Sistema de Detecção de Intrusões na Rede (NIDS)

Realizado por: Patrick Silva e Vasco Martins

Introdução ao Projeto NIDS

Este projeto visa configurar um NIDS (Network Intrusion Detection System) para monitorizar o tráfego de rede. O objetivo é identificar atividades suspeitas e responder a incidentes de segurança.

Monitorização de Tráfego

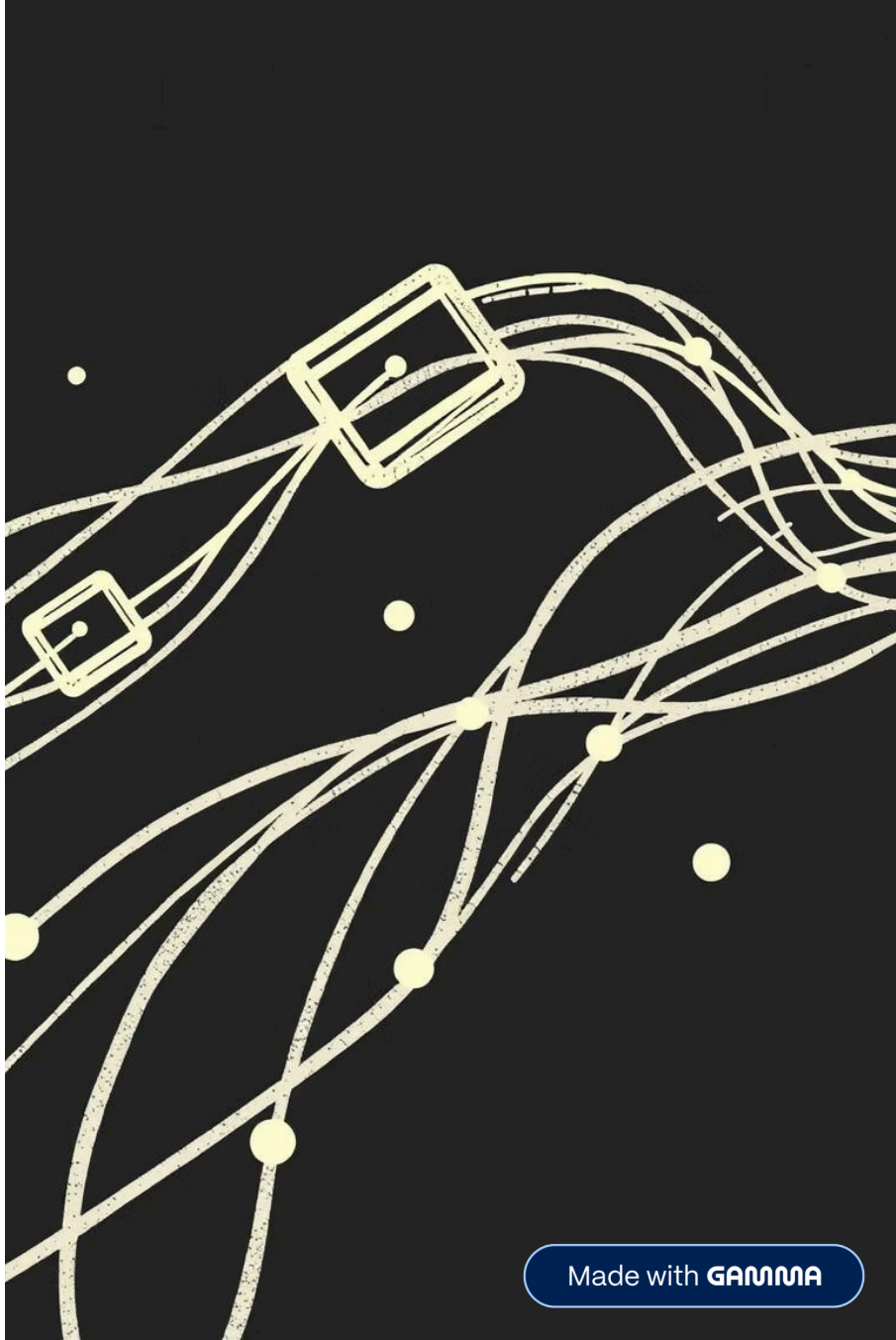
Identificação de atividades suspeitas.

