# **Relatório de Mapeamento de Rede**

## **Informações Gerais**

* **Data do Mapeamento**: [Data]
* **Ferramentas Utilizadas**: [Ferramentas]
* **Alcance do Mapeamento**: [Faixa de IP ou nome da rede]
* **Responsável pelo Mapeamento**: [Nome]

## **Objetivo**

[Descrever o objetivo do mapeamento de rede, como identificar dispositivos vulneráveis, atualizar o inventário de ativos de rede, ou verificar a conformidade com políticas de segurança.]

## **Metodologia**

[Breve descrição das ferramentas e técnicas utilizadas para realizar o mapeamento de rede, incluindo qualquer configuração específica ou parâmetros de varredura.]

## **Sumário dos Resultados**

* **Total de Hosts Identificados:** [Número]
* **Sistemas Operacionais Encontrados:** [Lista de SOs]
* **Serviços Comuns Identificados:** [Lista de Serviços]

## **Detalhamento dos Resultados**

### **Hosts Ativos**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP do Host** | **Nome do Host** | **Sistema Operacional** | **Serviços Identificados** |
| 192.0.2.1 | ExemploHost1 | Linux Debian 12 | SSH, HTTP |
| ... | ... | ... | ... |

[Incluir tabelas ou listas adicionais conforme necessária para detalhar os sistemas operacionais, versões e serviços identificados em cada host ativo.]

### **Análise de Vulnerabilidades Potenciais**

[Incluir uma análise baseada nos serviços identificados, versões de sistemas operacionais e quaisquer vulnerabilidades conhecidas associadas a essas versões ou serviços.]

## **Recomendações**

* **Atualizações de Segurança:** [Recomendações para atualizações de software ou SO com base nas vulnerabilidades identificadas.]
* **Configurações de Segurança:** [Sugestões para melhorar as configurações de segurança dos dispositivos na rede.]
* **Monitoramento e Análise Contínua:** [Recomendações para monitoramento contínuo e análise de segurança da rede.]

## **Conclusão**

[Um resumo dos principais achados, a importância desses achados para a segurança da rede, e os próximos passos recomendados.]