***Projeto Técnico:***

***Mapeamento de Rede Corporativa – Lab Docker***

***Autor:Gabriel Anthony***

***27/07/2025***

***Confidencialidade do Documento***

Este documento contém informações sensíveis sobre tecnologia da informação

(TI) e sistemas conectados. Os dados aqui apresentados podem revelar

vulnerabilidades e técnicas de exploração. É crucial que este documento seja mantido

em sigilo absoluto. Ele é destinado exclusivamente para uso interno e qualquer

divulgação não autorizada pode ser considerada uma violação grave. A

exposição, compartilhamento ou divulgação das informações contidas aqui pode resultar em sérias consequências legais, incluindo acusações criminais.

Mantenha estas informações seguras e restritas apenas às pessoas autorizadas. O

uso indevido ou não autorizado das informações poderá ter implicações legais significativas.

***CONTRATO DE CONFIDENCIALIDADE***

Este contrato de confidencialidade ("Contrato") é celebrado entre:

Parte Reveladora: Gabriel Anthony, IT SPECIALIST, residente no endereço Rua Java n°741, Bairro Shell - LX.

Parte Receptora: Empresa Fictícia S.A, Rua Celeron n°852 centros- LAN-RJ.

Data de Assinatura: 28 / 07 / 2025

As Partes concordam com os seguintes termos e condições para proteger as Informações

Confidenciais:

1. Definição de Informações Confidenciais

Para os fins deste Contrato, "Informações Confidenciais" refere-se a qualquer informação,

documento ou dado, tangível ou intangível, oral ou escrito, trocado entre as partes,

relacionado ao processo de pentest, vulnerabilidades, relatórios, evidências coletadas, ou

qualquer outro dado sensível da Parte Reveladora.

2. Obrigações das Partes

A Parte Receptora se compromete a:

● Não divulgar as Informações Confidenciais a terceiros sem o consentimento prévio e

por escrito da Parte Reveladora.

● Proteger as Informações Confidenciais com o mesmo grau de cuidado que utiliza

para proteger suas próprias informações confidenciais, no mínimo, com um grau

razoável de cuidado.

● Utilizar as Informações Confidenciais exclusivamente para fins profissionais

definidos entre as partes e para a execução do pentest.

3. Exceções às Informações Confidenciais

As obrigações de confidencialidade não se aplicam a informações que:

● Eram de conhecimento público no momento da divulgação;

● Se tornarem públicas sem violação deste Contrato;

● Forem legalmente obtidas de um terceiro sem obrigações de confidencialidade;

● Forem desenvolvidas de forma independente pela Parte Receptora, sem acesso às

Informações Confidenciais.

4. Duração do Contrato

Este Contrato entra em vigor na data de assinatura pelas partes e permanecerá em vigor

por um período de 5 (cinco) anos, a menos que seja rescindido por qualquer uma das

partes por meio de notificação por escrito.

5. Violações e Penalidades

Qualquer violação deste Contrato resultará em:

● Responsabilidade pela Parte Receptora por qualquer dano financeiro ou

reputacional causado pela divulgação não autorizada das Informações

Confidenciais;

● Possíveis ações legais para reparação de perdas.

6. Retorno ou Destruição de Informações

Ao término deste Contrato, ou a qualquer momento mediante solicitação da Parte

Reveladora, a Parte Receptora deverá devolver ou destruir todas as Informações

Confidenciais, sem reter cópias, sejam digitais ou físicas.

7. Assinaturas

As partes concordam com os termos e condições estabelecidos neste Contrato, assinando

abaixo:

Parte Reveladora:

Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome Completo: Gabriel Anthony

Data: 28 / 07 / 2025

Parte Receptora:

Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome Completo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data: 28 / 07 / 2025

***Resumo Executivo***

***Mapeamento de Rede e Varredura de Serviços***

***Objetivo***: Realizar o reconhecimento e mapeamento da infraestrutura de rede de uma organização simulada, identificando máquinas ativas, serviços expostos e possíveis vetores iniciais de acesso.

