Detecção de intrusão

Vítor Francisco Fonte
vff @di .uminho.ot

João Marco Silva
joaomarco@di.uminho.ot

Universidade do Minho

2019/20

Conceitos

Intrusão:

- tentativa de comprometer a confidencialidade, integridade ou disponibilidade (CIA) tentar ignorar os mecanismos de segurança de uma rede de computadores
-

Sistema de Detecção de Intrusões (IDS):

- processo de monitorização de eventos ocorridos num sistema informático ou rede, e analisá-los em busca de sinais de intrusões

Sistemas de prevenção de intrusões (IPS):

- Recursos IDS e mecanismos que visam parar possíveis incidentes

Tipos de Ataques: Intrusões Famosas

- Padrão estático e bem definido
- Normalmente simples de executar
- Muito pouca variabilidade inerente
- Por exemplo: correspondência de padrões em registros de auditoria ou eventos de log

Tipos de Ataques: Intrusões generalizadas

- Semelhante a intrusões bem conhecidas
- Mas têm um grau maior ou menor de variabilidade
- Explore falhas mais gerais no sistema atacado
- Por exemplo: usuários abusando de seus privilégios

Tipos de Ataques: Intrusões Desconhecidas

- De natureza muito geral

- IDS realmente não sabe o que esperar

- Por exemplo: comportamento mascarado de tra ffi c

Métodos de detecção: Detecção baseada em assinatura

- Baseado no conhecimento
- Assinatura é um padrão ou string correspondente a um conhecido ataque ou ameaça
- Compara padrões com eventos capturados para reconhecimento de possíveis intrusões

Métodos de detecção: Detecção baseada em assinatura

Vantagens:

- Método mais simples e eficaz para detectar ataques conhecidos

Desvantagens:

- Ie ff ective para detectar ataques desconhecidos e variantes de ataques conhecidos Difícil manter
- assinaturas/padrões atualizados

Métodos de detecção: Detecção baseada em anomalias

- Baseado no comportamento

- Anomalia é um desvio para um comportamento conhecido

- É preciso a atitude de que algo é anormal é provavelmente suspeito

- Por exemplo: tentativas de login falhadas, uso do processador, rede conexões, negação de serviço (DoS)

Métodos de detecção: Detecção baseada em anomalias

Vantagens:

- Eficaz para detectar vulnerabilidades novas e imprevistas
- Menos dependente do sistema operacional
  Facilitar a detecção de abuso de privilégios
-

Desvantagens:

- Às vezes complexo na definição de comportamento normal e anormal O culto para disparar alertas no tempo certo Precisão fraca devido a eventos
- observados sendo constantemente alterados
-

Métodos de detecção: Análise de Protocolo Stateful

- Baseado em especificações
- Rastreamento do estado do protocolo
- Por exemplo: emparelhamento de solicitações com respostas
- Com base em normas de protocolo

Métodos de detecção: Análise de Protocolo Stateful

Vantagens:

- Conhecer e rastrear o estado do protocolo Distinguir
- sequências inesperadas de comandos

Desvantagens:

- Consumo de recursos para rastreamento de estado de protocolo e exame Não é possível inspecionar ataques
- parecidos com protocolo benigno comportamentos Pode ser incompatível com protocolos proprietários
-

Abordagens de Detecção

Baseado em estatísticas:

- Limiares predefinidos Média e
- desvio-padrão

Baseado em regras:

- Regras If-Then ou If-Then-Else são aplicadas para construir o modelo e perfil de intrusões bem conhecidas

Baseado em padrões:

- Focado em ataques conhecidos através de correspondência de cordas Adequado para detecção baseada em assinaturas
-

Abordagens de Detecção

Baseado no estado:

- Exploração de máquina de estado finito derivada da rede comportamentos para identificar ataques Adequado para
- análise de protocolo baseada em anomalias e stateful

Baseado em heurística:

- Inspirado em conceitos biológicos e inteligência artificial Por
- exemplo: Respostas do sistema imunitário

Tipos de tecnologia

- IDS baseado em host (HIDS) IDS
- baseado em rede (NIDS) IDS baseado
- em wireless (WIDS) Análise do
- Comportamento de Rede (NBA) IDS
- mistos (MIDS)

Eficiência

Taxa de detecção:

- Grau de classificação correta de intrusão
- Evitar alarmes falsos

Falso Positivo

- Quando IDS identifica incorretamente a atividade benigna como maligna

Falsos negativos (FN)

- Quando o IDS falha ao identificar atividade mal-intencionada

Snort

- IDS muito popular Abordagem baseada em regras (mais de
- 4000 regras) Algoritmo Aho-Corasick para correspondência
- exata de assinatura Instalar e configurar o Snort de
-
  - https://www.snort.org/downloads
- Exercício:
  - Baixe o rastreamento, analise e discuta a identificação da intrusão
  - https://bit.ly/2PnRtaV