RELATÓRIO TÉCNICO – LAB SEGMENTAÇÃO DE REDE

Autor: Gonçalo Quissola Mateus Dala

Data: 24/07/2025 | Versão: 1.0

Sumário Executivo

Após realizada a análise da rede corporativa, composta por três sub-redes principais: corp_net, infra_net e guest_net. Foram identificados mais de 15 hosts ativos, com diversos serviços expostos, como FTP, LDAP, MySQL, SMB e HTTP e ZABBIX. Alguns serviços críticos estão acessíveis sem autenticação ou em redes sem segmentação adequada, outros ainda com permissões amplas ou desnecessárias, elevando o risco de ataques internos ou externos.

Principais recomendações:
- Isolamento de serviços sensíveis (ex: LDAP, MySQL)
- Fechamento de portas não utilizadas
- Reforço de segmentação entre redes (especialmente guest → infra)

- Revisão de serviços expostos e aplicação de políticas de controle de acesso.

Objetivo

Analisar a topologia e os serviços da rede simulada para identificar exposição riscos de segurança, falhas de segmentação e oportunidades de mitigação.

Escopo

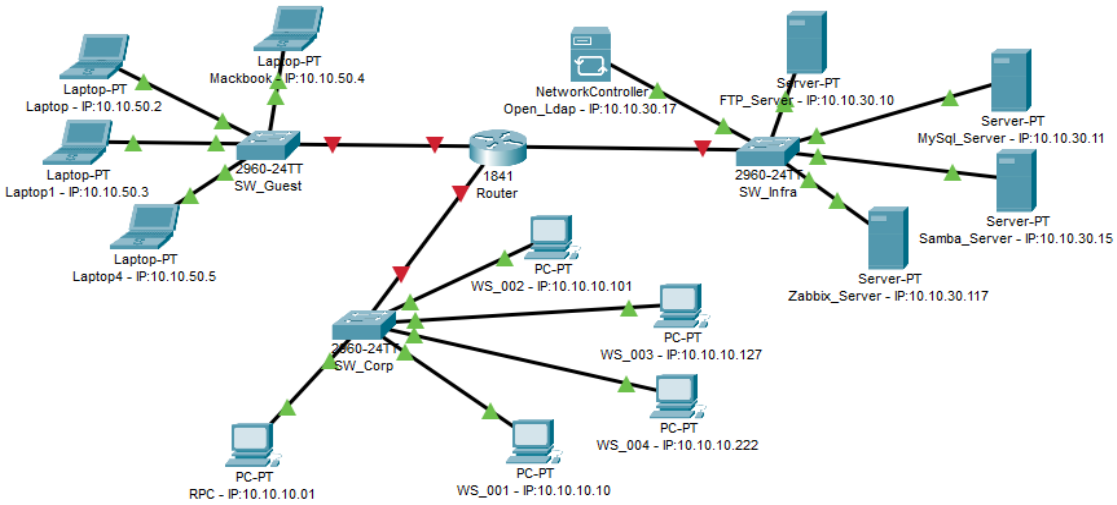
Ambiente Docker simulado com múltiplos dispositivos distribuídos entre três sub-redes:
- corp_net: 10.10.10.0/24
- infra_net: 10.10.30.0/24
- guest_net: 10.10.50.0/24

Metodologia

Ferramentas utilizadas:
- netdiscover, arp-scan: descoberta de hosts ativos
- nmap, rustscan: varredura de portas e serviços
- traceroute, dig, whois: coleta de dados complementares

Estratégia:
- Coleta ativa de dados
- Identificação de IPs e nomes de hosts
- Análise de serviços expostos
- Mapeamento de sub-redes
- Avaliação de riscos e recomendações

Diagrama de Rede



Diagnóstico (Achados)

10.10.30.10 - FTP Server - Porta 21
Risco: FTP sem autenticação pode expor arquivos sensíveis.
Evidência: Serviço FTP aberto detectado via Nmap.

10.10.30.11 - MySQL Server - Porta 3306
Risco: Banco de dados acessível via rede pode ser explorado se não protegido por firewall.
Evidência: Serviço MySQL 8.0.42 identificado com plugin de autenticação caching_sha2_password`.

