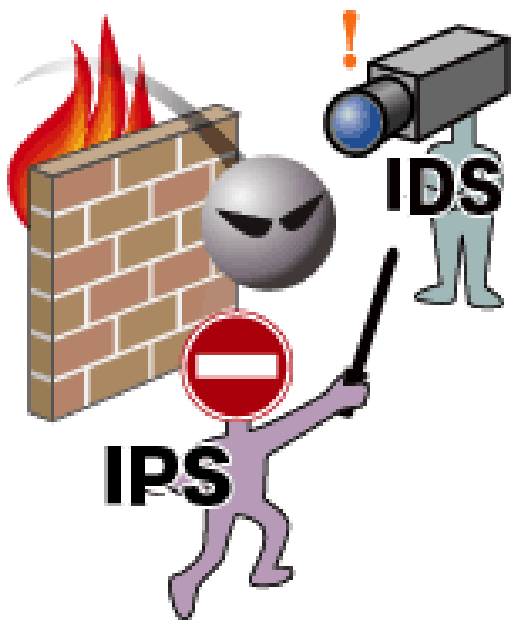
Universidade Federal do ABC

Segurança de Redes

Sistemas de Detecção de Intrusão e Honeypots

Prof. João Henrique Kleinschmidt

Sistemas de Detecção de Intrusão
IDS



Sistemas de Detecção de Intrusão

- Objetivo de um IDS é simples: detectar intrusões
  - Tarefa difícil:
  - De fato não há detecção de intrusão
  - Há apenas a identificação de evidências de intrusão, em andamento ou após o fato ter ocorrido
  - Evidências → manifestações de um ataque
    - Pode não haver manifestação
    - Pode não haver informação suficiente
    - A informação pode não ser confiável

→ detecção pode ser inviabilizada

Coleta de evidências

- Detecção confiável exige uma coleta de dados completa e confiável do sistema sendo monitorado
- Coleta de dados → informações devem se limitar a eventos relevantes para a segurança

  – Logs de auditoria gerados pelos SOs

  Informações sobre a atividade de usuários e processos

  Questão: Registro apenas das tentativas de login mal sucedidas ou registro completo de todas as chamadas de sistema (*syscalls)* realizadas por cada processo?

  – Logs de roteadores e firewalls

  Informações sobre a atividade na rede

  Questão: Registro apenas das conexões iniciadas e finalizadas ou registro completo de todos os pacotes que trafegam na rede?

Coleta de evidências

- Compromisso entre eficiência e sobrecarga
- Ex:
  - Coletar todo o tráfego de um enlace Ethernet (100 Mbps)

  100 Mbits = 12,5 MBytes → 1 s

  6000 Mbits = 750 MBytes → 1 min (60s)

  360000 Mbits ~ 44 GBytes → 1 h (3600s)

  8640000 Mbits ~ 1 TByte → 1 dia (86400s)
- Coletar informação é caro → armazenamento
  - Coletar a informação necessária
  - Dificuldade:
    - Que informações coletar?
    - Por quanto tempo?

      → diversos cenários com diferentes requisitos

Intrusão

- Definição:
- "**Ação (ou sequência de ações relacionadas)** realizada por um indivíduo malicioso (intruso) **que viola a política de segurança da organização.**"
- Pontos importantes:
  - Sem uma política de segurança não é possível definir o que é uma atividade maliciosa
  - A intrusão resulta no comprometimento de um recurso ou sistema em virtude da violação da política de segurança

Detecção de Intrusão

- Definição:

  "Processo de identificar e responder a atividades maliciosas direcionadas a recursos computacionais e de rede."

- Pontos importantes:

  – Detecção de Intrusão é um processo → envolve tecnologia, pessoas e ferramentas

  – Detecção de Intrusão é uma abordagem complementar as demais abordagens de segurança, como a adoção de mecanismos de controle de acesso, firewall e uso de criptografia.

