INTRODUÇÃO

Os contêineres Linux normalmente se comunicam com o núcleo do host através de chamadas ao sistema. Ao monitorar as chamadas do sistema entre o recipiente e o núcleo hospedeiro, pode-se aprender o comportamento do recipiente a fim de detectar qualquer mudança de comportamento, o que pode refletir uma tentativa de intrusão contra o recipiente.

Uma das abordagens básicas para a detecção de anomalias usando chamadas de sistema é a técnica da Bolsa de

Chamadas de Sistema . , cn >, onde n é o número total de chamadas de sistema distintas, e ci é o número de ocorrências da chamada de sistema, si , na seqüência de entrada dada. O menor número de processos em um contêiner, em comparação com o VM, resulta em menor complexidade.

Neste documento, estudamos a viabilidade de aplicar o

BoSC para detectar passivamente ataques contra contêineres. A técnica utilizada é semelhante àquela introduzida por . Mostramos que uma técnica baseada em freqüência é suficiente para detectar anormalidades no comportamento do recipiente. Neste trabalho, usamos uma técnica semelhante à descrita em aplicada aos recipientes Linux para detecção de intrusão.

VISÃO GERAL DO SISTEMA

O sistema emprega um serviço de fundo executado no kernel do host para monitorar as chamadas do sistema entre quaisquer containers Docker e o Kernel do host. Ao iniciar um container, o serviço usa a ferramenta strace Linux para rastrear todas as chamadas de sistema emitidas pelo container para o kernel do host. Uma tabela de todas as chamadas de sistema distintas no rastreamento também é relatada no final do rastreamento junto com o número total de ocorrências. O traço completo e a tabela de contagem são armazenados em um arquivo de registro que é processado off-line e usado para aprender o comportamento do contêiner após o término do contêiner.

Neste ponto, não estamos realizando nenhuma aprendizagem de comportamento em tempo real ou detecção de anomalias. Entretanto, para propósitos futuros, onde a aprendizagem do comportamento e a detecção de anomalias deve ser alcançada em tempo real , o algoritmo de aprendizagem aplicado seria ligeiramente diferente do descrito aqui. O arquivo de registro gerado é então processado para criar dois arquivos, ou seja, o arquivo da lista de chamadas de sistema e o arquivo de rastreamento. O arquivo da syscall-list contém uma lista de chamadas de sistema distintas, ordenadas pelo número de ocorrências.

Para cada época, uma janela deslizante de tamanho 10 é movida sobre as chamadas de sistema da época atual, contando o número de ocorrências de cada chamada de sistema distinto na janela atual, e produzindo um saco de chamadas de sistema. Como mencionado anteriormente, uma bolsa de chamadas de sistema é uma matriz < c1 , c2 , . > onde ci é o número de ocorrências de chamadas de sistema, si , na janela atual, e ns é o número total de chamadas de sistema distintas. Se o BoSC atual já existe no banco de dados de comportamento normal, sua freqüência é incrementada em 1.

O treinamento é concluído quando todos os padrões de comportamento normal esperados são aplicados ao sistema. Para detectar se um traço de entrada é anômalo, o traço é lido em épocas, e para cada época, uma janela deslizante é usada para verificar se o BoSC atual está presente no banco de dados de comportamento normal. Se um BoSC não estiver presente no banco de

dados, um descasamento é declarado.

Docker rodando em um sistema operacional host Ubuntu

Na partida do contêiner, o contêiner cria automaticamente um banco de dados padrão, adiciona usuários definidos pelo ambiente vari- sáveis passados para o contêiner, e então começa a ouvir as conexões. Como não há um conjunto de dados disponível que contenha chamadas de sistema coletadas de contêineres, precisávamos criar nossos próprios conjuntos de dados tanto para comportamentos normais quanto anômalos. Uma carga de trabalho de comportamento normal foi inicialmente aplicada ao contêiner, antes que ele fosse «atacado» usando uma ferramenta de teste de penetração. Além disso, ela dá ao usuário a opção de personalizar o banco de dados criado, por exemplo, especificando o número de colunas varcher e/ou int a serem usadas ao criar o banco de dados.

Além disso, o usuário pode selecionar o número de inserções e consultas a serem realizadas no banco de dados.

Para simular um ataque ao recipiente, usamos o sqlmap

Um serviço de fundo, executado no núcleo do host, detecta automaticamente qualquer contêiner Docker recéminiciado e rastreia as chamadas do sistema do novo contêiner usando a ferramenta Linux strace.

O serviço depende dos eventos de comando do

O mapa hash armazena chamadas de sistema distintas como a chave, e um índice correspondente como o valor. Uma chamada de sistema que aparece no traço inteiro menos do que o número total de chamadas de sistema distintas é armazenada no mapa como «outra». Usar «outro» para chamadas de sistema relativamente raras economiza espaço, memória e tempo de computação, como descrito em . Cada época atualiza o banco de dados de comportamento normal.

O banco de dados de comportamento normal é outro mapa de hash com o BoSC como chave e a freqüência da bolsa como o valor. Se a bolsa atual já existe no banco de dados, o valor da freqüência é incrementado. Caso contrário, uma nova entrada é adicionada ao banco de dados. Para cada época, a aplicação usa a técnica de janela deslizante para ler seqüências de chamadas do sistema a partir do arquivo de rastreamento, sendo que cada seqüência é de tamanho 10.

Um saco de chamadas de sistema é então criado pela contagem da freqüência de cada chamada de sistema distinto dentro da janela atual. A bolsa de chamadas de sistema criada é uma matriz de freqüência de tamanho ns , onde ns é o número de chamadas de sistema distintas. O novo BoSC é então adicionado ao banco de dados de comportamento normal.

Onde Ck é a entrada ith da matriz Ck , e nk é o número total de entradas no banco de dados após a época k. O banco de dados de comportamento normal gerado é então aplicado ao rastreamento pós-atacamento do recipiente para detecção de anomalias. BoSC atual está presente no banco de dados de comportamento normal. Um descasamento é declarado sempre que um BoSC não estiver presente no banco de dados.

DISCUSSÃO

Este parâmetro está atualmente definido para o número total de chamadas de sistema

distintas, ou seja, o tamanho do mapa de índice de escala de sistema.