UNIVERSIDADE PORTUCALENSE

Deteção de intrusões

IDS – Intrusion Detection System

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O que é a deteção de intrusões

- **Intrusões** são atividades que violam a politica de segurança de um sistema
- **Deteção de intrusões** é o processo utilizado para identificar as intrusões.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Deteção de intrusão - características

- O Sistema de deteção de intrusão **monitoriza** todo ou parte de um sistema
- A deteção da intrusão **ocorre quer durante quer depois da intrusão**
- O Sistema de deteção de intrusão pode ser **invisível ou anunciado**

DICT DEPARTAMENTO **INOVAÇÃO** **CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

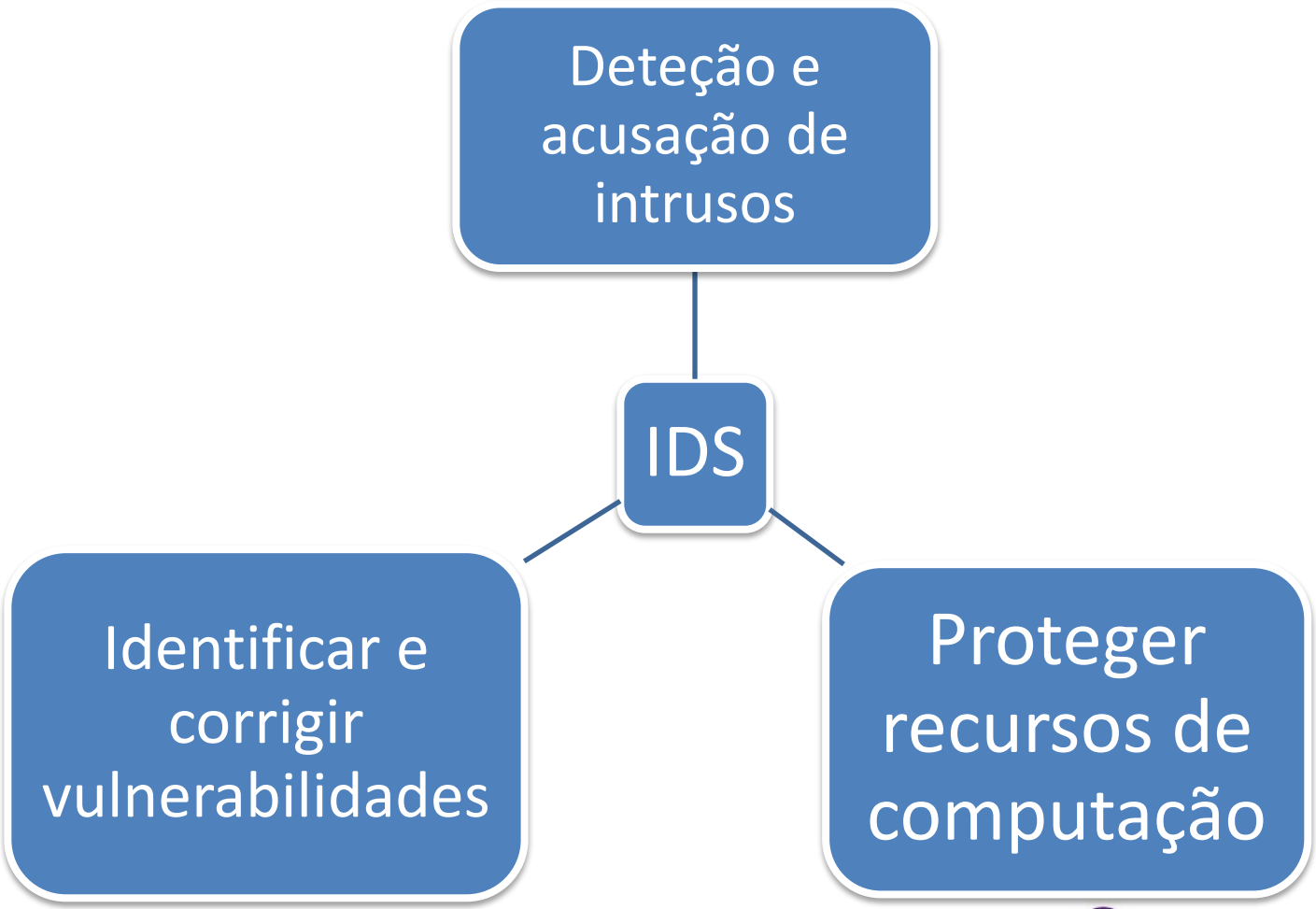
Deteção de intrusão - características

- Se uma **atividade suspeita** ocorre **é produzido um alarme (ou desencadeada uma ação),** ficando registada a atividade para possível desenvolvimento posterior
- **Pode ser necessária a intervenção humana** para o processamento de alarmes
- Os sistemas de deteção de intrusão podem **produzir alarmes ou respostas automatizadas**

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Porquê utilizar um IDS



UNIVERSIDADE PORTUCALENSE

Terminologia

- Categorias de análise de intrusão:
  - **Deteção por assinatura de ataque**: identifica padrões correspondentes a ataques conhecidos
  - **Deteção de anomalias:** identifica qualquer desvio inaceitável do comportamento esperado

UNIVERSIDADE PORTUCALENSE

Terminologia

Ataque:

- Uma **ação realizada pelo intruso**, contra a vítima.
- O intruso realiza um ataque com um objetivo específico em mente.
- Do ponto de **vista de um administrador** responsável pela manutenção de um sistema, um ataque é um **conjunto de um ou mais eventos que podem ter um ou mais efeitos de segurança**.
- Do **ponto de vista de um intruso**, um ataque **é um mecanismo para cumprir um objetivo**

UNIVERSIDADE PORTUCALENSE

Terminologia

Exploit

- **Processo de utilização de uma vulnerabilidade** para violar uma política de segurança.
