

# Modelo de Relatório Técnico – Lab Segmentação de Rede

**Autor:** Luiz Eduardo de Andrade

**Data:** 28/07/25

**Versão:** 1.0

## Sumário Executivo

Temos três redes CorpNet, InfraNet e GuestNet, este relatório avalia a segurança da rede simulada, identificando vulnerabilidades como portas abertas em serviços como FTP, MySQL, SMB, LDAP e Zabbix, que podem ser exploradas por ameaças externas ou internas. Destacamos a necessidade de ações prioritárias, como remover a porta 21 do FTP e instalar um firewall para controlar o acesso, fortalecendo a proteção dos ativos. Essas medidas visam reduzir riscos operacionais e melhorar a segurança geral da rede.

## Objetivo

Analisar a rede simulada para identificar exposição, segmentação e riscos operacionais.

O documento existe para mostrar as vulnerabilidades existentes através de portas que estão abertas e os riscos que elas representam e dar direcionamento para a mitigação destas vulnerabilidades.

## Escopo

A Análise foi realizada no ambiente docker simulado com múltiplos hosts e 3 redes segmentadas, divididas em CorpNet, InfraNet e GuestNet

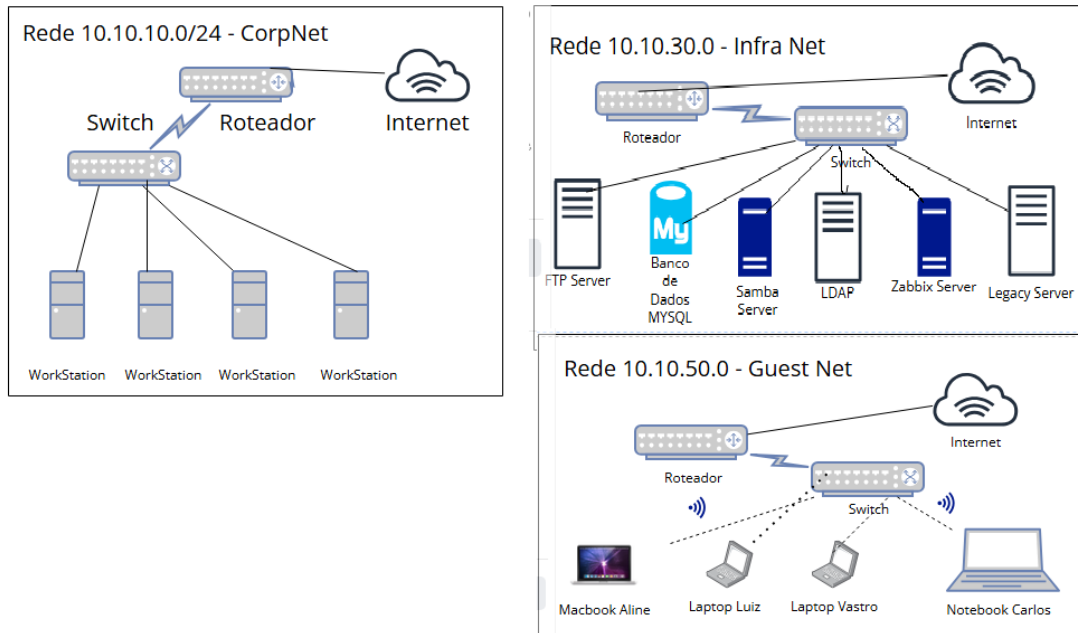
Os limites de atuação serão dentro destas 3 redes segmentadas fazendo coleta ativa de dados na rede para verificação de portas abertas e os serviços que rodam nestas portas.

## Metodologia

- Ferramentas: nmap, rustscan, netdiscover, ping, protocolo ARP, script anônimo de FTP, etc.
- Coleta ativa de dados de rede

- Análise manual e documentada

## Diagrama de Rede



## Documentação de Redes Descobertas

**Autor:** Luiz Eduardo de Andrade

**Data:** 28/07/2025

**Versão:** 1.0

# Redes Identificadas

Nome Estimado	Subnet Descoberta	Finalidade Suposta
CorpNet	10.10.10.0/24	Rede Corporativa
InfraNet	10.10.30.0/24	Rede de Infraestrutura
GuestNet	10.10.50.0/24	Rede Convidado

---

## Dispositivos por Rede

### Rede Corporativa

IP	Função	Evidência
10.10.10.1	Roteador	Portas fechadas
10.10.10.2	Switch	Porta 48660 aberta
10.10.10.10	Estação de Trabalho	Portas fechadas
10.10.10.101	Estação de Trabalho	Portas fechadas
10.10.10.127	Estação de Trabalho	Portas fechadas
10.10.10.127	Estação de Trabalho	Portas fechadas

