Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Tecnologia em Redes de Computadores

Anderson dos Santos Correia
Diego de Lima Gomes
Jefferson Bruno Gomes do Nascimento

TurtleGuard: Proteção contra ataques de negação de serviço (DDoS) em sistemas e serviços sensíveis usando Suricata e Zabbix

Natal
2023

Anderson dos Santos Correia
Diego de Lima Gomes
Jefferson Bruno Gomes do Nascimento

TurtleGuard: Proteção contra ataques de negação de serviço (DDoS) em sistemas e serviços sensíveis usando Suricata e Zabbix

Projeto da disciplina de Seminário de Orientação de Projeto Integrador do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte. Curso Tecnologia em Redes de Computadores.

Orientador: Prof. Francisco Sales

Natal
2023

SUMÁRIO

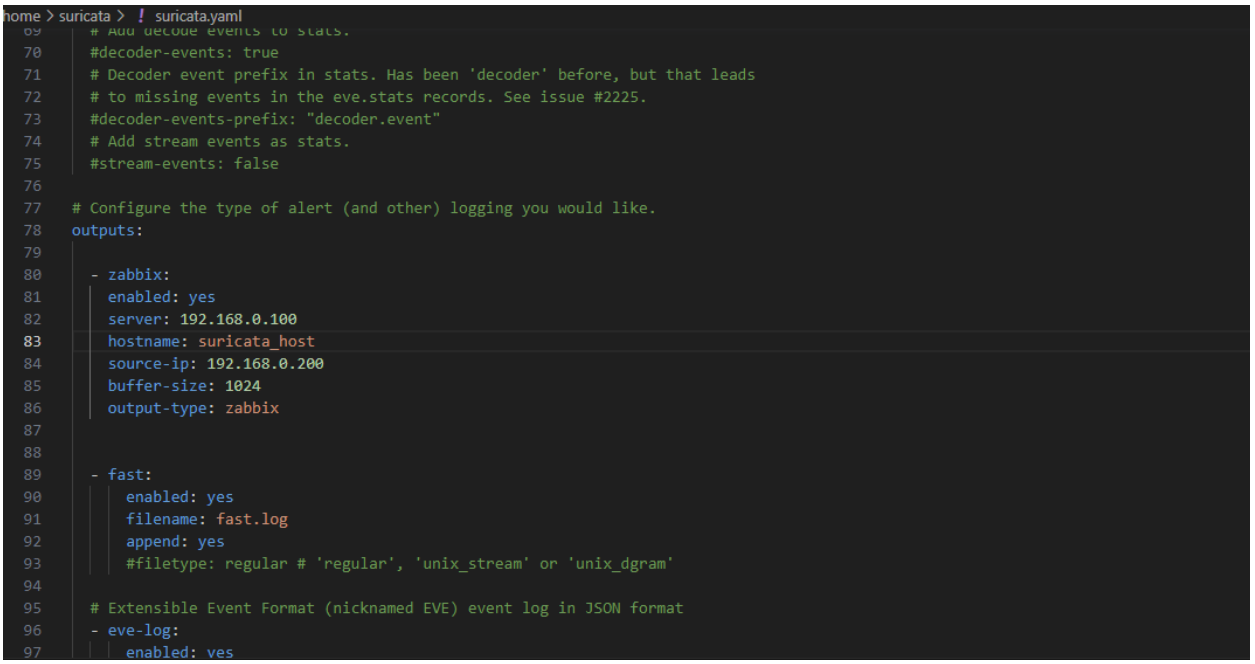
Introdução

O presente relatório tem como objetivo documentar as etapas de integração do Suricata com o Zabbix, bem como os testes de integração e validação realizados para garantir o correto funcionamento da solução. Além disso, descreveremos a elaboração de relatórios de segurança personalizados, utilizando as informações geradas pelo Suricata e Zabbix, e o desenvolvimento técnicas para enviar dados do Suricata para o Zabbix.

Configuração da integração entre o Suricata e o Zabbix

Responsável: **ANDERSON DOS SANTOS CORREIA**

- Foram realizadas modificações na documentação do Suricata para permitir o envio de dados ao Zabbix. Foi necessário configurar as opções adequadas no Suricata para que ele pudesse se comunicar com o Zabbix. Foram criados os itens de monitoramento e as ações necessárias no Zabbix para receber e processar os dados enviados pelo Suricata.

