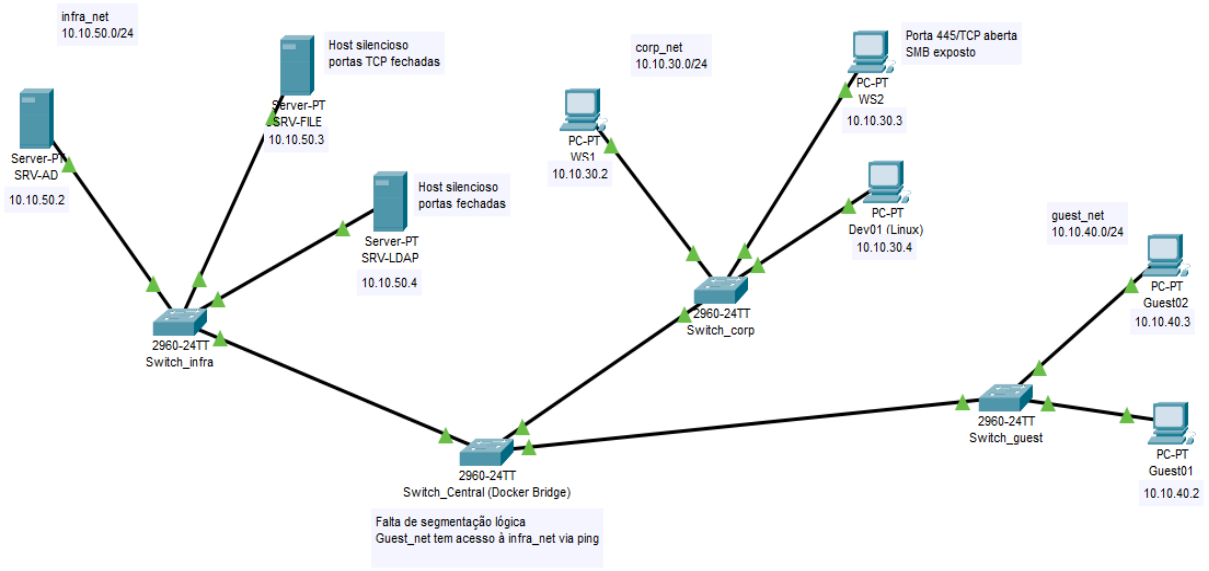
Autor: Pedro Simplicio

DIAGRAMA DA REDE

(Visualização da estrutura da rede)



Inventário de Ativos dos hosts mapeados (infra_net, corp_net e guest_net)

Sub-rede: infra_net (10.10.50.0/24)

IP	Hostname	Função/Serviço	Status da porta	Observações
10.10.50.2	SRV-AD	Active Directory	Silencioso	Sem resposta a TCP
10.10.50.3	SRV-FILE	Arquivos	Silencioso	Portas TCP fechadas
10.10.50.4	SRV-LDAP	Autenticação	Silencioso	Portas TCP fechadas

Sub-rede: corp_net (10.10.30.0/24)

IP	Hostname	Função/Serviço	Status da porta	Observações
10.10.30.2	WS1	Estação de trabalho	Fechada(s)	Nenhuma
10.10.30.3	WS2	Estação (SMB exp.)	445/TCP aberta	Risco – serviço SMB
10.10.30.4	Dev01	Dev Linux	Fechada(s)	Nenhuma

Sub-rede: guest_net (10.10.40.0/24)

IP	Hostname	Função/Serviço	Status da porta	Observações
10.10.40.2	Guest01	Cliente	Fechada(s)	Nenhuma
10.10.40.3	Guest02	Cliente	Fechada(s)	Nenhuma
10.10.10.5	(Desconhecido)	Silencioso	Fechada(s)	Host passivo fora do diagrama

DIAGNÓSTICO

Achados	Evidência	Impacto
Porta 111 exposta (RPC)	Scan nmap: porta 111/tcp aberta em 10.10.10.101	Pode permitir enumeração ou exploração de serviços RPC
Host sem resposta (silencioso)	Ping falhou: 10.10.10.5 não respondeu	Pode indicar host camuflado, com firewall ou ‘stealth’ ativo
Banner, exposto no SSH	nmap -sV revelou versão desatualizada do OpenSSH	Potencial vulnerabilidade conhecida CVE