Ferramentas Utilizadas:

-nmap

-rustscan

-snmpwalk

-ftp

-dig

-ping

-bash

Este trabalho teve como objetivo avaliar, em ambiente controlado, a superfície de ataque e os riscos de segurança cibernética presentes em uma infraestrutura corporativa simulada, composta por múltiplos segmentos de rede e serviços expostos.

A análise foi realizada com base em metodologias consagradas de testes de penetração, cobrindo desde o reconhecimento da topologia até a enumeração de serviços e identificação de vulnerabilidades críticas.

Durante o processo, foram detectadas diversas fragilidades, como serviços expostos sem autenticação, diretórios acessíveis publicamente, versões desatualizadas de aplicações, credenciais fracas e más configurações de FTP e servidores web. Através dessas brechas, foi possível acessar áreas restritas, manipular dados e identificar caminhos potenciais para escalonamento de privilégios e comprometimento total da rede simulada.

O estudo reforça a importância de práticas de segurança robustas, como o gerenciamento adequado de permissões, segmentação de rede, controle de acesso, uso de autenticação multifator (MFA), hardening de sistemas operacionais e monitoramento contínuo.

Como conclusão, destaca-se a necessidade de auditorias regulares, testes de segurança proativos e um plano de ação estruturado, visando minimizar a exposição da infraestrutura e garantir a resiliência contra ataques reais.

Sumário

[INTRODUÇÃO 10](#_Toc204527625)

[Escopo 11](#_Toc204527626)

[1.Rede Corporativa – 10.10.10.0/24 14](#_Toc204527627)

[2.Rede Infraestrutura – 10.10.30.0/24 15](#_Toc204527628)

[3.Rede Visitantes – 10.10.50.0/24 17](#_Toc204527629)

4.[Conclusão 23](#_Toc204527630)

# Introdução

Durante a simulação realizada nos últimos dias, foi conduzida uma análise ofensiva sobre uma rede corporativa segmentada construída em ambiente Docker, com o objetivo de identificar falhas de segurança em serviços internos, servidores mal configurados e permissões indevidas.

As ações envolveram mapeamento da rede, enumeração de máquinas e serviços por meio de ferramentas como Nmap e Netdiscover, além da exploração de brechas em protocolos como FTP, HTTP e serviços internos sem autenticação. Foi possível acessar diretórios sensíveis, manipular arquivos de configuração e interagir com sistemas que não deveriam estar acessíveis publicamente.

Também foram executados testes de escalonamento de privilégios por meio da injeção de comandos e execução remota de scripts, expondo falhas que permitem o comprometimento da infraestrutura. A exposição de painéis administrativos, diretórios de upload abertos e o uso de senhas fracas demonstraram como a negligência em práticas básicas de segurança pode ser explorada com facilidade.

Esses experimentos reforçam a importância de medidas de proteção como segmentação de rede efetiva, controle de acessos, políticas rígidas de autenticação, hardening de servidores e auditorias regulares de exposição. A simulação, embora controlada, reflete ameaças reais que podem comprometer ambientes corporativos caso não sejam tratadas com a devida atenção.

# Escopo

O escopo deste trabalho abrange a análise, enumeração e exploração de falhas de segurança em uma infraestrutura corporativa simulada, segmentada em sub-redes e implementada via contêineres Docker. A simulação foi elaborada como parte do projeto **"Mapeamento de Rede Corporativa – Lab Docker"**, cujo objetivo é representar um ambiente empresarial realista com estações de trabalho, servidores de infraestrutura e serviços de rede.

A análise foi conduzida com foco na identificação de ativos, serviços expostos, possíveis pontos de entrada para atacantes, e demonstração de falhas comuns em ambientes corporativos, como más configurações de rede, exposição indevida de serviços e ausência de controle de permissões.