10.10.30.15 - Samba Server - Porta 445
Risco: Compartilhamentos SMB podem ser abusados para movimentação lateral.
Evidência: Serviço SMB Microsoft-DS identificado.
10.10.30.17 - LDAP Server - Porta 389
Risco: Exposição de estrutura de diretório organizacional via LDAP.
Evidência: ldap-rootdse revela namingContexts e mecanismos de autenticação.

10.10.30.117 - Zabbix Server (Web)
Risco: Interface de monitoramento acessível na rede pode ser explorada se desatualizada.
Evidência: Página web do Zabbix acessível, evidenciada pelo HTML da interface de login.

10.10.10.1 - Serviço RPC - Porta 111
Risco: RPC pode ser usado para enumeração de serviços e ataques de negação.
Evidência: Porta 111 aberta identificada no `corp_net`.

Recomendações

- Desativar FTP anônimo no host `10.10.30.10`, substituindo por SFTP.
- Isolar sensíveis da rede guest, como FTP e LDAP atrás de firewall e autenticação forte.

- Auditar serviços ativos nas estações de trabalho WS_003
- Restringir o acesso à interface web do Zabbix a IPs autorizados.
- Fechar portas desnecessárias como 111 e 445 em servidores de produção.
- Reforçar segmentação de rede com VLANs e regras de firewall por função, firewall interno entre sub-redes

- Desativar portas RPC expostas em hosts internos (ex: porta 111), e serviços legados se possível

Plano de Ação (80/20)

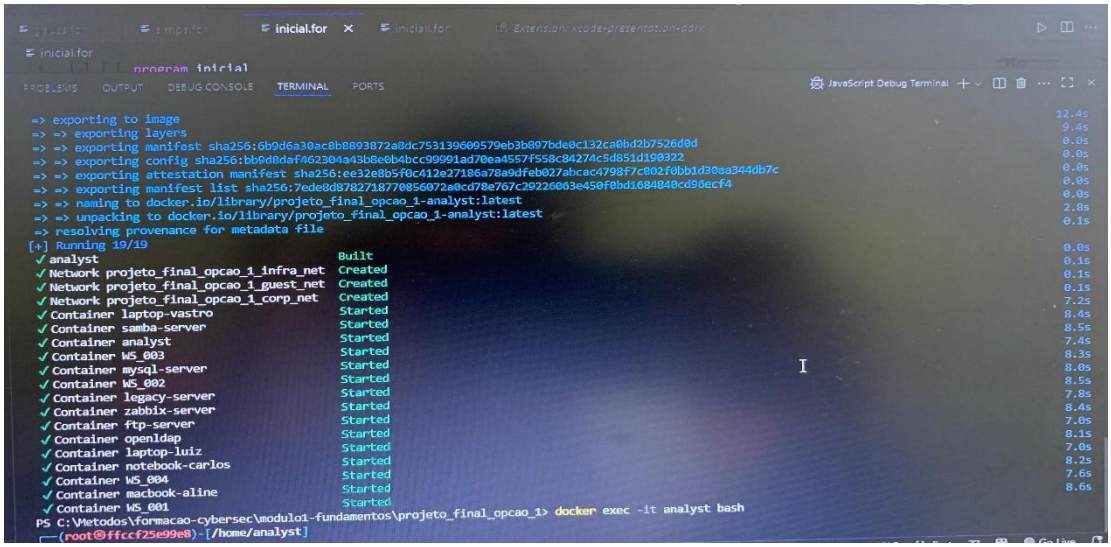
Ação	Impacto	Facilidade	Prioridade
Restringir acesso ao LDAP	Alto	Média	Alta
Desabilitar FTP ou usar SFTP	Alto	Alta	Alta
Proteger a interface do Zabbix	Médio	Alta	Alta
Fechar portas 445 e 111	Médio	Alta	Média
Auditar WS_003	Médio	Alta	Média
Bloquear guest → infra	Alto	Média	Alta
Aplicar firewall entre redes	Alto	Baixa	Média