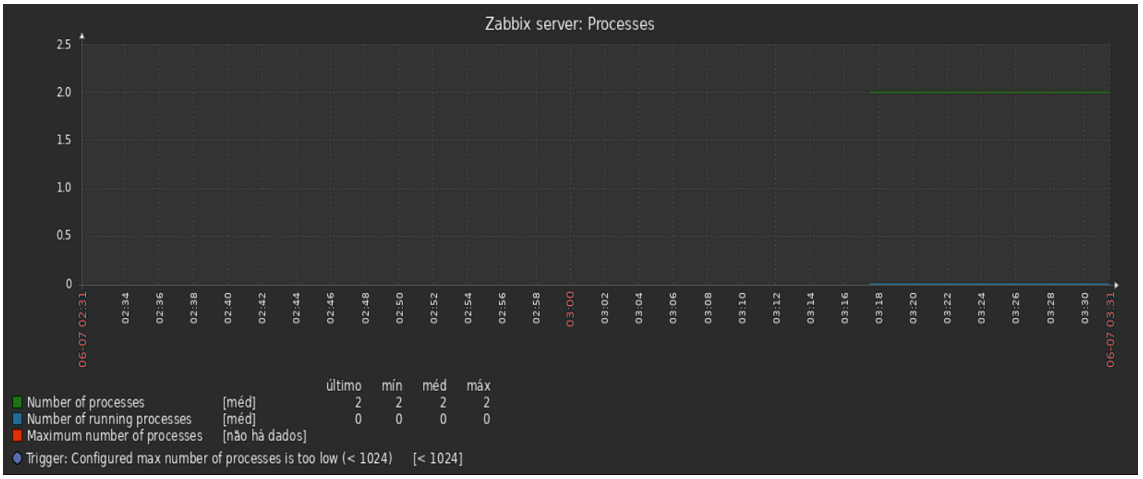


arquivo de configuração do suricata

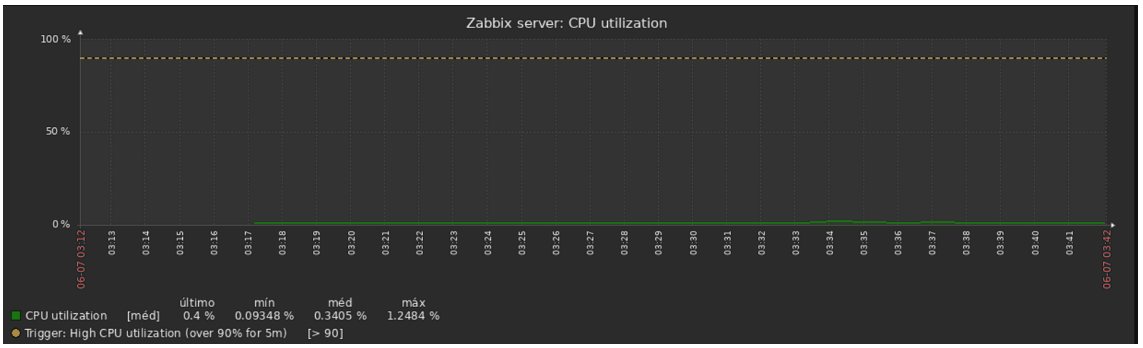
Testes de integração e validação

Responsável: **JEFFERSON BRUNO GOMES DO NASCIMENTO**

- Após a configuração da integração, foram realizados testes para verificar a correta integração e o funcionamento da solução. Foram gerados eventos de segurança no Suricata e verificou-se se esses eventos eram corretamente recebidos e processados pelo Zabbix. Foram analisados os logs e os dados exibidos pelo Zabbix para confirmar que os eventos estavam sendo registrados adequadamente.



