MicroSec Traffic: Manual do Usuário

Utilizando Estratégias de Engenharia de Tráfego para Aprimoramento da Eficiência de Sistemas de Detecção de Intrusão

Sumário

1 Introdução

O MicroSec Traffic é uma abordagem inovadora para melhorar a eficiência de soluções IDS tradicionais (baseadas em assinaturas e anomalias definidas por regras) através da redução da carga de dados do tráfego de rede, sem comprometer a detecção de ameaças. Esta técnica não requer modificações nas ferramentas IDS (como Snort ou Suricata), apenas ajustes nas regras utilizadas.

Avaliada em cenário controlado com o Snort, a abordagem demonstrou ser efetiva ao manter a geração de alertas com menor tempo de processamento e volume de dados.

2 Estrutura do Repositório

A estrutura do repositório do projeto é a seguinte:

```
SBSeg-2025-Herbele
 docker
    Dockerfile
    init.sh
 Guia_do_usuário_MicroSec.pdf
 LICENSE
 README.md
 rules
    microsec-pcap.rules
    original-pcap.rules
 scripts
    cenario-1.sh
    cenario-2.sh
    cenario-3.sh
    cenario-4.sh
    microsec.py
    requirements.txt
    roda-cenarios.sh
 teste-minimo
     teste-microsec.pcap
```

3 Requisitos do Sistema

3.1 Hardware

- CPU: AMD EPYC 7401 24-Core 2.0GHz
- RAM: 16 GB
- Kernel: 6.6.6-Atwood
- Sistema Operacional: Debian GNU/Linux 12 (bookworm)

3.2 Software

- Docker - versão 28.0.2 ou superior
- Wireshark - versão 4.0.17 ou superior
- Python - versão 3.12

4 Dependências

A execução do sistema depende de:

- Ambiente Python para execução dos scripts de processamento
- Docker para execução do Snort em container isolado

5 Instalação

5.1 Instalação do Docker

Execute os seguintes comandos para instalar o Docker:

```
sudo apt install ca-certificates curl gnupg
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg |
  sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg

echo "deb [arch=$(dpkg --print-architecture) \
  signed-by=/etc/apt/keyrings/docker.gpg] \
  https://download.docker.com/linux/debian \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt update
sudo apt install docker-ce docker-ce-cli \
  containerd.io docker-buildx-plugin docker-compose-plugin

cd SBSeg-2025-Herbele/docker
docker build -t snort3-docker .
```

6 Dataset

6.1 Dataset Original

O dataset utilizado neste projeto é o CIC-IDS-2017, disponível em:

`https://www.unb.ca/cic/datasets/ids-2017.html`

Para download direto via terminal:

```
wget http://cicresearch.ca/CICDataset/CIC-IDS-2017/Dataset/CIC-IDS-2017/PCAPs/
   Wednesday-workingHours.pcap
```

6.2 Dataset Processado

O dataset já processado com a técnica MicroSec está disponível em:

`https://www.inf.ufpr.br/msh22/microsec.html`

Para download direto via terminal:

```
wget https://www.inf.ufpr.br/msh22/dados/microsec.tar.gz
tar -zxvf microsec.tar.gz
```

7 Teste Mínimo

7.1 Execução do Teste

Siga os passos abaixo para executar o teste mínimo:

```
# Iniciar o container
docker run -d --name snort-container snort3-docker

# Acessar o container
sudo docker exec -it snort-container /bin/bash

# Executar o script de teste
cd /usr/src/init.sh
./init.sh
```

O script realiza automaticamente:

- Download do dataset original
- Configuração do ambiente Python
- Execução do microsec.py no dataset
- Criação dos chunks de dados
- Execução do teste com chunk pré-processado

8 Experimentos

8.1 Cenários de Execução

O projeto inclui 4 cenários de execução:

1. Snort com regras originais + dataset original
2. Snort com regras MicroSec + dataset processado

3. Snort com regras originais + chunks do dataset original
4. Snort com regras MicroSec + chunks do dataset processado

8.2 Execução dos Experimentos

Para executar os experimentos:

```
# Acessar o container
sudo docker exec -it snort-container /bin/bash

# Executar script de cenrios
cd /usr/src/scripts
./roda-cenarios.sh
```

9 Processamento e Análise

- Cada cenário é executado 10 vezes para coleta de médias;
- São então analisadas e feitas as médias de todos as respectivas execuções de cada cenário;
- E o script gera como saída métricas importantes como o tempo de execução e o número de alertas gerados.

10 Preocupações com Segurança

Não foram identificadas preocupações de segurança relevantes na execução deste projeto.

11 Licença

Este projeto está licenciado sob a **GNU GPL v3**. O texto completo da licença está disponível no arquivo `LICENSE` do repositório.