Sistema de Detecção de Intrusos

Thiago de Lima Vasconcelos

Elton do Amaral Ramos Monteiro

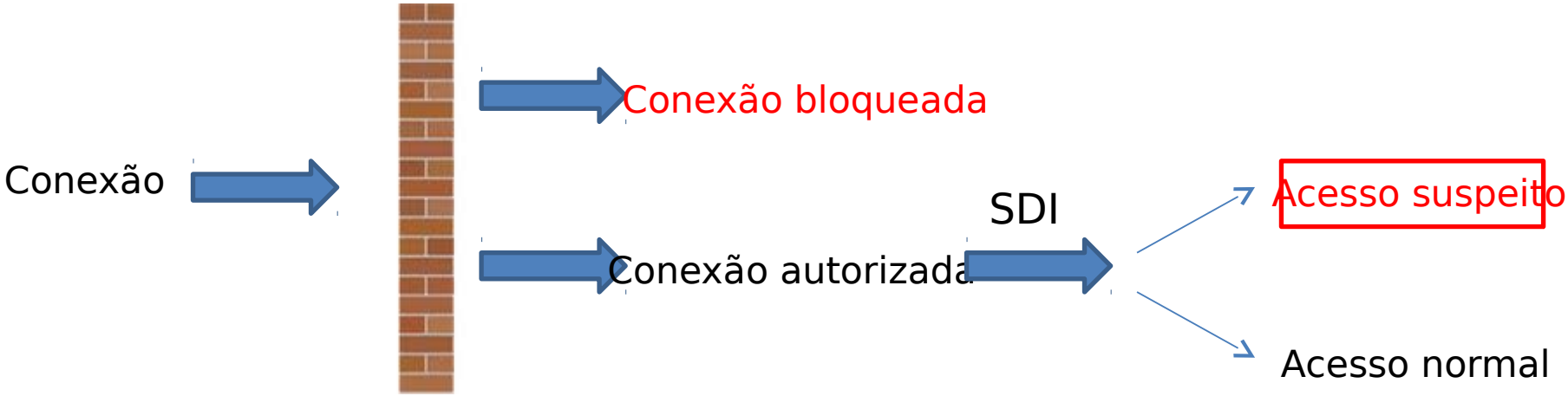
Riguel Pena de Góes

Definição

• Um sistema de detecção de intrusos (***I****nstrusion* ***D****etection* ***S****ystem*) dedica-se a descobrir quando uma rede está sendo acessada:

- Por indivíduos não autorizados;

- Com prática de utilização conflitante com as normas.



Agenda

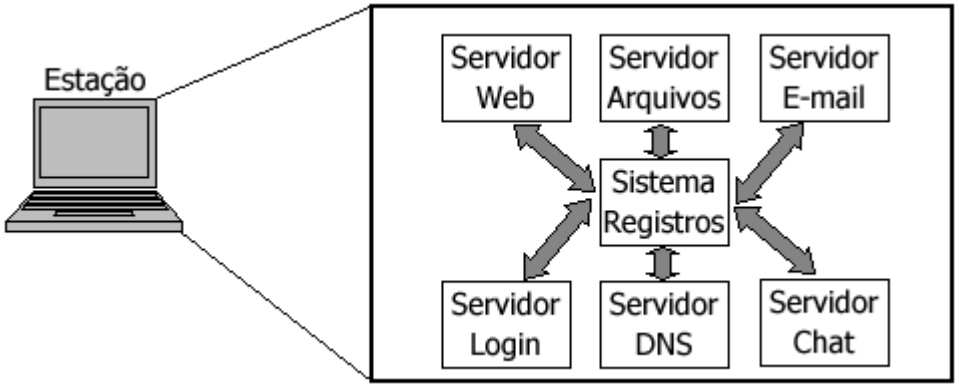
- Tipos de sistema de detecção e análise
  - SDI baseados em host
  - SDI baseados em redes
  - SDI baseados híbridos
- Potes de mel
- Aplicações nos registros
- Perguntas

Agenda

- Tipos de sistema de detecção e análise
  - SDI baseados em host
  - SDI baseados em redes
  - SDI baseados híbridos
- Potes de mel
- Aplicações nos registros
- Perguntas

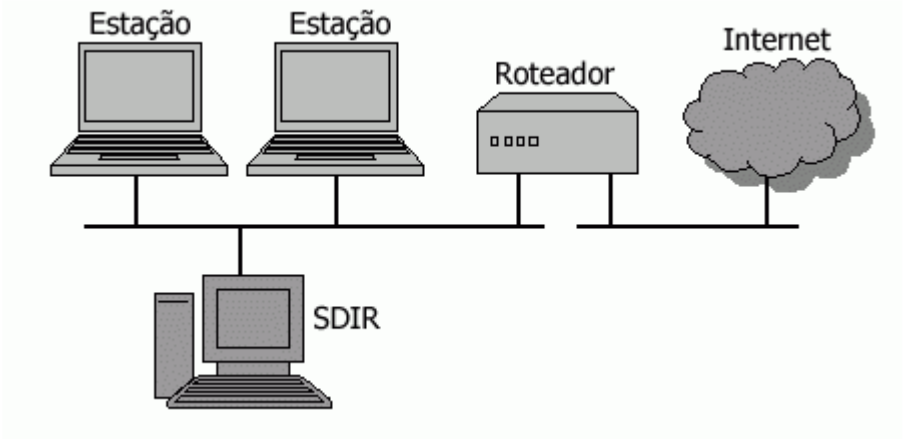
SDI baseados na estação

• Objetivo de monitorar toda atividade em uma máquina específica, geralmente um servidor



