

Aline Blotta Aguilar Jardim

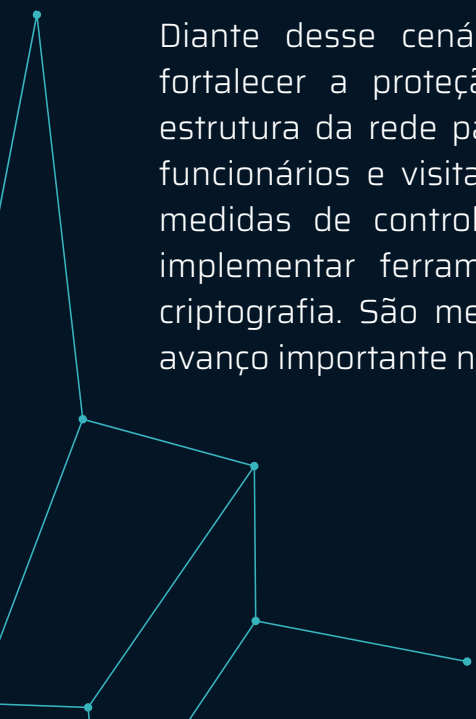


# Sumário Executivo

Atualmente, os ataques cibernéticos representam uma ameaça concreta às organizações, com potencial de causar prejuízos operacionais, financeiros e danos à reputação. Este relatório foi desenvolvido com o objetivo de avaliar se os recursos de tecnologia da empresa estão devidamente protegidos e alinhados às boas práticas de Segurança da Informação, a fim de antecipar riscos e evitar falhas que possam comprometer o ambiente.

Durante a análise, foram identificados 20 equipamentos em funcionamento, distribuídos em três redes distintas: uma de uso interno, uma dedicada a servidores e infraestrutura e outra destinada aos visitantes. Em 10 desses equipamentos foram encontradas falhas que permitem acessos externos sem nenhum tipo de bloqueio ou controle, o que representa risco de invasão e manipulação de dados. Também foi constatado o uso de sistemas desatualizados, com falhas conhecidas, o que aumenta significativamente a exposição da rede.

A análise indicou que a rede não está em conformidade com os padrões ideais de segurança. Os sistemas operam com níveis diferentes de proteção e não há uma separação clara entre áreas críticas e de uso geral, o que facilita acessos indevidos e a circulação de ameaças dentro do ambiente.



Diante desse cenário, recomenda-se a adoção de medidas urgentes para fortalecer a proteção das informações. Essas ações incluem: reorganizar a estrutura da rede para que cada grupo de equipamentos (como os usados por funcionários e visitantes) funcione de forma mais isolada e controlada; aplicar medidas de controle de acesso; revisar e atualizar os serviços expostos; e implementar ferramentas básicas de segurança como autenticação forte e criptografia. São medidas acessíveis, com alta eficácia, e que representam um avanço importante na maturidade da segurança da empresa.



# Objetivo

Este documento tem como finalidade apresentar um diagnóstico da estrutura de rede da empresa, com foco na identificação de riscos que possam comprometer a segurança das informações e o bom funcionamento dos sistemas. O objetivo é apontar vulnerabilidades existentes, propor melhorias e auxiliar a tomada de decisão estratégica sobre investimentos em segurança.

# Escopo

A análise foi realizada em um ambiente simulado com Docker, composto por múltiplos hosts e redes segmentadas, representando diferentes áreas de uma infraestrutura corporativa: rede interna, rede de servidores e rede de visitantes. O escopo da atuação se limitou a esse ambiente de laboratório, avaliando a exposição de serviços, a estrutura lógica da rede e os controles de acesso entre os segmentos.



# Metodologia

Durante a atividade prática de reconhecimento e análise da infraestrutura simulada, foi aplicada uma abordagem sistemática e confiável, dividida em três etapas principais: coleta ativa de dados, validação técnica e análise documentada.



## Ferramentas

Foram empregadas ferramentas especializadas para garantir abrangência, performance e precisão na identificação de ativos e serviços da rede. Utilizou-se o NETDISCOVER, responsável pela descoberta de hosts ativos sem a necessidade de varreduras agressivas; o RUSTSCAN, que otimizou a identificação rápida de portas abertas e serviços expostos; o NMAP, empregado para o mapeamento detalhado de portas, identificação de serviços e versões em execução; e o PING, utilizado para validar a conectividade entre os dispositivos e medir os tempos de resposta.



