Network Security: Open-Source Intrusion Detection Systems

Grupo 101

Ana Murta (A93284)
Ana Henriques (A93268)
Leonardo Freitas (A93281)

março, 2022

REDE DE COMPUTADORES
Licenciatura em Engenharia Informática

INTRODUÇÃO

Como proteger a informação de *cyber threats*?

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

— FROM WIKIPEDIA

SOLUÇÃO

Intrusion Detection System (IDS)

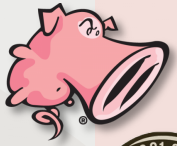
O que é? Como funciona?

Ativo..

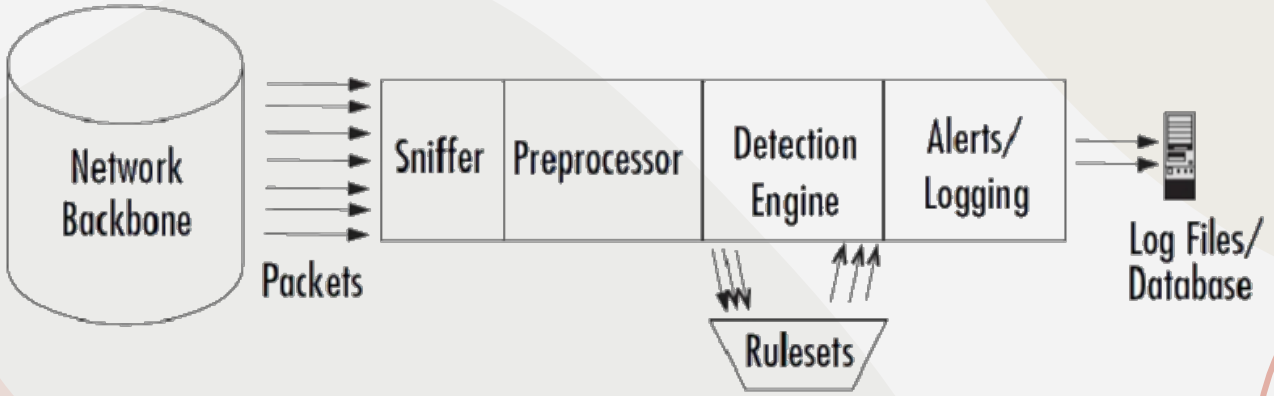
Passivo?

Open-Source IDS *Tools*

Network Based Intrusion Detection System (NIDS)	*Host Based Intrusion Detection System* (HIDS)
❑ Snort ❑ Suricata ❑ Security Onion	❑ OSSEC ❑ Samhain ❑ Security Onion



SNORT


Network Backbone
Packets
Sniffer
Preprocessor
Detection Engine
Alerts/ Logging
Log Files/ Database
Rulesets

VANTAGENS DESVANTAGENS

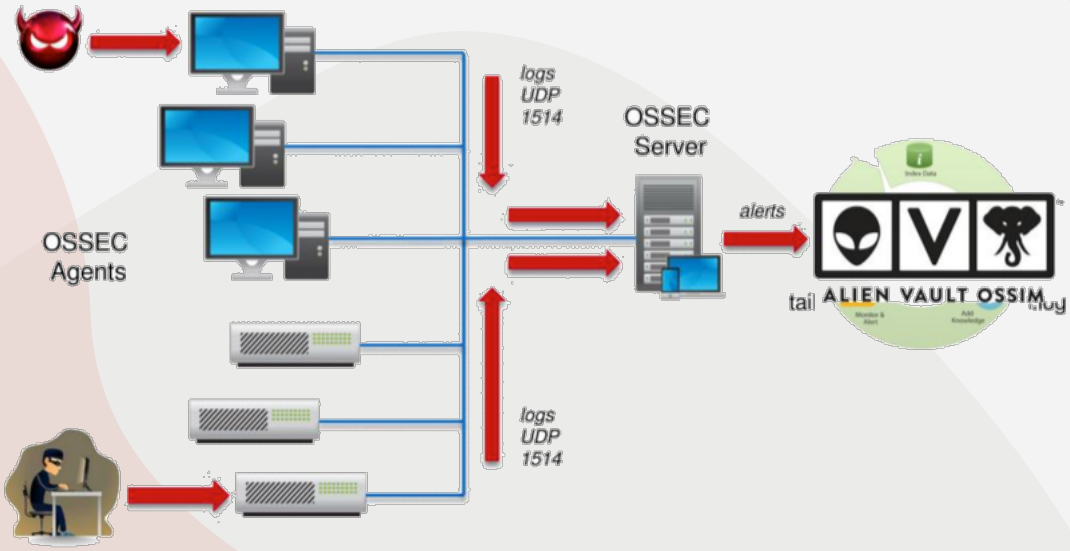
Gratuito e Portátil.
Rápidas respostas a ameaças.
Fácil de configurar e de implementar.
Conjunto bem documentado de assinaturas.

