Para mitigar estas preocupações, técnicas como a detecção de intrusão são uma necessidade, como sempre, no contexto dos contêineres, tem recebido atenção limitada. Assim, é necessário definir uma abordagem melhorada da detecção de intrusão no nível de contêineres para ambientes multitenant. Neste documento, fazemos uma análise preliminar de viabilidade da detecção de intrusão a nível de contêineres baseados em host.

B g f y

al propuseram um IDS em tempo real que usa n-gramas de chamadas de sistema e a probabilidade de sua ocorrência.

Por isso, procuramos definir perfis estáveis para os s contêineres sob monitoramento usando as chamadas do i sistema, por eles executadas, para treinar os referidos t algoritmos. A detecção de intrusão baseada em nuvens tem visto alguns desenvolvimentos, em termos de modo de implantação e monitoramento, por exemplo, o uso de IDSs distribuídos. Apesar dos grandes avanços na detecção de intrusões para ambientes baseados em máquinas virtuais, as abordagens a nível de contêineres foram negligenciadas e as melhorias neste contexto ainda são escassas. A detecção de intrusão é o processo de monitoramento dos eventos que ocorrem em um sistema ou rede de computadores e sua análise para sinais de possíveis incidentes , e é realizada pelo IDSes.

Enquanto os IDSs baseados em rede processam mais dados e são normalmente colocados no perímetro da rede, monitorando assim uma área mais ampla, os IDSs baseados em host são colocados em máquinas, presentes em uma rede, monitorando-os e, portanto, tendo uma visão mais local dos eventos. A abordagem baseada na assinatura consiste na identificação de padrões maliciosos conhecidos ao analisar novos eventos, tais como tráfego de rede ou dados de aplicação . Enquanto que a base da anomalia implica duas fases, uma fase de treinamento, para construir o perfil, e uma fase de detecção, onde novos eventos são avaliados com base no perfil definido . Isto normalmente implica o uso de algoritmos que vão desde métodos estatísticos até aprendizagem de máquinas e abordagens de mineração de dados, cujo uso tem provado ser útil no campo da detecção de intrusão.

Artificiais é uma metodologia que tem a capacidade de generalizar dados, sendo assim capazes de detectar intrusões a partir de dados de treinamento incompletos . Os Modelos Markov Escondidos são usados para descrever o sistema sendo modelado através de um conjunto de conexões ponderadas entre cada par de estados, que representam a probabilidade de transição de um para o outro . A aplicação do K- Nearest Neighbour à detecção de intrusão também teve alguns resultados positivos, classificando os eventos com base na heurística de distância . O método STIDE é baseado em uma janela que desliza sobre uma seqüência de chamadas do sistema .

Normalmente, na detecção de anomalias, é utilizada uma variação SVM chamada One-Class Support Vector Machines, que classifica os dados em apenas uma classe, eliminando assim a necessidade de fornecer dados anômalos para o classificador quando em fase de treinamento. O que de fato representa uma grande ameaça para as camadas subjacentes da pilha de serviços das nuvens e para a execução normal de outros contêineres honestamente obtidos sem motivações perversas.

AMBIENTE

Este trabalho surge como resultado de ameaças iminentes a implantações de nuvens baseadas em contêineres, que são representadas na Fig. Portanto, o foco principal deste trabalho é detectar tentativas de intrusão contra contêineres, que são implantados em um ambiente de

múltiplos arrendamentos, ficando assim sujeitos aos riscos inerentes de compartilhar recursos físicos e não ter o controle dos mesmos. Este trabalho visa atuar como uma melhoria do estado da arte na detecção de intrusões no nível de contêineres, devido ao crescimento do uso em serviços de nuvem e também para auxiliar com garantias de isolamento. Os contêineres são normalmente gerenciados por um middleware de orquestração, chamado de motor de contêineres.

Isto também atua como um local de ataque para atingir a camada de SO, assim, este software também pode ser comprometido em implementações de nuvens, por contêineres desonestos, assumindo um papel de caminho para atingir ambos os ataques, ou seja, para a máquina hospedeira e para outros inquilinos. Nesta seção, fornecemos uma visão geral da arquitetura preliminar para a abordagem de detecção de intrusão, descrita na Fig. Arquitetura preliminar proposta para a abordagem de detecção de intrusão.

Com relação ao sistema sob monitoramento, nosso foco se concentra novamente nos contêineres, ou seja, o detector de intrusão deve construir um perfil de um contêiner com base nas chamadas do sistema emitidas por ele para o sistema operacional subjacente. Por enquanto, estamos nos concentrando no Docker e no LXC, no entanto, nosso objetivo é ter uma plataforma que seja capaz de trabalhar de forma agnóstica com a tecnologia de contêineres. Para isso, coletamos ou implementamos algoritmos utilizados para a detecção de intrusão. Além disso, nosso objetivo é avaliar o estado dos algoritmos de detecção de intrusão, utilizando múltiplos cenários realistas, no contexto da detecção de intrusão a nível de contêineres.

Estes expertises ainda estão em seus primórdios, pois não há conjuntos de dados disponíveis para a detecção de intrusão de contêineres.