- Uma ferramenta ou um método definido que pode ser utilizado para violar uma política de segurança é muitas vezes referido como exploração de script

Falso negativo

- Um evento que **o IDS não consegue identificar como uma intrusão quando ocorreu**

UNIVERSIDADE PORTUCALENSE

Terminologia

Falso positivo

- Um evento que **o IDS identifica como uma intrusão quando não ocorreu nenhum**.

Incidente

- O **conjunto de dados que representam um ou mais ataques relacionados**. Os ataques podem estar relacionados pelo atacante, tipo de ataque, objetivos, locais, ou de tempo

Intruso

- A **pessoa que realiza um ataque**. Atacante é um sinónimo comum para intruso

UNIVERSIDADE PORTUCALENSE

Terminologia

Intrusão

- Ataque bem sucedido

Vulnerabilidade

- **Uma característica ou uma combinação de características de um sistema que permite que um adversário coloque o sistema num estado que é contrário aos desejos das pessoas responsáveis pelo sistem**a e aumenta a probabilidade ou magnitude de um comportamento indesejável do sistema

UNIVERSIDADE PORTUCALENSE

Metodologia da deteção da intrusão

- Passivo: (após o fato ou solução em linha)
  - Análise de pistas de auditoria
  - Análise de tráfego de rede
  - Deteção de anomalias
  - Deteção de uso indevido
  - Combinação destes métodos
- Positivo: (antes do fato)
  - Honeypot

UNIVERSIDADE PORTUCALENSE

Metodologia da deteção da intrusão

- Honeypot
  - Algo atraente deixado para o intruso
  - Fácil de encontrar, contas falsas com nomes interessantes com palavras-chave fáceis de descobrir que geram alarmes quando adulteradas.
  - O principal objetivo é atrair o intruso para uma armadilha, nova assinatura de intrusão, desviando o ataque de sistemas reais e fazer o intruso perder tempo

UNIVERSIDADE PORTUCALENSE

Métodos de deteção de intrusão

- Análise de pistas de auditoria
  - Baseado em host, geralmente uma combinação de dados de várias fontes
  - Normalmente, após a ocorrência do ataque
- Análise de tráfego de rede
  - On-line
  - Inspeciona o tráfego para detetar conteúdo proibido (certos tipos de pacotes, URLs ...)

