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

Este relatório descreve as tarefas realizadas no SPRINT 2, que incluem a instalação e configuração do Zabbix em Docker, a instalação do Suricata em Docker e a criação de regras de iptables para estudos de ataques em um ambiente controlado.

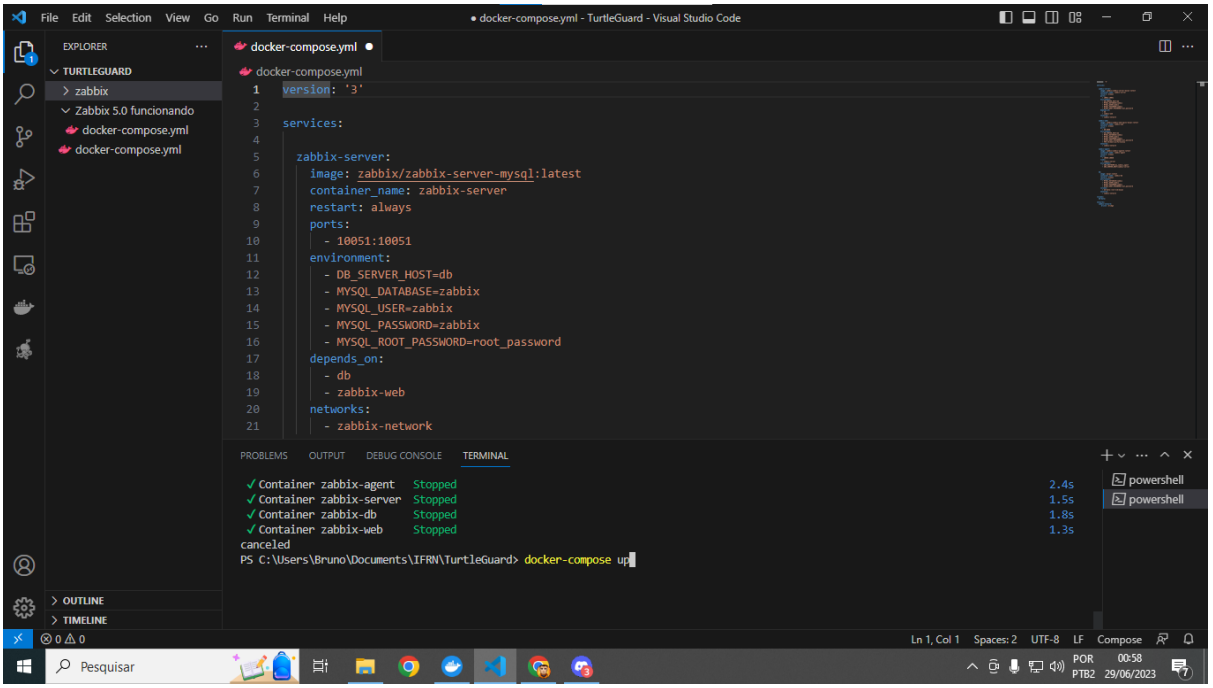
Realizações do SPRINT 2