tela de monitoramento do zabbix

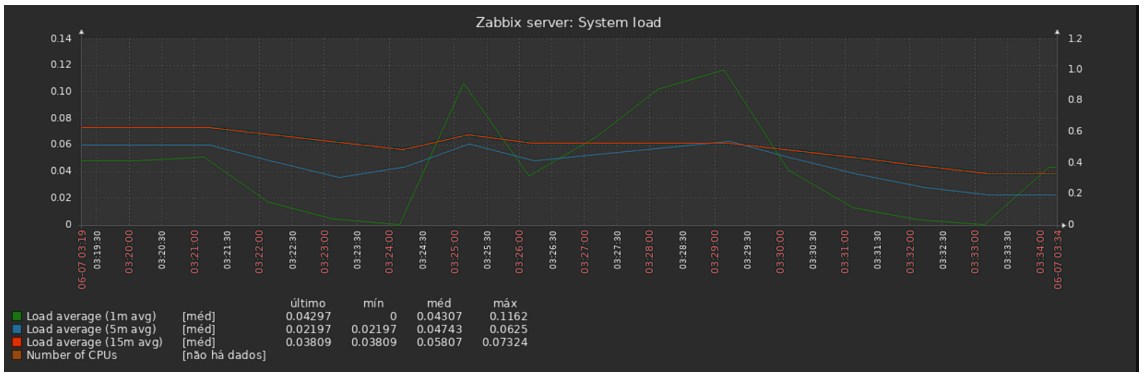


tela de monitoramento do zabbix

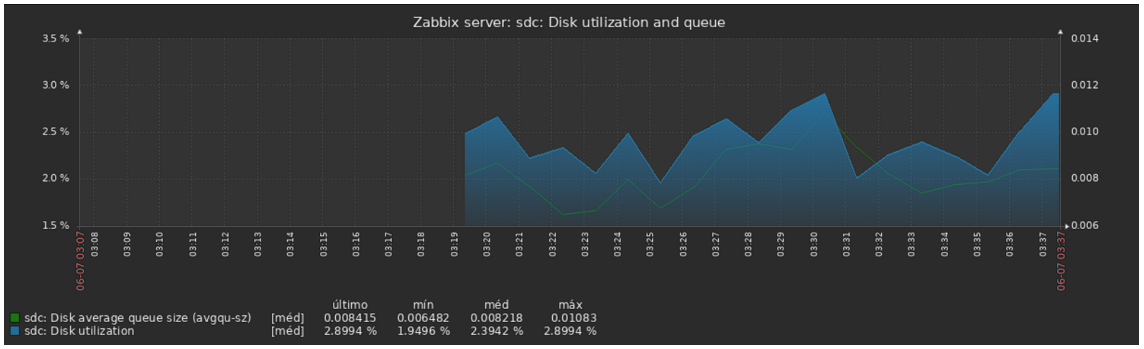
Elaboração de relatórios de segurança

Responsável: **JEFFERSON BRUNO GOMES DO NASCIMENTO**

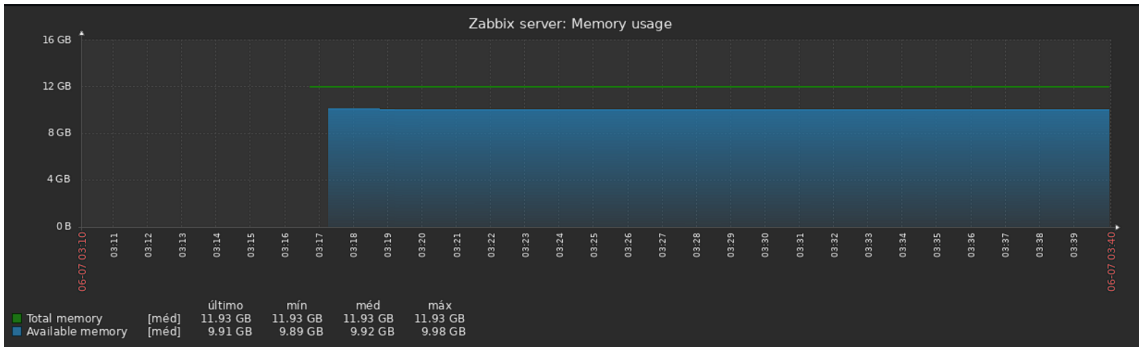
- Nesta etapa, foi verificado se o Zabbix estava gerando relatórios com as informações de segurança geradas pelo Suricata. Foram criados relatórios personalizados no Zabbix, utilizando as informações coletadas e armazenadas durante o monitoramento. Esses relatórios fornecem insights valiosos sobre as ameaças de segurança detectadas e permitem uma análise mais detalhada dos dados.



recebendo dados do suricata



monitorando o dispositivo



monitorando o dispositivo

Desenvolvimento de scripts para automação da coleta de dados

Responsável: **DIEGO DE LIMA GOMES**

Por fim, foram conduzidos estudos visando a implementação da coleta de dados no Suricata e sua integração com o Zabbix. Durante a análise da documentação do Suricata, foi identificado um potencial para modificar o documento de configuração do suricata a fim de habilitar o envio de dados para o Zabbix.

```
outputs:
  - zabbix:
      enabled: yes
      server: 192.168.0.100
      hostname: suricata_host
      source-ip: 192.168.0.200
      buffer-size: 1024
      output-type: zabbix
```

trecho que deve ser modificado no suricata. link para estudo completo clique aqui

Reuniões

ATA DE REUNIÃO 06/29/2023

Data: 29 de junho de 2023

Horário: 23:30 - 00:30

Local: Canal de voz/vídeo do Discord

Participantes:

- ANDERSON DOS SANTOS CORREIA
- DIEGO DE LIMA GOMES
- JEFFERSON BRUNO GOMES DO NASCIMENTO

Pauta:

1. Revisão das tarefas concluídas no SPRINT 2.
2. Atribuição de tarefas para o SPRINT 3 .
3. Definição da data da próxima reunião.

Deliberações:

1. Revisão das tarefas concluídas no SPRINT 2.

- Foi discutido o feedback recebido em sala de aula .

1. Atribuição de tarefas para o SPRINT 3 .

- Diego ficou responsável por fazer um script, para a integração.
- Jefferson vai elaborar o host do suricata para poder receber as informações necessárias
- Anderson vai fazer modificações no suricata para que ele envie de forma correta os dados ao zabbix.