SAÍDA DOS SCANS & COMANDOS UTILIZADOS

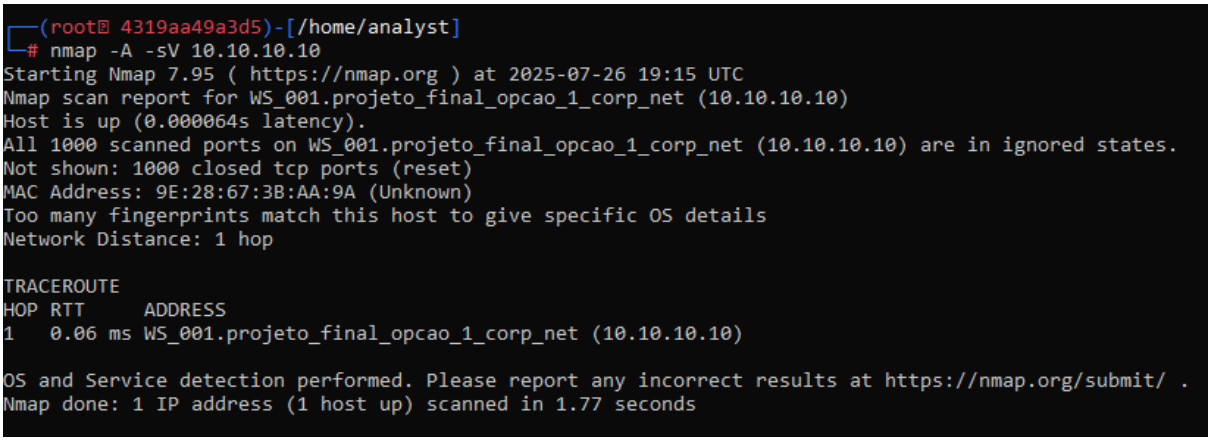
IPs da Rede Corporativa (corp_net)

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -sS -p- -T4 -n 10.10.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 19:24 UTC
Nmap scan report for 10.10.10.1
Host is up (0.000010s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE
111/tcp   open     rpcbind
8080/tcp  filtered http-proxy
58521/tcp open     unknown
MAC Address: F6:35:0F:2C:99:65 (Unknown)

Nmap scan report for 10.10.10.10
Host is up (0.000016s latency).
All 65535 scanned ports on 10.10.10.10 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 26:59:09:65:3E:F4 (Unknown)

Nmap scan report for 10.10.10.101
Host is up (0.000015s latency).
All 65535 scanned ports on 10.10.10.101 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 4A:B8:D1:74:FC:A5 (Unknown)

Nmap scan report for 10.10.10.127
Host is up (0.000016s latency).
All 65535 scanned ports on 10.10.10.127 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: B2:BE:1F:10:B6:3A (Unknown)

Nmap scan report for 10.10.10.222
Host is up (0.000015s latency).
All 65535 scanned ports on 10.10.10.222 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: AA:78:22:E8:18:23 (Unknown)

Nmap scan report for 10.10.10.2
Host is up (0.0000090s latency).
All 65535 scanned ports on 10.10.10.2 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 9.82 seconds
```

Foi utilizada a varredura nmap -sS -p- -T4 -n 10.10.10.0/24, que escaneia todas as 65.535 portas TCP de cada host no intervalo de uma sub-rede classe C. O método SYN scan (-sS) é rápido e discreto, e a flag -T4 aumenta a velocidade da varredura.

O escaneamento identificou apenas 6 hosts ativos entre 256 endereços IP, indicando uma rede com poucos dispositivos acessíveis no momento. Isso pode ser consequência de medidas de segurança ou inatividade dos hosts, o que reduz a superfície de análise e facilita a identificação de alvos relevantes.

IP 10.10.10.10



Saída do comando nmap -A -sV 10.10.10.10 mostrando host ativo, com todas as portas TCP fechadas e sem identificação precisa de sistema operacional.

Apesar de estar ativo na rede, o host não apresenta serviços acessíveis externamente nas portas TCP padrão já que estão fechadas com resposta *reset*, o que pode indicar presença de firewall ou configuração restritiva.

IP 10.10.10.1

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.10.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 19:20 UTC
Nmap scan report for 10.10.10.1
Host is up (0.000029s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
111/tcp  open     rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34849/tcp6  status
|   100024  1          48605/udp   status
|   100024  1          53350/udp6  status
|_  100024  1          53933/tcp   status
8080/tcp filtered http-proxy
MAC Address: B2:B6:18:E0:98:EB (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.
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   0.03 ms 10.10.10.1
```

Saída do comando nmap -A -sV 10.10.10.1 mostrando detecção de sistema operacional, serviços RPC e filtragem de porta 8080.

O host 10.10.10.1 possui serviços RPC ativos e a porta 8080 filtrada, indicando possível firewall. A detecção sugere que é um roteador baseado em Linux, possivelmente MikroTik, com papel central na rede.

IP 10.10.10.2

```
chronos@DESKTOP-70P2F4B:~$ docker exec -it analyst bash
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.10.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 15:27 UTC
Nmap scan report for 4319aa49a3d5 (10.10.10.2)
Host is up (0.000018s latency).
All 1000 scanned ports on 4319aa49a3d5 (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: 1 IP address (1 host up) scanned in 1.78 seconds
```

Saída do comando nmap -A -sV 10.10.10.2 mostrando o host local como ativo, com todas as portas TCP fechadas e sem identificação precisa do sistema operacional.

Esse IP corresponde a minha própria máquina visto que todas as portas estão fechadas, não foi possível identificar o sistema operacional e a distância da rede consta como “0 hops”, o que significa que não houve nenhum salto na rede, logo, a máquina é minha.

IP 10.10.10.101

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.10.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 15:29 UTC
Nmap scan report for WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)
Host is up (0.000041s latency).
All 1000 scanned ports on WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 92:90:24:1B:ED:8C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

Saída do comando nmap -A -sV 10.10.10.101, com host ativo, portas fechadas e sistema operacional não identificado com precisão.