### Rede de Infraestrutura

<b>IP</b>	<b>Função</b>	<b>Evidência</b>
10.10.30.1	Roteador	Portas fechadas
10.10.30.2	Switch	Portas 41658 e 41910 abertas
10.10.30.10	Server FTP	Porta 21 aberta FTP – Transferência de Arquivos
10.10.30.11	Server MySQL	Portas 3306 e 33060 abertas MYSQL Banco de Dados
10.10.30.15	Server Samba	Porta 139 e 445 abertas SMB compartilhamento de diretórios Windows
10.10.30.17	OpenLDAP	Porta 636 aberta LDAP
10.10.30.117	Server Zabbix	Porta 80, 10051 e 10052 abertas serviço web ZABBIX
10.10.30.227	Server Legacy	Portas fechadas

## Rede de Convidados

<b>IP</b>	<b>Função</b>	<b>Evidência</b>
10.10.50.1	Roteador	Portas fechadas
10.10.50.2	Switch	Portas 33948 e 39470 abertas
10.10.50.3	Laptop Vastro	Portas fechadas
10.10.50.4	MacBook Aline	Portas fechadas
10.10.50.5	Laptop Luiz	Portas fechadas
10.10.50.6	Notebook Carlos	Portas fechadas

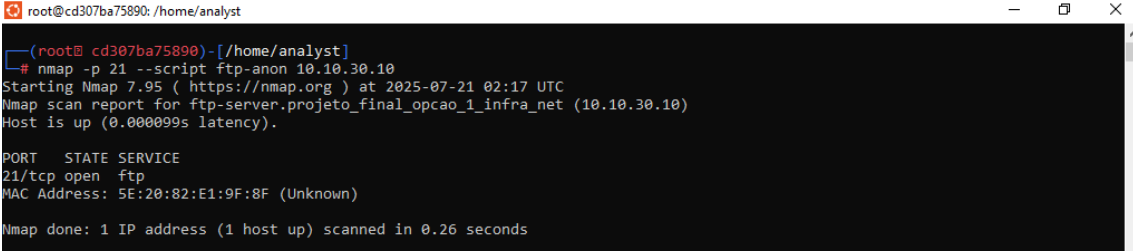
---

## Observações de Risco

- A rede Infraestrutura é necessário colocar um firewall, para proteger as portas abertas.
- A rede Guest tem que ser segmentada, ou seja, separada das redes corp e infra para evitar movimentação lateral.
- Poucos serviços na rede Guest.
- Muitas portas fechadas na rede Corporativa.

## Diagnóstico (Achados)

- 10.10.30.10 – FTP – 21
- Conseguir entrar no serviço ftp informando a porta aberta, no MACADDRESS



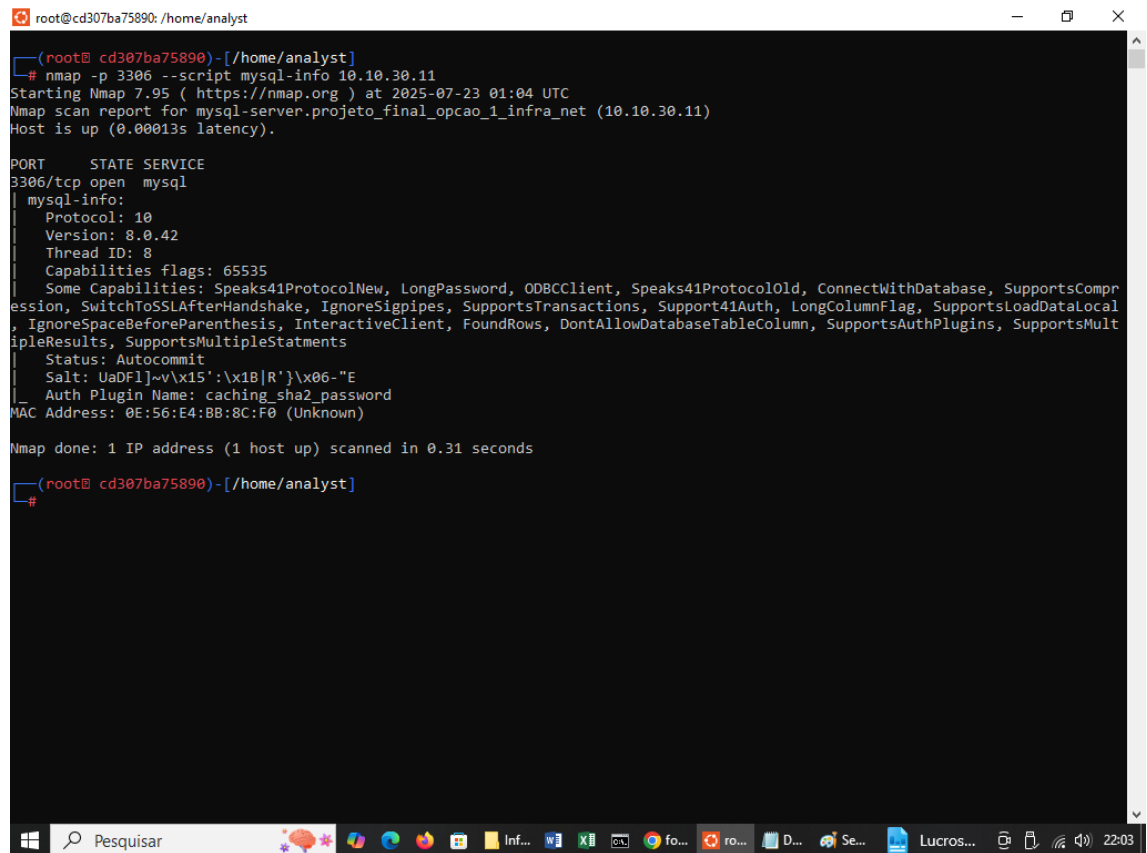
```
root@cd307ba75890: /home/analyst
(root@cd307ba75890)-[/home/analyst]
# nmap -p 21 --script ftp-anon 10.10.30.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 02:17 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000099s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 5E:20:82:E1:9F:8F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

- 10.10.30.11 – MYSQL- 3306 e 33060

- Informações do serviço mysql que está rodando como a versão 8.0.42, com o método de autenticação sha2 podemos procurar na internet as vulnerabilidades desta versão e quebrar o sha2 para termos acesso ao mysql.