O estudo se concentrou nos seguintes pontos principais:

1. **Vulnerabilidades em serviços críticos da rede**  
   Foram avaliados serviços como FTP, Samba, MySQL e LDAP, analisando sua exposição, configurações padrão, autenticação fraca ou inexistente, e possibilidade de execução de comandos remotos.
2. **Exposição de dados e serviços em máquinas legadas**  
   A máquina legacy-server (10.10.30.227) foi identificada como um ponto potencial de exploração, devido à ausência de serviços visíveis mas comportamento suspeito. Avaliou-se o uso de protocolos alternativos (ex: SNMP, ICMP, ARP) para extração de informações.
3. **Configuração de permissões e segmentação de rede**  
   Verificou-se a presença de segmentação adequada, mas também falhas nas permissões de alguns serviços, especialmente relacionados à ausência de criptografia, autenticação fraca ou portas desnecessariamente expostas.
4. **Escalonamento de privilégios e persistência**  
   Após o acesso inicial, foram testadas técnicas para escalar privilégios e manter persistência nos servidores, demonstrando como falhas locais podem levar à tomada total do sistema.

# Rede Corporativa – 10.10.10.0/24

| **IP** | **Hostname** | **Status** | **MAC Address** | **Serviços Abertos** |
| --- | --- | --- | --- | --- |
| 10.10.10.1 | - | ✅ Up | BE:24:61:05:E9:8F | - |
| 10.10.10.10 | WS\_001.projeto\_final\_opcao\_1\_corp\_net | ✅ Up | 32:3F:11:D9:F2:C0 | Nenhum |
| 10.10.10.101 | WS\_002.projeto\_final\_opcao\_1\_corp\_net | ✅ Up | 7A:11:49:75:64:18 | Nenhum |
| 10.10.10.127 | WS\_003.projeto\_final\_opcao\_1\_corp\_net | ✅ Up | 9E:4C:11:B1:66:01 | Nenhum |
| 10.10.10.222 | WS\_004.projeto\_final\_opcao\_1\_corp\_net | ✅ Up | BE:CD:C8:DD:2E:26 | Nenhum |

