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

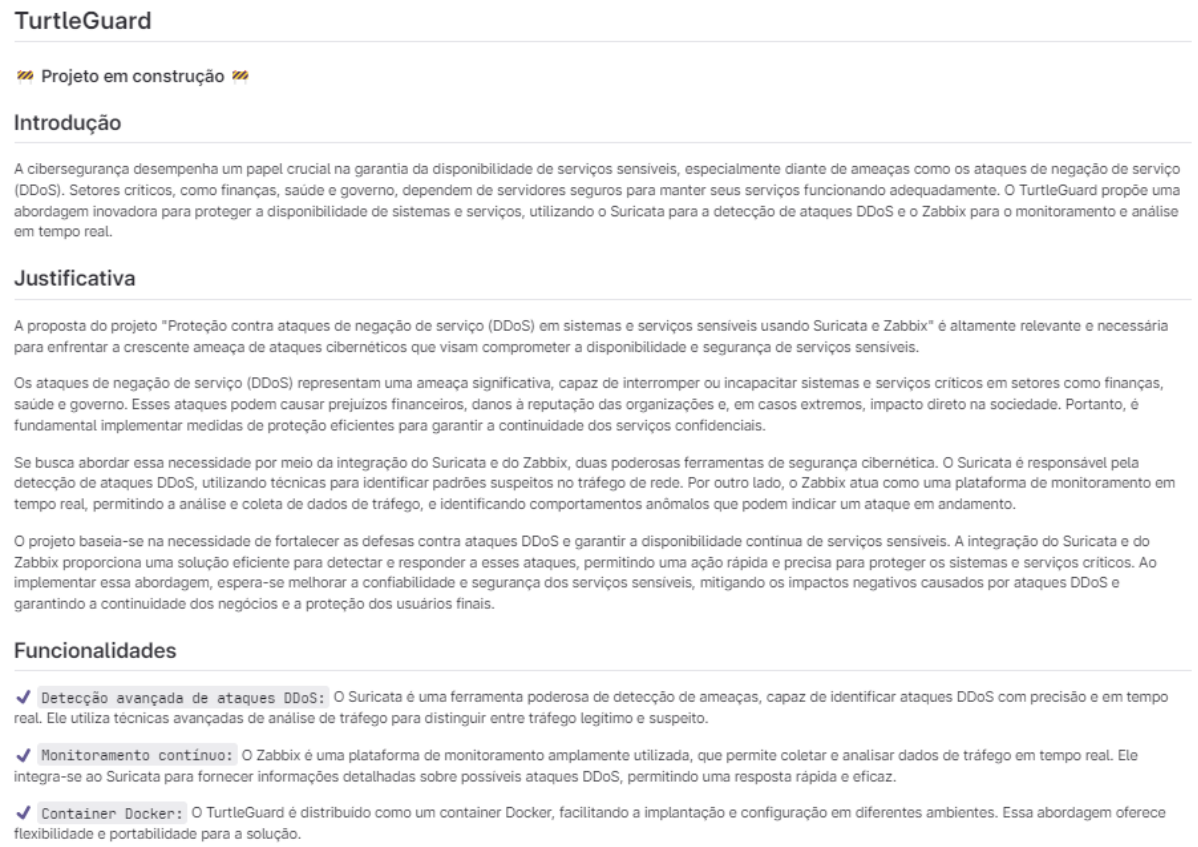
O relatório do Sprint 1 de um projeto é um documento que apresenta as atividades realizadas durante o primeiro ciclo de desenvolvimento do projeto. O Sprint é um evento do Scrum que tem como objetivo entregar incrementos de produto funcionais e de valor para o cliente em curtos períodos de tempo. O relatório do Sprint 1 menciona que foram definidos o modelo de arquitetura do sistema e o planejamento do projeto, além da identificação dos requisitos técnicos e definição das tecnologias a serem utilizadas.

Realizações do SPRINT 1

Definição do escopo, objetivos e requisitos do projeto

Foi delimitado o tema do projeto, que é a proteção contra ataques de negação de serviço (DDoS) em sistemas e serviços sensíveis. - Identificou-se o problema a ser abordado, que é a vulnerabilidade desses sistemas e serviços a ataques DDoS. - Definiu-se a justificativa do projeto, destacando a importância de proteger esses sistemas contra ataques DDoS para garantir a disponibilidade e integridade dos serviços. - Estabeleceram-se os objetivos do projeto, que incluem desenvolver um sistema de detecção de ataques DDoS eficiente e implementar medidas de proteção

para minimizar seu impacto.