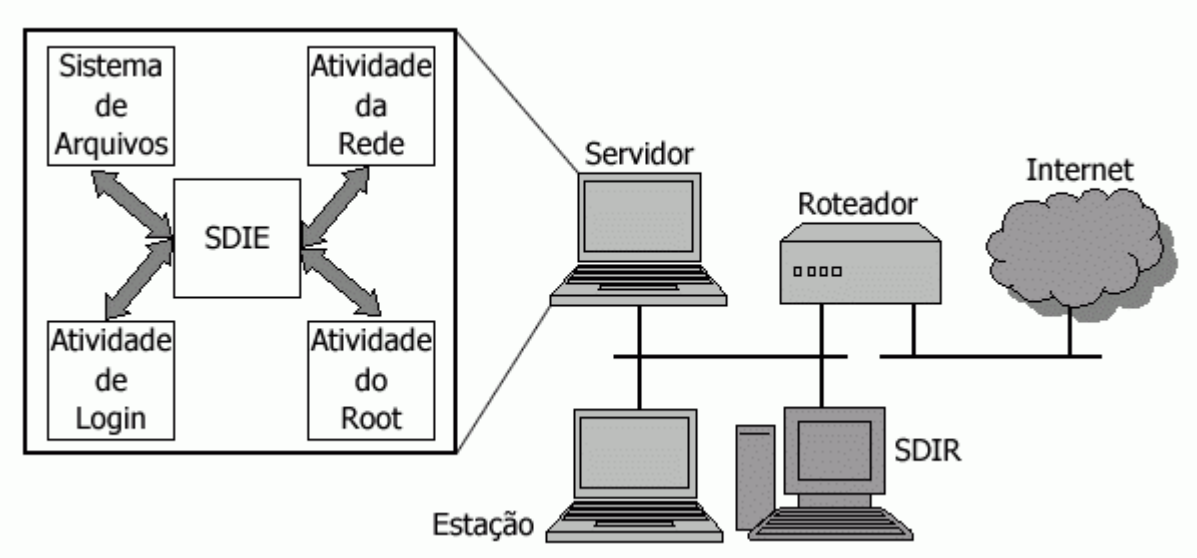
SDI baseados na Rede

- Monitora todos os dados que passam pela rede e faz uma análise para saber se estão dentro dos padrões permitidos



SDI Híbridos

• Sistema onde os dois tipos de detecção se completam, onde os SDIEs atuam nas estações críticas e o SDIR atua analisando o tráfego da rede



Análise de SDI baseados na estação

Existem alguns tipos de atividades que podem ser monitoradas na estação, como:

- Monitoramento da atividade da rede
- Monitoramento da atividade de login
- Monitoramento da atividade do super-usuário
- Monitoramento do sistema de arquivos

Análise de SDI baseados na Rede

Existem alguns tipos de atividades que podem ser monitoradas na rede, como:

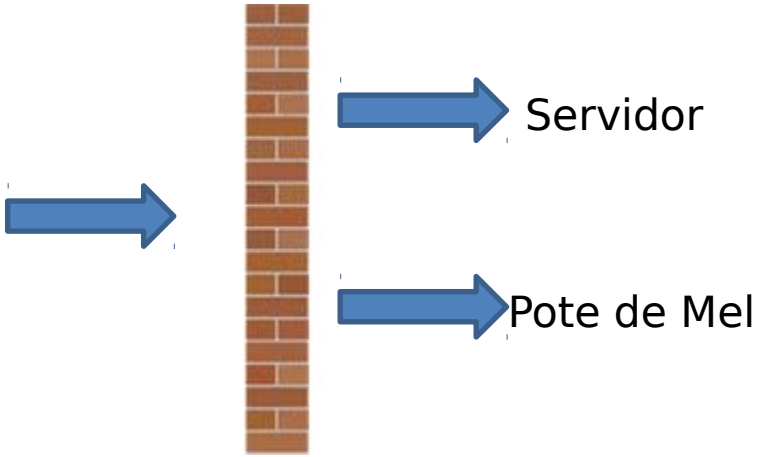
- Análise por assinatura
- Análise por protocolo
- Análise por estado do protocolo

Agenda

- Tipos de sistema de detecção e análise
  - SDI baseados em host
  - SDI baseados em redes
  - SDI baseados híbridos
- Potes de mel
- Aplicações nos registros
- Perguntas

Potes de mel

• Estação disponível para invasão, com a função de coletar informações de como foi feita a invasão, assim servindo como gerador de informações para melhorias na rede



Agenda

- Tipos de sistema de detecção e análise
  - SDI baseados em host
  - SDI baseados em redes
  - SDI baseados híbridos
- Potes de mel
- Aplicações nos registros
- Perguntas

Base de dados

- As informações são armazenadas, podendo ser pesquisadas e acessadas por um navegador web.

Alertas

- Pode ser dado de duas formas:
  - Local (e-mail)
  - Sistema remoto

Agenda

- Tipos de sistema de detecção e análise
  - SDI baseados em host
  - SDI baseados em redes
  - SDI baseados híbridos
- Potes de mel
- Aplicações nos registros
- Perguntas

Perguntas

1) Qual a função de um sistema de detecção de intrusos?

2) Qual a diferença entre os sistemas de detecção de intrusos baseados na rede e baseados na estação?

3) Por que é importante o uso de potes de mel?

4) De que formas pode ser dado o alarme ao usuário, quando seu computador está sofrendo ataque?

OBRIGADO