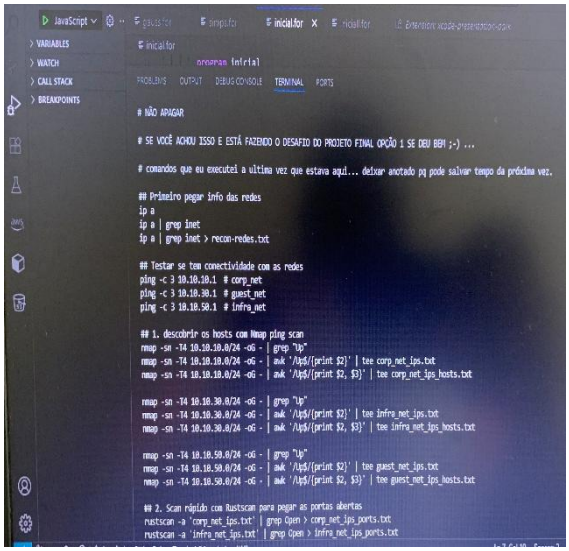
Conclusão

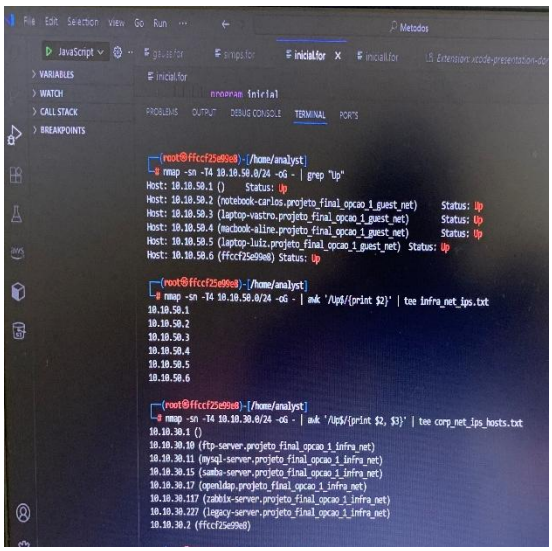
A análise demonstrou que, apesar da segmentação de rede inicial, vários serviços sensíveis e críticos e estão expostos de forma inadequada, em redes acessíveis publicamente. A ausência de filtragem entre redes permite que qualquer estação guest possa interagir com servidores de infraestrutura. A adoção de medidas como fechamento de portas, reforço de autenticação e aplicação de políticas de segmentação pode reduzir significativamente a superfície de ataque e melhorar a postura de segurança da rede, assim como a aplicação imediata do plano de ação proposto e reavaliação contínua da topologia.