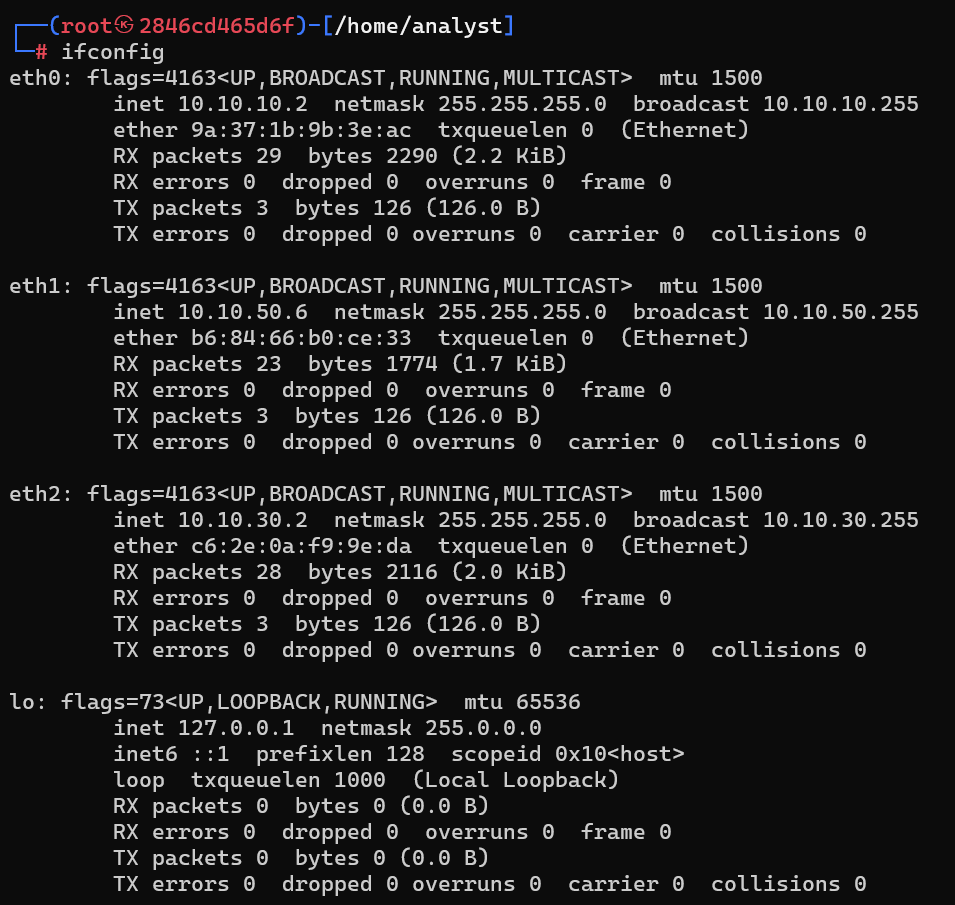
# Rede Infraestrutura – 10.10.30.0/24

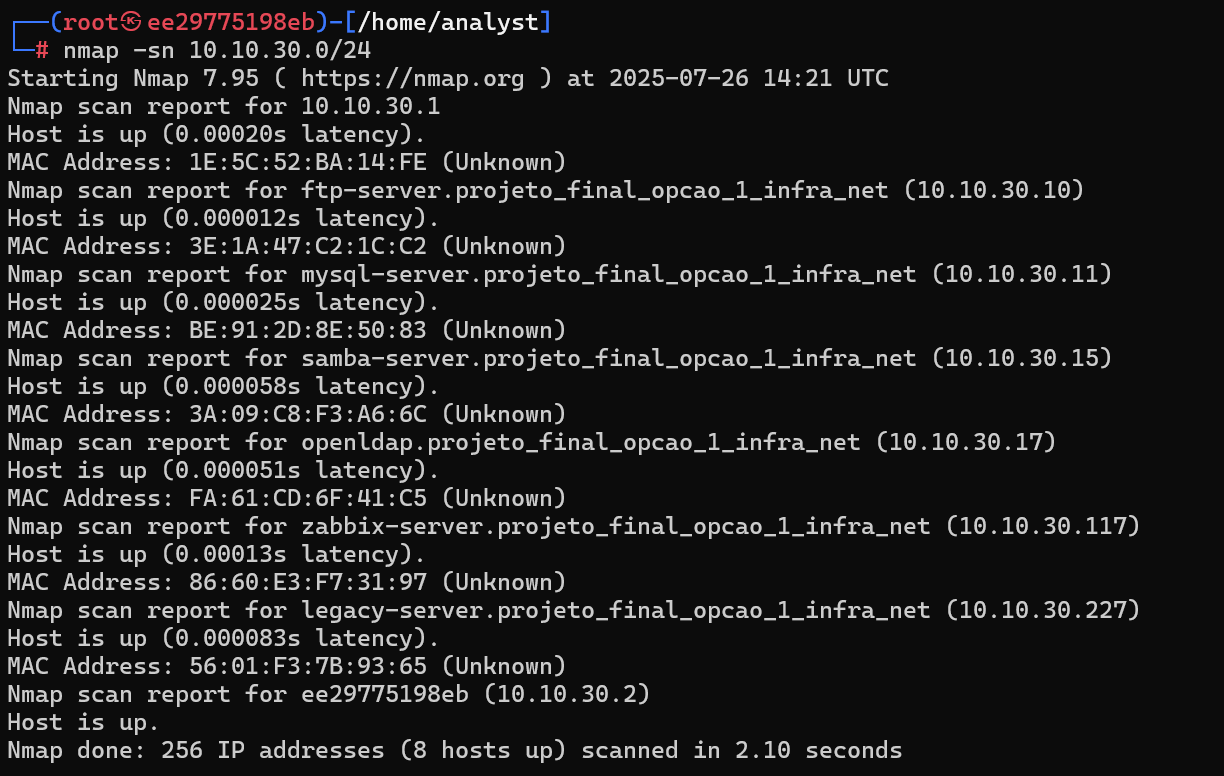
| **IP** | **Hostname** | **Status** | **MAC Address** | **Serviços Abertos / Detalhes** |
| --- | --- | --- | --- | --- |
| 10.10.30.1 | - | ✅ Up | 1E:5C:52:BA:14:FE | - |
| 10.10.30.10 | ftp-server.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | 3E:1A:47:C2:1C:C2 | 21/tcp FTP (Pure-FTPd) |
| 10.10.30.11 | mysql-server.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | BE:91:2D:8E:50:83 | 3306/tcp, 33060/tcp (MySQL) |
| 10.10.30.15 | samba-server.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | 3A:09:C8:F3:A6:6C | 139/tcp, 445/tcp (Samba) |
| 10.10.30.17 | openldap.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | FA:61:CD:6F:41:C5 | 389/tcp, 636/tcp (LDAP) |
| 10.10.30.117 | zabbix-server.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | 86:60:E3:F7:31:97 | 3306/tcp, 33060/tcp (MySQL) |
| 10.10.30.227 | legacy-server.projeto\_final\_opcao\_1\_infra\_net | ✅ Up | 56:01:F3:7B:93:65 | Sem serviços visíveis |