Instalação e configuração do Zabbix

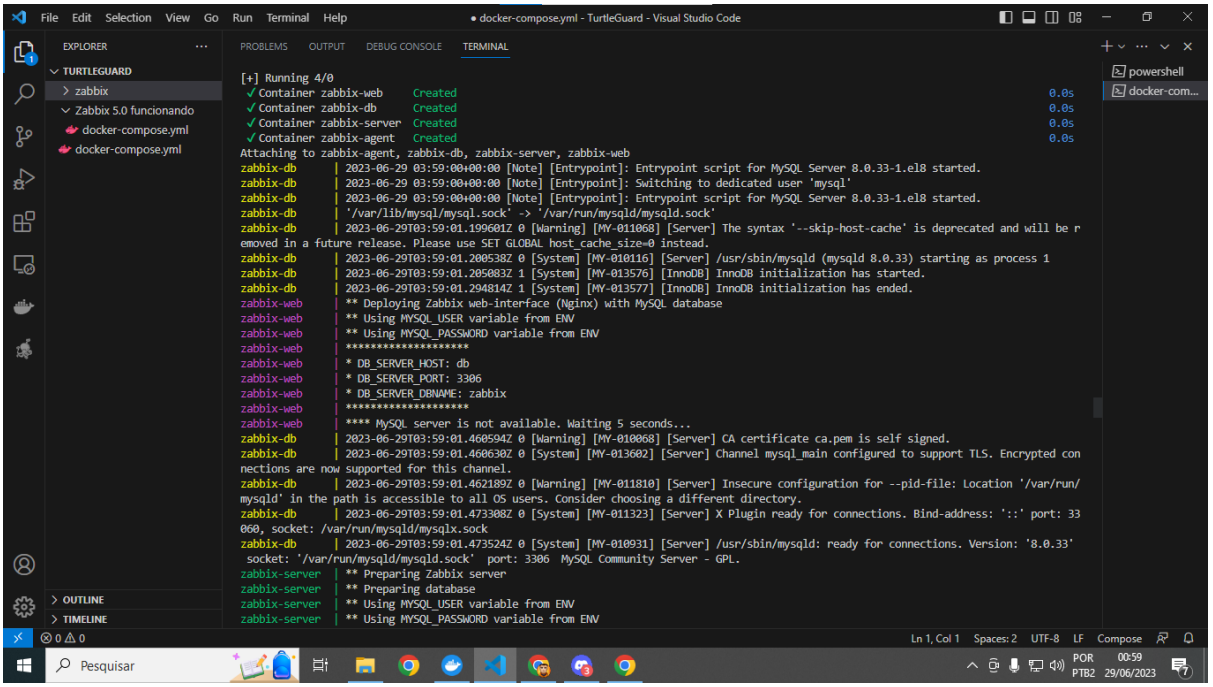
Configuração do ambiente de trabalho e instalação do Zabbix e Configuração de alertas e notificações. Definir e configurar alertas e notificações para eventos de segurança .

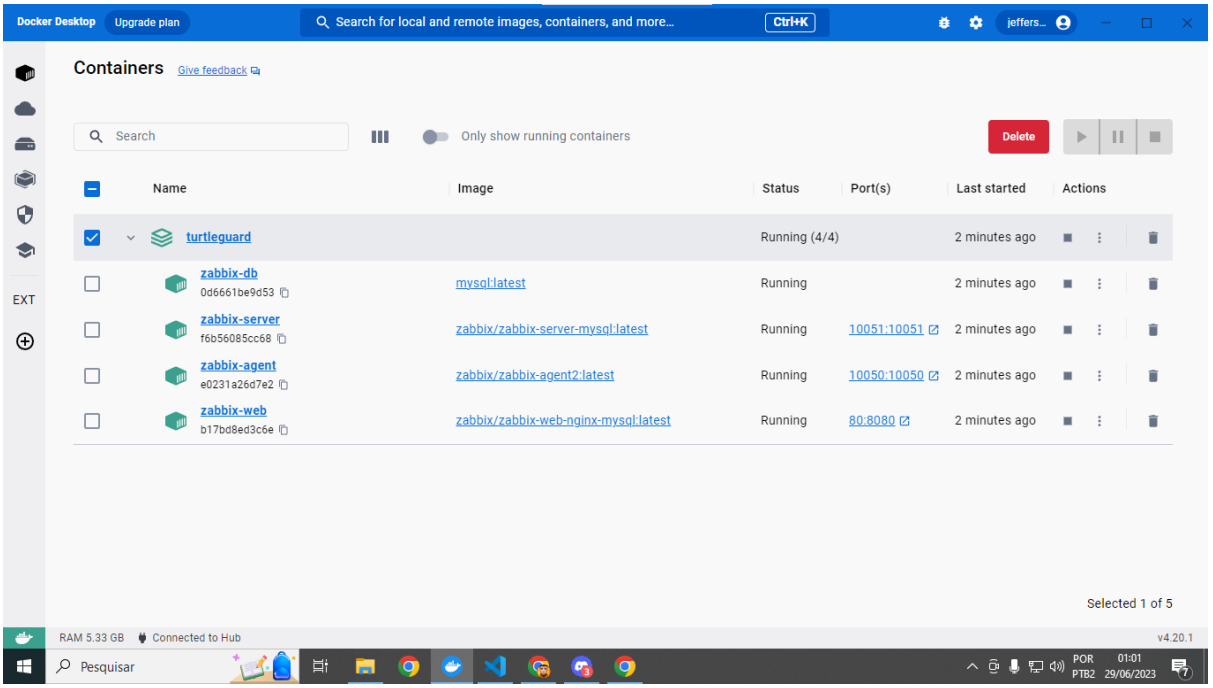
Responsável: **JEFFERSON BRUNO GOMES DO NASCIMENTO**

