A tecnologia de Contentores-Abstractos tem sido amplamente utilizada em ambientes de computação de ponta. Contudo, estudos recentes demonstraram que o ambiente de contentores é vulnerável a vários ataques de segurança. Neste documento, propomos uma nova estrutura de detecção de anomalias combinando algoritmo de cluster para melhorar a eficiência da detecção de anomalias no ambiente de computação de bordo que contém um grande número de contentores. Utiliza o algoritmo de cluster para identificar automaticamente recipientes que executam a mesma aplicação, e constrói um modelo de detecção de anomalias para cada categoria separadamente.

FPR da detecção de anomalias de 0,61% para 0,09%, e aumentar a TPR de 90,3% para 96,2% em comparação com o método tradicional.

Termos de índice - Segurança de Contentores, Ambiente de

A investigação actual sobre segurança de contentores inclui a análise estática de imagens de contentores e a detecção de anomalias de um contentor em funcionamento. A tecnologia de contentor é uma tecnologia de virtualização de nível de sistema operacional que tem múltiplos blocos de construção dentro do kernel Linux, incluindo isolamento de recursos, técnicas de controlo e mecanismos de segurança . Neste documento, concentramo-nos nesta última abordagem, estudando o método de detecção de comportamento anómalo de contentores causados por ataques de segurança, ou seja, a detecção de intrusão baseada em anomalias. Um sistema de detecção de intrusão é um dispositivo ou aplicação de software que monitoriza uma rede ou sistema em relação a actividades maliciosas ou violações de políticas .

Os métodos geralmente utilizados para a detecção de intrusões incluem a detecção baseada em assinaturas e anomalias. A tecnologia de contentores trouxe novos desafios à detecção de intrusão. Devido à leveza e à eficiência das características de actuação, uma máquina hospedeira contém frequentemente múltiplas instâncias de contentores, pelo que o sistema de detecção de intrusão da máquina hospedeira não consegue detectar eficazmente os comportamentos anómalos de cada contentor. Além disso, devido à grande variedade e à natureza altamente personalizável do recipiente, é sempre difícil generalizar o modelo de detecção entre diferentes recipientes, enquanto que a construção de um modelo para cada recipiente implicará uma grande sobrecarga de desempenho.

Por conseguinte, são urgentemente necessários novos métodos para melhorar a detecção de anomalias nos contentores. Detecção de comportamentos de anomalias de con- tiner utilizando a agregação. A estrutura pró-agrupamento utiliza algoritmo de agrupamento para identificar os que contêm a mesma aplicação sem qualquer etiquetagem manual, construir um modelo para cada aplicação e efectuar a detecção de anomalias para cada uma delas. Apresentamos uma classificação eficiente de contentores e detecção de anomalias através da integração de algoritmos de agrupamento com métodos leves de aprendizagem de máquinas.

Este trabalho mostra como as chamadas de sistema podem ser utilizadas inspeccionar o comportamento de um Contentor e para efectuar a classificação e detecção de anomalias. A Secção III apresenta a nossa proposta de abordagem da detecção de anomalias, que é depois avaliada na Secção IV.

Detecção de anomalias baseadas em chamadas de sistema. A ideia básica da detecção de anomalias é criar um modelo para operações de confiança através do método de aprendizagem de máquinas, e depois utilizar o modelo para detectar comportamentos anormais. propuseram um método de representação denominado saco de chamadas de sistema para a detecção de

anomalias. Este método divide a sequência de chamadas de sistema em segmentos, conta a frequência das diferentes chamadas de sistema em cada segmento, depois utiliza a sequência estatística para a detecção de anomalias.

Tomaram a detecção como um problema de classificação e utilizaram a aprendizagem da máquina para detectar anomalias. A maior parte da detecção da anomalia baseada na chamada do sistema usa apenas o nome da chamada do sistema como características, mas para métodos de ataque deliberadamente construídos de forma errónea, tais como o ataque mímico, muitas vezes não consegue encontrar a tempo um comportamento anormal. Propôs um método de ataque mímico interactivo, no qual o atacante poderia modificar constantemente os dados e inserir código no script malicioso com base nos resultados do ataque, contornando assim o sistema de detecção de intrusão. Detecção de anomalias em contentores.

Assim, a detecção da anomalia baseada na chamada do sistema também é aplicável aos contentores. propuseram aplicar o saco de chamadas de sistema à detecção de anomalias em contentores. Quando a detecção, se a sequência de chamadas de sistema actual não aparecer na base de dados, é marcada como uma anomalia. propuseram um método de detecção para resolver o problema de que os recipientes são utilizados para realizar operações de criptografia em computação de alto desempenho.

Métodos de detecção de corrente para recipientes concentram-se principalmente em campos específicos e não se podem aplicar ao ambiente de computação de bordo com vários tipos e uma enorme quantidade de contentores. Por conseguinte, é necessário um quadro de detecção de anomalias - trabalho que pode ser generalizado a diferentes aplicações de contentores. Uma ferramenta open-source, out-of-the-box, sysdig , é utilizada para obter dados de chamada de sistema gerados por contentores para conseguir a detecção de anomalias não intrusivas e de baixo custo. Durante a detecção, a estrutura constrói um classificador RandomForest para cada categoria de aplicação, para detectar anomalias nas chamadas de sistema observadas.

QUADRO II

VECTOR DE FREQUÊNCIA DO MYSQL de chamada do sistema é suficiente para a classificação de contentores e detecção de anomalias.

Tabela I e Tabela

Devido às suas características altamente personalizáveis, os contentores no ambiente de computação de bordo muitas vezes não têm informação detalhada da categoria de aplicação, e a grande quantidade dos mesmos torna difícil a etiquetagem manual.