UNIVERSIDADE PORTUCALENSE

Análise de pistas de auditoria

- A forma mais popular para detetar intrusões
- A maioria dos sistemas de guarda mensagens de erro, avisos e outras mensagens em algum tipo de log do sistema
- O principal obstáculo no desenvolvimento de ferramentas eficazes de análise de auditoria é como lidar com as enormes quantidades de dados.

UNIVERSIDADE PORTUCALENSE

Análise de pistas de auditoria

- A análise manual de pistas de auditoria é complicada
- Um sistema de auditoria é composto por duas partes:
  - Coletor de dados: Responsável pela coleta de dados de auditoria
  - Analisador de dados: Responsável pela análise dos dados de auditoria

UNIVERSIDADE PORTUCALENSE

Análise de pistas de auditoria

- Fontes de dados
  - System logs, Application logs
- Unix
  - lastlog –file, UTMP, who
  - Syslog, sulog
  - Logs de aplicações (sendmail, ftp, httpd)
  - ps

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Análise de pistas de auditoria

- Windows

  System/Security Log

  Administrative Tools ->Event Viewer

- Eventos auditáveis em rede
  - Logs de utilizadores em horas não habituais
  - Reboots não explicados
  - Trocas de horas não explicadas
  - Mensagens de erro anormais
  - Tentativas e falhas de login (inicio da sessão)
  - Utilizadores entrando a partir de sites não familiares

UNIVERSIDADE PORTUCALENSE

Análise de pistas de auditoria

Problemas principais

- Determinar quais são as provas boas é uma tarefa difícil
- Tendem a ser caros em termos de esforço e tempo de instalação e manutenção
- Podem consumir muitos recursos

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Análise do tráfego de rede

- Monitorização de rede:
  - Gera um alarme em caso de problemas Geralmente necessita de intervenção humana para solucionar o problema
  - Em alguns casos, uma ferramenta de gestão de rede também pode funcionar como uma ferramenta de ID
    - Pode detetar Denial of Service
    - Pode detetar as condições de erro que podem ser resultado de um ataque
    - Pode detetar anomalias no tráfego da rede e carga

UNIVERSIDADE PORTUCALENSE

Análise do tráfego de rede

- A análise estatística de tráfego com limites de tolerância é um bom ponto de partida para a deteção de novos ataques
- Um comportamento anormal é sempre um motivo para investigar
  - Quantidade incomum de tráfego
  - O tráfego entre hosts que normalmente não falam uns com os outros
  - Protocolos desconhecidos

UNIVERSIDADE PORTUCALENSE

Análise do tráfego de rede

Principais problemas

- Normalmente é necessária mais informação para reconhecer um ataque
- Uma vez que é guardado todo o tráfego da rede é necessário uma grande quantidade de recursos

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Métodos de deteção de intrusão

- Assinaturas de comportamento anormal
  - Deteta apenas ataques previamente conhecidos
  - Perfis de comportamento normal
  - O comportamento normal é difícil de definir
- A análise heurística
  - Inteligência artificial, redes neurais, etc.
  - Gera muitos falsos positivos

UNIVERSIDADE PORTUCALENSE

Técnicas de deteção de intrusão

- Deteção de utilização indevida
  - Deteta as intrusões baseando-se nas características de ataques conhecidos ou vulnerabilidades do sistema.
- Deteção de anomalias
  - Deteta qualquer ação que significativamente se desvia do comportamento normal.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Deteção de utilização indevida

- Baseada em ações conhecidas de ataques.
- A informação é extraída de ataques conhecidos
- Integram conhecimento humano
- As regras são definidas previamente
- Desvantagem:
  - Não detetam ataques novos ou desconhecidos

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Deteção de anomalias

- Baseado na utilização normal de um assunto.
- A informação de treino de auditoria pode não incluir dados de intrusão.
- Qualquer ação que se desvie significativamente do comportamento normal é considerada uma intrusão.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Deteção de anomalias vantagens e desvantagens

- Baseado na informação adquirida num período de operação normal.
  - Quando um ataque é efetuado no momento em que se está a recolher a informação vai causar uma classificação errada.
- Como decidir sobre quais as características a utilizar?