```

root@cd307ba75890: /home/analyst
(root@ cd307ba75890) - [/home/analyst]
# nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:04 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.00013s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql

mysql-info:
  Protocol: 10
  Version: 8.0.42
  Thread ID: 8
  Capabilities flags: 65535
  Some Capabilities: Speaks41ProtocolNew, LongPassword, ODBCClient, Speaks41ProtocolOld, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, IgnoreSigpipes, SupportsTransactions, Support41Auth, LongColumnFlag, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, InteractiveClient, FoundRows, DontAllowDatabaseTableColumn, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatements
  Status: Autocommit
  Salt: UaDF1j~v\x15':\x1B|R'}\x06-"E
  Auth Plugin Name: caching_sha2_password
  MAC Address: 0E:56:E4:BB:8C:F0 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
(root@ cd307ba75890) - [/home/analyst]
#

```

- 10.10.30.15 – Protocolo SMB – Portas 139 e 445
- O protocolo SMB pode ter algumas vulnerabilidades como execução remota de código, enumeração dos ativos

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:13 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.00011s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 52:87:04:52:36:FC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

(root@ cd307ba75890)-[/home/analyst]
#
```

- 10.10.30.17 – LDAP – 389 e 636
- A porta do LDAP 389 está aberta e neste protocolo não possui criptografia onde a comunicação acontece em texto claro

```
root@cd307ba75890: /home/analyst

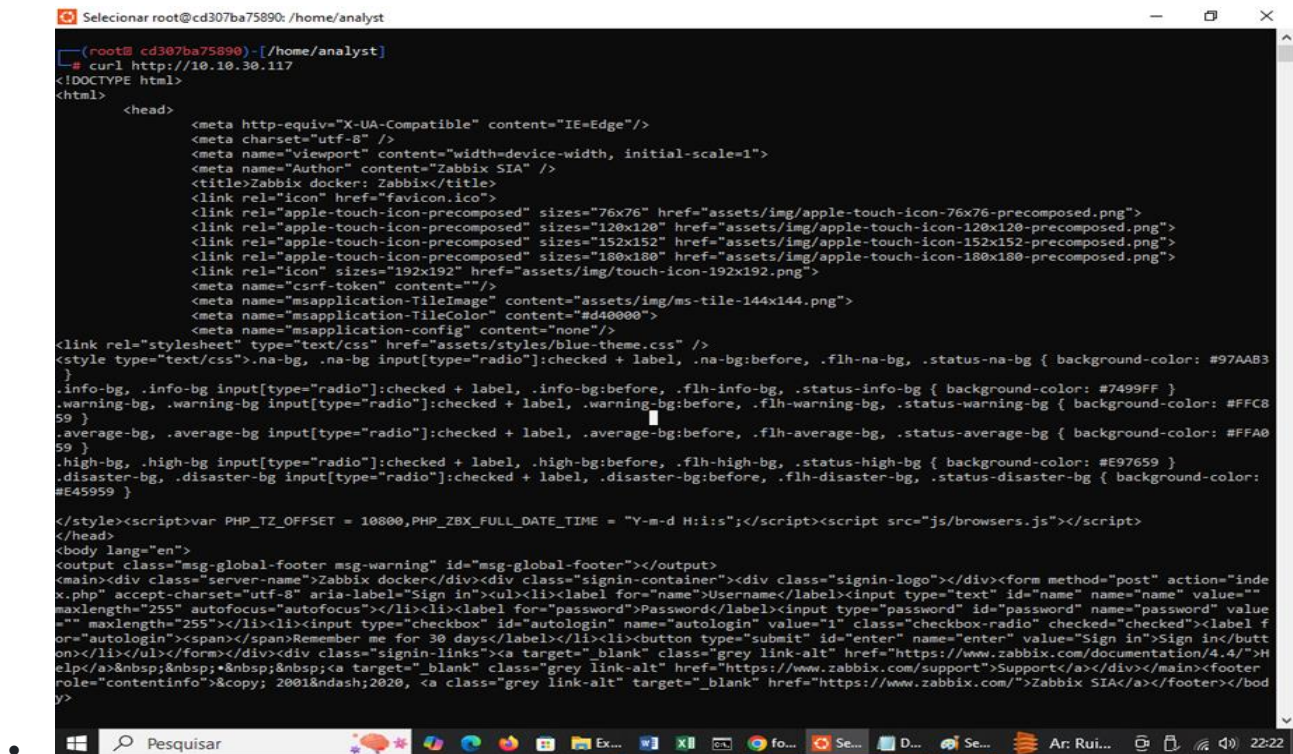
(root@ cd307ba75890)-[/home/analyst]
# nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:10 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00015s latency).

PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-rootdse:
| LDAP Results
| <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: 1.3.6.1.1.22
|   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: GS2-IAKRB
|   supportedSASLMechanisms: GS2-KRB5
|   supportedSASLMechanisms: SCRAM-SHA-1
|   supportedSASLMechanisms: SCRAM-SHA-256
|   supportedSASLMechanisms: GSSAPI
|   supportedSASLMechanisms: DIGEST-MD5
|   supportedSASLMechanisms: OTP
|   supportedSASLMechanisms: NTLM
|   supportedSASLMechanisms: CRAM-MD5
|   subschemaSubentry: cn=Subschema
|_ MAC Address: 2E:9F:1F:CC:AF:D4 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

(root@ cd307ba75890)-[/home/analyst]