1. Definição da data da próxima reunião.

- Ficou acordado que a próxima reunião será realizada no dia 3 de julho de 2023, às 23:30.
- Ficou definido que na próxima reunião, será mostrado o andamento do SPRINT 3.

Encerramento:

- Anderson agradeceu a todos pela participação e contribuição na reunião.
- A ata da reunião será compartilhada com os membros da equipe para referência futura.
- A reunião foi encerrada às 00:30.

ATA DE REUNIÃO 07/03/2023

Data: 03 de julho de 2023

Horário: 23:30 - 00:30

Local: Canal de voz/vídeo do Discord

Participantes:

- ANDERSON DOS SANTOS CORREIA
- DIEGO DE LIMA GOMES
- JEFFERSON BRUNO GOMES DO NASCIMENTO

Pauta:

1. Verificar o andamento das tarefas do SPRINT 3 .
2. Listar as dificuldades e procurar soluções.
3. Definição da data da próxima reunião.

Deliberações:

1. Verificar o andamento das tarefas do SPRINT 3 .

- Diego relatou que fez um estudo sobre a implementação do suricata com o zabbix.
- Jefferson mostrou a criação do host pronto para receber os dados do suricata.
- Com o estudo que diego fez, a equipe chegou à conclusão, da melhor forma para mandar dados do suricata ao zabbix

- Anderson falou que ainda não tinha modificado os documentos do suricata pois estava esperando qual solução seria adotada.

3. Listar as dificuldades e procurar soluções.

- Jefferson está enfrentando um erro com o banco de dados do zabbix
- Diego atualizará o Trello, com suas tarefas.
- Anderson vai fazer modificações no documento de configurações do suricata

4.Definição da data da próxima reunião.

- Ficou acordado que a próxima reunião será realizada no dia 05 de julho de 2023, às 23:30.
- Ficou definido que na próxima reunião, serão mostrados os resultados do SPRINT 3, e o relatório.

Encerramento:

- Anderson agradeceu a todos pela participação e contribuição na reunião.
- A ata da reunião será compartilhada com os membros da equipe para referência futura.
- A reunião foi encerrada às 00:30.

ATA DE REUNIÃO 06/05/2023

Data: 05 de julho de 2023

Horário: 23:30 - 00:30

Local: Canal de voz/vídeo do Discord

Participantes:

- ANDERSON DOS SANTOS CORREIA
- DIEGO DE LIMA GOMES
- JEFFERSON BRUNO GOMES DO NASCIMENTO

Pauta:

1. Mostra os resultados do SPRINT 3.
2. Atualização do Gitlab e Trello.
3. Relatório Semanal do SPRINT 3.
4. Planejamento do SPRINT 4.

Deliberações:

1.Mostra os resultados do SPRINT 2.

- Anderson pediu que todos mostrassem suas tarefas do SPRINT 3.
- Diego mencionou que já havia concluído sua tarefa.
- Jefferson comunicou que já tinha feito o host e solucionado o problema citado na reunião anterior.
- Anderson mostrou as modificações feitas no suricata para enviar dados ao zabbix.

2. Atualização do Gitlab e Trello.

- Anderson perguntou sobre as atualizações do Gitlab e Trello.
- Diego falou que realizou o upload dos mesmos para o GitLab, e modificou a página wiki.
- Jefferson mencionou que tinha atualizado o Trello, fez o upload das modificações para o GitLab.
- Anderson fez o upload das modificações para o GitLab.

3.Relatório Semanal do SPRINT 3.

- Foi concluído o relatório semanal referente ao SPRINT 3, abordando as tarefas realizadas

4.Planejamento do SPRINT 4.

- Foi determinada as tarefas de cada integrante para o 4 sprint.
- Diego ficou responsável por Realização de testes em cenários reais para validar a eficácia da solução implementada
- Jefferson ficou responsável pela Implementação do container Docker com Suricata e Zabbix integrados
- Anderson ficou responsável pela Criação de cenários de teste realistas com o GNS3

Encerramento:

- Anderson agradeceu a todos pela participação e contribuição na reunião.
- A ata da reunião será compartilhada com os membros da equipe para referência futura.
- A reunião foi encerrada às 00:30.

Referências

Manual do Zabbix. Disponível em: <https://www.zabbix.com/documentation/5.4/pt/manual>. Acesso em: 30 jun. 2023.

Suricata 6.0.1 documentation. Disponível em: <https://docs.suricata.io/en/suricata-6.0.1/what-is-suricata.html>. Acesso em: 2 jul 2023.

What is Zabbix? Disponível em: <https://github.com/zabbix/zabbix-docker>. Acesso em: 2 jul. 2023.