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

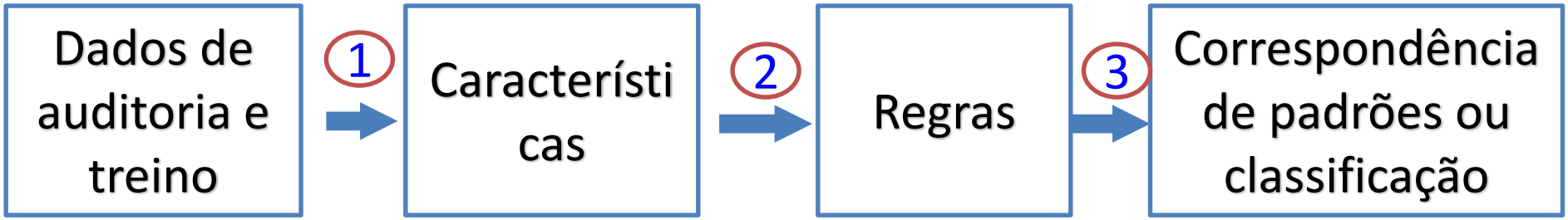
Comparação Utilização indevida/Deteção de anomalias

	Vantagem	Desvantagem
Utilização indevida	Precisão Gera menos alarmes falsos	Não deteta ataques novos ou desconhecidos
Deteção de anomalias	Pode detetar ataques não conhecidos baseando-se na informação da auditoria	Nível alto de alarmes falsos

UNIVERSIDADE PORTUCALENSE

Deteção de intrusões

1. Definir e extrair as características de comportamento no sistema
2. Definir e extrair as regras da intrusão
3. Aplicar as regras para detetar uma intrusão



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Método de descoberta de regras

- Expert System
- Métodos baseados em medidas
  - Estatísticas
  - Medidas de informação teórica
- Descoberta de regras de associação
- Classificação

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Métodos para a correspondência de e reconhecimento de padrões

- Correspondência de padrões
- Transição de estado
- Expert System
- Baseados em medidas
  - Estatísticas
  - Medidas de informação teórica
- Associação de padrões

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Técnicas de deteção de intrusão

- Correspondência de padrões
- Baseadas em medidas
- Data Mining
- Machine Learning

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Honeypot

- Um honeypot é um sistema que é deliberadamente nomeado e configurado de modo a convidar ataque
- Objetivos:
  - Parecer convidativo
  - Parecer fraco e fácil de saquear
  - Monitorar todo o tráfego de entrada e saída
  - Alerta o administrador quando é acedido por alguém

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Honeypot

Vantagens

- Fácil de implementar e entender
- Confiável
- Observar a evolução das tendências em segurança de rede
- Encontrar novas ameaças para hosts em rede
- Sem custo de desempenho

