

Segurança Lógica e Física de Redes

PRINCIPAIS TIPOS DE ATAQUES A REDES E COMO EVITÁ-LOS

Prof. Felipe Oliveira
fdoprof@gmail.com

Agenda

- Segurança de acesso
- Senhas
 - Fragilidades e como corrigí-las
- Controle de acesso físico
- Controles biométricos
- Controles de acesso lógico
- **Detecção de Intrusão**
- Histórico de acessos e auditoria
- Protocolos de Autenticação



Detecção de Intrusão

Introdução

- **Segurança = visibilidade + controle**
- **Visibilidade:** É a habilidade de ver e entender a natureza e o tráfego de uma rede
- **Controle:** É a habilidade de afetar o tráfego da rede incluindo o acesso à rede ou a partes dela.

Detecção de Intrusão

Analogia com a segurança de um aeroporto

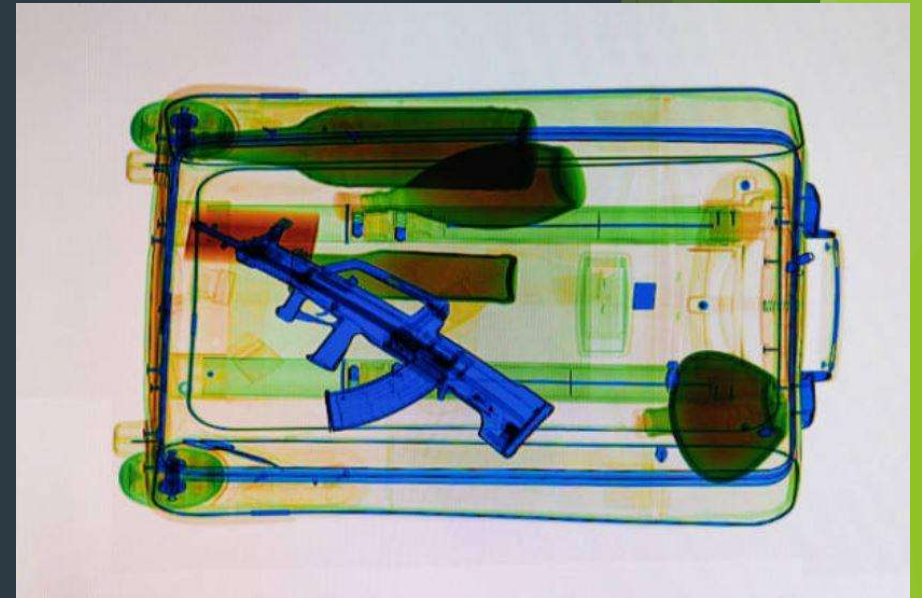
- **Controle:** guarda de aeroporto



Detecção de Intrusão

Analogia com a segurança de um aeroporto

- **Visibilidade:** detector de metais, raio-x de bagagem, etc.



Detecção de Intrusão

Analogia com a segurança de um aeroporto

- Dispositivos de visibilidade **aumentam a eficiência dos guardas**

Sem a combinação de **controle e visibilidade**, neste exemplo, o aeroporto é mais ou menos seguro dependendo de **quão bons são os guardas em realizar seu trabalho**.

- Se o guarda for insuficientemente treinado para identificar possíveis ameaças ou muito ocupados com outras tarefas para efetivamente reforçar o controle da entrada, resulta diretamente numa queda da segurança.

Detecção de Intrusão

Analogia com a segurança de um aeroporto

- Nas redes de computadores não é diferente, pois possuem informações sobre:
 - **Pessoas**
 - **Negócios**
 - **Clientes**
 - **Etc.**
- Necessitam também de **dispositivos que proporcionem visibilidade** do que está trafegando por elas, **para melhorar a performance dos dispositivos de controle**, e com isso aumentar a segurança.

Detecção de Intrusão

Analogia com a segurança de um aeroporto

- Principais dispositivos de controle uma rede são:
 - Firewall
 - Roteadores
 - Listas de controle de acesso (ACLs)
 - Permissões de usuários.
- Principal dispositivo de visibilidade é o **sistema de detecção de intrusos (IDS)** e estende-se aos scanners de vulnerabilidades.

Detecção de Intrusão

O que são sistemas de detecção de intrusos?

- Sistemas de Detecção de Intrusos **são programas** (softwares independentes ou embutidos em hardware proprietário) **que monitoram uma rede ou um host a procura de sinais padrões de comportamento que sejam considerados maliciosos**, ou seja, que podem constituir um ataque ou uma outra atividade não permitida.

Detecção de Intrusão

O que são sistemas de detecção de intrusos?

