Bloqueio de IP no Suricata

Nome	Bloqueio de IP no Suricata
Descrição	Este runbook fornece um guia detalhado sobre como efetuar o bloqueio de um endereço IP utilizando o Suricata.
Autores	SecDay
Versão	1.0.0
Data da Versão	Data de criação: 26/06/2024 Data de atualização: 26/06/2024
Neste Runbook	

Procedimento

Acesso via SSH

1. Abrir o Terminal ou Prompt de Comando:
    - Se você estiver usando Windows, pode usar o MobaXterm, PuTTY ou o Windows PowerShell;
    - No macOS ou Linux, abra o Terminal.
2. Conectar ao servidor via SSH
    - Digite o seguinte comando, substituindo ***username*** pelo seu nome de usuário e ***server_address*** pelo endereço IP ou nome do host do servidor onde o Suricata está instalado:

      ssh username@server_address

- Insira sua senha ou autentique com sua chave privada quando solicitado

Localizar o Arquivo de Configuração do Suricata

1. Acessar o diretório de configuração das regras do Suricata:
    - O arquivo de regras (***custom.rules***) está localizado em ***/var/lib/suricata/***. Use este comando para ir até o diretório:

      cd /var/lib/suricata/

Criar uma Regra de Bloqueio de IP

1. Editar o arquivo de regra
    - Abra o arquivo com um editor de texto, como o nano:

      nano suricata.rules

2. Adicionar uma nova regra
    - Insira a seguinte regra no arquivo para bloquear o tráfego de um IP específico, substituindo ***IP_SUSPEITO*** pelo IP e que deseja bloquear:

      drop ip IP_SUSPEITO any -> any any (msg:"Bloqueio de IP suspeito Relativo ao incidente XYZ "; sid:1000001; rev:1;)

    - Essa regra instrui o Suricata a descartar todo o tráfego de e para o IP especificado;

    - **Importante**: Certifique-se de que o identificador sid (Signature ID) é único e não duplica o de outras regras já existentes. Cada regra deve ter um sid distinto para evitar conflitos e garantir o correto funcionamento do sistema.
3. Salvar e fechar o arquivo
    - Pressione CTRL + X, depois Y para salvar as alterações e Enter para fechar o editor.

Recarregar as Configurações do Suricata

1. Recarregar o Suricata para aplicar as mudanças
    - Use o seguinte comando para recarregar o Suricata com as novas regras:

suricata -T -c /etc/suricata/suricata.yaml -S /etc/suricata/suricata.rules

- O parâmetro -T testa a configuração para garantir que não há erros.

2. Reiniciar o serviço do Suricata
    - Após confirmar que não há erros na configuração, reinicie o Suricata para aplicar as alterações:

      systemctl restart suricata

Verificar o Bloqueio

1. Monitorar os logs do Suricata
    - Acompanhe os logs para garantir que o IP está sendo efetivamente bloqueado. É importante notar que eventos relacionados ao IP bloqueado só aparecerão nos logs se ainda houver tentativas de conexões de ou para o IP bloqueado. Isso serve como uma confirmação de que o bloqueio está ativo e funcionando corretamente:

      tail -f /var/log/suricata/eve.json | grep "Bloqueio de IP suspeito Relativo ao incidente XYZ"