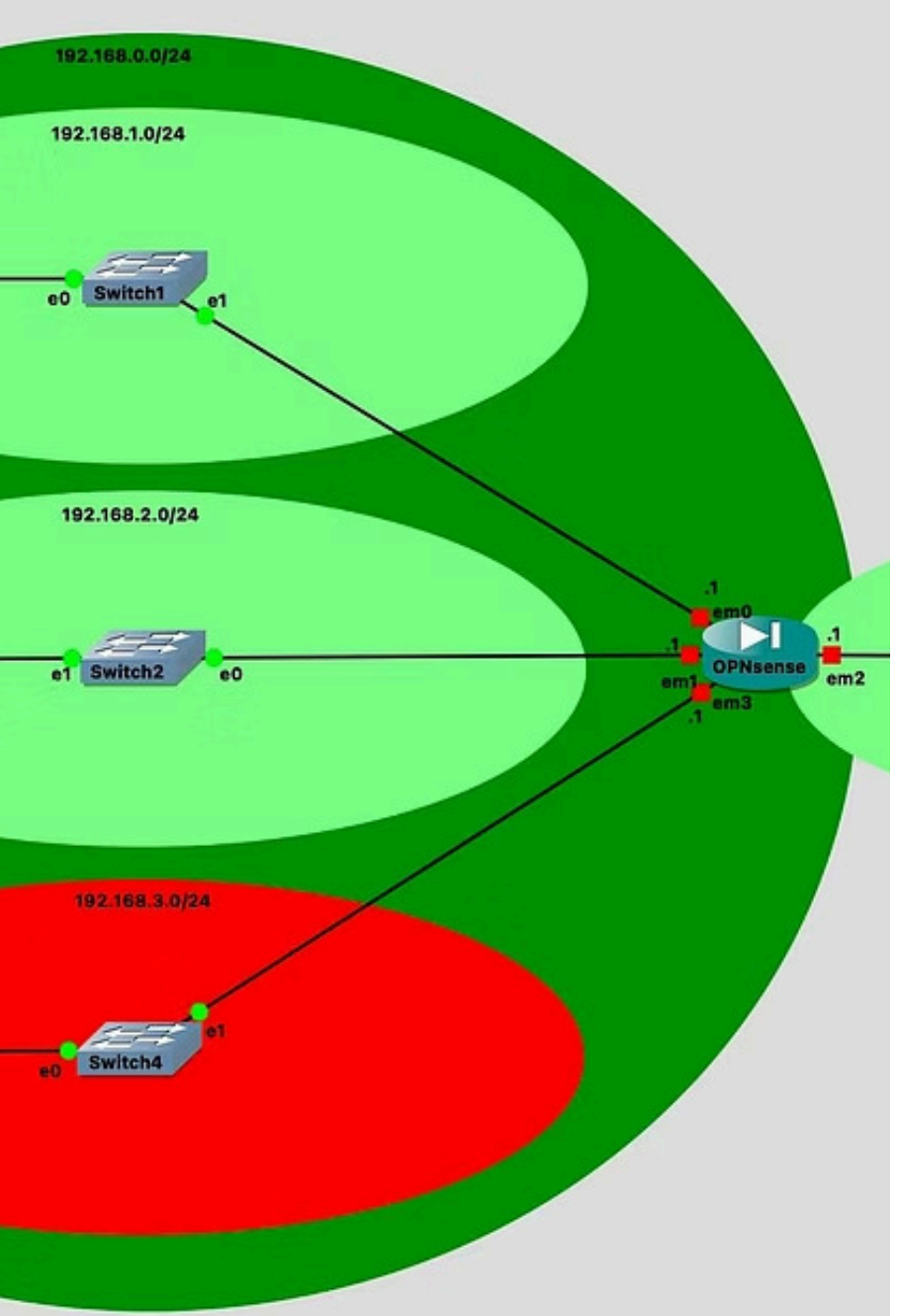
Detecção de Ataques

DDoS, SQL Injection, Port Scanning.

Alertas em Tempo Real

Análise de registos de tráfego.





Topologia

A rede está organizada em diferentes zonas, com destaque para a rede interna (segura), composta pelas sub-redes 192.168.1.0/24, 192.168.2.0/24 e 192.168.3.0/24. Estas redes são utilizadas por máquinas legítimas como o Ubuntu e o PC1, e todas têm como gateway o OPNsense, que atua também como firewall e ponto central de monitorização com Suricata ativado em múltiplas interfaces.

A rede externa, representada pela sub-rede 209.20.1.0/24, simula o acesso à Internet e está conectada ao OPNsense através do roteador R1. Já as zonas vermelhas representam redes de ataque: a 10.0.0.0/24 simula um atacante externo, enquanto a 192.168.3.0/24 contém um atacante interno. Essas redes foram montadas para realizar ataques DDoS SYN-Flood e port scanning.