- Criação e Configuração de um arquivo docker-compose.yml para definir os serviços necessários e configurações necessárias, como a versão do Docker Compose, serviços, redes, volumes, etc., foram definidas no arquivo YAML.para executar o Zabbix em containers Docker.

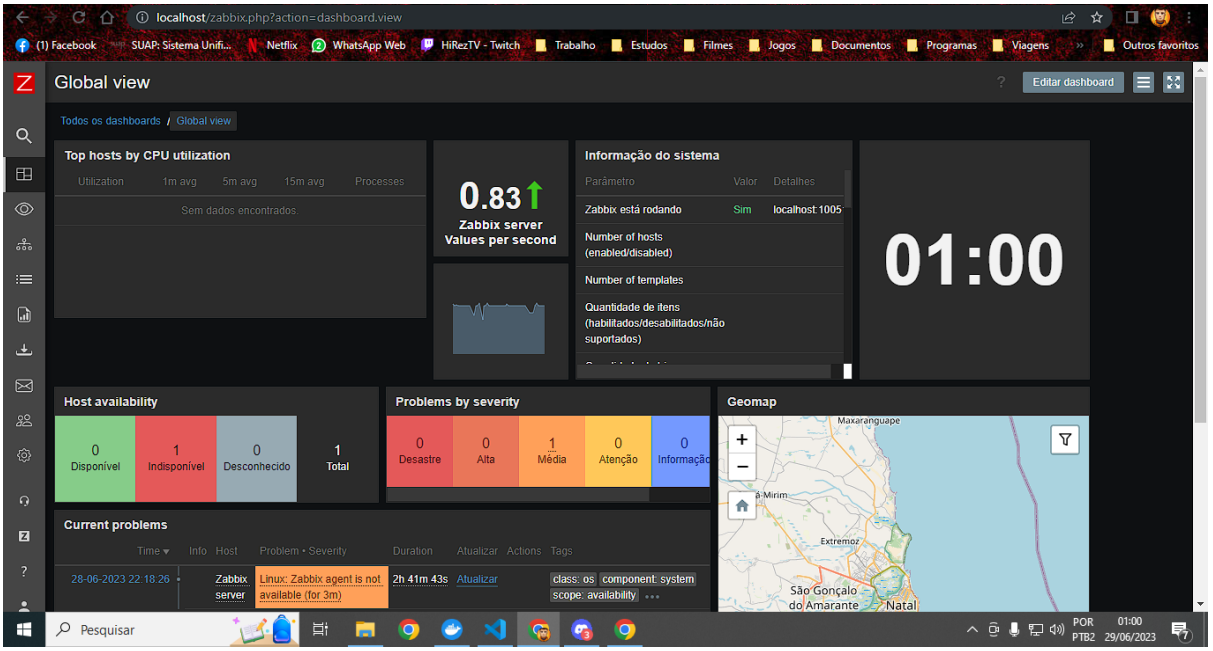


- Execução do Docker Compose: O comando "docker-compose up" foi executado para iniciar os contêineres definidos no arquivo YAML.





- Acesso ao Zabbix: Após a conclusão da execução, o Zabbix ficou acessível em um navegador da web, utilizando o endereço fornecido na configuração.