O host 10.10.10.101 está ativo, mas não apresenta serviços acessíveis externamente. Todas as portas TCP estão fechadas, e a identificação do sistema operacional foi inconclusiva. Pode estar protegido por firewall ou configurado para rejeitar conexões externas.

IP 10.10.10.127

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.10.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 15:30 UTC
Nmap scan report for WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)
Host is up (0.000041s 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: D6:F5:23:6F:C0:19 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

Saída do comando nmap -A -sV 10.10.10.127 mostrando host ativo, portas fechadas e sistema operacional não identificado.

O host 10.10.10.127 está ativo, porém sem serviços acessíveis externamente. Todas as portas TCP estão fechadas e a detecção do sistema operacional foi inconclusiva, indicando possível proteção via firewall ou configuração restritiva.

IP 10.10.10.222

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.10.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 15:44 UTC
Nmap scan report for WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)
Host is up (0.000045s 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: 92:31:A1:AF:3E:B5 (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)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

Saída do comando nmap -A -sV 10.10.10.222 mostrando host ativo, portas fechadas e sistema operacional não identificado.

O host 10.10.10.222 está ativo, porém sem serviços acessíveis externamente. Todas as portas TCP estão fechadas e a detecção do sistema operacional foi inconclusiva, indicando possível proteção via firewall ou configuração restritiva.

IPs da Rede de visitantes/dispositivos pessoais (guest_net)

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -sn 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-27 16:44 UTC
Nmap scan report for 10.10.30.1
Host is up (0.000063s latency).
MAC Address: EA:D8:06:13:20:00 (Unknown)
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000019s latency).
MAC Address: 26:54:5B:33:BF:77 (Unknown)
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000019s latency).
MAC Address: EE:9C:5C:24:5B:44 (Unknown)
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000026s latency).
MAC Address: 66:EC:ED:36:3A:45 (Unknown)
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000021s latency).
MAC Address: 1A:A6:6A:4C:19:50 (Unknown)
Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000026s latency).
MAC Address: 2E:B4:26:F2:D3:DB (Unknown)
Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000034s latency).