## Etapas Executadas

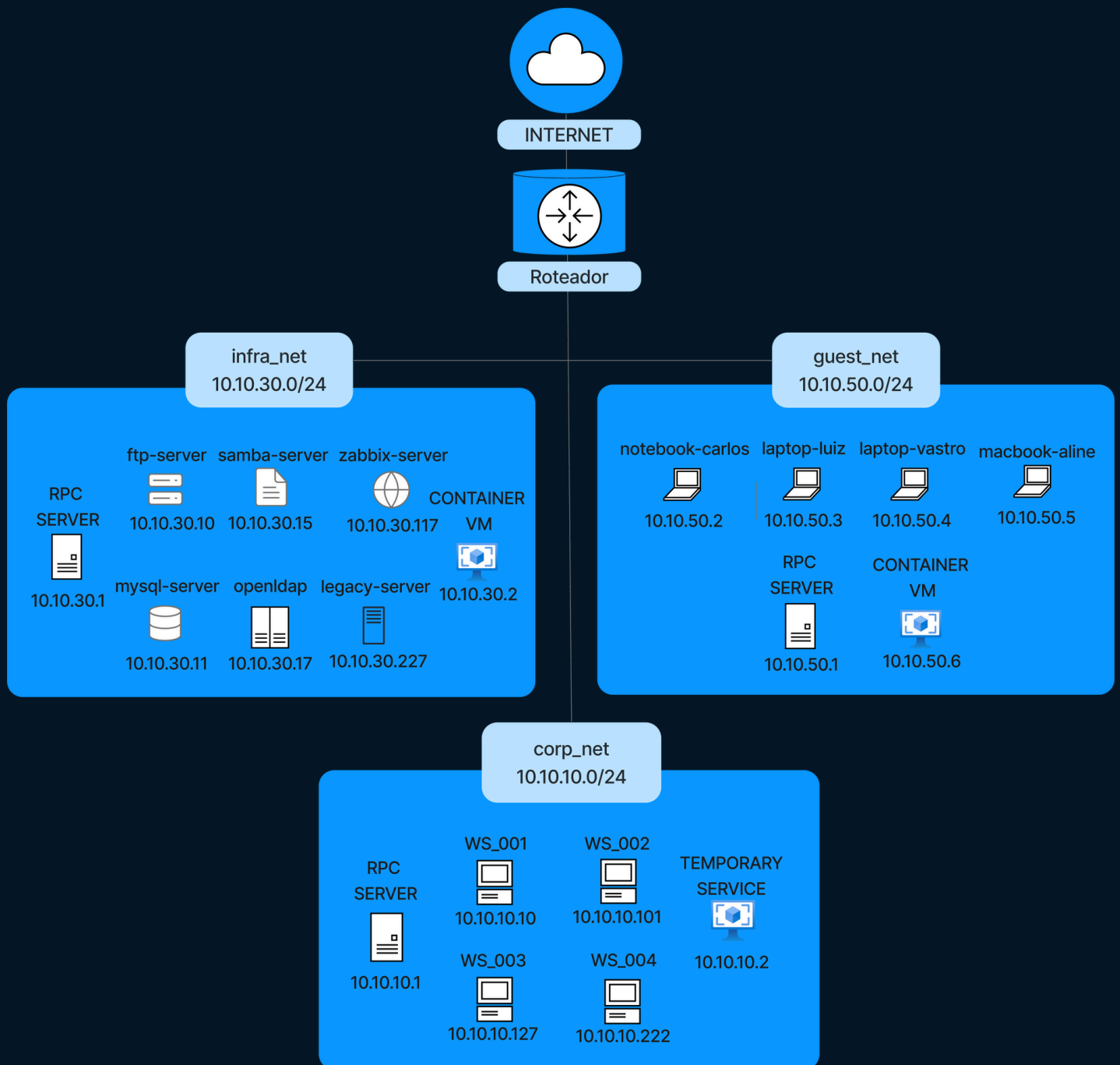
As atividades seguiram três etapas principais. Primeiro, foi realizada a coleta ativa de dados, por meio de varreduras com ferramentas específicas para identificar IPs ativos, portas abertas, serviços em execução e detalhes dos dispositivos conectados. Em seguida, ocorreu a validação técnica, com checagem manual da disponibilidade dos serviços, eliminação de inconsistências e consolidação das evidências. Por fim, a análise e documentação interpretou as informações coletadas com foco em exposições indevidas, configurações vulneráveis, ausência de segmentação e riscos associados.



## Abordagem Analítica

A análise foi conduzida de forma manual, crítica e orientada à segurança, com foco na identificação de serviços desnecessários ou expostos indevidamente, na correlação entre endereços IP, MAC Address e funções dos ativos, além do registro estruturado das informações para embasar recomendações com respaldo técnico e estratégico.

# Diagrama de Rede



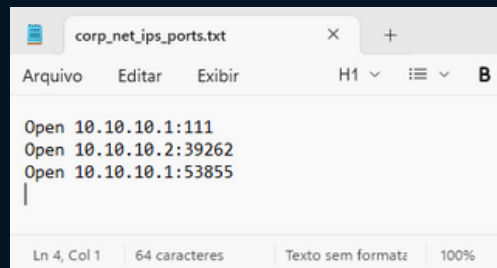
# Diagnóstico

Durante a análise, foram identificadas três sub-redes com fragilidades distintas: GUEST: expõe serviços inseguros (RPC, NFS) em uma zona que deveria ser isolada, violando boas práticas e ampliando o risco de exploração externa; CORP: apresenta serviços sem autenticação (ex: RPC nas portas 111 e 53855), aumentando a superfície de ataque lateral e interna e INFRA: contém serviços críticos (como SSH e DNS) sem autenticação forte ou segmentação, além da presença de serviços legados com alto potencial de exploração.