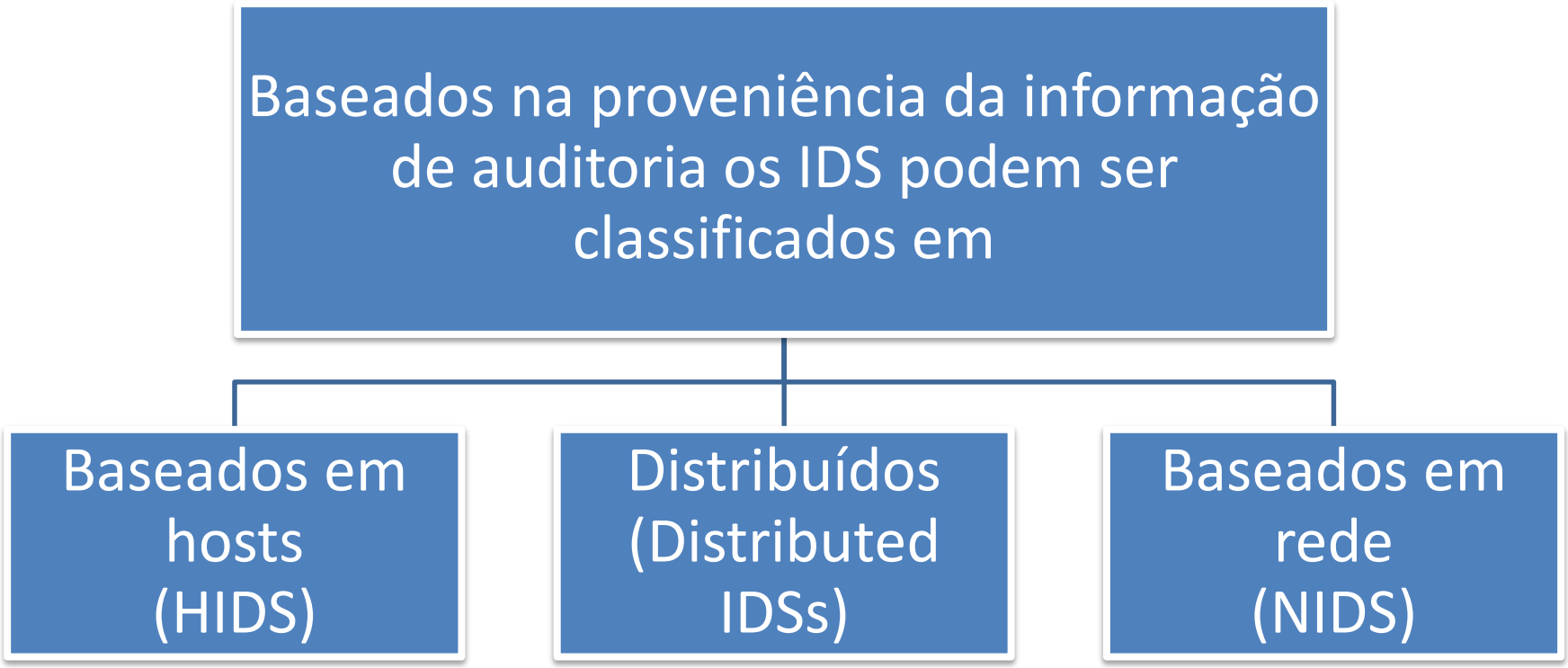
Desvantagens

- Só para alguns serviços
- Assume os hackers não percebem a armadilha
- Perca de tempo

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Tipos de sistemas de deteção de intrusão



UNIVERSIDADE PORTUCALENSE

Tipos de sistemas de deteção de intrusão

Baseados em hosts - Host-based

- Obtêm a informação de auditoria do host onde estão instalados
- Detetam ataques a um único host

Distribuídos - Distributed

- Obtêm a informação de vários hosts, com possibilidade de recolher informação da rede que os interliga
- Deteta ataques que envolvam vários hosts

UNIVERSIDADE PORTUCALENSE

Tipos de sistemas de deteção de intrusão

Baseados em rede - Network-Based IDSs

- Utilizam o tráfego da rede como fonte de informação libertando essa tarefa das máquinas que disponibilizam os serviços normais de computação
- Detetam ataques da rede

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

HOST BASED IDS (HIDS)

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Host based IDS

- Um sistema de deteção de intrusão baseado em host **monitora os logs** de eventos de segurança ou **verifica as alterações ao sistema**, por exemplo **tentativas de logon não autorizado** e **acessos indevidos a ficheiros** na máquina de destino real.

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Host based IDS
Porque utilizar?

- A carga da rede muitas vezes ultrapassa a capacidade de processamento de detetores de análise da rede;
- Tráfego de rede criptografada não pode ser analisado;
- Os NIDS (network IDS) pode não entender todos os protocolos
- Nem todos os ataques acontecem através da rede

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Host based IDS
Porque utilizar?