MAC Address: 36:33:88:EE:D3:3C (Unknown)
Nmap scan report for 4319aa49a3d5 (10.10.30.2)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.98 seconds
```

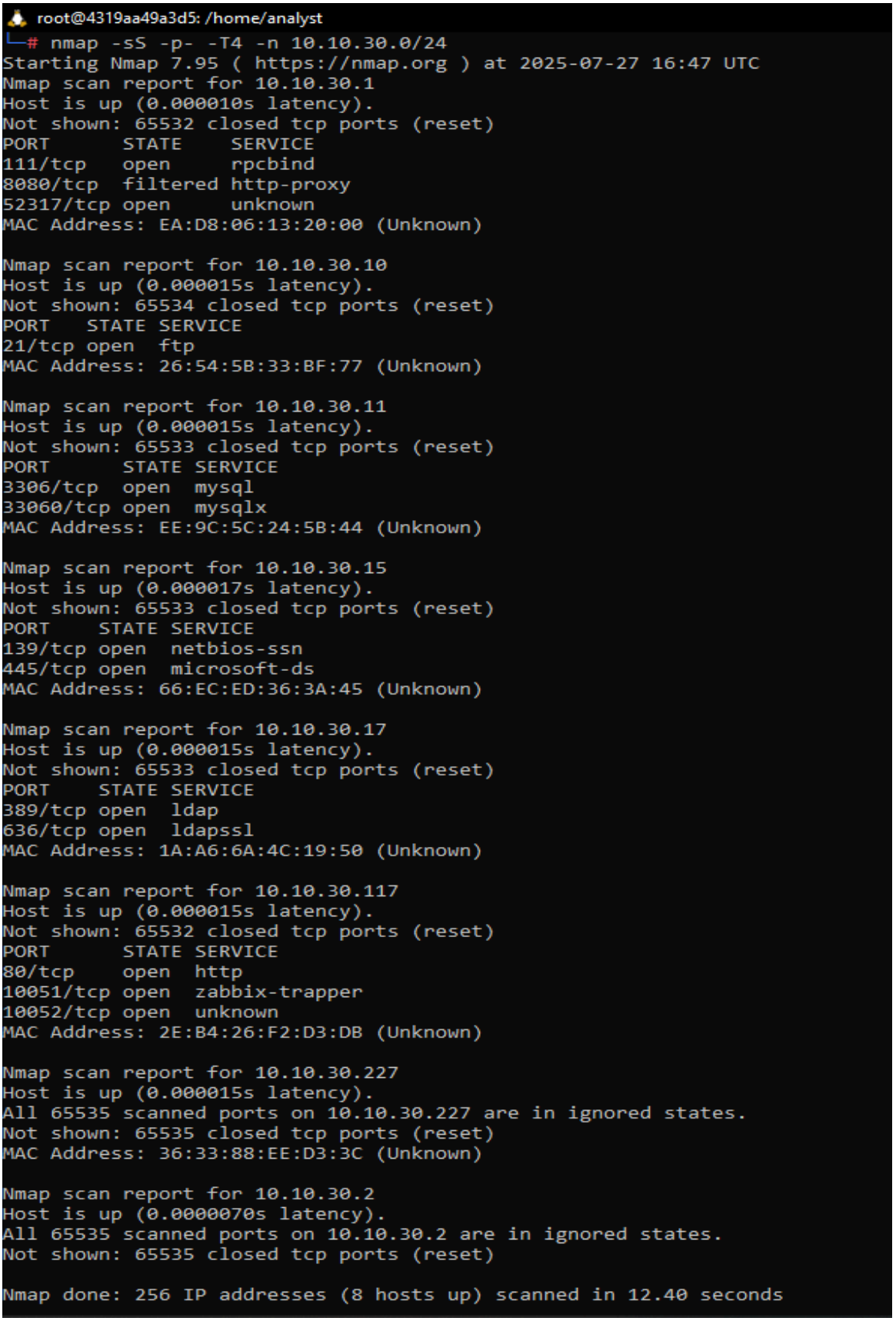
Na figura acima, foi utilizado o comando nmap -sn 10.10.30.0/24 do tipo *ping scan* (-sn) cujo objetivo principal é identificar quais dispositivos estão ativos na sub-rede

especificada, sem realizar a análise das portas ou serviços que esses hosts possam estar oferecendo.

Durante essa varredura, o Nmap envia pacotes ICMP Echo Request (mensagens usadas para verificar se um dispositivo está ativo em uma rede) e outras sondas para determinar se os hosts estão respondendo.

No total, foram escaneados 256 endereços IP pertencentes à faixa 10.10.30.0/24. Desses, apenas 8 hosts retornaram respostas positivas, o que indica que cerca de 3% dos dispositivos estavam ativos e acessíveis no momento do scan. Essa baixa taxa pode refletir tanto uma rede com poucos dispositivos ligados quanto uma configuração robusta de firewalls ou políticas de segurança que bloqueiam respostas a sondas de rede.

Esse mapeamento inicial é fundamental para delimitar o escopo da análise de segurança, pois permite focar os esforços de varredura detalhada e testes apenas nos dispositivos realmente presentes e acessíveis na rede, evitando tempo e recursos gastos em IPs inativos ou inacessíveis.



Nessa figura foi utilizado o comando de varredura nmap -sS -p- -T4 -n 10.10.30.0/24 para escanear todas as portas TCP dos hosts da sub-rede, com execução rápida (-T4) e sem resolução de nomes (-n).

O escaneamento identificou 8 hosts ativos em um total de 256 IPs analisados. Alguns desses hosts apresentaram portas abertas associadas a serviços comuns como FTP, HTTP, MySQL, SMB e LDAP, enquanto outros estavam ativos mas com todas as portas fechadas, o que pode indicar medidas de proteção como firewalls ou serviços desativados. O resultado fornece um panorama inicial útil para reconhecimento e avaliação de possíveis vetores de ataque.

IP 10.10.30.1

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 19:54 UTC
Nmap scan report for 10.10.30.1
Host is up (0.000029s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
111/tcp  open     rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35685/udp   status
|   100024  1          38381/tcp6  status
|   100024  1          39060/udp6  status
|_  100024  1          58521/tcp   status
8080/tcp filtered http-proxy
MAC Address: 4A:7D:87:25:FC:5A (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   0.03 ms 10.10.30.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.01 seconds
```