HOST/IP	SERVIÇO	PORTA(S)	RISCO IDENTIFICADO
10.10.10.1	RPCbind	111, 53855, 59079	RPC aberto na rede corp, vetor para ataques laterais
10.10.30.10	FTP	21	Protocolo inseguro, transmite credenciais em texto claro
10.10.30.1	RPCbind	111, 59079	RPC aberto, permite movimentação lateral e ataques internos
10.10.30.15	SMB (Samba)	139, 445	SMB vulnerável, possibilidade de acesso não autorizado
10.10.30.11	MySQL	3306, 33060	Banco de dados acessível sem restrição, risco de vazamento
10.10.30.17	LDAP	389, 636	LDAP sem criptografia obrigatória, expõe credenciais
10.10.30.117	HTTP (Zabbix)	80, 10051, 10052	Falta de criptografia nas comunicações, risco de interceptação
10.10.50.1	RPCbind	111, 53855	RPC aberto em rede guest, risco de exploração interna
10.10.50.6	RPCbind	43956	A porta alta aberta (43956) está associada ao serviço rpcbind, podendo indicar serviço RPC em execução. Risco similar ao host 10.10.50.1.

## Rede corp\_net - portas expostas

```
(root@12f46b1a7f91)-[/home/analyst]
# cat corp_net_ips_ports.txt~
Open 10.10.10.1:111
Open 10.10.10.1:59079
```

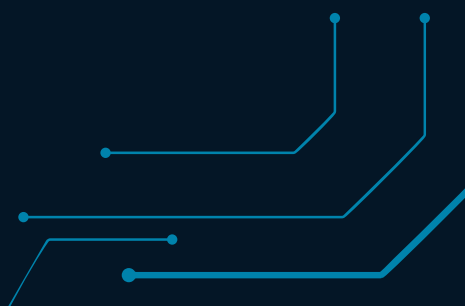


## Rede infra\_net - portas expostas

```
(root@12f46b1a7f91)-[/home/analyst]
# cat infra_net_ips_ports.txt
Open 10.10.30.10:21
Open 10.10.30.117:80
Open 10.10.30.1:111
Open 10.10.30.15:139
Open 10.10.30.17:389
Open 10.10.30.15:445
Open 10.10.30.17:636
Open 10.10.30.11:3306
Open 10.10.30.117:10051
Open 10.10.30.117:10052
Open 10.10.30.11:33060
Open 10.10.30.1:52981
```

## Rede guest\_net - portas

```
(root@12f46b1a7f91)-[/home/analyst]
# cat guest_net_ips_ports.txt
Open 10.10.50.1:111
Open 10.10.50.6:46268
Open 10.10.50.6:50250
Open 10.10.50.1:52981
```





# Recomendações

Com base nos achados da análise, recomenda-se uma reestruturação da rede, visando maior organização dos ativos e redução de serviços expostos ou desnecessários. A falta de separação clara entre áreas críticas e zonas de uso geral facilita a circulação de ameaças e aumenta a superfície de ataque.

É imprescindível a implementação de um firewall entre a rede interna e externa, com políticas restritivas por padrão. Além de uma segmentação lógica da rede por meio de VLANs, separando ambientes como corp\_net, infra\_net e guest\_net. Cada uma dessas VLANs deve possuir seu próprio firewall interno, aplicando uma abordagem de segurança do tipo zero trust, limitando estritamente o tráfego entre segmentos com base em regras claras de IP, porta e protocolo.

Serviços desnecessários identificados durante os escaneamentos devem ser desabilitados. Aqueles que permanecerem ativos devem contar com autenticação, criptografia e aplicações regulares de patches. Durante a análise, também foram identificadas portas abertas em diversos sistemas, muitas sem justificativa operacional clara. Recomenda-se, portanto, a revalidação criteriosa da necessidade dessas exposições, promovendo o fechamento ou aplicação de restrições rigorosas sempre que possível.

No caso de serviços legados ou sem suporte a mecanismos modernos de segurança, recomenda-se o isolamento completo da máquina em uma VLAN restrita, com controle rígido de acesso e monitoramento contínuo, evitando qualquer tipo de propagação de riscos.

Por fim, reforça-se a importância de integrar ferramentas de monitoramento contínuo (como SIEMs e IDS/IPS), consolidar um inventário técnico detalhado de ativos, e aplicar o princípio do menor privilégio na gestão de acessos. Os colaboradores também devem ser continuamente orientados quanto às boas práticas de cibersegurança, através de programas regulares de treinamento e conscientização, para que possam compreender seu papel na proteção dos ativos e sistemas da organização. A segurança eficaz nasce da combinação entre tecnologia, processos bem definidos e pessoas treinadas e engajadas.



# Plano 80/20

AÇÃO ESTRATÉGICA	IMPACTO	FACILIDADE	PRIORIDADE
Implementar firewall entre VLANs e na borda da rede	Alto	Média	Alta
Segmentação lógica via VLANs + ACLs	Alto	Média	Alta
Bloquear/desativar RPC (porta 111) e portas dinâmicas não essenciais	Alto	Média	Alta
Fechar portas desnecessárias e restringir acesso às essenciais (21, 139, 445)	Alto	Alta	Alta
Migrar FTP para FTPS/SFTP, HTTP para HTTPS, LDAP para LDAPS (Criptografia)	Alto	Média	Alta
Implementar autenticação multifator (MFA) para acessos críticos	Alto	Média	Alta
Atualizar sistemas legados e aplicar patches	Médio	Média	Média
Implementar monitoramento com SIEM e alertas	Médio	Média	Média
Realizar treinamentos básicos de segurança para usuários	Médio	Alta	Média

# Conclusão

A análise realizada evidencia que, embora a infraestrutura simulada apresente iniciativas relevantes de segmentação e organização por áreas funcionais, ainda há vulnerabilidades críticas que comprometem a confidencialidade, integridade e disponibilidade das informações. Foram identificados serviços expostos sem controles adequados, ausência de criptografia, autenticação frágil e uso de sistemas legados; todos elementos que aumentam a superfície de ataque e facilitam ações maliciosas.