#
```

- 10.10.30.117 – Zabbix – 80, 10051 e 10052
- Protocolo de comunicação do Zabbix



## Recomendações

- Implantar firewall para filtrar as portas, desativar o login FTP anônimo.

## Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Remover porta 21	Médio	Alta	Alta
Instalar Firewall	Alto	Média	Alta

## Conclusão

[Resumo da exposição geral e próximos passos.]

Com base na análise realizada, ficou evidente que a rede simulada apresenta diversas vulnerabilidades, como portas abertas em serviços críticos (FTP, MySQL, SMB, LDAP e Zabbix), que podem ser exploradas por ameaças internas ou externas. Para fortalecer a segurança, recomenda-se a implementação de um



firewall para controlar o acesso às portas abertas, além de desativar o login anônimo no FTP. Essas ações, prioritárias e de fácil execução, são essenciais para reduzir riscos operacionais e proteger os ativos da rede, contribuindo para uma infraestrutura mais segura e resiliente.

## Anexos

- Saída dos scans
- Prints de ferramentas
- Diagrama da rede

Redes Encontradas através do comando ip a

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# ip a | grep inet
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host proto kernel lo
inet 10.10.10.2/24 brd 10.10.10.255 scope global eth0
inet 10.10.50.2/24 brd 10.10.50.255 scope global eth1
inet 10.10.30.2/24 brd 10.10.30.255 scope global eth2
```

Ping em todas as redes

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# ping -c 3 10.10.10.1 # corp_net
10.10.10.1 # guest_net
ping -c 3 10.10.50.1 # infra_netPING 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=0.129 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.083 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.086 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2209ms
rtt min/avg/max/mdev = 0.083/0.099/0.129/0.021 ms

(root@ cd307ba75890)-[/home/analyst]
# ping -c 3 10.10.30.1 # guest_net
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=0.162 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.086 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2228ms
rtt min/avg/max/mdev = 0.064/0.104/0.162/0.041 ms

(root@ cd307ba75890)-[/home/analyst]
# ping -c 3 10.10.50.1 # infra_net
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=0.085 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.088 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2241ms
rtt min/avg/max/mdev = 0.082/0.085/0.088/0.002 ms

(root@ cd307ba75890)-[/home/analyst]
#
```