Sistemas de Detecção de Intrusão

- **IDS -** Definição:
- "Software dedicado a realizar a detecção de intrusão em um ambiente computacional."
- Requisitos desejáveis:
  - Precisão: um IDS não deve detectar uma atividade legítima como intrusão **(falso-positivo)**
  - Desempenho: um IDS deve ser capaz de detectar uma intrusão a tempo de evitar danos ao recurso atacado
  - Completude: um IDS não deve identificar uma intrusão como uma atividade legítima **(falso-negativo)**
  - Tolerância a falhas: um IDS deve ser resistente a ataques
  - Escalabilidade: um IDS deve ser capaz de processar eventos sem perda de informação

Arquitetura

- Existem diferentes IDSs baseados em diferentes frameworks conceituais → no entanto, é possível identificar uma arquitetura comum
- Terminologia introduzida pelo grupo de trabalho CIDF (*Common Intrusion Detection Framework*):

– **Event boxes (E-boxes):**

Gera eventos utilizando dados de auditoria do sistema

– **Analysis boxes (A-boxes):**

Analisa os eventos produzidos pelo E-boxes ou em alguns casos outros A-boxes, gerando alertas (ou alarmes)

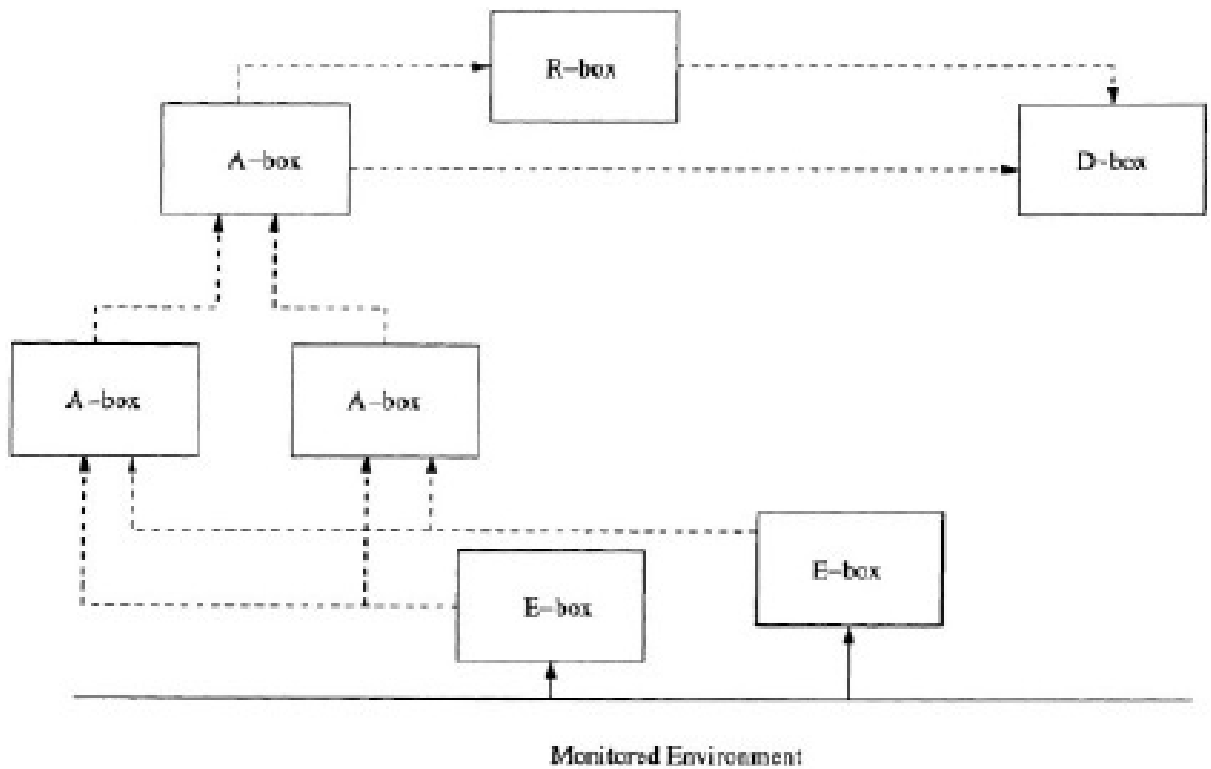
– **Database boxes (D-boxes):**

Armazenam eventos e/ou alertas → permitindo uma análise *postmortem*

– **Response boxes (R-boxes):**

Disparam a reação a um ataque detectado

- Exemplo de um IDS
- 1. Dois E-boxes produzem eventos para dois A-boxes
- 2. Os dois A-boxes analisam os eventos recebidos e geram alertas para um terceiro A-box
- 3. O terceiro A-box correlaciona os alertas recebidos e envia os resultados para o D-box e o R-box, que armazenam os alertas e disparam a resposta apropriada, respectivamente



Taxonomia

- Diferentes critérios de classificação:

– **Método de detecção:**

Define como um A-box realizará a análise dos eventos

– **Comportamento pós-detecção:**

Define como um R-box realizará a resposta aos alertas

– **Fonte de eventos:**

Define de onde um E-box obterá os dados de auditoria

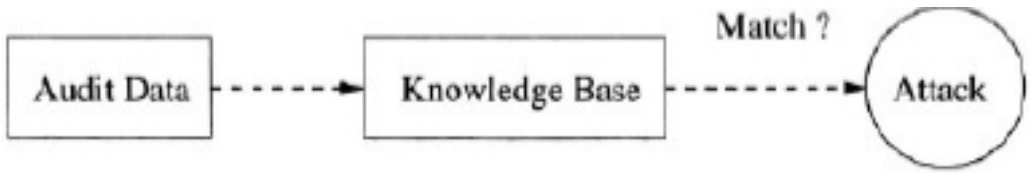
– **Frequência de análise:**

Define com que frequência um A-box realizará a análise dos eventos

Métodos de Detecção

- Duas abordagens :
- **Detecção por Mau Uso:**

  Definir assinaturas de ataques previamente conhecidos e buscar por essas assinaturas.



- **Detecção por Anomalia:**

  Definir o que é o comportamento normal do sistema e buscar por atividades que se desviam do comportamento normal.

Métodos de Detecção

- **Detecção por Mau Uso**
- Utiliza uma base de assinaturas de ataques
  - Primeiro passo: obter/construir assinaturas de ataques previamente conhecidos
- Eventos gerados são comparados com a base de dados de assinaturas
  - há correspondência → alerta gerado
  - não há correspondência → evento considerado legítimo
- Vantagens:
  - Menor taxa de falso-positivos (dependendo da qualidade da assinatura)
- Desvantagens:
  - Detecta apenas ataques conhecidos ou variações previamente modeladas (maior taxa de falso-negativos)

Métodos de Detecção

- **Detecção por Anomalia**
- Baseado na ideia de que toda atividade anômala é maliciosa
  – Primeiro passo: construir o modelo de comportamento normal do sistema (perfil)
- Eventos gerados são comparados com o perfil
  – há proximidade → evento considerado legítimo
  – não há proximidade → alerta gerado
- Vantagens:
  – Capazes de detectar ataques desconhecidos (menor taxa de falso negativos)
- Desvantagens:
  – Maior taxa de falso-positivos (dependendo da qualidade do perfil gerado)

Comportamento Pós-Detecção

- A maior parte dos IDSs são passivos
  - Quando um ataque é detectado um alerta é gerado
  - Especialista deve analisar os alertas gerados e realizar as ações necessárias
  - Demora na resposta ao ataque
- Alguns IDSs possuem capacidade de resposta
  - IPS: Sistema de Proteção a Intrusão
  - Objetivo: mitigar o ataque detectado
  - Diferentes abordagens:
    - Modificar permissões de arquivos
    - Adicionar regras de firewall
    - Finalizar processos em execução
    - Encerrar conexões de rede

Fonte de Eventos

- **Host-based IDS (HIDS)**
  - Detecta ataques contra um host específico
  - Analiza eventos produzidos pelo SO
- **Application-based IDS**
  - Detecta ataques contra uma aplicação específica
- **Network-based IDS (NIDS)**
  - Detecta ataques analisando o tráfego de rede
  - Atuam como sniffers capturando tráfego em um enlace
- **Correlation Systems**
  - Detecta ataques analisando os alertas de IDSs
  - Permite identificar correlação entre eventos de diversos IDSs

Frequência de análise

– **Análise dinâmica**

- Analisam em tempo real as atividades do sistema monitorado
- Permite disparar uma resposta apropriada quando um ataque é detectado
- Pode introduzir uma sobrecarga significativa no sistema monitorado

– **Análise estática**

- Executadas offline em períodos de tempo específicos
- Analisam um snapshot do estado do sistema
- Utilizados em análise *postmortem* → *não permitem uma* resposta ao ataque em tempo hábil
- Permite uma análise mais apurada sem impactar no desempenho do sistema monitorado

IDS

- Existem vários IDSs (*free* e comerciais)
  - Snort
  - Suricata
  - OSSEC HIDS
  - Bro IDS
  - Juniper Networks
  - Cisco IDS
  - etc

Honeypots

Definições

- *“Honeypots são recursos computacionais dedicados a serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades” (SPITZNER, 2002)*