TurtleGuard

🚧 Projeto em construção 🚧

Introdução

A cibersegurança desempenha um papel crucial na garantia da disponibilidade de serviços sensíveis, especialmente diante de ameaças como os ataques de negação de serviço (DDoS). Setores críticos, como finanças, saúde e governo, dependem de servidores seguros para manter seus serviços funcionando adequadamente. O TurtleGuard propõe uma abordagem inovadora para proteger a disponibilidade de sistemas e serviços, utilizando o Suricata para a detecção de ataques DDoS e o Zabbix para o monitoramento e análise em tempo real.

Justificativa

A proposta do projeto "Proteção contra ataques de negação de serviço (DDoS) em sistemas e serviços sensíveis usando Suricata e Zabbix" é altamente relevante e necessária para enfrentar a crescente ameaça de ataques cibernéticos que visam comprometer a disponibilidade e segurança de serviços sensíveis.

Os ataques de negação de serviço (DDoS) representam uma ameaça significativa, capaz de interromper ou incapacitar sistemas e serviços críticos em setores como finanças, saúde e governo. Esses ataques podem causar prejuízos financeiros, danos à reputação das organizações e, em casos extremos, impacto direto na sociedade. Portanto, é fundamental implementar medidas de proteção eficientes para garantir a continuidade dos serviços confidenciais.

Se busca abordar essa necessidade por meio da integração do Suricata e do Zabbix, duas poderosas ferramentas de segurança cibernética. O Suricata é responsável pela detecção de ataques DDoS, utilizando técnicas para identificar padrões suspeitos no tráfego de rede. Por outro lado, o Zabbix atua como uma plataforma de monitoramento em tempo real, permitindo a análise e coleta de dados de tráfego, e identificando comportamentos anômalos que podem indicar um ataque em andamento.

O projeto baseia-se na necessidade de fortalecer as defesas contra ataques DDoS e garantir a disponibilidade continua de serviços sensíveis. A integração do Suricata e do Zabbix proporciona uma solução eficiente para detectar e responder a esses ataques, permitindo uma ação rápida e precisa para proteger os sistemas e serviços críticos. Ao implementar essa abordagem, espera-se melhorar a confiabilidade e segurança dos serviços sensíveis, mitigando os impactos negativos causados por ataques DDoS e garantindo a continuidade dos negócios e a proteção dos usuários finais.

Funcionalidades

✓ `Detecção avançada de ataques DDoS:` O Suricata é uma ferramenta poderosa de detecção de ameaças, capaz de identificar ataques DDoS com precisão e em tempo real. Ele utiliza técnicas avançadas de análise de tráfego para distinguir entre tráfego legítimo e suspeito.

✓ `Monitoramento contínuo:` O Zabbix é uma plataforma de monitoramento amplamente utilizada, que permite coletar e analisar dados de tráfego em tempo real. Ele integra-se ao Suricata para fornecer informações detalhadas sobre possíveis ataques DDoS, permitindo uma resposta rápida e eficaz.

✓ `Container Docker:` O TurtleGuard é distribuído como um container Docker, facilitando a implantação e configuração em diferentes ambientes. Essa abordagem oferece flexibilidade e portabilidade para a solução.

Responsável: **ANDERSON DOS SANTOS CORREIA**
Documento completo, [click aqui]

Identificação das tecnologias a serem utilizadas

Realizou-se uma pesquisa e análise das tecnologias Suricata e Zabbix. - O Suricata foi identificado como uma ferramenta adequada para a detecção de ataques DDoS, devido à sua capacidade avançada de análise de tráfego e eficiência. - O Zabbix foi escolhido como a plataforma de monitoramento em tempo real, oferecendo recursos robustos para análise e coleta de dados.

Tecnologias do projeto

Zabbix

O Zabbix, o poderoso sistema de monitoramento de redes, traz diversos benefícios para as organizações. Ele é equipado com amplos recursos capazes de supervisionar uma infinidade de dispositivos e serviços para fornecer uma visão panorâmica de vários ambientes de rede de computadores. Por ser escalável, seu alcance pode abranger desde pequenas até grandes estruturas, lidando com a carga de trabalho entre inúmeros servidores conforme a necessidade. Uma força chave do Zabbix é sua adaptabilidade e versatilidade. Você pode criar itens, gráficos e gatilhoss personalizados e personalizar as configurações de monitoramento de acordo com as necessidades de sua infraestrutura. Ao receber notificações e alertas em tempo real, fica mais eficaz lidar com falhas e problemas. Esse conjunto de recursos permite que você execute ações corretivas mais eficientes.