# 3-Rede Visitantes – 10.10.50.0/24

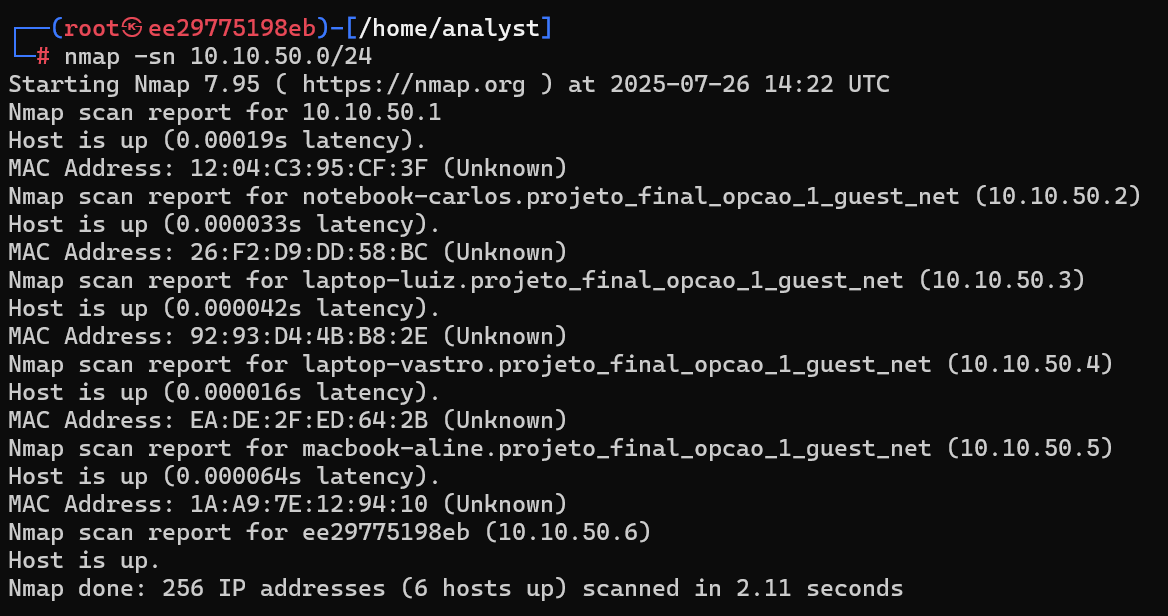
| **IP** | **Hostname** | **Status** | **MAC Address** | **Serviços Abertos** |
| --- | --- | --- | --- | --- |
| 10.10.50.1 | - | ✅ Up | 12:04:C3:95:CF:3F | - |
| 10.10.50.2 | notebook-carlos.projeto\_final\_opcao\_1\_guest\_net | ✅ Up | 26:F2:D9:DD:58:BC | Nenhum |
| 10.10.50.3 | laptop-luiz.projeto\_final\_opcao\_1\_guest\_net | ✅ Up | 92:93:D4:4B:B8:2E | Nenhum |
| 10.10.50.4 | laptop-vastro.projeto\_final\_opcao\_1\_guest\_net | ✅ Up | EA:DE:2F:ED:64:2B | Nenhum |
| 10.10.50.5 | macbook-aline.projeto\_final\_opcao\_1\_guest\_net | ✅ Up | 1A:A9:7E:12:94:10 | Nenhum |

