| | |
|---|---|
| **Nome: Luiz Paulo Medeiros da Cunha Junior** | **Matrícula: 202310962** |
| **Disciplina: Redes de computadores** | **Data de Entrega: 24/06/2023** |
| **Curso: TADS** | |

## Arquivo coleta e Análise de Tráfego em Redes de Computadores

A coleta e análise de tráfego em redes de computadores são processos fundamentais para entender e monitorar as comunicações dentro de uma rede. Essas atividades permitem identificar problemas de desempenho, detectar atividades maliciosas, analisar padrões de comunicação e tomar decisões baseadas em dados. Neste resumo, abordaremos algumas técnicas de coleta, bem como a análise de tráfego, incluindo a identificação e classificação.

Técnicas de coleta de tráfego: Espelhamento de porta (Port Mirroring): O espelhamento de porta envolve a cópia do tráfego de uma ou mais portas de rede e o encaminhamento desses dados para uma porta de destino. Essa técnica permite que um analisador de protocolos ou outra ferramenta de monitoramento capture o tráfego em tempo real, sem interromper a comunicação normal. Dessa forma, é possível analisar o tráfego de forma não invasiva e obter insights valiosos sobre o comportamento da rede.

Hobbing out: O hobbing out é uma técnica usada em redes de alta velocidade para coletar e analisar o tráfego de forma mais eficiente. Nesse método, o tráfego é direcionado para um dispositivo externo especializado, que realiza a coleta e análise de pacotes em tempo real. Essa abordagem ajuda a reduzir a carga nos equipamentos de rede, garantindo uma análise mais detalhada do tráfego.

TAP (Test Access Port): O TAP é um ponto de acesso de teste que permite a monitoração e coleta de tráfego em uma rede. Ele é instalado entre os dispositivos de rede e fornece uma maneira de capturar pacotes de rede sem interromper o fluxo normal do tráfego. O TAP é uma solução confiável para obter acesso aos dados de tráfego sem depender de recursos internos de espelhamento de porta.

Envenenamento de cache ARP: O envenenamento de cache ARP é uma técnica maliciosa que envolve o envio de informações falsas de mapeamento de endereços IP para a tabela ARP de um host na rede. Isso pode resultar no redirecionamento de tráfego para um dispositivo malicioso, permitindo a coleta indevida de informações ou ataques de intermediário. Embora seja uma técnica prejudicial, ela pode ser estudada e compreendida para fins de segurança e detecção de atividades maliciosas.

Posicionamento do analisador de protocolos: O posicionamento do analisador de protocolos refere-se à localização física ou lógica do dispositivo de análise de tráfego na rede. É essencial posicionar o analisador de protocolos estrategicamente para capturar o tráfego de interesse e obter informações valiosas. Isso pode envolver a colocação do dispositivo em um ponto de estrangulamento de rede, onde o tráfego é concentrado, ou próximo a um ponto crítico da rede onde a análise detalhada é necessária.

Análise de tráfego: A análise de tráfego é uma etapa crucial para entender e interpretar os dados coletados. Envolve a identificação e classificação dos diferentes tipos de tráfego que fluem pela rede. Através da análise, é possível determinar os protocolos utilizados, quantificar o volume de tráfego, identificar padrões de comunicação, bem como identificar as origens e destinos do tráfego. A análise de

tráfego é essencial para detectar problemas de desempenho, monitorar a segurança da rede e auxiliar no planejamento de capacidade.

A coleta e análise de tráfego em redes são processos vitais para entender e monitorar a comunicação na rede. Diferentes técnicas de coleta, como espelhamento de porta, hobbing out e TAP, permitem a obtenção de dados de tráfego valiosos. O posicionamento estratégico do analisador de protocolos e a análise adequada são cruciais para obter insights significativos sobre o comportamento da rede.