Além de ser um sistema de monitoramento de rede de código aberto que oferece uma série de vantagens significativas. Sendo uma solução de código aberto, o Zabbix é gratuito, proporcionando economia de custos em comparação com soluções proprietárias. Além disso, a natureza de código aberto permite que os usuários personalizem e modifiquem o sistema de acordo com suas necessidades específicas, oferecendo flexibilidade e liberdade. A transparência do código aberto do Zabbix fornece aos usuários a capacidade de examinar e compreender o funcionamento interno do software, garantindo segurança e confiança. A comunidade ativa de usuários contribui constantemente com melhorias, correções de bugs e recursos adicionais, proporcionando suporte e inovação contínuos.

Suricato

O Suricata é um sistema de detecção e prevenção de intrusões de rede (IDPS) de código aberto que oferece várias vantagens significativas para a segurança de uma infraestrutura de rede. Com recursos avançados de detecção de ameaças, incluindo análise de protocolo em

Responsável: **JEFFERSON BRUNO GOMES DO NASCIMENTO**
Documento completo, click aqui

Planejamento do projeto

Definiu-se a estrutura do projeto, estabelecendo as etapas necessárias para alcançar os objetivos propostos. - Estimaram-se os prazos para cada etapa, considerando as restrições de tempo e recursos. - Identificaram-se os recursos necessários, como equipe de projeto, hardware e software. - Atribuiu-se responsabilidades claras para cada membro da equipe, definindo suas funções e contribuições.

Sprint	Atividade	Descrição	Responsável	Recursos	Data de início	Data de tér
SPRINT 1	Definição do escopo, dos objetivos e dos requisitos do projeto	Consiste em delimitar o tema, o problema, a justificativa e os objetivos do projeto	Integrante 1	Computador, internet, documentos	09/06/23	15/06/23
SPRINT 1	Identificação das tecnologias a serem utilizadas	Pesquisa e análise das tecnologias Suricata e Zabbix	Equipe do projeto	Internet, materiais de referência	16/06/23	18/06/23
SPRINT 1	Planejamento do projeto	Definição das etapas, prazos, recursos necessários e responsabilidades	Equipe do projeto	Computador, internet	19/06/23	22/06/23
SPRINT 2	Instalação e configuração do Suricata	Configuração do ambiente de trabalho e instalação do Suricata	Integrante 1	Computador, internet	23/06/23	25/06/23
SPRINT 2	Instalação e configuração do Zabbix	Configuração do ambiente de trabalho e instalação do Zabbix	Integrante 1	Computador, internet	26/06/23	29/06/23
SPRINT 2	Criação de regras personalizadas para detecção de ataques DDoS	Desenvolvimento de regras específicas para a detecção de ataques DDoS	Equipe do projeto	Computador, internet	30/06/23	02/07/23
SPRINT 2	Configuração de alertas e notificações	Definir e configurar alertas e notificações para eventos de segurança	Integrante 2	Computador, internet	26/06/23	29/06/23
SPRINT 3	Integração do Suricata com o Zabbix	Configuração da integração entre o Suricata e o Zabbix	Integrante 2	Computador, internet	03/07/23	06/07/23
SPRINT 3	Desenvolvimento de scripts para automação da coleta de dados	Criação de scripts para automatizar a coleta de dados do Suricata e envio para o Zabbix	Equipe do projeto	Computador, internet	07/07/23	09/07/23
SPRINT 3	Elaboração de relatórios de segurança	Criar relatórios personalizados com informações de segurança geradas pelo Suricata e Zabbix	Integrante 3	Computador, internet	03/07/23	06/07/23
SPRINT 3	Testes de integração e validação	Realização de testes para verificar a correta integração e funcionamento da solução	Equipe do projeto	Computador, internet	10/07/23	13/07/23
SPRINT 4	Criação de cenários de teste realistas com o GNS3	Configuração de cenários de teste realistas usando o GNS3	Integrante 1	Computador, internet, GNS3	14/07/23	17/07/23
SPRINT 4	Implementação do container Docker com Suricata e Zabbix integrados	Criação e configuração do container Docker contendo o Suricata e o Zabbix integrados	Integrante 3	Computador, internet, Docker	18/07/23	20/07/23
SPRINT 4	Validação da solução implementada em cenários realistas	Realização de testes em cenários reais para validar a eficácia da solução implementada	Equipe do projeto	Computador, internet	21/07/23	25/07/23
SPRINT 5	Teste e validação da abordagem proposta em cenários realistas	Realizar testes e validar a abordagem proposta em cenários realistas	Equipe do projeto	Cenários de teste, documentação	14/07/23	17/07/23
SPRINT 5	Análise dos resultados e ajustes na configuração do Suricata e do Zabbix conforme necessário	Analisar os resultados dos testes e fazer ajustes na configuração do Suricata e do Zabbix, se necessário	Integrante 2	Documentação, acesso aos sistemas	18/07/23	20/07/23
SPRINT 5	Testes de desempenho	Realização de testes de desempenho para avaliar a eficiência da solução implementada	Equipe do projeto	Computador, internet	03/08/23	06/08/23
SPRINT 6	Documentação da solução implementada	Elaborar a documentação da solução implementada	Integrante 3	Documentação, acesso aos sistemas	21/07/23	24/07/23
SPRINT 6	Preparação para a apresentação final do projeto	Preparar-se para a apresentação final do projeto	Equipe do projeto	Apresentação, ensaios	25/07/23	26/07/23
BANCA FINAL DE PI	Apresentação da solução implementada para a banca examinadora	Apresentar a solução implementada para a banca examinadora	Equipe do projeto	Apresentação, documentação	27/07/23	27/07/23
SPRINT 7 (RECUPERAÇÃO)	Realização de ajustes finais na solução implementada com base no feedback recebido durante a apresentação final	Realizar ajustes finais na solução implementada com base no feedback recebido durante a apresentação final	Equipe do projeto	Documentação, acesso aos sistemas	28/07/23	02/08/23