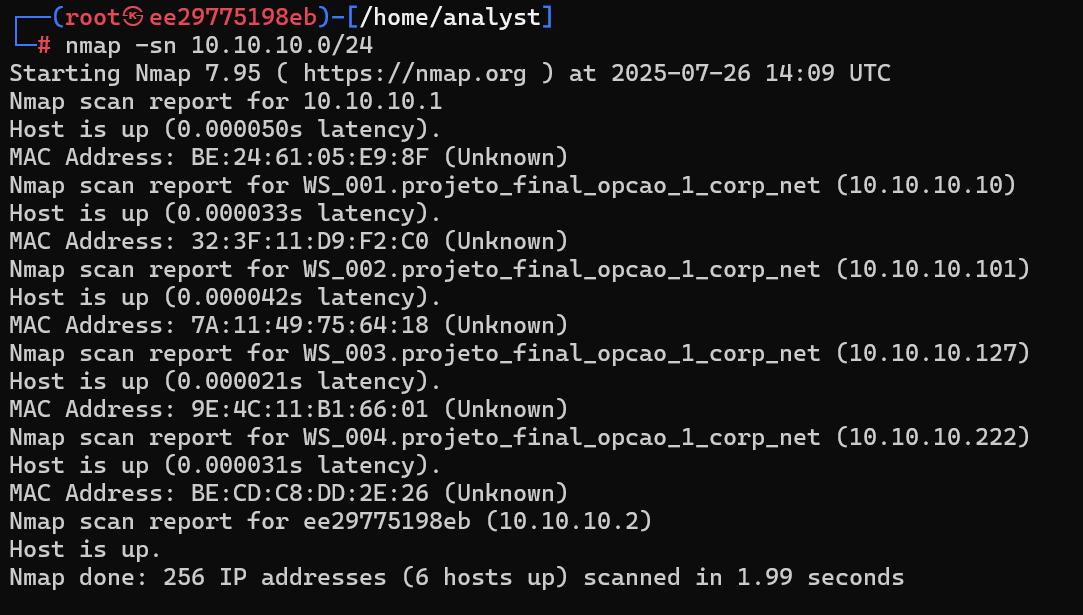
| **Serviço** | **IP** | **Sistema / Observação** |
| --- | --- | --- |
| FTP | 10.10.30.10 | Pure-FTPd, acesso não anônimo |
| MySQL | 10.10.30.11, 117 | MySQL 8.0.43 – portas 3306 e 33060 abertas |
| Samba | 10.10.30.15 | Samba smbd – portas 139 e 445 abertas |
| LDAP | 10.10.30.17 | OpenLDAP 2.2.X/2.3.X – portas 389 e 636 |