## Comandos NMAP

```
root@cd307ba75890: /home/analyst
(root@ cd307ba75890)-[/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 (cd307ba75890) Status: Up

(root@ cd307ba75890)-[/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@ cd307ba75890)-[/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 (cd307ba75890)

(root@ cd307ba75890)-[/home/analyst]
#
```

```
root@cd307ba75890: /home/analyst
(root@ cd307ba75890)-[/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 (cd307ba75890) Status: Up

(root@ cd307ba75890)-[/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@ cd307ba75890)-[/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 (cd307ba75890)

(root@ cd307ba75890)-[/home/analyst]
#
```

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890) - [/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
Host: 10.10.50.1 () Status: Up
Host: 10.10.50.3 (notebook-carlos.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.4 (laptop-vastro.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.5 (laptop-luiz.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.6 (macbook-aline.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.2 (cd307ba75890) Status: Up

(root@ cd307ba75890) - [/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2}' | tee guest_net_ips.txt
10.10.50.1
10.10.50.3
10.10.50.4
10.10.50.5
10.10.50.6
10.10.50.2

(root@ cd307ba75890) - [/home/analyst]
# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee guest_net_ips_hosts.tx

(root@ cd307ba75890) - [/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 ()
10.10.50.3 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.4 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.5 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.6 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.2 (cd307ba75890)

(root@ cd307ba75890) - [/home/analyst]
#
```

Comando Rustscan

```
(root@cd307ba75890)-[/home/analyst]
# rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

(root@cd307ba75890)-[/home/analyst/recon/corp_net]
# cat corp_net_ips_ports.txt
Open 10.10.10.2:48660
```

```
root@cd307ba75890: /home/analyst

(root@cd307ba75890)-[/home/analyst]
# rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

(root@cd307ba75890)-[/home/analyst]
# cat infra_net_ips_ports.txt
Open 10.10.30.10:21
Open 10.10.30.117:80
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 10.10.30.2:41658
Open 10.10.30.2:41910
Open 10.10.30.2:57422

(root@cd307ba75890)-[/home/analyst]
#
```

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

(root@ cd307ba75890)-[/home/analyst]
# cat guest_net_ips_ports.txt
Open 10.10.50.2:33948
Open 10.10.50.2:39470

(root@ cd307ba75890)-[/home/analyst]
#
```

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# arp -a
samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) at 52:87:04:52:36:fc [ether] on eth2
openldap.projeto_final_opcao_1_infra_net (10.10.30.17) at 2e:9f:1f:cc:af:d4 [ether] on eth2
mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11) at 0e:56:e4:bb:8c:f0 [ether] on eth2
zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117) at c2:06:ba:5b:ef:21 [ether] on eth2

(root@ cd307ba75890)-[/home/analyst]
#
```

Comando NMAP script anônimo

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890) -[/home/analyst]
# nmap -p 21 --script ftp-anon 10.10.30.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 02:17 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000099s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 5E:20:82:E1:9F:8F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

## Comando NMAP LDAP

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890) -[/home/analyst]
# nmap -p 389 --script ldap-rootse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:10 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00015s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
| ldap-rootse:
| LDAP Results
| <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: 1.3.6.1.1.22
|   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: GS2-IKRB
|   supportedSASLMechanisms: GS2-KRB5
|   supportedSASLMechanisms: SCRAM-SHA-1
|   supportedSASLMechanisms: SCRAM-SHA-256
|   supportedSASLMechanisms: GSS-SPNEGO
|   supportedSASLMechanisms: GSSAPI
|   supportedSASLMechanisms: DIGEST-MD5
|   supportedSASLMechanisms: OTP
|   supportedSASLMechanisms: NTLM
|   supportedSASLMechanisms: CRAM-MD5
|   subschemaSubentry: cn=Subschema
|_
MAC Address: 2E:9F:1F:CC:AF:D4 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

(root@ cd307ba75890) -[/home/analyst]
#
```

## Comando NMAP MYSQL

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:04 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.00013s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 8
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolNew, LongPassword, ODBCClient, Speaks41ProtocolOld, ConnectWithDatabase, SupportsCompr
|   session, SwitchToSSLAfterHandshake, IgnoreSigpipes, SupportsTransactions, Support41Auth, LongColumnFlag, SupportsLoadDataLocal
|   , IgnoreSpaceBeforeParenthesis, InteractiveClient, FoundRows, DontAllowDatabaseTableColumn, SupportsAuthPlugins, SupportsMult
|   ipleResults, SupportsMultipleStatements
|   Status: Autocommit
|   Salt: UaDFl]-v\x15':\x18|R')\x06-"E
|   Auth Plugin Name: caching_sha2_password
|   MAC Address: 0E:56:E4:BB:8C:F0 (Unknown)
|_
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