Saída do comando nmap -A -sV 10.10.30.1 mostrando host ativo, portas TCP 111 aberta (RPC) e porta TCP 8080 filtrada e sistema operacional detectado.

O host respondeu com serviços ativos na porta 111/tcp (RPC) e uma porta filtrada (8080/tcp), sugerindo proteção por firewall. O sistema operacional identificado indica que o host pode ser um roteador MikroTik com base Linux.

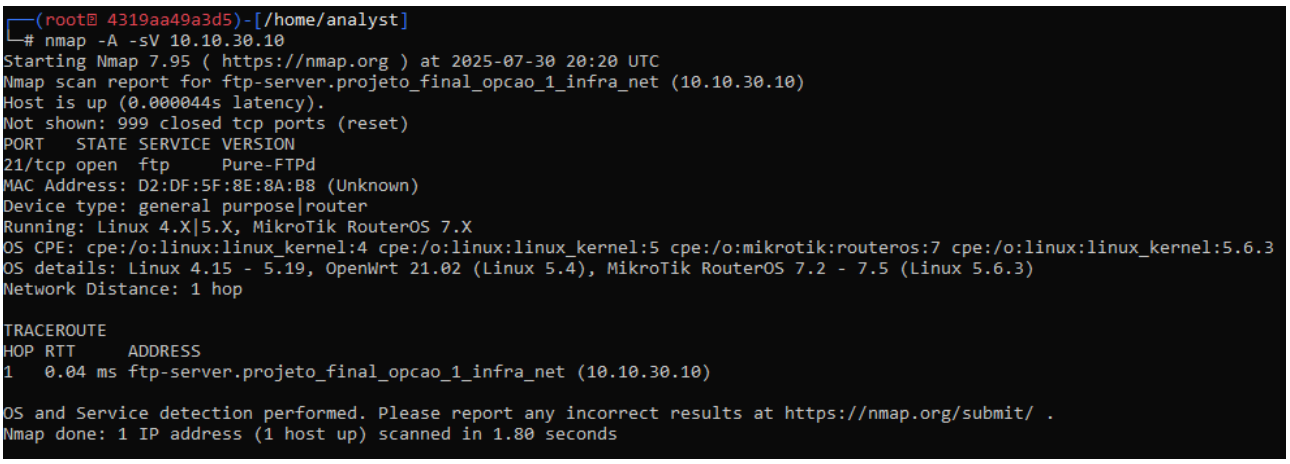
IP 10.10.30.2

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:35 UTC
Nmap scan report for 4319aa49a3d5 (10.10.30.2)
Host is up (0.000031s latency).
All 1000 scanned ports on 4319aa49a3d5 (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: 1 IP address (1 host up) scanned in 1.02 seconds
```

Saída do comando nmap -A -sV 10.10.30.2 mostrando host ativo, todas as portas TCP fechadas e sistema operacional não identificado.

O host 10.10.30.2 respondeu, porém todas as portas TCP estão fechadas, sem serviços acessíveis. A detecção do sistema operacional foi inconclusiva devido à alta similaridade com múltiplas impressões digitais, indicando que pode ser o próprio dispositivo do scanner ou um host com configuração restritiva.

IP 10.10.30.10



Saída do comando nmap -A -sV 10.10.30.10 mostrando host ativo, porta TCP 21 aberta (FTP) e sistema operacional identificado.

O serviço identificado na porta 21/tcp é o Pure-FTPd, uma implementação do protocolo FTP, utilizado para transferência de arquivos. Ele está ativo no host 10.10.30.10, indicando que o dispositivo pode estar operando como um servidor de arquivos ou backup dentro da rede.

IP 10.10.30.11

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 20:21 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000038s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 8.0.43
| mysql-info:
|   Protocol: 10
|   Version: 8.0.43
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, ODBCClient, FoundRows, Speaks41ProtocolOld, SupportsTransactions, IgnoreSpac
eBeforeParenthesis, LongColumnFlag, LongPassword, InteractiveClient, DontAllowDatabaseTableColumn, ConnectWithData
base, SupportsCompression, SupportsLoadDataLocal, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, IgnoreSigpipes,
SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: 9\x0B\x1DF4=]%^\x11xqx\x0E \x0C\x01B*S
|_  Auth Plugin Name: caching_sha2_password
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.0.43_Auto_Generated_Server_Certificate
| Not valid before: 2025-07-26T18:35:36
|_Not valid after:  2035-07-24T18:35:36
MAC Address: CE:9C:69:F0:FF:02 (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.4 - 5.10
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

Saída do comando nmap -A -sV 10.10.30.11 mostrando host ativo, porta TCP 3306 aberta e sistema operacional identificado como Linux 5.4 a 5.10.

O host 10.10.30.11 possui a porta 3306/tcp aberta, executando o serviço MySQL 8.0.43, com autenticação via plugin cashing_cha2_password e certificado SSL recente (2025). O sistema operacional identificado é Linux com kernel entre 5.4 e 5.10, indicando que se trata de um servidor de banco de dados ativo na rede interna.

IP 10.10.30.15

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 21:10 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000076s 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: D2:C1:1A:CB:0B:CF (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_kern
el: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

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-30T21:11:03
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.74 seconds
```

Saída do comando nmap -A -sV 10.10.30.15 mostrando host ativo com as portas 139/tcp e 445/tcp abertas, executando Samba SMBd v4.

O sistema operacional identificado é Linux (kernel entre 4.15 e 5.19) ou MikroTik RouterOS 7.X. O host aceita SMBv2 com assinatura de mensagens habilitada, mas não obrigatória.

IP 10.0.30.17

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:17 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000061s 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: 0E:15:BF:43:83:13 (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_kern
el: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 openldap.projeto_final_opcao_1_infra_net (10.10.30.17)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
```

Saída do comando nmap 10.10.30.17 mostrando host ativo, portas TCP 389 e 636 abertas, e sistema operacional identificado como Linux kernel 4.15 a 5.4 ou RouterOS 7.2-7.5

O host 10.10.30.17 possui as portas 389/tcp e 636/tcp abertas, indicando um servidor LDAP possivelmente com suporte a LDAPS. O sistema operacional sugere Linux (4.15–5.19) ou RouterOS (7.2), apontando para um dispositivo de rede com função de autenticação centralizada.

IP 10.10.30.117

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:23 UTC
Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000059s 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: 1A:D8:89:4A:AE:80 (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_ker
el: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 zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds
```

Saída do comando nmap -A -sV 10.10.30.117 mostrando host ativo, porta 80/tcp aberta e sistema operacional identificado.