- *“Honeynets são ferramentas de pesquisa, que consistem de uma rede projetada especificamente para ser comprometida e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes” (HOEPERS, STEDING-JESSEN & MONTES, 2003)*

Aplicações

- **Honeypots de Pesquisa** são ferramentas de pesquisa que podem ser utilizadas para observar o comportamento de invasores , permitindo análises detalhadas de suas motivações , das ferramentas utilizadas e vulnerabilidades exploradas

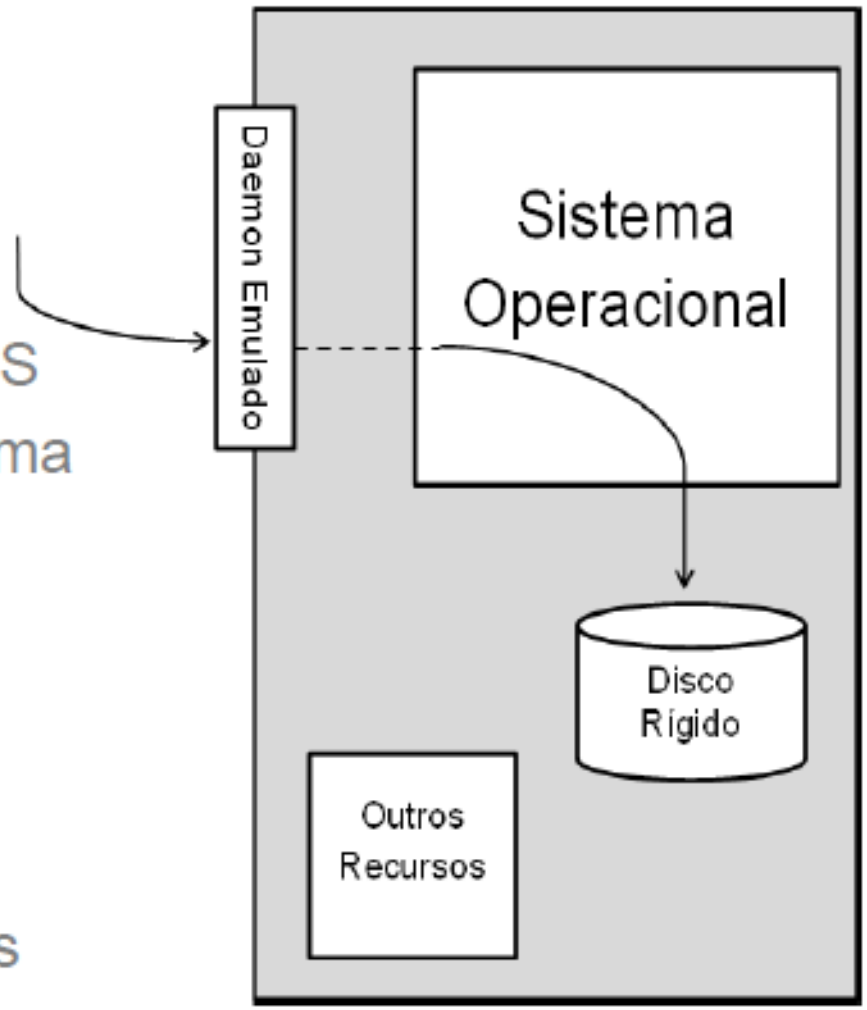
- **Honeypots de Produção** podem ser utilizados em redes de produção como complemento de sistemas de detecção de intrusão.

Honeypots

- Tradicionalmente segurança sempre foi sinônimo de defesa passiva; honeypots e honeynet provocaram uma mudança de postura, permitindo maior pró-atividade por parte dos administradores.
- **Vantagem**: são instalados de maneira que todo tráfego destinado a um honeypot é anômalo ou malicioso, sem falsos-positivos; dados de alto valor.
- **Desvantagem**: Só vê tráfego destinado a ele, introduz um risco adicional.