Destaca-se especialmente o número elevado de portas abertas em diversos hosts, muitas delas sem justificativa operacional clara. Serviços como FTP, SMB, LDAP, MySQL e RPC estão sendo executados sem os devidos mecanismos de proteção. A presença dessas portas expostas pode permitir invasões, vazamento de dados, movimentação lateral de atacantes e exploração de falhas conhecidas.

Recomenda-se a atualização para protocolos mais seguros, como FTPS/SFTP, HTTPS e LDAPS, bem como a aplicação de políticas de restrição de acesso por IP, porta e protocolo. O bloqueio de portas desnecessárias e a aplicação rigorosa de regras de firewall são medidas de alto impacto com custo acessível.

A adoção das recomendações propostas: reestruturação da rede por VLANs, implementação de firewalls internos, desativação de serviços não essenciais, fortalecimento da autenticação e segmentação lógica — representa um salto importante na postura de segurança da organização. Tais ajustes reduzem drasticamente a superfície de exposição e aumentam a capacidade de resposta frente a ameaças cada vez mais sofisticadas.

Além do aspecto técnico, é fundamental promover a cultura da segurança, com capacitação contínua dos colaboradores. A maturidade em cibersegurança só é alcançada com a sinergia entre infraestrutura robusta, processos bem definidos e envolvimento humano consciente.

Este relatório oferece uma base sólida para decisões estratégicas de investimento, revisão de políticas e definição de prioridades, contribuindo para o desenvolvimento sustentável da maturidade cibernética da organização.

