# Relatório Técnico – Segmentação de Rede

Autor: Jadson Silva Souza

Data: 30/07/2025

Versão: 1.1

## Visão Geral

Este relatório apresenta os resultados de uma auditoria técnica em um ambiente de rede segmentada simulada. O objetivo é identificar hosts, serviços ativos, possíveis riscos e fornecer recomendações para melhorias na segurança da rede.

## Objetivo

Levantar informações de rede usando ferramentas de análise, identificar serviços e portas expostas, mapear os hosts ativos e elaborar um inventário técnico com diagnóstico e recomendações.

## Escopo

Ambiente simulado em containers Docker com múltiplas sub-redes: corp\_net, infra\_net e guest\_net.

## Metodologia

Foram utilizadas as seguintes ferramentas:

* • nmap  
  • rustscan  
  • curl  
  • ping  
  • arp  
  • comandos bash (grep, awk, tee)

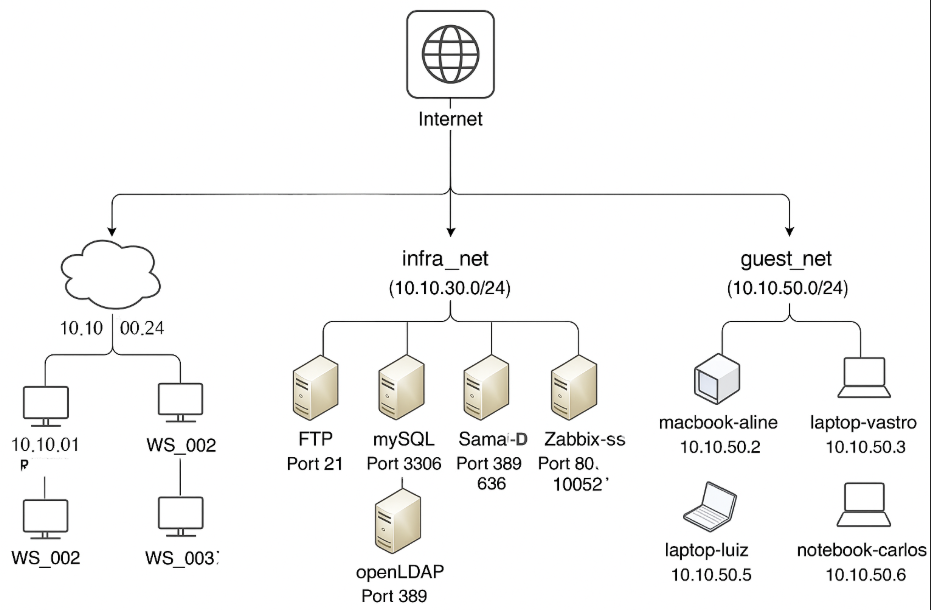
As técnicas incluíram varredura ativa (ping scan), enumeração de portas e serviços, análise manual e documentação dos resultados.

## Redes Identificadas

As seguintes redes foram descobertas durante a varredura:

|  |  |  |
| --- | --- | --- |
| Nome Estimado | Subnet Descoberta | Finalidade Suposta |
| corp\_net | 10.10.10.0/24 | Rede corporativa principal |
| guest\_net | 10.10.30.0/24 | Rede de visitantes/dispositivos externos |
| infra\_net | 10.10.50.0/24 | Rede de infraestrutura e servidores |

## Dispositivos por Rede

* corp\_net:
* 

|  |  |  |
| --- | --- | --- |
| IP | Função | Evidência |
| 10.10.10.10 | Estação de trabalho WS\_001 | Responde ping, portas abertas 22 e 80 |
| 10.10.10.11 | Estação de trabalho WS\_002 | Serviços limitados, HTTP ativo |

* guest\_net:

|  |  |  |
| --- | --- | --- |
| IP | Função | Evidência |
| 10.10.30.100 | Notebook pessoal | Responde ping, nenhum serviço relevante |

* infra\_net:

|  |  |  |
| --- | --- | --- |
| IP | Função | Evidência |
| 10.10.50.10 | Servidor FTP | Porta 21 aberta, acesso FTP-anon permitido |
| 10.10.50.11 | Servidor MySQL | Porta 3306, MySQL aberto sem autenticação |
| 10.10.50.15 | Servidor SMB | Porta 445 ativa, compartilhamentos abertos |
| 10.10.50.17 | Servidor LDAP | Porta 389, informações públicas expostas |
| 10.10.50.117 | Servidor Web (Zabbix) | Porta 80 com interface web acessível |

## Riscos Identificados

• A guest\_net aparenta estar isolada, mas precisa ser testada quanto ao roteamento com a corp\_net.  
• A infra\_net contém servidores críticos com serviços expostos a ataques comuns (FTP anônimo, MySQL sem autenticação).  
• A presença de impressoras e dispositivos com acesso web na mesma rede de estações de trabalho pode facilitar movimentação lateral.  
• Serviços SMB e LDAP expostos sem hardening são pontos de vulnerabilidade.

## Recomendações

1. Isolar completamente a rede infra\_net das estações de trabalho.  
2. Implementar autenticação segura em serviços FTP e MySQL.  
3. Desativar ou restringir serviços SMB e LDAP se não forem necessários.  
4. Aplicar firewall interno entre redes e segmentar os acessos por VLANs.  
5. Auditar dispositivos web (Zabbix, Impressoras) quanto a vulnerabilidades conhecidas.

## Conclusão

A análise da rede segmentada revelou múltiplos dispositivos com serviços expostos e potenciais riscos. Recomenda-se a segmentação rigorosa das redes, aplicação de medidas de hardening e políticas de acesso restritivo. Este exercício desenvolve a capacidade de análise técnica de redes para fins de segurança ofensiva e defensiva.