Ferramentas Chave para o NIDS

Estas ferramentas são a base da nossa solução NIDS neste projeto, cada uma com um papel específico na simulação, segurança e deteção de ameaças.

GNS3

Emulador gráfico para simular redes complexas.

OPNsense

Firewall open-source com segurança avançada.

Suricata

Motor de deteção de intrusões (NIDS/IPS) de alto desempenho.

Docker

Plataforma de contentorização para isolar aplicações.

OPNsense vs. Suricata: Sinergia

A combinação de OPNsense e Suricata oferece uma solução robusta. A integração simplificada e o desempenho superior são vantagens chave.

Integração Simplificada

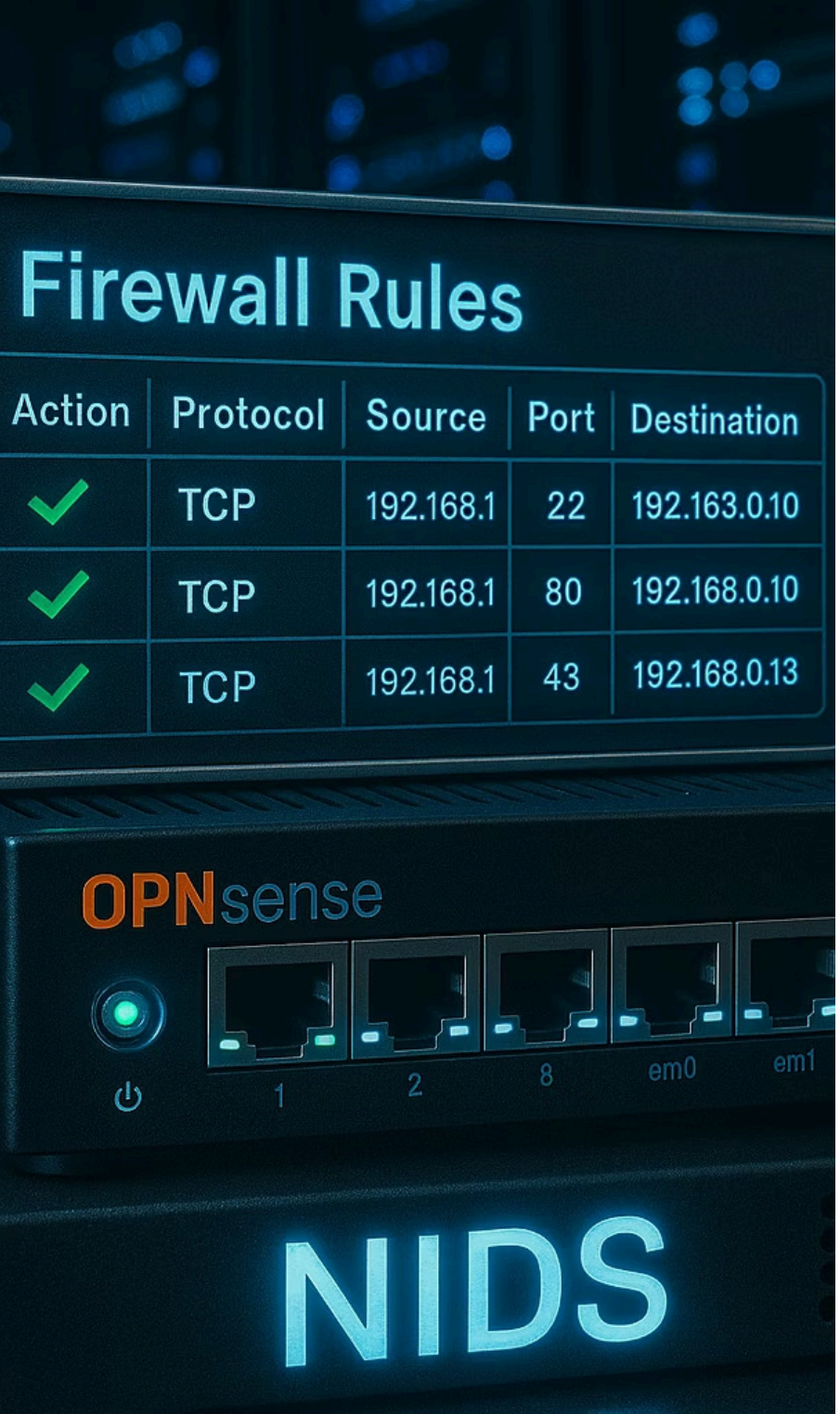
OPNsense integra Suricata como plugin nativo, configurável via interface gráfica.

Desempenho Superior

Utiliza multithreading e módulos de offload para alta performance.