# Anexos

## Iniciando o ambiente e descoberta do arquivo

```
I workstation2 Interrupted 1.1s
Error response from daemon: Head "https://registry-1.docker.io/v2/library/alpine/manifests/latest": unauthorized: incorrect username or password
PS C:\Users\aline\formacao-cybersec\noduloi-fundamentos\projeto_final_opcao_1> docker logout
Removing login credentials for https://index.docker.io/v1/
PS C:\Users\aline\formacao-cybersec\noduloi-fundamentos\projeto_final_opcao_1> docker-compose up -d
time="2025-07-16T21:24:44-03:00" level=warning msg="C:\\Users\\aline\\formacao-cybersec\\noduloi-fundamentos\\projeto_final_opcao_1\\docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 12/12
  ✓ printer Pulled
  ✓ 9824c27679d3 Pull complete
  ✓ workstation1 Pulled
  ✓ workstation2 Pulled
  ✓ fileservier Pulled
  ✓ 3da95a905ed5 Already exists
  ✓ 7188edcd16b Pull complete
  ✓ 4f4fb700ef54 Pull complete
  ✓ 3b9386c3888b Pull complete
  ✓ c5894facdbb Pull complete
  ✓ 14bacd2841b0 Pull complete
  ✓ guest_device Pulled
[+] Running 9/9
  ✓ Network projeto_final_opcao_1_corp_net Created
  ✓ Network projeto_final_opcao_1_guest_net Created
  ✓ Network projeto_final_opcao_1_infra_net Created
  ✓ Container fileservier Started
  ✓ Container guest_device Started
  ✓ Container workstation2 Started
  ✓ Container printer Started
  ✓ Container webserver Started
  ✓ Container workstation1 Started
PS C:\Users\aline\formacao-cybersec\noduloi-fundamentos\projeto_final_opcao_1>
```

```
PS C:\Users\aline> docker exec -it analyst bash
(root@12f46b1a7f91): /home/analyst#
# ls -la
total 144
drwxr-xr-x 1 analyst analyst 4096 Jul 26 21:55 .
drwxr-xr-x 1 root root 4096 Jul 18 21:49 ..
-rw-r--r-- 1 root root 2892 Jul 18 21:49 ANOTACAO-ULTIMO-SCAN.TXT
-rw-r--r-- 1 analyst analyst 220 May 19 10:11 bash_logout
-rw-r--r-- 1 analyst analyst 5551 Jun 1 04:02 bashrc
-rw-r--r-- 1 analyst analyst 3526 May 19 10:11 bashrc.original
drwxr-xr-x 3 analyst analyst 4096 Jun 1 04:02 .config
drwxr-xr-x 3 analyst analyst 4096 Jun 1 04:02 .java
drwxr-xr-x 3 analyst analyst 4096 Jun 1 04:02 .local
-rw-r--r-- 1 analyst analyst 807 May 19 10:11 .profile
-rw-r--r-- 1 analyst analyst 336 May 21 10:30 .pprofile
-rw-r--r-- 1 analyst analyst 10856 May 21 10:30 .zshrc
-rw-r--r-- 1 root root 0 Jul 26 21:49 corp_net_ips_ports.txt
-rw-r--r-- 1 root root 42 Jul 19 21:38 corp_net_ips_ports.txt
-rw-r--r-- 1 root root 86 Jul 26 22:19 guest_net_ips_ports.txt
-rw-r--r-- 1 root root 456 Jul 21 22:09 infra_net_10.10.30.117_80_webserver.txt
-rw-r--r-- 1 root root 3412 Jul 21 22:09 infra_net_10.10.30.117_80_zabbix.txt
-rw-r--r-- 1 root root 80 Jul 21 20:58 infra_net_ips.txt
-rw-r--r-- 1 root root 302 Jul 21 20:58 infra_net_ips_hosts.txt
-rw-r--r-- 1 root root 260 Jul 26 21:53 infra_net_ips_ports.txt
-rw-r--r-- 1 root root 314 Jul 21 22:00 infra_net_servico_ftp-anon.txt
-rw-r--r-- 1 root root 1501 Jul 21 22:07 infra_net_servico_ldap-rootds.txt
-rw-r--r-- 1 root root 943 Jul 21 22:17 infra_net_servico_mysql-info.txt
-rw-r--r-- 1 root root 328 Jul 21 22:07 infra_net_servico_nginx.txt
-rw-r--r-- 1 root root 456 Jul 21 22:08 infra_net_servico_webserver.txt
-rw-r--r-- 1 root root 3412 Jul 21 22:08 infra_net_servico_zabbix.txt
-rw-r--r-- 1 root root 2607 Jul 21 21:29 infra_net_servicos.txt
-rw-r--r-- 1 root root 7530 Jul 26 21:50 output.txt
drwxr-xr-x 5 root root 4096 Jul 19 22:38 recon
-rw-r--r-- 1 root root 255 Jul 21 20:56 recon-redes.txt
-rw-r--r-- 1 root root 1473 Jul 21 22:27 recon_ip_naps.txt
-rw-r--r-- 1 root root 516 Jul 19 22:28 script.sh

# (root@12f46b1a7f91): /home/analyst#
# cat ANOTACAO-ULTIMO-SCAN.TXT
# NÃO APAGAR

# SE VOCÊ ACHOU ISSO E ESTÁ FAZENDO O DESAFIO DO PROJETO FINAL OPÇÃO 1 SE DEU BEM :;) ...

# comandos que eu executei a última vez que estava aqui... deixar anotado pq pode salvar tempo da próxima vez.

## Primeiro pegar info das redes
ip a
ip a | grep inet
ip a | grep inet > recon-redes.txt

## Testar se tem conectividade com as redes
ping -c 3 10.10.10.1 # corp_net
ping -c 3 10.10.30.1 # guest_net
ping -c 3 10.10.50.1 # infra_net

## 1. descobrir os hosts com Nmap ping scan
nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up/{print $2}' | tee corp_net_ips.txt
nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up/{print $2, $3}' | tee corp_net_ips_hosts.txt

nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up/{print $2}' | tee infra_net_ips.txt
nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up/{print $2, $3}' | tee infra_net_ips_hosts.txt

nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up/{print $2}' | tee guest_net_ips.txt
nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up/{print $2, $3}' | tee guest_net_ips_hosts.txt

## 2. Scan rápido com Rustscan para pegar as portas abertas
rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt
rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt
rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

## 3. Analisar os serviços específicos
## FTP
nmap -p 21 --script ftp-anon 10.10.30.10
nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
```

## Informações da rede

```
# SO estimado:
# Portas abertas:
# Serviços:
# Notas: login anônimo? dados sensíveis? falhas visíveis?

(root@12f46b1a7f91): /home/analyst#
# cat
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0@if50: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 56:6a:07:0a:92:41 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth0
        valid_lft forever preferred_lft forever
3: eth1@if58: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether fe:ec:7b:10:37:97 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth1
        valid_lft forever preferred_lft forever
4: eth2@if60: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 5a:8a:0e:6a:5f:fe brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth2
        valid_lft forever preferred_lft forever

(root@12f46b1a7f91): /home/analyst#
# ip a | grep inet
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host proto kernel_lo
inet 10.10.30.2/24 brd 10.10.30.255 scope global eth0
inet 10.10.10.2/24 brd 10.10.10.255 scope global eth1
inet 10.10.50.6/24 brd 10.10.50.255 scope global eth2

(root@12f46b1a7f91): /home/analyst#
# cat recon-redes.txt
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host proto kernel_lo
inet 10.10.30.2/24 brd 10.10.30.255 scope global eth0
inet 10.10.10.2/24 brd 10.10.10.255 scope global eth1
inet 10.10.50.6/24 brd 10.10.50.255 scope global eth2
```