(root@ cd307ba75890)-[/home/analyst]
#
```

Comando resolv.conf

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/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(172.23.0.1)]
# Overrides: []
# Option ndots from: internal

(root@ cd307ba75890)-[/home/analyst]
#
```

## Comando SMB

```
root@cd307ba75890: /home/analyst

(root@ cd307ba75890)-[/home/analyst]
# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 01:13 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.00011s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 52:87:04:52:36:FC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

(root@ cd307ba75890)-[/home/analyst]
#
```





```

TRACEROUTE
HOP RTT ADDRESS
1 0.05 ms WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)

Nmap scan report for WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)
Host is up (0.000052s latency).
All 1000 scanned ports on WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 4A:BD:2F:67:24:6C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.05 ms WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)

Nmap scan report for WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)
Host is up (0.000053s latency).
All 1000 scanned ports on WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: CA:5C:06:91:56:16 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.05 ms WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)

Nmap scan report for cd307ba75890 (10.10.10.2)
Host is up (0.000056s latency).
All 1000 scanned ports on cd307ba75890 (10.10.10.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 9.54 seconds

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3)

Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000061s latency).
All 1000 scanned ports on laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.4) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 22:73:46:13:C4:C4 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.4)

Nmap scan report for laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000070s latency).
All 1000 scanned ports on laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: AA:8D:73:35:3E:6C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.07 ms laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5)

Nmap scan report for cd307ba75890 (10.10.50.6)
Host is up (0.000071s latency).
All 1000 scanned ports on cd307ba75890 (10.10.50.6) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 17.76 seconds

```

```
(root@ cd307ba75890)-[/home/analyst/recon/infra_net]
# nmap -A 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 02:45 UTC
Nmap scan report for 10.10.30.1
Host is up (0.000036s latency).
All 1000 scanned ports on 10.10.30.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 82:A9:1D:34:7E:95 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.04 ms 10.10.30.1

Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000097s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
MAC Address: 8E:C1:66:B1:4C:62 (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
```

```
(root@ cd307ba75890)-[/home/analyst/recon/guest_net]
# nmap -A 10.10.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 03:46 UTC
Nmap scan report for 10.10.50.1
Host is up (0.00012s latency).
All 1000 scanned ports on 10.10.50.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 56:31:22:E0:8B:12 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.12 ms 10.10.50.1

Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000069s latency).
All 1000 scanned ports on notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 46:7C:C8:F7:79:F9 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.07 ms notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)

Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3)
Host is up (0.000057s latency).
All 1000 scanned ports on macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 56:30:FC:9D:78:5B (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Versão Mysql Server

```

TRACEROUTE
HOP RTT ADDRESS
1 0.08 ms mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)

Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000062s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
MAC Address: 36:CD:1C:95:2F:00 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop

Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
|_ date: 2025-07-24T02:45:27
|_ start_date: N/A

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.10 ms ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)

Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000082s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 8.0.42
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.42_Auto_Generated_Server_Certificate
|_ Not valid before: 2025-07-20T22:14:21
|_ Not valid after: 2035-07-18T22:14:21
|_ ssl-date: TLS randomness does not represent time
| mysql-info:
|_ Protocol: 10
|_ Version: 8.0.42
|_ Thread ID: 10
|_ Capabilities flags: 65535
|_ Some Capabilities: Support41Auth, InteractiveClient, SupportsTransactions, Speaks41ProtocolNew, ODBCClient, SwitchToSSLAf
terHandshake, Speaks41ProtocolOld, LongColumnFlag, ConnectWithDatabase, SupportsLoadDataLocal, IgnoreSigpipes, SupportsCompre
ssion, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, FoundRows, LongPassword, SupportsAuthPlugins, SupportsMult
ipleResults, SupportsMultipleStatements
|_ Status: Autocommit
|_ Salt: (6K\x1C<v&T|\x03\x01kL%p (2'G
|_ Auth Plugin Name: caching_sha2_password
MAC Address: 36:7A:AE:C8:D4:7C (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)

Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
636/tcp open ldapssl?
MAC Address: EE:1F:81:CC:48:BE (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms openldap.projeto_final_opcao_1_infra_net (10.10.30.17)

Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000054s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http nginx
|_ http-robots.txt: 2 disallowed entries
|_ / /zabbix/"
|_ http-title: Zabbix docker: Zabbix
MAC Address: BA:6B:CC:83:92:36 (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

```

## Zabbix

```

TRACEROUTE
HOP RTT ADDRESS
1 0.05 ms zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)

Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000085s latency).
All 1000 scanned ports on legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:93:15:C8:0A:3B (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.09 ms legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)