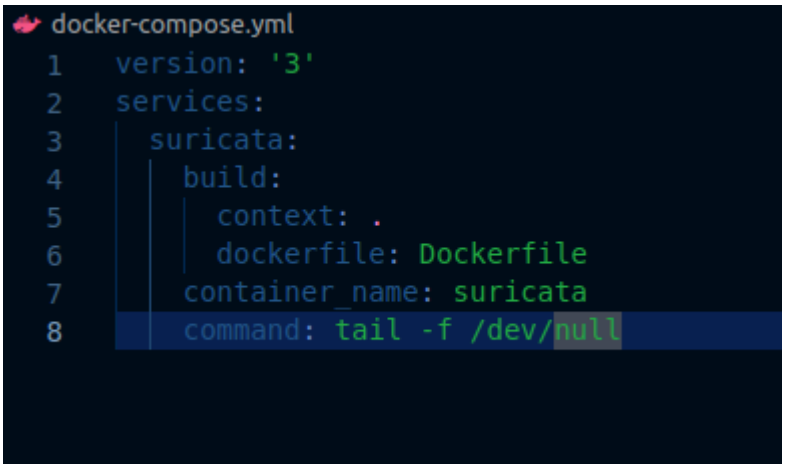
Instalação e configuração do Suricata

Configuração do ambiente de trabalho e instalação do Suricata

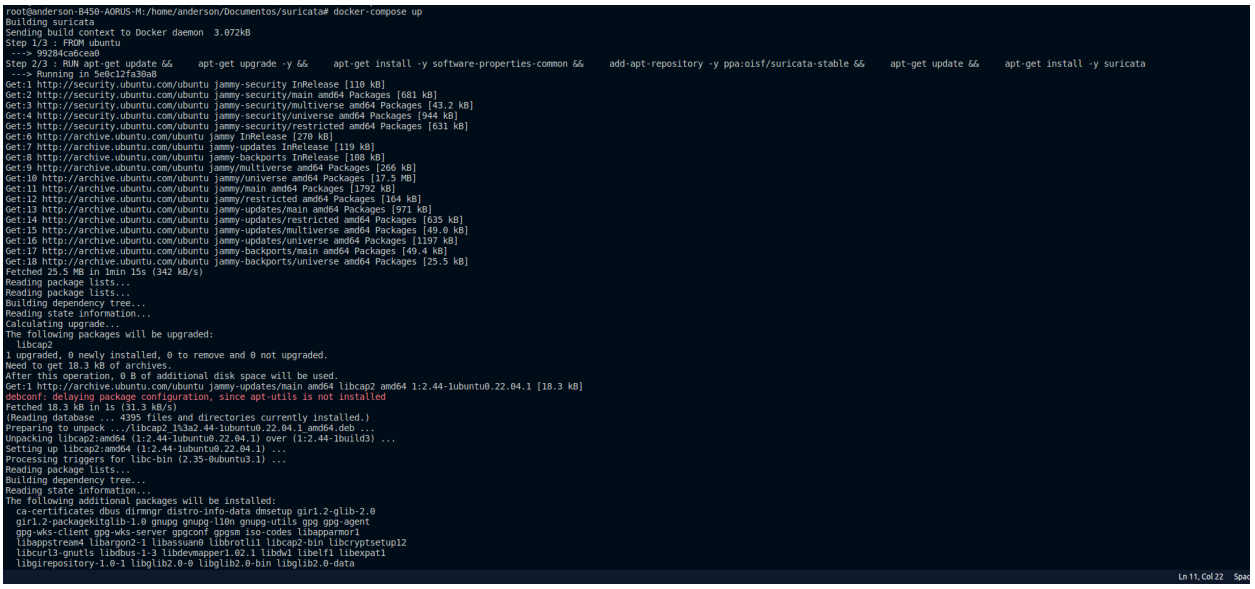
Responsável: **ANDERSON DOS SANTOS CORREIA**

- Criação do Dockerfile: Um arquivo Dockerfile foi criado para definir a imagem base, as dependências necessárias e as instruções para a instalação do Suricata.

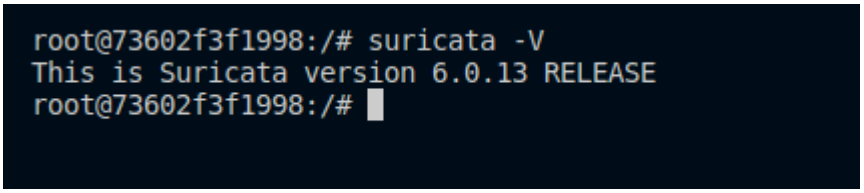
- Configuração do Docker Compose: Um arquivo YAML foi criado para definir o serviço do Suricata e suas configurações



- Execução do Docker Compose: O comando "docker-compose up" foi executado para iniciar o contêiner do Suricata com base na imagem criada.