Atualizações e Comunidade

Ambas são open-source, com atualizações regulares e suporte ativo da comunidade.



Configuração do OPNsense

A configuração do OPNsense é crucial para o funcionamento do NIDS. Envolve a definição de interfaces, regras de NAT e firewall, e ativação de serviços.

Interfaces de Rede

WAN, LAN, OPT1 e OPT2.

Regras de NAT

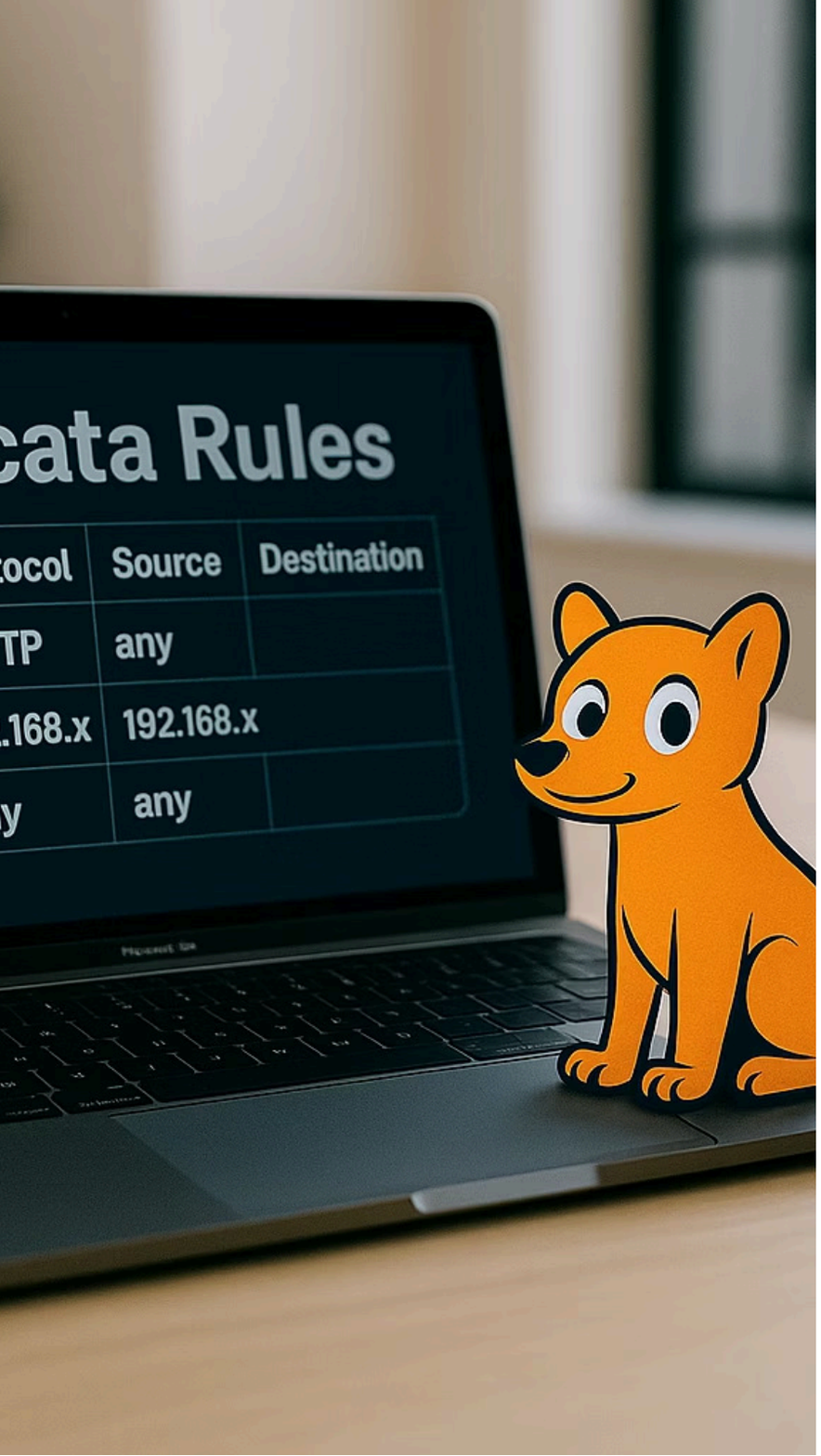
Acesso à rede interna.

Regras de Firewall

Permissão/bloqueio de tráfego.

Ativação de Serviços

Ativação do Suricata.



Configuração do Suricata: O Motor de Detecção

A ativação e configuração das regras do Suricata são essenciais para a deteção de intrusões. A monitorização e análise de logs permitem ajustar a eficácia.