✖

Capacidade analítica limitada.
Implementação lenta.
Falha na detação de pacotes fragmentados a altas velocidades.

S — N — O — R — T

OSSEC


logs
UDP
1514
OSSEC
Server
alerts
OSSEC
Agents
tail
ALIEN VAULT OSSIM
logs
UDP
1514

VANTAGENS DESVANTAGENS

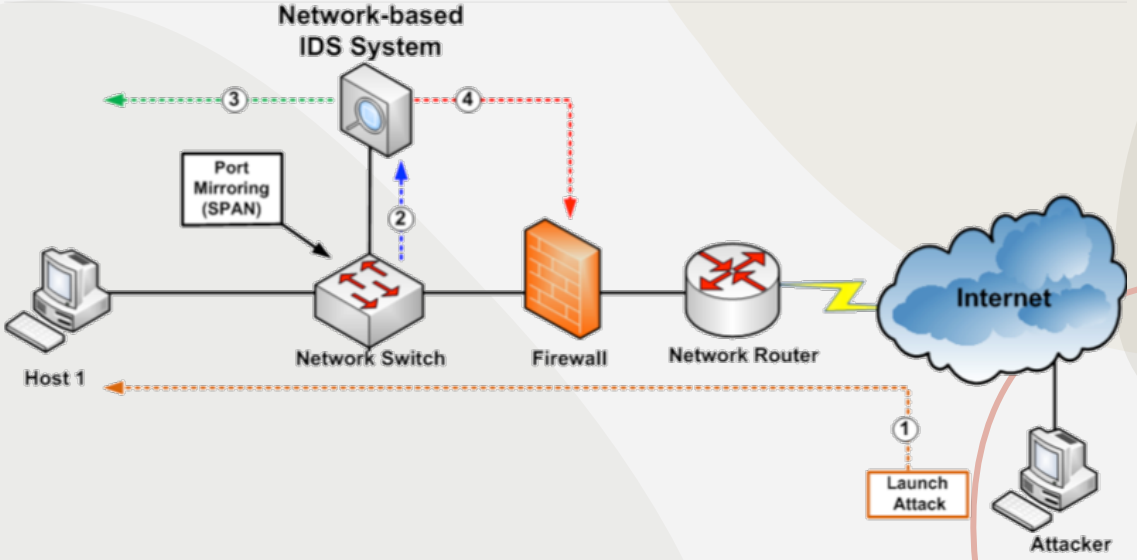
Usado tanto no modo local como no modo *server-agent*.
Versão de código aberto compatível com vários sistemas operativos.
Quase todos os recursos na versão de código aberto.

✖

Dificuldade em efetuar *upgrades* entre versões.
Problemas em coordenar chaves pré-compartilhadas.

O — S — S — E — C

Security Onion



VANTAGENS DESVANTAGENS

Gratuito e sem custo de licenças.
Boa base de apoio.
Fácil instalação e configuração.
Simples interface.

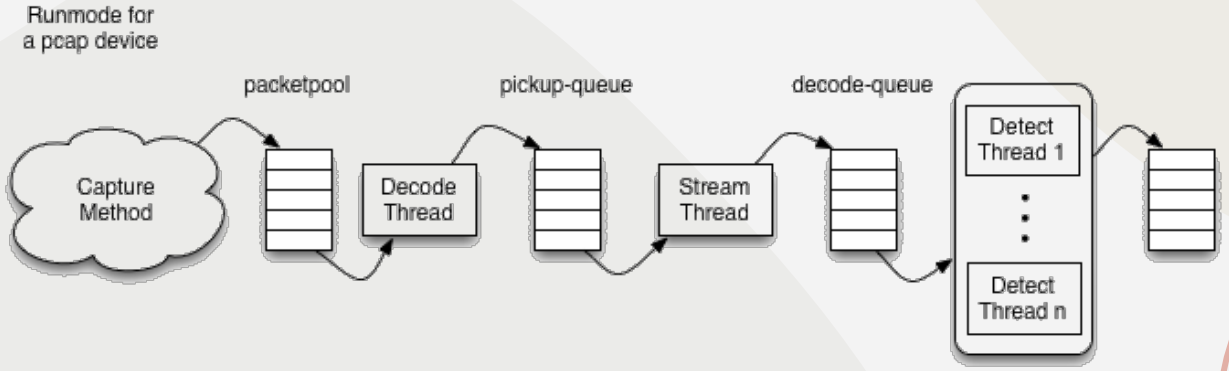
✖

Algum conhecimento intermédio de GNU/Linux.
Necessita de mais recursos para redes maiores.

S. — O — N — I — O — N

Breve abordagem...

Suricata



CONCLUSÃO

IMPORTÂNCIA DO IDS