Nmap scan report for cd307ba75890 (10.10.30.2)
Host is up (0.000068s latency).
All 1000 scanned ports on cd307ba75890 (10.10.30.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 25.54 seconds

```

## Endereço MAC CORPNET com o comando ARP

```

(root@cd307ba75890)-[/home/analyst]
# arp-scan 10.10.10.0/24
Interface: eth0, type: EN10MB, MAC: fa:79:11:e5:50:e1, IPv4: 10.10.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.10.1 9a:ed:f8:4f:36:41 (Unknown: locally administered)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.849 seconds (138.45 hosts/sec). 1 responded

```

## Endereço MAC INFRANET com o comando ARP

```
(root@ cd307ba75890) - [/home/analyst]
# arp-scan 10.10.30.0/24
Interface: eth0, type: EN10MB, MAC: fa:79:11:e5:50:e1, IPv4: 10.10.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.30.1    9a:ed:f8:4f:36:41    (Unknown: locally administered)
10.10.30.10   56:61:68:c0:d8:4d    (Unknown: locally administered)
10.10.30.11   fe:9d:e9:0a:ee:33    (Unknown: locally administered)
10.10.30.15   ce:9f:f8:ce:87:1c    (Unknown: locally administered)
10.10.30.17   56:2c:f9:f3:f6:88    (Unknown: locally administered)
10.10.30.117  7a:87:e2:ac:d1:45    (Unknown: locally administered)
10.10.30.227  46:ba:11:37:30:95    (Unknown: locally administered)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.854 seconds (138.08 hosts/sec). 7 responded
```

```
(root@ cd307ba75890) - [/home/analyst]
# arp-scan 10.10.50.0/24
Interface: eth0, type: EN10MB, MAC: fa:79:11:e5:50:e1, IPv4: 10.10.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.50.1    9a:ed:f8:4f:36:41    (Unknown: locally administered)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.837 seconds (139.36 hosts/sec). 1 responded
```

## Comando Whois

```
(root@ cd307ba75890) - [/home/analyst]
# whois 10.10.10.1

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:      10.0.0.0 - 10.255.255.255
CIDR:          10.0.0.0/8
NetName:       PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:     NET-10-0-0-1
Parent:        ()
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:       2024-05-24
Comment:       These addresses are in use by many millions of independently operated networks, which might be as small as a single computer co
nnected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a privat
e context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:       These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these
addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http
://www.iana.org/abuse/answers
Comment:
Comment:       These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice docu
ment, RFC 1918 which can be found at:
Comment:       http://datatracker.ietf.org/doc/rfc1918
Ref:           https://rdap.arin.net/registry/ip/10.0.0.0
```

```
root@cd307ba75890: /home/analyst
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

(root@ cd307ba75890)-[/home/analyst]
#
```

```
(root@ cd307ba75890)-[/home/analyst]
# whois 10.10.30.1

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange: 10.0.0.0 - 10.255.255.255
CIDR: 10.0.0.0/8
NetName: PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle: NET-10-0-0-1
Parent: ()
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate:
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer co
nnected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a privat
e context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these
addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http
://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice docu
ment, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/10.0.0.0
```

```
root@cd307ba75890: /home/analyst

OrgName:      Internet Assigned Numbers Authority
OrgId:        IANA
Address:      12025 Waterfront Drive
Address:      Suite 300
City:         Los Angeles
StateProv:    CA
PostalCode:   90292
Country:      US
RegDate:
Updated:      2024-05-24
Ref:          https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

(root@ cd307ba75890)-[/home/analyst]
```

```
(root@ cd307ba75890)-[/home/analyst]
# whois 10.10.50.1

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange:      10.0.0.0 - 10.255.255.255
CIDR:          10.0.0.0/8
NetName:       PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle:     NET-10-0-0-1
Parent:        ()
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:       2024-05-24
Comment:       These addresses are in use by many millions of independently operated networks, which might be as small as a single computer co
nnected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a privat
e context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:       These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these
addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http
://www.iana.org/abuse/answers
Comment:
Comment:       These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice docu
ment, RFC 1918 which can be found at:
Comment:       http://datatracker.ietf.org/doc/rfc1918
Ref:           https://rdap.arin.net/registry/ip/10.0.0.0
```



```
root@cd307ba75890: /home/analyst

OrgName:      Internet Assigned Numbers Authority
OrgId:        IANA
Address:      12025 Waterfront Drive
City:        Los Angeles
StateProv:    CA
PostalCode:   90292
Country:      US
RegDate:
Updated:      2024-05-24
Ref:          https://rdap.arin.net/registry/entity/IANA