- A maioria dos IDSs pode ser descrita em termos de 3 componentes fundamentais:
 - **Fonte de Informações:** As diferentes fontes de informações sobre eventos usados para determinar quando uma intrusão ocorre. As fontes mais comuns são um **host** ou um **segmento de rede**.
 - **Análise:** É a parte do sistema de detecção de intrusos que efetivamente, **organiza e dá sentido aos eventos derivados da fonte de informações** decidindo quando estes eventos indicam que uma intrusão está ocorrendo ou já foi realizada. Os métodos de análise mais comuns são **detecção baseada em assinaturas** e **detecção baseada em anomalias**.

Detecção de Intrusão

O que são sistemas de detecção de intrusos?

- A maioria dos IDSs pode ser descrita em termos de 3 componentes fundamentais:
 - **Resposta:** É o conjunto de ações que o sistema faz quando detecta uma intrusão. Estas são tipicamente agrupadas em medidas ativas e passivas, com medidas ativas envolvendo intervenção automatizada em parte do sistema e medidas passivas envolvendo a geração de relatórios para posterior interpretação e intervenção humana.
- De acordo com a fonte de informações podemos classificar os IDSs em: **baseado em rede** e **baseado em host**.

Detecção de Intrusão

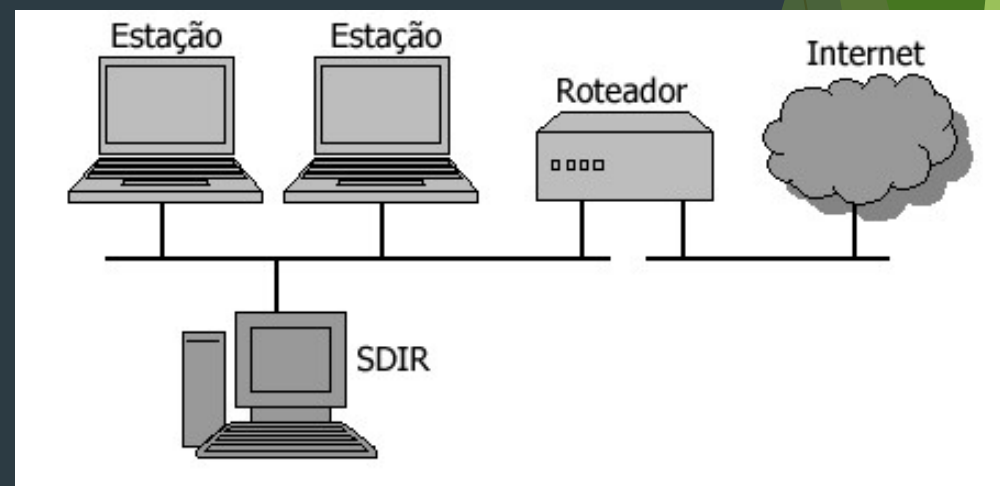
O que são sistemas de detecção de intrusos?

- A maioria dos IDSs pode ser descrita em termos de 3 componentes fundamentais:
 - **Resposta:** É o conjunto de ações que o sistema faz quando detecta uma intrusão. Estas são tipicamente agrupadas em medidas ativas e passivas, com medidas ativas envolvendo intervenção automatizada em parte do sistema e medidas passivas envolvendo a geração de relatórios para posterior interpretação e intervenção humana.
- De acordo com a fonte de informações podemos classificar os IDSs em: **baseado em rede** e **baseado em host**.

Detecção de Intrusão

Baseada na Rede (SDIR)

- A maioria dos IDSs comerciais é baseada em rede.
- É um sensor que monitora o tráfego da rede
- Vantagens:
 - Poucos IDS conseguem monitorar uma rede grande
 - São passivos, ou seja, não realizam ações na rede
 - São seguros e geralmente invisíveis



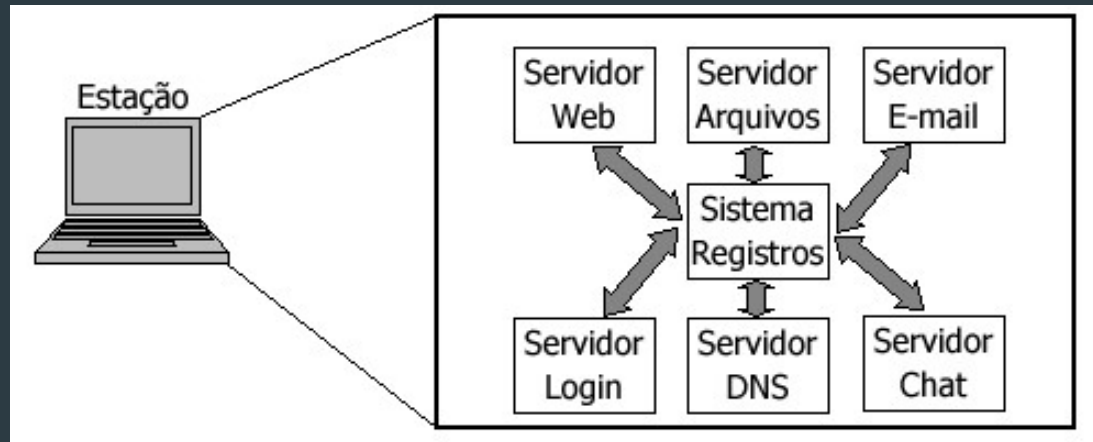
Detecção de Intrusão

Baseada na Rede (SDIR)