O host 10.10.30.117 possui o serviço HTTP (porta 80) ativo com Nginx, hospedando uma interface do Zabbix. O sistema operacional é Linux (kernel 4.15–5.19) ou RouterOS (7.2–7.5), indicando possível servidor de monitoramento ou dispositivo de rede com interface web exposta.

IP 10.10.30.227

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.30.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:28 UTC
Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000048s 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: FE:A1:E4:24:9F:1F (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

Saída do comando nmap 10.10.30.227 mostrando que as 1000 portas TCP estão fechadas (reset) e o sistema operacional não foi identificado devido a múltiplas assinaturas.

O host 10.10.30.227 está ativo, mas não possui serviços TCP acessíveis, indicando um sistema possivelmente desligado logicamente, protegido por firewall ou desativado. Ao rodar o escaneamento com nmap, não foi possível identificar o sistema operacional com precisão.

IPs da Rede de Infraestrutura (infra_net)

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -sn 10.10.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 22:52 UTC
Nmap scan report for 10.10.50.1
Host is up (0.00028s latency).
MAC Address: 0E:A1:33:F0:7B:A4 (Unknown)
Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000068s latency).
MAC Address: 5E:D7:A7:38:77:17 (Unknown)
Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000068s latency).
MAC Address: 02:EF:23:DA:10:4A (Unknown)
Nmap scan report for laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000040s latency).
MAC Address: D2:06:26:98:08:B2 (Unknown)
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.6)
Host is up (0.000064s latency).
MAC Address: 06:5E:7F:83:2C:46 (Unknown)
Nmap scan report for 4319aa49a3d5 (10.10.50.3)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.13 seconds
```

Saída do comando nmap -sn 10.10.50.0/24 mostrando hosts ativos na sub-rede.

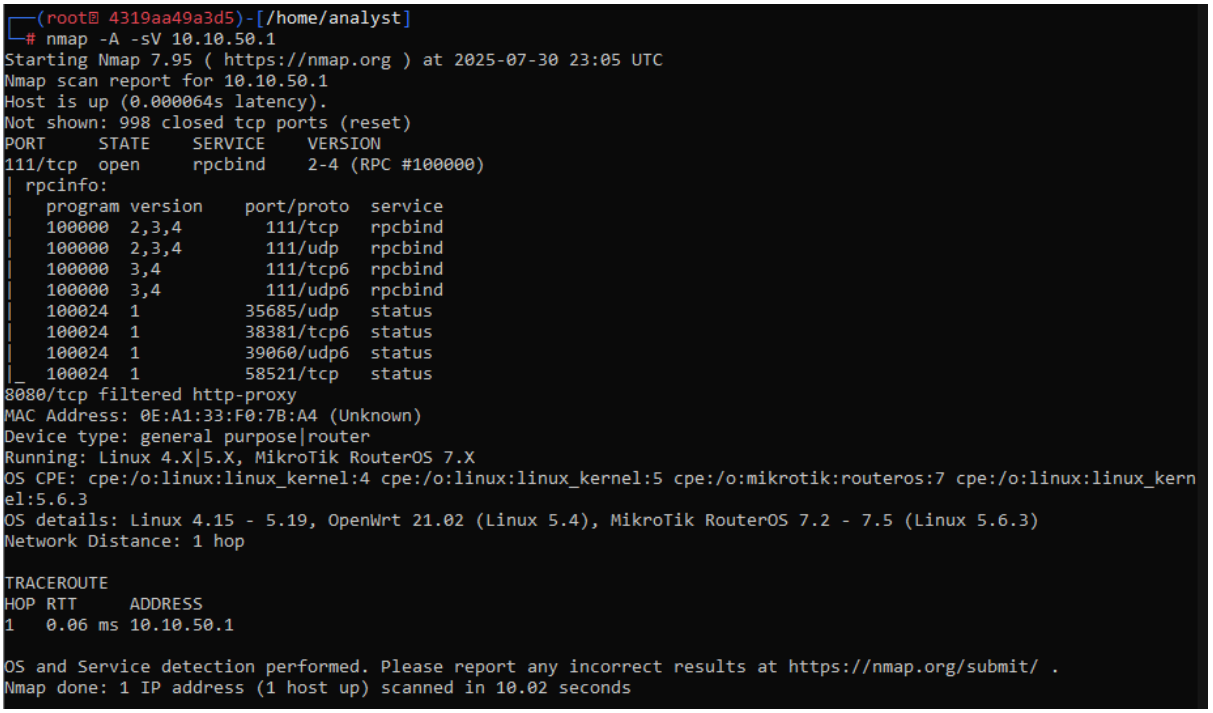
Foi realizada uma varredura de *ping scan* para identificar hosts ativos na sub-rede 10.10.50.0/24. Dos 256 endereços IP escaneados, 6 responderam, indicando uma taxa moderada de dispositivos conectados na rede convidada no momento da análise. Entre os hosts detectados estão notebooks e laptops com nomes identificados, além de um dispositivo sem identificação, o que sugere diversidade de equipamentos e usuários na rede.

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -sS -p- -T4 -n 10.10.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 23:00 UTC
Nmap scan report for 10.10.50.1
Host is up (0.000011s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE
111/tcp   open     rpcbind
8080/tcp  filtered http-proxy
58521/tcp open     unknown
MAC Address: 0E:A1:33:F0:7B:A4 (Unknown)

Nmap scan report for 10.10.50.2
Host is up (0.000016s latency).
All 65535 scanned ports on 10.10.50.2 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 5E:D7:A7:38:77:17 (Unknown)

Nmap scan report for 10.10.50.4
Host is up (0.000016s latency).
All 65535 scanned ports on 10.10.50.4 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 02:EF:23:DA:10:4A (Unknown)

Nmap scan report for 10.10.50.5
Host is up (0.000016s latency).
All 65535 scanned ports on 10.10.50.5 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: D2:06:26:98:08:B2 (Unknown)

Nmap scan report for 10.10.50.6
Host is up (0.000017s latency).
All 65535 scanned ports on 10.10.50.6 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 06:5E:7F:83:2C:46 (Unknown)

Nmap scan report for 10.10.50.3
Host is up (0.000010s latency).
All 65535 scanned ports on 10.10.50.3 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 10.31 seconds
```