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

(root@ cd307ba75890)-[/home/analyst]
```

## Netdiscover

### Netdiscover da Rede CorpNet

```
← Currently scanning: Finished! | Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 210

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.10.10.1    26:24:7d:ee:a6:56    1      42  Unknown vendor
10.10.10.10   76:20:93:09:b4:1d    1      42  Unknown vendor
10.10.10.101  7a:d6:90:2d:18:fc    1      42  Unknown vendor
10.10.10.127  02:bb:3c:13:c3:55    1      42  Unknown vendor
10.10.10.222  72:35:99:62:68:36    1      42  Unknown vendor

Currently scanning: Finished! | Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 42

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.10.30.1    26:24:7d:ee:a6:56    1      42  Unknown vendor
```

Currently scanning: Finished! | Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 42

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.10.50.1	26:24:7d:ee:a6:56	1	42	Unknown vendor

## Traceroute

```
(root@ cd307ba75890) - [/home/analyst]
# traceroute 10.10.10.0/24
10.10.10.0/24: Name or service not known
Cannot handle "host" cmdline arg `10.10.10.0/24' on position 1 (argc 1)

(root@ cd307ba75890) - [/home/analyst]
# traceroute 10.10.10.1
traceroute to 10.10.10.1 (10.10.10.1), 30 hops max, 60 byte packets
 1 10.10.10.1 (10.10.10.1) 1.690 ms 1.425 ms 1.329 ms

(root@ cd307ba75890) - [/home/analyst]
# traceroute 10.10.30.1
traceroute to 10.10.30.1 (10.10.30.1), 30 hops max, 60 byte packets
 1 10.10.30.1 (10.10.30.1) 0.287 ms 0.051 ms 0.047 ms

(root@ cd307ba75890) - [/home/analyst]
# traceroute 10.10.50.1
traceroute to 10.10.50.1 (10.10.50.1), 30 hops max, 60 byte packets
 1 10.10.50.1 (10.10.50.1) 1.014 ms 0.799 ms 0.726 ms
```

## Sistema Operacional da InfraNet

```
(root@ cd307ba75890) - [/home/analyst/recon/infra_net]
# nmap -A 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 02:45 UTC
Nmap scan report for 10.10.30.1
Host is up (0.000036s latency).
All 1000 scanned ports on 10.10.30.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 82:A9:1D:34:7E:95 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.04 ms 10.10.30.1

Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000097s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
MAC Address: 8E:C1:66:B1:4C:62 (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.10 ms ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)

Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000082s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
3306/tcp open mysql MySQL 8.0.42
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.42_Auto_Generated_Server_Certificate
|_ Not valid before: 2025-07-20T22:14:21
|_ Not valid after: 2035-07-18T22:14:21
|_ ssl-date: TLS randomness does not represent time
mysql-info:
|_ Protocol: 10
|_ Version: 8.0.42
|_ Thread ID: 10
|_ Capabilities flags: 65535
|_ Some Capabilities: Support41Auth, InteractiveClient, SupportsTransactions, Speaks41ProtocolNew, ODBCClient, SwitchToSSLAF
|_ terHandshake, Speaks41ProtocolOld, LongColumnFlag, ConnectWithDatabase, SupportsLoadDataLocal, IgnoreSigpipes, SupportsCompre
|_ ssion, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, FoundRows, LongPassword, SupportsAuthPlugins, SupportsMult
|_ ipleResults, SupportsMultipleStatements
|_ Status: Autocommit
|_ Salt: (6K\X1C\Xv&T|\x03\x01kL%p (2'G
|_ Auth Plugin Name: caching_sha2_password
MAC Address: 36:7A:AE:C8:D4:7C (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.08 ms mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)

Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000062s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
MAC Address: 36:CD:1C:95:2F:00 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop

Host script results:
|_ smb2-security-mode:
|_ 3:1:1:
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2025-07-24T02:45:27
|_ start_date: N/A

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)

Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X
636/tcp open ldapssl?
MAC Address: EE:1F:81:CC:48:BE (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms openldap.projeto_final_opcao_1_infra_net (10.10.30.17)

Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000054s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
80/tcp open http nginx
|_ http-robots.txt: 2 disallowed entries
|_ / /zabbix/
|_ http-title: Zabbix docker: Zabbix
MAC Address: BA:6B:CC:83:92:36 (Unknown)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

```

```

TRACEROUTE
HOP RTT ADDRESS
1 0.05 ms zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)

Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000085s latency).
All 1000 scanned ports on legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:93:15:C8:0A:3B (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.09 ms legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)

Nmap scan report for cd307ba75890 (10.10.30.2)
Host is up (0.000068s latency).
All 1000 scanned ports on cd307ba75890 (10.10.30.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 25.54 seconds

```