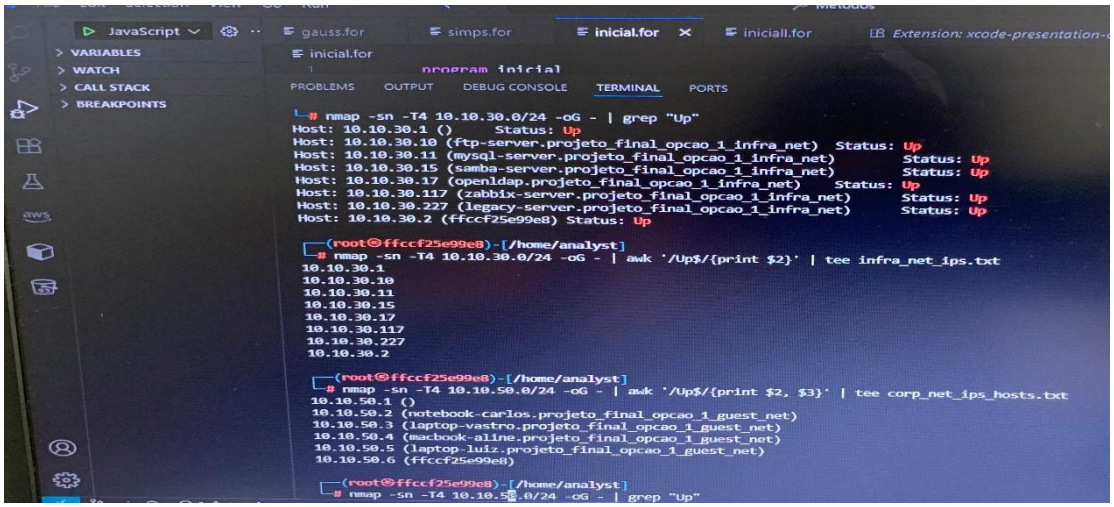
Anexos

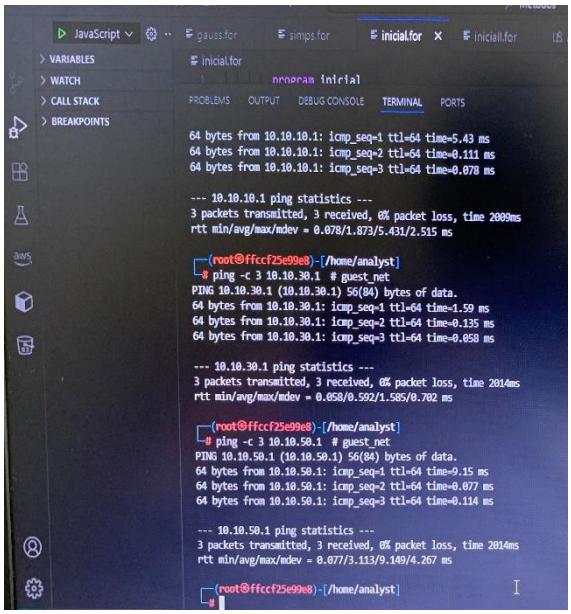
- Saída de Nmap: FTP, LDAP, MySQL, SMB, Zabbix
- Prints da interface do Zabbix
- Sigla, Terminologia