Responsável: **DIEGO DE LIMA GOMES**
Documento completo, click aqui

Próximas etapas

Após a conclusão bem-sucedida do SPRINT 1, as próximas etapas do projeto incluirão: - Elaborar o detalhamento da arquitetura do sistema, considerando a integração do Suricata e do Zabbix. - Realizar a configuração e implementação do Suricata e do Zabbix, conforme as necessidades identificadas. - Testar e validar o sistema em ambiente controlado, a fim de garantir sua eficácia na detecção e proteção contra ataques DDoS. - Monitorar e ajustar continuamente o sistema ao longo das iterações do projeto.

Conclusão

O SPRINT 1 foi crucial para definir o modelo de arquitetura do sistema, realizar o planejamento geral do projeto, identificar os requisitos técnicos e selecionar as tecnologias Suricata e Zabbix. Essas etapas iniciais forneceram uma base sólida para o desenvolvimento e implementação do sistema de proteção contra ataques DDoS. Com a conclusão bem-sucedida deste SPRINT, a equipe está pronta para avançar para as próximas etapas do projeto, com o objetivo de alcançar os objetivos propostos

Reunião

ATA DE REUNIÃO

Data: 20 de junho de 2023

Horário: 23:30 - 00:30

Participantes:

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

Pauta:

1. Revisão das tarefas no SPRINT 1.
2. Criação do quadro no Trello para o projeto.
3. Definição da data da próxima reunião.

Deliberações:

1. Revisão das tarefas no SPRINT 1:
- Anderson solicitou que os demais participantes compartilhassem o status das tarefas atribuídas no SPRINT 1.
- Diego relatou que concluiu a criação de todo o cronograma do projeto (Definição das etapas, prazos, recursos necessários e responsabilidades).
- Jefferson informou que estava com dificuldades para concluir as tarefas, pois não localizava referências relevantes.
- Anderson relatou que ainda não tinha iniciado a criação da documentação dentro do repositório.

1. Criação do quadro no Trello para o projeto:
- Anderson propôs a criação de um quadro no Trello para gerenciar as tarefas e o fluxo de trabalho do projeto.
- A equipe concordou com a ideia, reconhecendo que isso facilitará a organização e a comunicação entre os membros.
- Anderson foi designado para criar o quadro no Trello e compartilhar o acesso com os demais membros da equipe.

1. Definição da data da próxima reunião:
- Ficou acordado que a próxima reunião será realizada no dia 6 de julho de 2023, às 23:30.
- Ficou definido que na próxima reunião, fosse determinado o que cada integrante iria fazer no 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.