- Validações de contas
  - Contas sem palavras-chave
  - Contas padrão que acompanham o produto
  - Conta instalado com produtos de software
- Rootkit
  - Ethernet sniffer, especializado no registo de senhas
  - Substituição do ecrã de login com Trojan
  - Substituição de programas do sistema operativo que podem detetar um sniffer instalado
  - Utilitário para instalar um cavalo de Tróia

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Como funciona o HIDS?

- Auditoria de logs
  - A maioria dos sistemas guarda mensagens de erro, avisos e outras mensagens em algum tipo de log do sistema
  - Os logs de eventos registrados os comportamentos "anormais“
- Verificação de integridade de arquivos
  - Calcular um conjunto de impressão digital de um arquivo
- Disparar um alarme se a atividade levanta suspeitas e produz um relatório para futura investigação

UNIVERSIDADE PORTUCALENSE

Auditoria de logs

- Dependem de uma **configuração apropriada** dos mecanismos de registo do sistema operativo
  - Sistemas baseados em Windows: **o log de eventos**
  - Unix, sistema Linux: **Syslog**
- Recolha de dados que são registados nos ficheiros de log do sistema e procurar informação que corresponda a "assinatura de intrusão"
- Um par de tentativas de login não autorizadas dentro de um minuto

UNIVERSIDADE PORTUCALENSE

Validação da integridade de ficheiros

- HIDS armazena um conjunto de **impressões digitais** dos ficheiros **numa base de dados**;
- Se houver **alterações nos ficheiros** ao calcular os dígitos novamente irá resultar em valores diferentes e as **mudanças podem ser detetadas**
  - Verificação pode ser ultrapassada se se elaborar cuidadosamente a mudança
  - Hashes criptográficos são muito mais difíceis de enganar
- O HIDS que precisa de calcular mais do que um tipo de hash do arquivo são mais seguros na maioria das situações

UNIVERSIDADE PORTUCALENSE

HIDS
Vantagens e desvantagens

Vantagens

- Poder **analisar as atividades** no host com alto **nível de detalhe**
- Muitas vezes pode **determinar** quais os **processos e / ou utilizadores que estão envolvidos** em atividades maliciosas
- HIDS pode **detetar ataques indetetáveis pelo NIDS**
- HIDS pode usar o **serviço de encriptação** do host para examinar o tráfego e criptografar dados ...
- HIDS **não têm dificuldades** em **redes baseadas em switch**

Desvantagens

- **Sistema passivo** que tem que esperar por um evento para indicar um ataque. Não pode impedir os ataques de forma proactiva
- A **coleta de dados** ocorre numa uma base per-host
- Hackers inteligentes podem atacar e **desativar HIDS** aquando do ataque
- HIDS **consome** tempo de processamento, armazenamento, memória e outros **recursos do sistema**.

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Deceção e honeypots

- Enganar os atacantes
  - Dar informações erradas sobre a versão
- Falso vulnerabilidade provoca o alerta
  - Transferência de senhas facilmente atacadas na rede
  - Buracos de segurança conhecidos
- Requer competência e conselhos advogados

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

NETWORK BASED IDS (NIDS)

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Porque precisamos do NIDS

- Muitas **intrusões vêm da rede**
- **Não é muito difícil** de **implementar**
- Ajuda o administrador de rede a proteger a sua rede de intrusões

DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

O que é o NIDS?

É um sistema que **monitora pacotes na rede** e tenta descobrir se um atacante está a tentar entrar num sistema (ou causar um ataque de negação de serviço).

DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Implementação do NIDS?

- O NIDS pode ser **instalado num host** da rede que monitora.
- O NIDS pode ser implementado **em vários sensores** que enviam informação para um ponto central para análise.

DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Metodologias do NIDS?

- Métodos mais comuns
  - **Deteção de assinaturas** da intrusão
  - Análise de **tráfego de rede**
- Outros métodos
  - Análise de **protocolos**, análise de **conteúdo**, etc.

DEPARTAMENTO **INOVAÇÃO** **CIÊNCIA E TECNOLOGIA**