Monitoramento

DOCENTE: DR. SÉRGIO MAVIE, MSC. & ENG. C. MACULUVE

MAPUTO, 2023

Sumário

1. Monitoramento;
2. Detenção de Intrusos;
3. IDSs Baseados em Rede e em Hosts;
4. Detenção baseada em Conhecimento e Comportamento;
5. Ferramentas Relacionadas com IDSs;

Monitoramento

Monitoramento é um método programático pelo qual os sujeitos são responsabilizados por suas ações enquanto autenticados em um sistema;

O monitoramento é necessário para detectar ações maliciosas dos sujeitos, bem como para detectar tentativas de invasão e falhas do sistema.

Monitoramento

Ele pode ajudar a reconstruir eventos, fornecer evidências para acusação, e produzir análise e relatório de problemas e;

Auditoria e *Logging* (registo de eventos) são geralmente características nativas de um sistema operativo e da maioria das aplicações e serviços.

Monitoramento

O *logging* gera uma quantidade enorme de informação que exige ferramentas para a busca de eventos e códigos de ID concretos.

As ferramentas utilizadas para extrair detalhes significativos, importantes ou relevantes em colecções amplas de registos são conhecidas como ferramentas de mineração de dados;

Monitoramento

Para uma real automação, e até mesmo análise a tempo real de eventos de sistemas, requer-se uma ferramenta de mineração de dados específica: o SISTEMA DE DETENÇÃO DE INTRUSÃO (IDS = Intrusion Detection Systems)

A Prestação de contas é garantida através da gravação das actividades de sujeitos e objectos, assim como daquelas funções principais do sistema que sustentam o ambiente de funcionamento e os mecanismos de segurança.

Monitoramento

As trilhas de auditoria criadas por gravação de eventos do sistema em ficheiros de registos (*log files*) podem ser usados para avaliar a saúde e o desempenho de um sistema;

As falhas do sistema podem indicar programas defeituosos, falha de hardware, *drivers* corrompidos, ou tentativas de intrusão.

Monitoramento

Os ficheiros de *logs* fornecem uma trilha de auditoria para recriar uma história passo-a-passo de uma falha de evento, intrusão, ou sistema;

Para a inspecção de logs de auditoria e eventos do sistema a tempo real utiliza-se um sistema de detecção de intrusão.

Detenção de Intrusão(IDS)

IDS são utilizados principalmente para detectar tentativas de intrusão, mas que também pode ser utilizado para detectar falhas do sistema e para avaliar o desempenho global;

IDSs velam pela violações de confidencialidade, integridade e disponibilidade;

Detenção de Intrusão(IDS)

Um IDS pode reconhecer ataques que vêm de conexões externas (como as redes de Internet ou parceiros), vírus, códigos maliciosos, sujeitos internos confiáveis que tentam realizar atividades não autorizadas, e as tentativas de acesso não autorizado a partir de locais confiáveis;

Um IDS é considerado como sendo uma forma do método técnico de controlo de segurança detectivo.

Detenção de Intrusão(IDS)

Um IDS pode vigiar activamente por atividade suspeitas, examinar os logs de auditoria, e enviar alertas para os administradores assim que determinados eventos ocorram;

As alertas do IDS podem ser enviadas como uma notificação na tela (o mais comum), um som , o envio de uma notificação por e-mail, alertando via sms, ou gravar informações em um arquivo de log.

Detenção de Intrusão(IDS)

A resposta de um IDS pode ser ativa, passiva ou híbrida:

Resposta ativa: Afeta diretamente a atividade maliciosa no tráfego de rede ou um aplicativo do host;

Resposta passiva: Não afeta a atividade maliciosa, mas regista informações sobre o problema e notifica o administrador;

Resposta híbrida: Bloqueia a atividade indesejada, regista informações sobre o evento, e possivelmente até mesmo notifica o administrador.

Detenção de Intrusão(IDS)

Quando uma intrusão é detectada, sua primeira resposta deve ser a contenção de intrusão, evitando danos adicionais a outros sistemas.

De entre muitas variações em tipo e classificação de IDS, existem elementos complementares entre si que permitem a sua combinações para alcançar um objectivo comum na rede.

Detenção de Intrusão(IDS)

IDS baseado em host e em Rede

IDS são mais comummente classificados pela sua fonte de informação: (1) Baseado em host e (2) Baseados em rede.

IDS Baseado em host controlam atividades em um único sistema de computador, especialmente, observando as trilhas de auditoria, *logs* de eventos e logs de aplicação.

Detenção de Intrusão(IDS)

- **IDS baseado em rede** controla actividades que ocorrem no meio de rede, inspecionando pacotes e observando os padrões de tráfego de rede.

- Algumas literaturas consideram mais um IDS baseado em aplicativos, que monitora a actividade de aplicativos em um ambiente de rede.
- Outros IDS são os baseados em conhecimento e comportamento.

Exemplos de ferramentas

Nome	Categoria	Descrição
WIRESHARK	analisador de rede (*sniffer*) completo	open source, grátis e multiplataforma
METASPLOIT	exploração (*exploit*)	plataforma de código aberto avançada para desenvolver, testar e usar o código de exploração (*exploit*)
SNORT	IDS	IDS de rede mais completo para análise de tráfego e registo de pacotes em redes IP
KALI	ferramenta de segurança e Forense	Conhecida como BackTrack, a Kali é uma distribuição Linux que possui uma enorme variedade de ferramentas de segurança e Forense
OPENVAS	Sniffer	É um framework para detecção de vulnerabilidades de sistemas computacionais

TPC

1. IDS baseados em conhecimento vs IDS baseados e comportamento
2. Ferramentas relacionadas com IDS (Honeypots, padded cell, vulnerability scanner, penetration testing).
3. IDPS (Intrusion Detection and Prevention Systems)