Considerando a proximidade do hospedeiro a um contentor, as abordagens que utilizam sistemas de detecção de anomalias tentam monitorizar e detectar comportamentos inesperados. O nosso trabalho visa utilizar chamadas de sistema para identificar ameaças dentro de um ambiente de contentor, utilizando estratégias baseadas na aprendizagem de máquinas para distinguir entre comportamentos esperados e inesperados.

Isto permite que vários recipientes com diferentes estruturas e aplicações funcionem lado a lado, partilhando o mesmo kernel do sistema operativo. Intrusão e o Sistema de Prevenção de Intrusão. Especificamente, um IDS realiza a identificação de intrusão utilizando diferentes técnicas que podem ser baseadas na assinatura, que realiza a comparação de assinaturas com uma base conhecida de ameaças, ou baseada em anomalias, na qual o comportamento normal do sistema é previamente conhecido e os desvios do mesmo são classificados como ameaças . Olhando apenas para a detecção de intrusão visando contentores, algumas diferenças poderiam ser apontadas.

Um observador externo ao contentor recolhe informações detalhadas sobre a sua execução, sob a forma de uma sequência de chamada do sistema emitida pela aplicação.

Do ponto de vista do atacante, existem várias possibilidades - ligações de ataque a um sistema de virtualização, tais como a exploração de vir- tualização para extrair informação privada dos utilizadores, o lançamento de ataques de Negação Distribuída de Serviço ou a escalada da intrusão para múltiplas instâncias de VM. Assim, um IDS a funcionar directamente no SO anfitrião é capaz de observar plenamente o comportamento dos processos em curso num contentor . Um dos primeiros estudos que explorou o campo da detecção de intrusão baseada em chamadas de sistema foi apresentado por . O estudo observou que sequências curtas de chamadas de sistema pareciam manter uma consistência notável entre os muitos conjuntos possíveis de chamadas de sistema dos possíveis caminhos de execução de um programa.

Isto inspirou o uso de sequências curtas de chamadas de sistema para definir o comportamento normal do sistema e apresentou uma forma simples e eficiente de detectar anomalias, com possíveis aplicações a cenários em tempo real.

Sequence Time-Delay Embedding e Bag of System

O estudo treinou ambos os algoritmos com janelas de 3 a 6 chamadas de sistema, e calculou a inclinação da curva de crescimento, o que significa a taxa de novas janelas adicionadas à base de comportamento normal de cada classificador após um período de tempo. O estudo de , centra-se na detecção de intrusão por anomalias em ambientes de contentores, aplicando uma técnica que combina BoSC com a técnica de STIDE. A análise do comportamento do recipiente é feita após o seu encerramento, com a ajuda de uma tabela contendo todas as chamadas distintas do sistema com o respectivo número total de ocorrências. O método lê o fluxo de chamadas de sistema por épocas, e desliza uma janela de tamanho 10 através de cada época produzindo uma BoSC para cada janela, que é utilizada para detectar anomalias, que por sua vez é declarada se o número de disparidades na base de comportamento normal exceder um limiar definido.

O classificador atingiu uma taxa de detecção de 100% e uma taxa de falso positivo de 0,58% para a época de tamanho 5. Esta secção apresenta os principais conceitos para a compreensão do trabalho, discutindo pontos tais como a detecção de anomalias, os chamados sistemas para IDS e a virtualização de contentores. As chamadas de sistema são mecanismos disponíveis para a interacção entre uma aplicação e o núcleo do sistema operativo. Quando um programa

necessita de executar operações privilegiadas, os pedidos são feitos através de chamadas de sistema, geralmente porque os processos ao nível do utilizador não estão autorizados a executar tais operações.

O núcleo do SO implementa assim políticas de segurança que determinam quais as chamadas de sistema que podem ser chamadas por que processos ao nível do utilizador. Devido à posição em que as chamadas de sistema são implementadas, a sua observação fornece informação rica sobre as actividades realizadas pelos processos ao nível do utilizador. Ferramentas como strace e ftrace , permitem mostrar a sequência de todas as chamadas de sistema utilizadas por um comando ou por um processo em execução. Independentemente das abordagens utilizadas para executar código malicioso num sistema, eles exploram normalmente a interface de chamadas do sistema para executar operações maliciosas .

É apenas através desta interface que uma aplicação comprometida interage com os serviços e recursos do sistema. A monitorização de chamadas de sistema é uma técnica amplamente utilizada que faz uso desta característica em comum para detectar comportamentos suspeitos de uma aplicação que possa ter sido comprometida, de modo a que seja possível uma contramedida para minimizar o problema . O contentor é um ambiente virtual que corre num único SO e permite o carregamento e execução de uma aplicação específica e as suas dependências contidas numa virtualização de um sistema operativo . Por conseguinte, uma opção seria monitorizar os processos dos hóspedes a partir do sistema anfitrião, utilizando como dados que o sistema chama, os processos gerados.

Neste contexto, introduz um método de monitorização de chamadas de sistema baseado em janelas, que é simples e eficaz para a detecção em tempo real.