## Teste de conectividade

```
(root@12f46b1a7f91)-[/home/analyst]
# ping -c 3 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.099 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2058ms
rtt min/avg/max/ndev = 0.070/0.517/1.382/0.611 ms

(root@12f46b1a7f91)-[/home/analyst]
# ping -c 3 10.10.30.1
PING 10.10.30.1 (10.10.30.1) 56(84) bytes of data.
64 bytes from 10.10.30.1: icmp_seq=1 ttl=64 time=0.576 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.231 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.094 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2089ms
rtt min/avg/max/ndev = 0.094/0.300/0.576/0.202 ms

(root@12f46b1a7f91)-[/home/analyst]
# ping -c 3 10.10.50.1
PING 10.10.50.1 (10.10.50.1) 56(84) bytes of data.
64 bytes from 10.10.50.1: icmp_seq=1 ttl=64 time=11.9 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.167 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.067 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2867ms
rtt min/avg/max/ndev = 0.067/4.056/11.935/5.571 ms
```

## Descoberta dos hosts

```
(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
Host: 10.10.10.1 () Status: Up
Host: 10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.2 (12f46b1a7f91) Status: Up

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/ {print $2}' | tee corp_net_ips.txt
10.10.10.1
10.10.10.10
10.10.10.101
10.10.10.127
10.10.10.222
10.10.10.2

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/ {print $2, $3}' | tee corp_net_ips_hosts.txt
10.10.10.1 ()
10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net)
10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net)
10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net)
10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net)
10.10.10.2 (12f46b1a7f91)
```

```
(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
Host: 10.10.30.1 () Status: Up
Host: 10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.17 (openldap.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.2 (12f46b1a7f91) Status: Up

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/ {print $2}' | tee infra_net_ips.txt
10.10.30.1
10.10.30.10
10.10.30.11
10.10.30.15
10.10.30.17
10.10.30.117
10.10.30.227
10.10.30.2

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/ {print $2, $3}' | tee infra_net_ips_hosts.txt
10.10.30.1 ()
10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)
10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)
10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)
10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)
10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)
10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)
10.10.30.2 (12f46b1a7f91)
```

```
(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
Host: 10.10.50.1 () Status: Up
Host: 10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.4 (laptop-luiz.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.5 (notebook-carlos.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.6 (12f46b1a7f91) Status: Up

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/ {print $2}' | tee guest_net_ips.txt
10.10.50.1
10.10.50.2
10.10.50.3
10.10.50.4
10.10.50.5
10.10.50.6

(root@12f46b1a7f91)-[/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/ {print $2, $3}' | tee guest_net_ips_hosts.txt
10.10.50.1 ()
10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.4 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.5 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.6 (12f46b1a7f91)
```

## Scan rápido de portas

```
(root@12f46b1a7f91)-[/home/analyst]
# rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

(root@12f46b1a7f91)-[/home/analyst]
# rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

(root@12f46b1a7f91)-[/home/analyst]
# rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

(root@12f46b1a7f91)-[/home/analyst]
# docker ps
bash: docker: command not found

(root@12f46b1a7f91)-[/home/analyst]
# docker cp analyst:/home/analyst/recon C:\Users\aline\Desktop\
> exit
bash: docker: command not found

(root@12f46b1a7f91)-[/home/analyst]
# exit
exit
PS C:\Users\aline> docker cp analyst:/home/analyst/corp_net_ips_ports.txt C:\Users\aline\Desktop\
Successfully copied 2.05kB to C:\Users\aline\Desktop\
PS C:\Users\aline> docker cp analyst:/home/analyst/corp_net_ips_ports.txt C:\Users\aline\Desktop\
Successfully copied 2.05kB to C:\Users\aline\Desktop\
PS C:\Users\aline> docker cp analyst:/home/analyst/infra_net_ips_ports.txt C:\Users\aline\Desktop\
Successfully copied 2.05kB to C:\Users\aline\Desktop\
PS C:\Users\aline> docker cp analyst:/home/analyst/guest_net_ips_ports.txt C:\Users\aline\Desktop\
Successfully copied 2.05kB to C:\Users\aline\Desktop\
```



## Análise de serviços específicos

```
(root@12f46b1a7f91) ~/home/analyst
nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 22:07 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00076s latency).
```

```

PORT      STATE SERVICE
389/tcp   open  ldap
          ldap-rootdse:
LDAP Request
  <Root>

    namingContexts: dc=example,dc=org
    supportedControl: 2.16.840.1.113730.3.4.18
    supportedControl: 2.16.840.1.113730.3.4.2
    supportedControl: 1.3.6.1.4.1.4203.1.10.1
    supportedControl: 1.3.6.1.1.122
    supportedControl: 2.16.840.113556.1.4.319
    supportedControl: 1.2.826.0.1.3344810.2.3
    supportedControl: 1.3.6.1.1.13.2
    supportedControl: 1.3.6.1.1.13.1
    supportedControl: 1.3.6.1.1.12
    supportedExtension: 1.3.6.1.4.1.1466.20037
    supportedExtension: 1.3.6.1.4.1.4203.1.11.1
    supportedExtension: 1.3.6.1.4.1.4203.1.11.3
    supportedExtension: 1.3.6.1.1.8
    supportedLDAPVersion: 3
    supportedSASLMechanisms: SCRAM-SHA-1
    supportedSASLMechanisms: SCRAM-SHA-256
    supportedSASLMechanisms: GS2-TAKERB
    supportedSASLMechanisms: GS2-KRBB
    supportedSASLMechanisms: GSSAPI
    supportedSASLMechanisms: GSS-SPNEGO
    supportedSASLMechanisms: DIGEST-MD5
    supportedSASLMechanisms: OTP
    supportedSASLMechanisms: CRAM-MD5
    supportedSASLMechanisms: NTLM