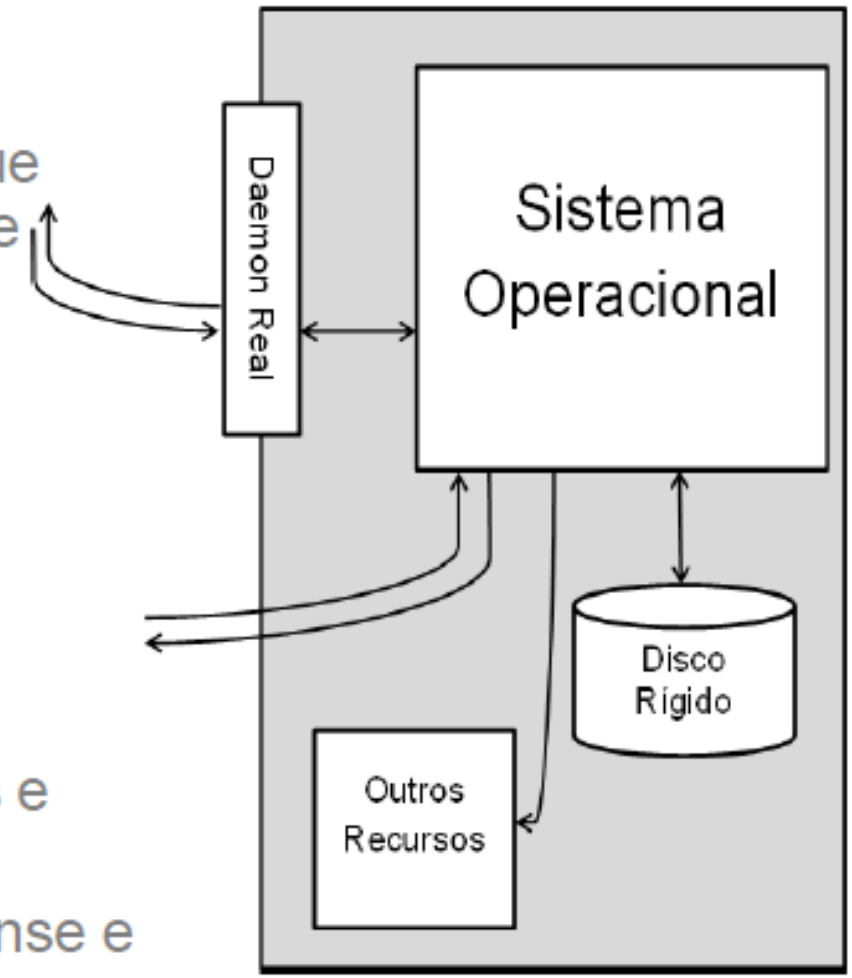
Honeypots

- Baixa interatividade
  - Emula serviços e sistemas
  - Fácil configuração/manutenção
  - Baixo Risco de comprometimento
  - Excelentes complementos para IPS
  - Atacante não tem acesso ao sistema operacional real
- Aplicabilidade:
  - Detectar e identificar ataques internos/externos
  - Coletar assinaturas de ataques
  - Detectar máquinas comprometidas
  - Coletar códigos maliciosos



Honeypots

- Alta interatividade
  - Serviços legítimos
  - Cuidados especiais para evitar que sejam usados para lançamento de ataques
  - Coleta de inteligência, análise de tendências, *0-day attacks* (novas vulnerabilidades), captura de ferramentas, entre outros
  - Difíceis de administrar e manter
- Aplicabilidade
  - Análise detalhada de ferramentas e vulnerabilidades exploradas
  - Coletar material para análise forense e treinamento de pessoal