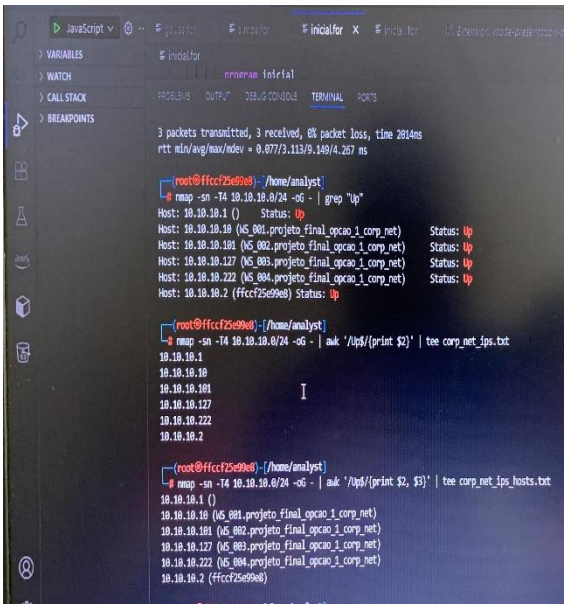




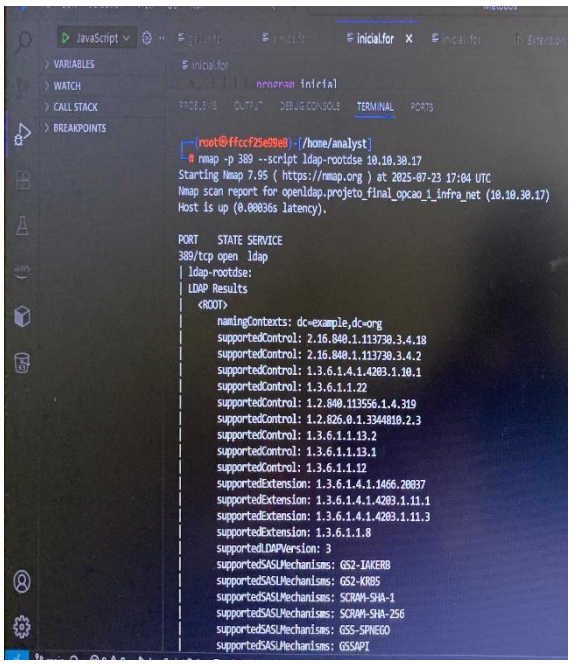




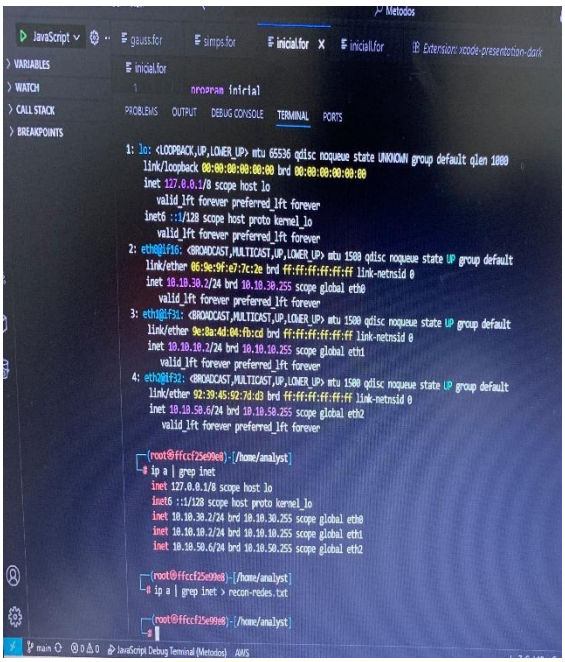
```
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=5.43 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.078 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.078/1.873/5.431/2.515 ms

┌──(root㉿ffccf25e99e8)-[/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=1.59 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.135 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.058 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.058/0.592/1.585/0.702 ms

┌──(root㉿ffccf25e99e8)-[/home/analyst]
└─# ping -c 3 10.10.50.1  # guest_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=9.15 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.077 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.114 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.077/3.113/9.149/4.267 ms

┌──(root㉿ffccf25e99e8)-[/home/analyst]
└─#
```



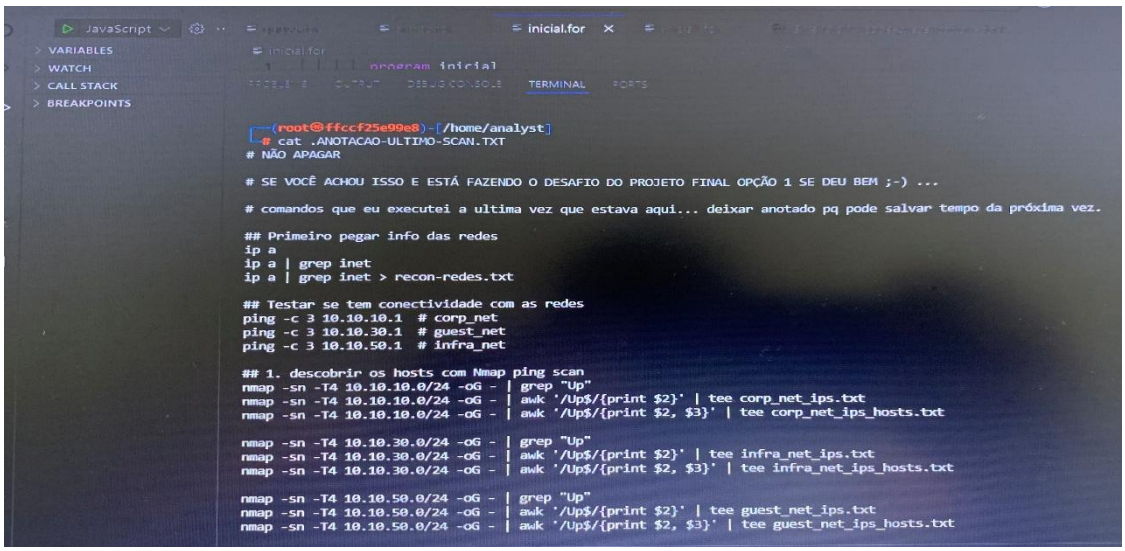
```
3 packets transmitted, 3 received, 0% packet loss, time 2014ms
rtt min/avg/max/mdev = 0.077/3.113/9.149/4.267 ms

┌──(root㉿ffccf25e99e8)-[/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 (W5_001.projeto_final_opcao_1_corp_net)       Status: Up
Host: 10.10.10.101 (W5_002.projeto_final_opcao_1_corp_net)      Status: Up
Host: 10.10.10.127 (W5_003.projeto_final_opcao_1_corp_net)      Status: Up
Host: 10.10.10.222 (W5_004.projeto_final_opcao_1_corp_net)      Status: Up
Host: 10.10.10.2 (ffccf25e99e8) Status: Up

┌──(root㉿ffccf25e99e8)-[/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㉿ffccf25e99e8)-[/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 (W5_001.projeto_final_opcao_1_corp_net)
10.10.10.101 (W5_002.projeto_final_opcao_1_corp_net)
10.10.10.127 (W5_003.projeto_final_opcao_1_corp_net)
10.10.10.222 (W5_004.projeto_final_opcao_1_corp_net)
10.10.10.2 (ffccf25e99e8)
```