- Verificação do Suricata: O Suricata foi instalado no container docker.



Criação de regras personalizadas para detecção de ataques DDoS

Desenvolvimento de regras específicas para a detecção de ataques DDoS
Responsável: **DIEGO DE LIMA GOMES**

- Identificação das regras necessárias: Com base nos objetivos do estudo de ataques, foram identificadas as regras de iptables necessárias para permitir ou bloquear determinados tipos de tráfego.

Atividade: Criação de regras personalizadas para detecção de ataques DDoS Descrição: Desenvolvimento de regras especificas para a detecção de ataques DDoS Responsável: Diego de Lima Resultados esperados: Conjunto de regras personalizadas para detecção de ataques DDoS

Desenvolvimento de regras personalizadas para detecção de ataques DDoS

A segurança cibernética é uma prioridade para empresas e organizações que precisam garantir a disponibilidade e a integridade de seus sistemas e serviços online. Um dos tipos de ataque mais frequentes e nocivos é o DDoS (Distributed Denial of Service), que tem como objetivo sobrecarregar os recursos de rede e servidor, impedindo o acesso dos usuários legítimos.

Para se defender de ataques DDoS, é fundamental adotar medidas de detecção e mitigação apropriadas. Uma das formas de reforçar sua segurança é usar o iptables, um firewall muito usado no mundo Linux, para aplicar regras específicas de detecção de ataques DDoS.

As regras a seguir foram elaboradas com base em boas práticas e podem ser ajustadas conforme as necessidades e requisitos do seu ambiente. Elas visam limitar a taxa de pacotes ICMP, conexões TCP, pacotes UDP e conexões HTTP, auxiliando a identificar e mitigar ataques DDoS de maneira mais eficiente.

1. Regra: Detecção de tráfego anormal de UDP com alto volume

- Descrição: Esta regra visa identificar o tráfego UDP com um volume anormalmente alto, que pode ser um indicativo de um ataque DDoS.
- Condição: source_ip: any, destination_port: any, protocol: UDP, packet_count > X (valor a ser definido com base no ambiente)

Limitar a taxa de pacotes UDP:

```
iptables -A INPUT -p udp -m hashlimit --hashlimit-above 10/sec --hashlimit-mode srcip --hashlimit-name udp_attack -j DROP
iptables -A INPUT -p udp -j ACCEPT
```

Essas regras limitam a taxa de pacotes UDP recebidos para 10 por segundo por IP e descartam os pacotes excedentes.

2. Regra: Detecção de conexões HTTP GET excessivas

- Descrição: Essa regra tem como objetivo identificar múltiplas solicitações GET HTTP vindas de um mesmo endereço IP em um curto período de tempo, o que pode indicar um ataque DDoS.
- Condição: source_ip: any, destination_port: 80, protocolo: TCP, http_method: GET, connection_count > Y (valor a ser definido com base no ambiente)

- Criação das regras de iptables: Utilizando os comandos do iptables, as regras foram criadas para filtrar o tráfego de acordo com os requisitos do ambiente controlado.

Código para aplicação das regras.

```
#!/bin/bash


# Excluir todas as regras de firewall
iptables -F


# Limitar a taxa de pacotes ICMP
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
# Aceita um pacote ICMP (ping) a cada segundo e descarta os excedentes
iptables -A INPUT -p icmp -j DROP


# Limitar a taxa de conexões TCP
# Descarta as conexões TCP que excedem 20 por segundo
iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 20 -j DROP
# Descarta as conexões TCP que excedem 10 por minuto de um mesmo IP
iptables -A INPUT -p tcp --syn -m recent --name tcp_attack --update --seconds 60 --hitcount 10 -j DROP
# Aceita as conexões TCP dentro dos limites definidos
iptables -A INPUT -p tcp --syn -m recent --name tcp_attack --set -j ACCEPT



# Limitar a taxa de pacotes UDP
# Descarta os pacotes UDP que excedem 10 por segundo por IP
iptables -A INPUT -p udp -m hashlimit --hashlimit-above 10/sec --hashlimit-mode srcip --hashlimit-name udp_attack -j DROP
# Aceita os pacotes UDP dentro do limite definido
iptables -A INPUT -p udp -j ACCEPT
```