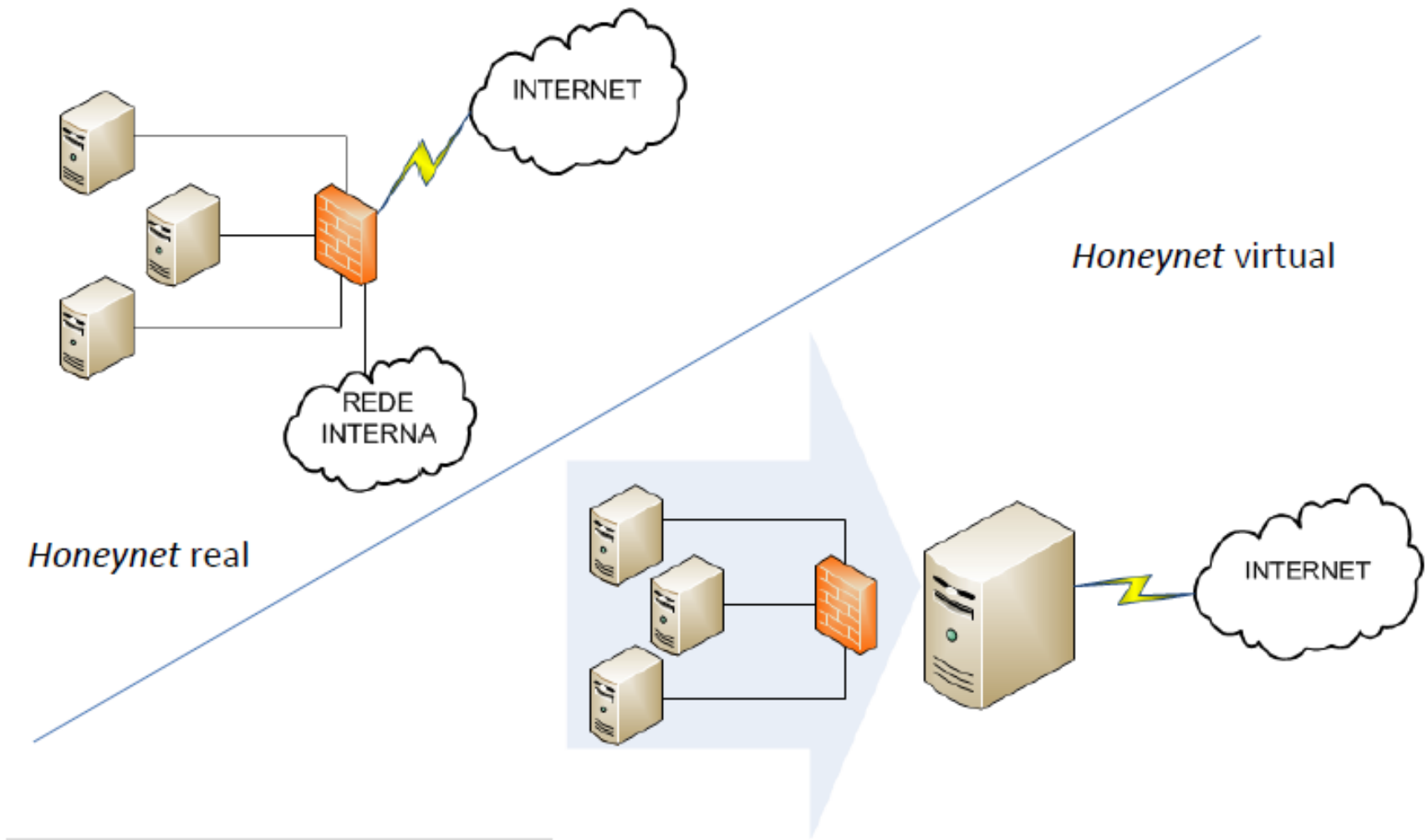


Honeynets

- Redes com múltiplos sistemas e aplicações
- Possuem mecanismos robustos de contenção
- Possuem mecanismos de captura de dados e geração de alertas
- Devem permitir o trabalho do invasor
- Não haver poluição de dados

  – **somente tráfego gerado por "*blackhats", sem testes ou tráfego gerado pelos administradores***
- Controle

Honeynets


INTERNET
REDE
INTERNA
Honeynet real
Honeynet virtual
INTERNET

Aplicação - Honeynets

- Detectar sondas e ataques automatizados
- Captura de ferramentas, novos *worms, entre outros*
- Identificação de ataques internos (*honeypots internos, honeytokens)*
- Auxiliar mecanismos de defesa como *firewall, IDS e IPS*
- Identificar as máquinas infectadas/comprometidas
- Utilizar os dados para gerar relatórios

Riscos

- Ocorrer o comprometimento
  - – do sistema operacional
  - – do *software do honeypot*
- Atrair atacantes para a rede onde está o *honeypot*
- Um erro nos mecanismos de controle ou na configuração pode:
  - –permitir que o *honeypot seja usado para prejudicar outras redes*
  - –abrir uma porta para a rede da sua organização
  - –Um comprometimento associado com sua organização pode afetar a sua imagem

- Honeynet.BR Project
  –http://www.honeynet.org.br/
- Brazilian Honeypots Alliance
  –http://www.honeypots-alliance.org.br/
- The Honeynet Project
  –http://www.honeynet.org/
- Honeynet Research Alliance
  –http://www.honeynet.org/alliance/
- Honeypots: Tracking Hackers
  –http://www.tracking-hackers.com/book/
- Know Your Enemy, 2nd Edition
  –http://www.honeynet.org/book/