```

```
supportedControl: 2.10.840.1.113730.3.4.2
supportedControl: 1.3.6.1.4.1.4203.1.10.1
supportedControl: 1.3.6.1.1.22
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.826.0.1.3344810.2.3
supportedControl: 1.3.6.1.1.13.2
supportedControl: 1.3.6.1.1.13.1
supportedControl: 1.3.6.1.1.12
supportedExtension: 1.3.6.1.4.1.1466.20037
supportedExtension: 1.3.6.1.4.1.4203.1.11.1
supportedExtension: 1.3.6.1.4.1.4203.1.11.3
supportedExtension: 1.3.6.1.1.8
supportedLDAPVersion: 3
supportedSASLMechanisms: SCRAM-SHA-1
supportedSASLMechanisms: SCRAM-SHA-256
supportedSASLMechanisms: GS2-IAKERB
supportedSASLMechanisms: GS2-KRB5
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: DIGEST-MD5
supportedSASLMechanisms: OTP
supportedSASLMechanisms: CRAM-MD5
supportedSASLMechanisms: NTLM
subschemaSubentry: cn=Subschema
MAC Address: AE:C2:D8:11:65:C2 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

```
(root@12f46b1a7f91)-[~/home/analyst]
# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 22:07 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.00015s latency).
```

```
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: CA:80:84:8A:04:50 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

```
(root@12f46b1a7f91)-[/home/analyst]
# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 >
```

```
(root@12f46b1a7f91) - [/home/analyst]
# ### FTP
```

```
nmap -p 21 --script ftp-anon 10.10.30.10
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 22:00 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.0011s latency).
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: FA:C7:C3:5C:17:D7 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

```
(root@12f46b1a7f91)-[/home/analyst]
# nnap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
```

```
(root@127.0.0.1:7793) [/home/analyst]
nmap -p 3306 --script mysql-info 10.10.10.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 22:56 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.10.11)
Host is up (0.0000ms latency).
```

[illegible]

```
(root@12f40b1a7f91)~# nmap -p 3306 --script mysql-info 10.10.10.11 -sS --service mysql-info.txt
```

```
[root@12f46b1a7f91: /home/analyst]
# curl -I http://10.10.30.117
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Jul 2025 22:08:18 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Keep-Alive: timeout=20
X-Powered-By: PHP/7.3.14
Set-Cookie: PHPSESSID=129db61f307f188eb44afd594cd94dee; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
```

[illegible]

```
(root@12f46b1a7f91)~# curl http://10.10.10.117:10000/infoca.net/service/zabbix.txt
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed

```
(root@12f46b1a7f91)-[/home/analyst]
```

```
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
```

```
(root@12f46b1a7f91)-[/home/analyst]
```

```

ftp-server.project_final_opaco_1_guinst (10.30.18.33) at 36:30:51:09:1c:0d [ether] on eth1
ftp-server.project_final_opaco_1_infra_net (10.30.18.10) at Fa-7/3-31:17:07 [ether] on eth2
(10.30.18.3) at 6a:3d:32:ed:f5:d3 [ether] on eth1
W5001.project_final_opaco_1_corp_net (10.30.15.15) at 3c:80:84:84:84:58 [ether] on eth0
W5001.project_final_opaco_1_corp_net (10.30.18.10) at 12:7f:a2:8a:3c:7 [ether] on eth0
W5001.project_final_opaco_1_corp_net (10.30.18.10) at 4b:54:3c:5f:af:f0 [ether] on eth0
W5001.project_final_opaco_1_infra_net (10.30.18.10) at 3c:80:84:84:84:58 [ether] on eth1
zabbix-server.project_final_opaco_1_infra_net (10.30.18.17) at 6e:03:d3:10:5c:6f [ether] on eth0
(10.30.18.3) at aa:cf:32:7c:7b:72 [ether] on eth1
W5001.project_final_opaco_1_infra_net (10.30.18.22) at 1a:ee:55:b2:9e:b6 [ether] on eth1
openldap.project_final_opaco_1_infra_net (10.30.18.17) at ca:c2:02d1:86:5c:62 [ether] on eth2
LDAP-server.project_final_opaco_1_infra_net (10.30.18.22) at fe:b2:2b:2b:ac:37 [ether] on eth0
W5001.project_final_opaco_1_infra_net (10.30.18.22) at 3c:80:84:84:84:58 [ether] on eth1
mysql-server.project_final_opaco_1_infra_net (10.30.18.11) at 26:c4:00:35:cc:dc [ether] on eth2
(10.30.18.5) at 1e:24:38:3a:2:3f [ether] on eth1
W5001.project_final_opaco_1_corp_net (10.30.18.22) at 7e:2c:8c:3f:99:08 [ether] on eth0
W5001.project_final_opaco_1_corp_net (10.30.18.22) at 7e:2c:8c:3f:99:08 [ether] on eth0
W5001.project_final_opaco_1_corp_net (10.30.18.22) at 7e:2c:8c:3f:99:08 [ether] on eth0

