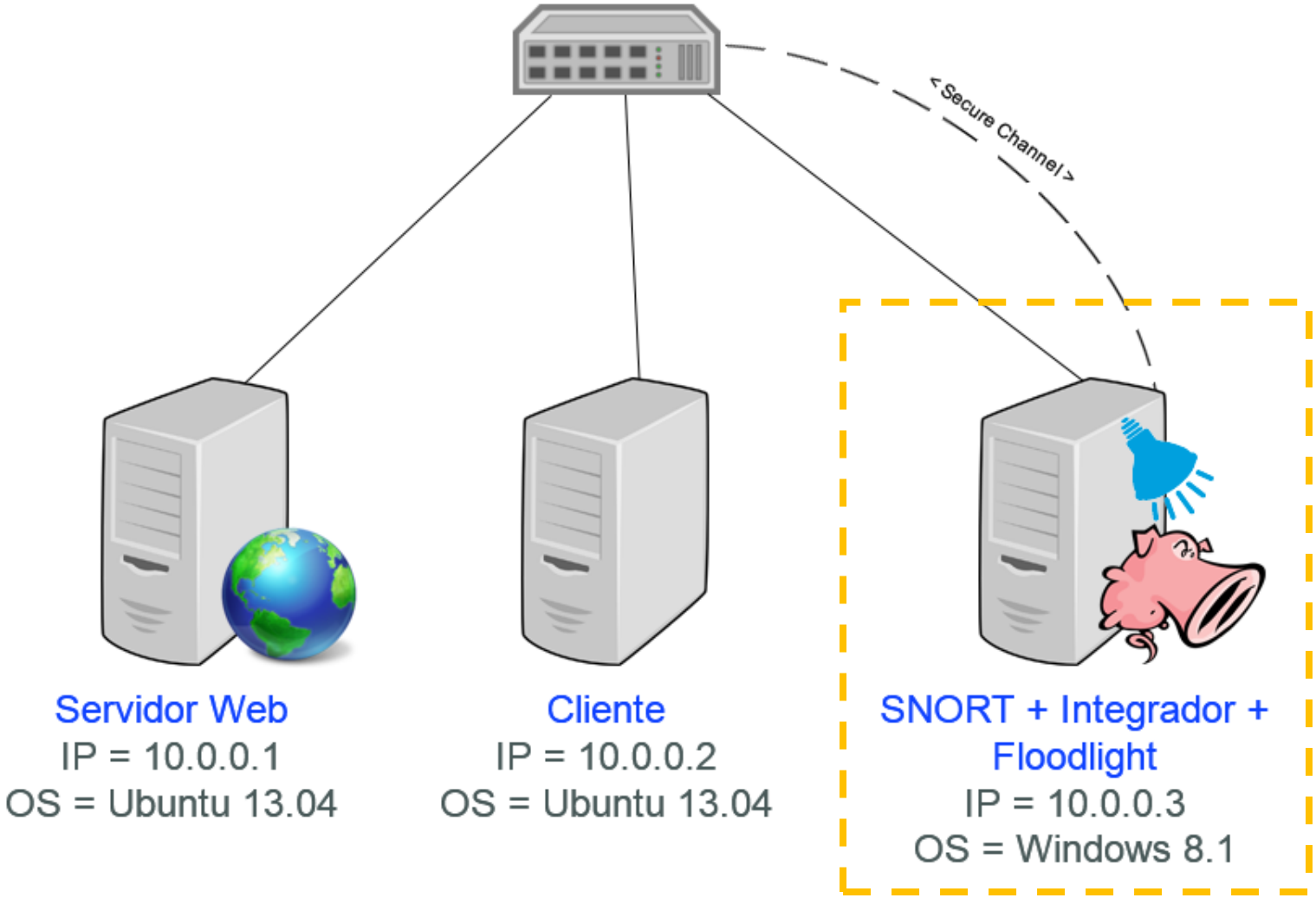


Topologia/Arquitetura
Cliente

- Um host Linux virtual criado pelo Mininet com o IP 10.0.0.2

- Presente apenas para servir como teste para simular a comunicação com o host Servidor Web

Topologia/Arquitetura
SNORT



Topologia/Arquitetura
SNORT

- Um host real Windows 8.1 com o IP 10.0.0.3

- Esse host possui duas placas de rede, uma com o IP 10.0.0.3 que está conectada no switch virtual OpenFlow e uma outra que é utilizada pelo Floodlight como "Secure Channel" para se conectar no switch virtual do Mininet.

- O SNORT fica monitorando a placa de rede com o IP 10.0.0.3

- O Integrador fica orquestrando o SNORT e o Floodlight

Passo-a-passo

1. O Controlador Floodlight é iniciado;
2. O Mininet é iniciado com o Servidor Web e o Cliente;
3. O Integrador adiciona rotas estáticas entre o Servidor Web e o Cliente e também sempre para o SNORT;
4. O SNORT é iniciado, com o seu *stdout* redirecionado para o Integrador;

5. *<< inicia a comunicação entre o Servidor Web e o Cliente >>*

6. O SNORT emite um alerta no seu *stdout*;
7. O Integrador faz o *parse* desse alerta, e identifica os hosts envolvidos;
8. O Integrador decide que o Cliente foi comprometido, e ele deve ser retirado da rede (quarentena);
9. O Integrador remove as rotas que possuem como origem o Cliente;

Próximos Passos

- Refazer o mesmo protótipo em Java, como um módulo do Floodlight;
- Explorar a mecânica do SNORT que grava os alertas em um Banco de Dados, ao invés do stdout, e verificar se é mais vantajoso ou não;
- Fazer testes de performace;
- Criar uma interface gráfica (GUI) web para facilitar as configurações.