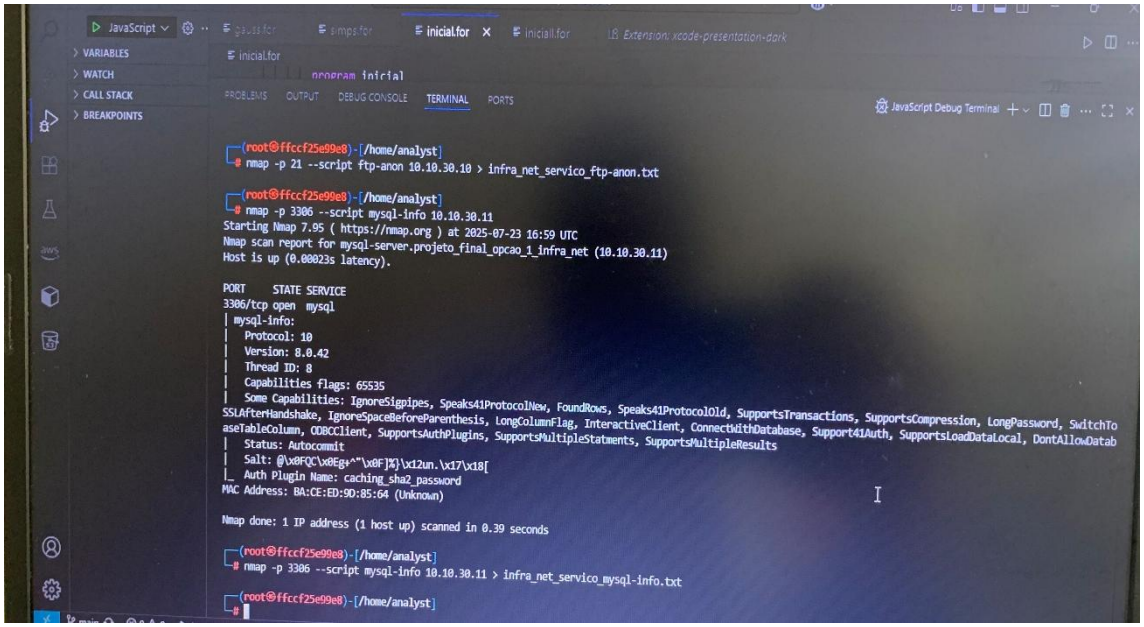
```
┌──(root㉿ffccf25e99e8)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 17:04 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00036s latency).

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-IAKERB
|       supportedSASLMechanisms: GS2-KRB5
|       supportedSASLMechanisms: SCRAM-SHA-1
|       supportedSASLMechanisms: SCRAM-SHA-256
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: GSSAPI
```

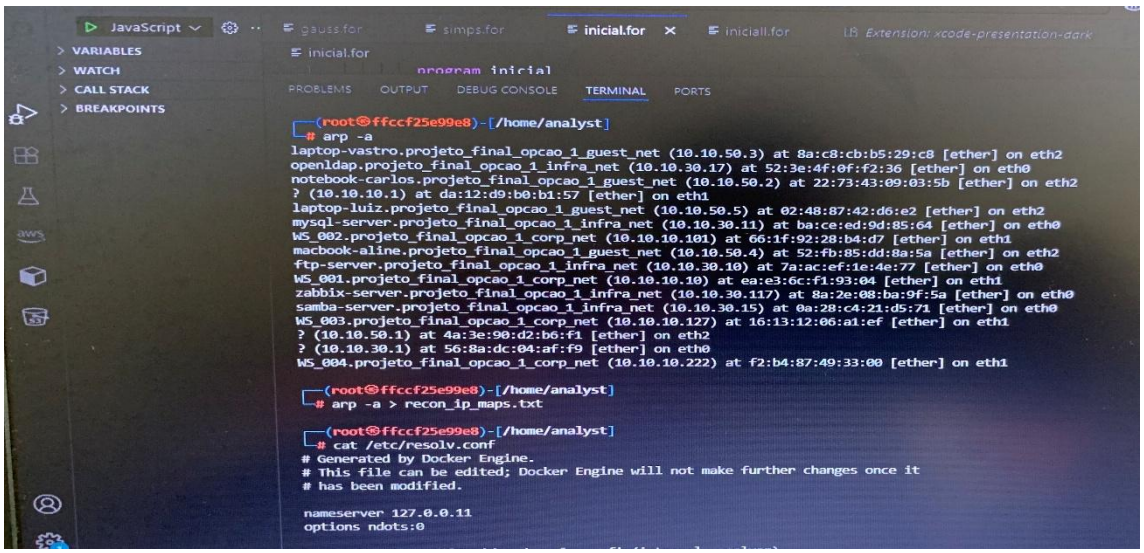


```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0@if16: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 06:9e:9f:e7:7c:2e 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@if31: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 9e:8a:4d:04:fb:cd 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@if32: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 92:39:45:92:7d:d3 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㉿ffccf25e99e8)-[/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㉿ffccf25e99e8)-[/home/analyst]
└─# ip a | grep inet > recon-redes.txt

┌──(root㉿ffccf25e99e8)-[/home/analyst]
└─#
```