- Desvantagens:
 - Se o tráfego na rede for intenso, pode ter dificuldades de processamento
 - Não analisam informações criptografadas
 - Muitas empresas (e atacantes)utilizam VPNs
 - Não informa se um ataque foi bem sucedido.
 - Apenas se um ataque foi iniciado
 - O administrador deve investigar cada host atacado

Detecção de Intrusão

Baseada em Estação (SDIE)



- **Vantagens:**

- Com sua habilidade de monitorar eventos localmente num host, podem detectar ataques que não são detectados por um IDS baseado em rede
- Podem operar em ambientes onde o tráfego seja criptografado, quando os dados são encriptados no host antes do envio e decryptados no host após a recepção

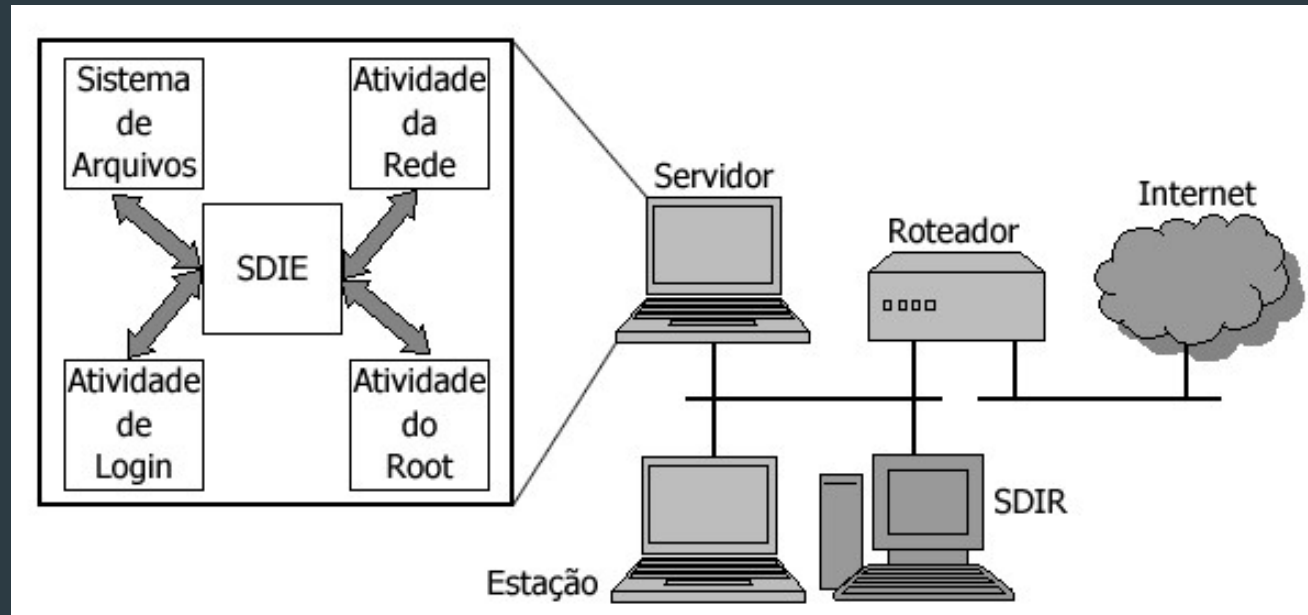
Detecção de Intrusão

Baseada em Estação (SDIE)

- Desvantagens:
 - São difíceis de gerenciar, pois para cada host monitorado deve ser instalado e configurado um IDS.
 - IDS pode ser atacado e desativado mascarando assim um ataque
 -

Detecção de Intrusão

Híbrido



Detecção de Intrusão

Sistema de detecção de intrusão

- **Registros de alarmes:** Define procedimentos de catalogação e arquivamento dos alarmes ocorridos e as providências tomadas. Deve-se atentar para a formatação dos dados, que deve ser de tal forma que possam vir a ser utilizados posteriormente em juízo, se for o caso.
- **Locais sensíveis:** Define os locais sensíveis da empresa onde deverá ser dada maior atenção.
- **Previsão de falhas e interferências.** Define regras e procedimentos caso haja falhas ou interferências nos equipamentos.
- **Localização do Painel Monitoração.**