```

```
(root@12f46b1a7f91)-[/home/analyst]
# arp -a > recon_ip_maps.txt
```

```
(root@12f46b1a7f91)-[/home/analyst]
# cat /etc/resolv.conf
# Generated by Docker Engine.
# This file can be edited; Docker Engine will not make further changes once it
# has been modified.
```

```
nameserver 127.0.0.11
options ndots:0

# Based on host file: '/etc/resolv.conf' (internal resolver)
# ExtServers: [host(192.168.65.7)]
# Overrides: []
# Option ndots from: internal
```

# Documentação de Rede

Autor: Aline Blotta Aguilar Jardim  
Data: 23/07/2025

NOME ESTIMADO	SUBNET DESCOBERTA	FINALIDADE SUPOSTA
corp_net	10.10.10.0/24	Rede principal dos dispositivos
infra_net	10.10.30.0/24	Infraestrutura / servidores
guest_net	10.10.50.0/24	Rede de Visitantes

## CORP\_NET

IP	FUNÇÃO	EVIDÊNCIA
10.10.10.1	Servidor RPC/Gateway	Porta 111 (rpcbind padrão) aberta, Portas 53855 e 59079, que são portas dinâmicas associadas a serviços RPC alocados pelo rpcbind.
10.10.10.10	Estação de Trabalho	A nomenclatura sugere que se trata de uma workstation e segue um padrão.
10.10.10.101	Estação de Trabalho	A nomenclatura sugere que se trata de uma workstation e segue um padrão.
10.10.10.127	Estação de Trabalho	A nomenclatura sugere que se trata de uma workstation e segue um padrão.
10.10.10.222	Estação de Trabalho	A nomenclatura sugere que se trata de uma workstation e segue um padrão.
10.10.10.2	Serviço personalizado (possivelmente temporário)	Serviço interno ou aplicação personalizada que utiliza porta dinâmica, possivelmente para comunicação RPC ou troca de dados entre sistemas. Atua como endpoint para funções específicas da infraestrutura, podendo ser um componente temporário (ex: container, serviço de microserviço) ou serviço em desenvolvimento.



## INFRA\_NET

IP	FUNÇÃO	EVIDÊNCIA
10.10.30.1	Dispositivo gateway / servidor RPC	Porta 111 (rpcbind) e 59079 abertas, indica serviços de chamada remota (RPC), comuns em servidores intermediários ou gateways.
10.10.30.10	Servidor FTP / Proxy	Porta 21 aberta (FTP), geralmente vinculada a servidor FTP ou serviço de transferência de arquivos.
10.10.30.11	Servidor de Banco de Dados	Portas 3306 e 33060 abertas (MySQL padrão). Indica banco de dados MySQL ou MariaDB.
10.10.30.15	Servidor de Arquivos / AD	Portas 139 e 445 abertas (SMB/CIFS). Possível servidor Windows de arquivos ou Active Directory.
10.10.30.17	Servidor LDAP / Autenticação	Portas 389 (LDAP) e 636 (LDAPS) abertas. Indica servidor LDAP com autenticação via SSL/TLS.
10.10.30.117	Servidor Web / Monitoramento	Portas 80 (HTTP), 10051 e 10052 abertas (Zabbix padrão). Indica servidor web e ferramenta de monitoramento Zabbix.
10.10.30.227	Servidor legado / Reservado	O nome legacy-server indica se tratar de um servidor legado, sem exposição de portas.
10.10.30.2	Container ou VM de testes	Sem portas abertas. Nome sugere container ou VM usada para testes/varreduras. Provável uso temporário, sem serviços expostos externamente.

## GUEST\_NET

IP	FUNÇÃO	EVIDÊNCIA
10.10.50.1	Servidor RPC / Gateway	Portas 111 (rpcbind padrão) e 53855 (porta dinâmica RPC) abertas, indicam serviços de chamada remota ativos.
10.10.50.2	Estação de Trabalho (cliente)	Sem portas abertas e em uma rede para convidados, os nomes das redes (notebook-carlos, laptop-luiz, laptop-vastro, macbook-aline) indica que se tratam de estações de trabalho pessoais ou portáteis de usuários finais, o que reforça que são clientes na guest_net.
10.10.50.3	Estação de Trabalho (cliente)	Sem portas abertas e em uma rede para convidados, os nomes das redes (notebook-carlos, laptop-luiz, laptop-vastro, macbook-aline) indica que se tratam de estações de trabalho pessoais ou portáteis de usuários finais, o que reforça que são clientes na guest_net.
10.10.50.4	Estação de Trabalho (cliente)	Sem portas abertas e em uma rede para convidados, os nomes das redes (notebook-carlos, laptop-luiz, laptop-vastro, macbook-aline) indica que se tratam de estações de trabalho pessoais ou portáteis de usuários finais, o que reforça que são clientes na guest_net.
10.10.50.5	Estação de Trabalho (cliente)	Sem portas abertas e em uma rede para convidados, os nomes das redes (notebook-carlos, laptop-luiz, laptop-vastro, macbook-aline) indica que se tratam de estações de trabalho pessoais ou portáteis de usuários finais, o que reforça que são clientes na guest_net.
10.10.50.6	Estação de Trabalho / Container	Nome "12f46b1a7f91" sugere container Docker ou máquina virtual. Porta 43956, podendo estar relacionada ao RPC.