Reuniões

ATA DE REUNIÃO 06/22/2023

Data: 22 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

Participante Ausente:

- JEFFERSON BRUNO GOMES DO NASCIMENTO

Pauta:

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

Deliberações:

1. Revisão das tarefas concluídas no SPRINT 1.

- Anderson propôs que todas as atualizações sobre o projeto fossem colocadas no gitlab .
- Diego concordou com a proposta, e ressaltou que dessa forma facilitaria a criação do relatório semanal.

1. Atribuição de tarefas para o SPRINT 2 .

- Anderson propôs que fosse determinado cada tarefa do sprint com a afinidade de cada .
- Diego concordou com a ideia, e se colocou à disposição para fazer a Criação de regras personalizadas para detecção de ataques DDoS
- A equipe determinou que Jefferson ficaria responsável pela instalação e configuração do Zabbix e Configuração de alertas e notificações.
- Anderson se colocou à disposição de fazer a Instalação e configuração do Suricata

1. Definição da data da próxima reunião.

- Ficou acordado que a próxima reunião será realizada no dia 26 de julho de 2023, às 23:30.
- Ficou definido que na próxima reunião, será mostrado o andamento do SPRINT 2.

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 06/26/2023

Data: 26 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. Verificar o andamento das tarefas do SPRINT 2 .
2. Verificar as atualizações do Trello e Gitlab.
3. Listar as dificuldades e procurar soluções.
4. Definição da data da próxima reunião.

Deliberações:

1. Verificar o andamento das tarefas do SPRINT 2 .

- Anderson relatou que estava enfrentando dificuldades no Docker.
- Jefferson ajudou com algumas dicas.
- Diego informou que concluiu as tabelas "iptables" para o projeto
- Jefferson comunicou que concluiu a instalação do Zabbix.
- foi decidido que ele irá atualizar o Zabbix da versão 5 para a versão 6

2. Verificar as atualizações do Trello e Gitlab.

- Anderson questionou a falta de atualização no Trello e no Gitlab.
- Foi acordado que todos da equipe fizessem as atualizações.

3. Listar as dificuldades e procurar soluções.

- Jefferson efetuará a atualização do Zabbix da versão 5 para a versão 6.
- Diego atualizara o Trello e Gitlab, com suas tarefas.
- Anderson buscará solucionar as dificuldades enfrentadas no Docker
- Definição da data da próxima reunião.

4.Definição da data da próxima reunião.

- Ficou acordado que a próxima reunião será realizada no dia 29 de julho de 2023, às 23:30.
- Ficou definido que na próxima reunião, serão mostrados os resultados do SPRINT 2, 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 06/28/2023

Data: 28 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. Mostra os resultados do SPRINT 2.
2. Atualização do Gitlab e Trello.
3. Relatório Semanal do SPRINT 2.
4. Marcação Reunião Planejamento do SPRINT 3.

Deliberações:

1.Mostra os resultados do SPRINT 2.

- Anderson pediu que todos mostrassem suas tarefas do SPRINT 2.
- Diego mencionou que já havia concluído seus scripts de IPTables.
- Jefferson comunicou que finalizou a atualização do Zabbix da versão v5 para a v6.

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.
- Jefferson mencionou que tinha atualizado o Trello, porém não tinha feito as atualizações no GitLab.
- Durante a reunião Jefferson, realizou o upload dos arquivos relacionados à atualização para o GitLab.

3.Relatório Semanal do SPRINT 2.

- Foi concluído o relatório semanal referente ao SPRINT 2, abordando as tarefas realizadas

4.Marcação Reunião Planejamento do SPRINT 3.

- Ficou acordado que será realizada no dia 29/06/2023 às 23:30, para comentar o feedback recebido, e definir os direcionamento sobre o 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.