Saída do comando nmap -sS -p- -T4 -n 10.10.50.0/24 que faz uma varredura completa, detalhando os serviços, portas abertas e informações adicionais desses hosts ativos.

Foi realizada uma varredura TCP SYN em todas as 65.535 portas de cada host da sub-rede, com execução acelerada (-T4) e sem resolução de nomes (-n). Dos 256 IPs, 6 hosts responderam, sendo que apenas um apresentou portas abertas (111/tcp e 58521/tcp), além de uma porta filtrada (8080/tcp), indicando possível proteção por firewall. Os demais hosts possuem todas as portas fechadas, sugerindo baixa exposição de serviços na rede convidada.

IP 10.10.50.1

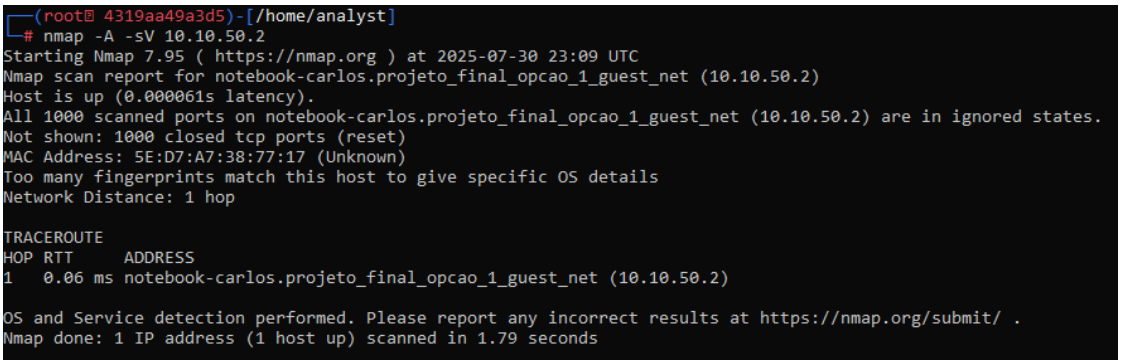


```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.50.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 23:05 UTC
Nmap scan report for 10.10.50.1
Host is up (0.000064s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
111/tcp  open     rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35685/udp   status
|   100024  1          38381/tcp6  status
|   100024  1          39060/udp6  status
|_  100024  1          58521/tcp   status
8080/tcp filtered http-proxy
MAC Address: 0E:A1:33:F0:7B:A4 (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_kern
el: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 10.10.50.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds
```

Saída do comando nmap -A -sV 10.10.50.1 mostrando host ativo, portas 111/tcp e 58521/tcp abertas, porta 8080/tcp filtrada e sistema operacional identificado como Linux 4.15–5.19 ou MikroTik RouterOS 7.2.

O host 10.10.50.1 respondeu com o serviço rpcbind ativo na porta 111/tcp, além de uma porta 58521/tcp aberta relacionada a status RPC. A porta 8080/tcp está filtrada, indicando possível proteção via firewall. O sistema operacional detectado sugere um dispositivo de borda, como roteador, baseado em Linux ou MikroTik RouterOS.

IP 10.10.50.2



```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.50.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 23:09 UTC
Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000061s 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: 5E:D7:A7:38:77:17 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

Saída do comando nmap -A -sV 10.10.50.2 mostrando host ativo e todas as 1000 portas TCP fechadas. O sistema operacional não pôde ser identificado devido a múltiplas assinaturas.

O host está ativo, porém sem portas TCP acessíveis, indicando possível firewall ou dispositivo em modo protegido. Não foi possível identificar o sistema operacional de forma precisa.

IP 10.10.50.3

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.50.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 23:17 UTC
Nmap scan report for 4319aa49a3d5 (10.10.50.3)
Host is up (0.000029s latency).
All 1000 scanned ports on 4319aa49a3d5 (10.10.50.3) 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: 1 IP address (1 host up) scanned in 1.77 seconds
```

Saída do comando nmap -A -sV 10.10.50.3 mostrando que todas as 1000 portas TCP estão fechadas (reset) e o sistema operacional não foi identificado devido a múltiplas assinaturas.