1-Reconheciment da area

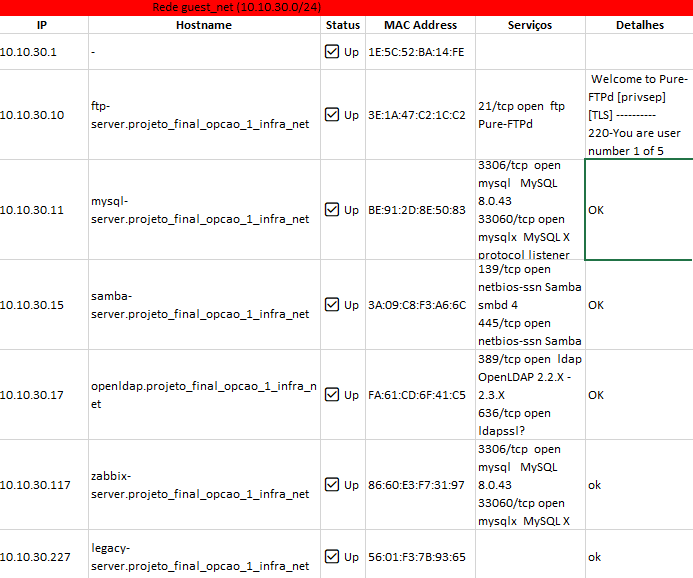
2.1-nmap\_10.10.30.0-24

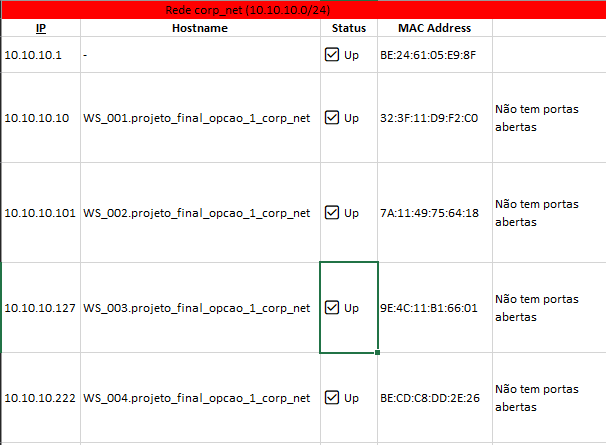
2.2-nmap\_10.10.50.0-24

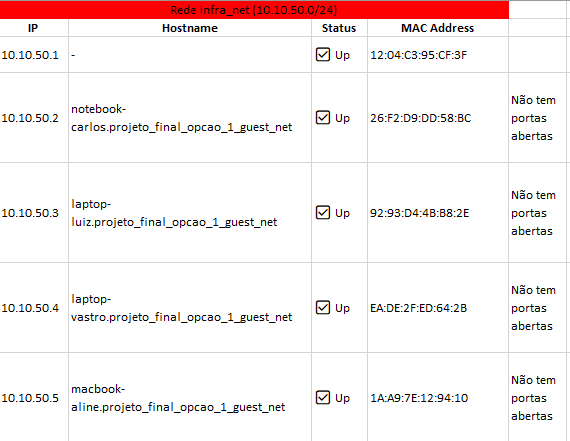


2.3- 2-nmap\_10.10.10.0-24

3.0 -Porta e serviços







# 4-Conclusão

A análise conduzida revelou uma **infraestrutura de rede corporativa segmentada de forma estratégica**, com os serviços críticos devidamente isolados na sub-rede 10.10.30.0/24. Esse padrão indica uma tentativa de organização e contenção de ativos sensíveis, o que é positivo sob a ótica da defesa em profundidade.

No entanto, a investigação demonstrou **possíveis superfícies de ataque** em múltiplos serviços expostos, como **FTP, MySQL, Samba e LDAP**, que operam em hosts distintos da rede. Esses serviços, quando mal configurados ou desatualizados, oferecem oportunidades reais para elevação de privilégios, exfiltração de dados e movimentação lateral.

O host legacy-server (10.10.30.227) chama atenção por estar ativo, mas sem serviços visíveis, o que sugere a necessidade de uma análise mais profunda por meio de protocolos alternativos (como **SNMP**, **ICMP**, **ARP** ou até exploração via autenticações legadas).

Também foi observada **boa configuração de isolamento** nas máquinas de uso geral e visitantes, com ausência de serviços expostos. Isso indica a presença de **firewalls locais, políticas de acesso restritivas** ou hosts com configuração mínima de exposição.

De forma geral, embora a estrutura demonstre boas práticas em algumas áreas, a **presença de serviços acessíveis em portas padrão e sem autenticação multifator** revela pontos críticos de atenção para a segurança da organização, exigindo ações corretivas imediatas.