1

Ativação

Associar Suricata às interfaces de rede para monitorização.

2

Criação de Regras

Definem comportamentos suspeitos, criadas manualmente. (Custom Rules)

3

Monitorização

Escolher interfaces de rede a analisar (LAN, WAN).

4

Análise de Logs

Alertas e eventos detetados para ajuste de regras.

Criação de Regras no Suricata

ação protocolo ïp_origem porta_origem → p_destinoo porta_destino (opções)

Ação

alert **drop**, **reject**, pass, log

alert → gera um alerta

drop → bloqueia o pacote

Protocolo

tcp, udp, icmp, ip

Opções

sid → identificador único da regra

rev → versão da regra

msg → mensagem de alerta

content → padrão a procurar no payload

Origem e destino

any any → 192.168.1.1.00.10 80

→ qualquer origem para destino 19.168.1.100 na porta 80

Exemplo completo:

alert tcp any any → 192.168.1.1.100 80 (msg:"Tentativa de acceso HTTP"; content:"GET"; sid:10001; rev:1;)

Ataques Comuns e Defesa

Port-scanning e SYN-Flood são ataques comuns. O NIDS ajuda a identificar e mitigar estas ameaças, protegendo os serviços.

Port-Scanning

Primeiro passo de um ataque cibernético. Mapeia serviços disponíveis num alvo.

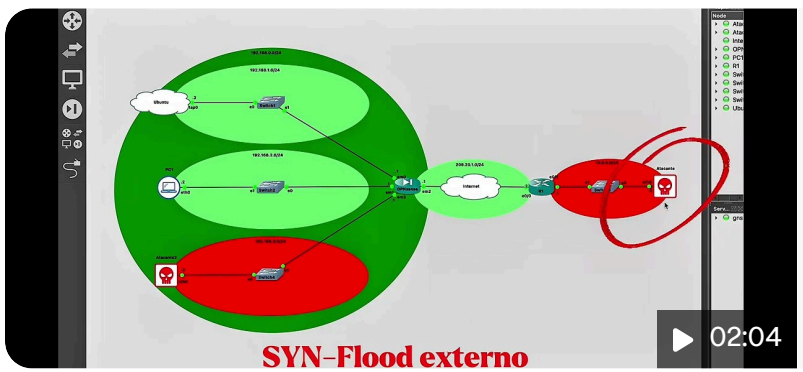
```
alert tcp any any -> any any (msg:"Possible Port Scan Detected"; flags:S; thresh
old: type both, track by_src, count 10, seconds 5; classtype:attempted-recon; si
d:1000001; rev:1;)
```

SYN-Flood

Ataque DDoS que sobrecarrega um servidor ou site.

```
alert tcp any any -> any 80 (msg:"Possible DDos Attack-SYN Flood"; flags:S; thre
shold: type both, track by_src, count 30, seconds 1; sid:1000002; rev:1;)
```

Simulação do ataque



YouTube

Sistema de detecção de intrusões na rede (NIDS)

• Objectivo: Configurar e implementar um Sistema de Detecção de Intrusão na Rede para monitorizar o tráfego da rede e detectar actividades ou ataques suspeitos. •...

Análise Pós-Ataque e Desafios

A análise pós-ataque evidencia desafios importantes, como a sofisticação crescente dos ataques, a limitação de regras de deteção e eventuais restrições de desempenho do sistema. A ocorrência de falsos negativos permanece uma preocupação crítica, exigindo ajustes contínuos nas regras e na estratégia de monitorização.

1 **Ataques Sofisticados**

Disfarçados ou complexos.

2 **Regras Incompletas**

Ou desatualizadas.

3 **Má Configuração**

Erros na configuração.

4 **Limitações de Desempenho**

Muito tráfego ou ataques em volume.

5 **Falsos Negativos**

Semelhança com tráfego legítimo.

6 **Rede Segura, Acesso Inteligente**

Uma rede segura que ao mesmo tempo se comunique com o exterior

Conclusão e Melhorias Futuras

O projeto NIDS demonstrou a capacidade de monitorizar e detetar ameaças. Melhorias futuras incluem otimização de regras e integração com outras ferramentas de segurança.

NIDS Eficaz

Monitorização e deteção de ameaças.

Análise Avançada

Melhorar a inteligência de ameaças.

Otimização de Regras

Redução de falsos positivos/negativos.

Integração

Com outras ferramentas de segurança e IA.

Agradecimentos

Agradeçemos aos Professores **Pedro Sobral** e **Bruno Gomes** (Redes II) e ao Professor **Paulo Rurato** (LPI) pelo apoio e orientação ao longo do projeto.