O host 10.10.50.3 está ativo, mas não possui serviços TCP acessíveis. Isso pode indicar que o sistema está protegido por firewall, com serviços desativados ou bloqueados. A detecção do sistema operacional não foi conclusiva.

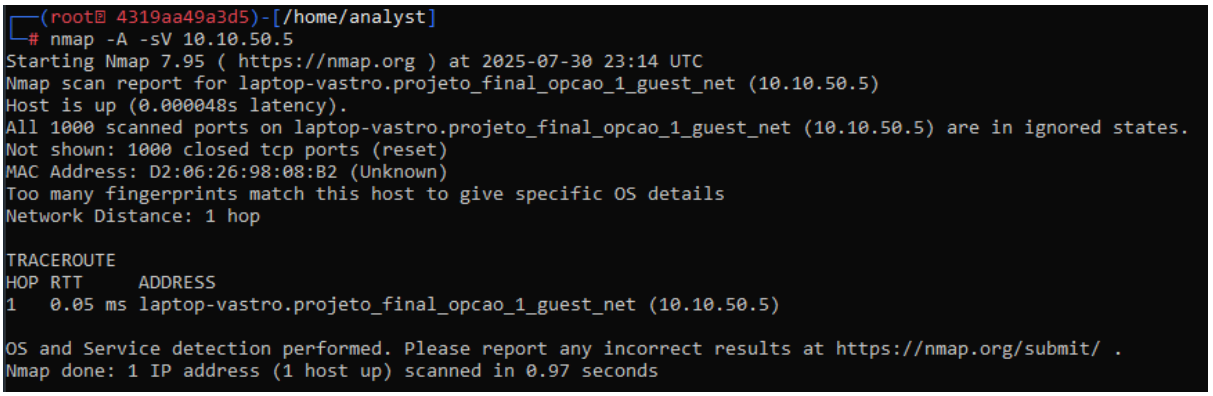
IP 10.10.50.4

```
┌──(root㉿ 4319aa49a3d5)-[/home/analyst]
└─# nmap -A -sV 10.10.50.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 23:11 UTC
Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000042s latency).
All 1000 scanned ports on macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:EF:23:DA:10:4A (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.04 ms macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
```

Saída do comando nmap -A -sV 10.10.50.4 mostrando host ativo e todas as 1000 portas TCP fechadas. O sistema operacional não pôde ser identificado devido a múltiplas assinaturas.

O host está ativo, mas sem portas TCP acessíveis, sugerindo presença de firewall ou configuração de segurança restritiva. A identificação do sistema operacional não foi possível.

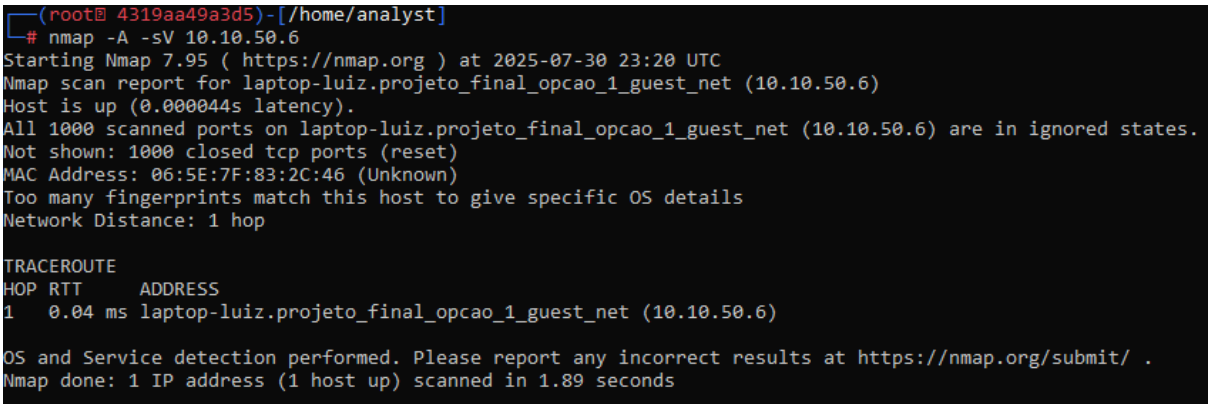
IP 10.10.50.5



Saída do comando nmap -A -sV 10.10.50.5 mostrando host ativo e todas as 1000 portas TCP fechadas. O sistema operacional não foi identificado devido a múltiplas assinaturas.

O host está ativo, porém sem portas TCP acessíveis, indicando possível proteção por firewall ou restrição de serviços. A identificação do sistema operacional não foi possível.

IP 10.10.50.6



Saída do comando nmap -A -sV 10.10.50.6 mostrando que todas as 1000 portas TCP estão fechadas (reset) e o sistema operacional não foi identificado devido a múltiplas assinaturas.

O host 10.10.50.6 está ativo, mas não apresenta serviços TCP acessíveis. Pode estar com os serviços desativados ou protegido por firewall. A identificação do sistema operacional não foi possível com precisão.