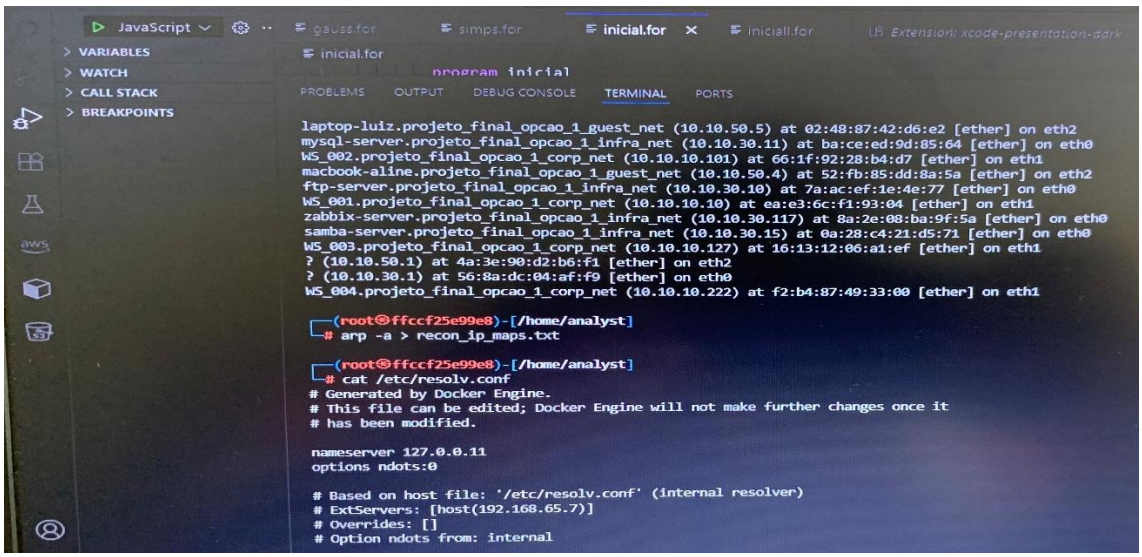


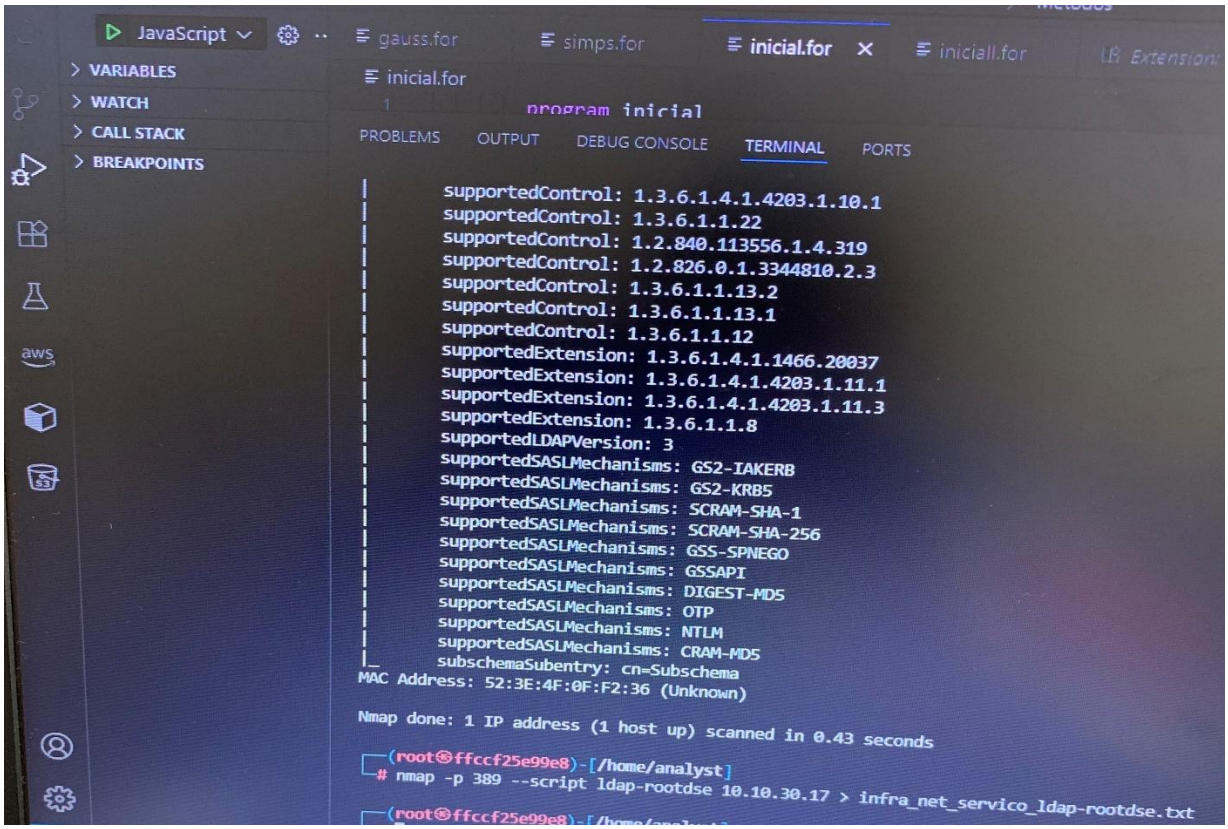
```
┌──(root㉿ffccf25e99e8)-[/home/analyst]
└─# cat .ANOTACAO-ULTIMO-SCAN.TXT
# NÃO APAGAR

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

# comandos que eu executei a ultima 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
```


JavaScript
VARIABLES
WATCH
CALL STACK
BREAKPOINTS
inicial.for
program inicial
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
JavaScript Debug Terminal
(root㉿ffccf25e99e8)-[/home/analyst]
nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
(root㉿ffccf25e99e8)-[/home/analyst]
nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 (https://nmap.org) at 2025-07-23 16:59 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.00023s latency).
PORT STATE SERVICE
3306/tcp open mysql
| mysql-info:
| Protocol: 10
| Version: 8.0.42
| Thread ID: 8
| Capabilities flags: 65535
| Some Capabilities: IgnoreSigpipes, Speaks41ProtocolNew, FoundRows, Speaks41ProtocolOld, SupportsTransactions, SupportsCompression, LongPassword, SwitchToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, LongColumnFlag, InteractiveClient, ConnectWithDatabase, Support41Auth, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, ODBCClient, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults
| Status: Autocommit
| Salt: @\x0FQC\x0Eg+^"\x0F]%}\x12un.\x17\x18[
|_ Auth Plugin Name: caching_sha2_password
MAC Address: BA:CE:ED:9D:85:64 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
(root㉿ffccf25e99e8)-[/home/analyst]
nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt
(root㉿ffccf25e99e8)-[/home/analyst]
#


JavaScript
VARIABLES
WATCH
CALL STACK
BREAKPOINTS
inicial.for
program inicial
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
(root㉿ffccf25e99e8)-[/home/analyst]
arp -a
laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.3) at 8a:c8:cb:b5:29:c8 [ether] on eth2
openldap.projeto_final_opcao_1_infra_net (10.10.30.17) at 52:3e:4f:0f:f2:36 [ether] on eth0
notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2) at 22:73:43:09:03:5b [ether] on eth2
? (10.10.10.1) at da:12:d9:b0:b1:57 [ether] on eth1
laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.5) at 02:48:87:42:d6:e2 [ether] on eth2
mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11) at ba:ce:ed:9d:85:64 [ether] on eth0
WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) at 66:1f:92:28:b4:d7 [ether] on eth1
macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4) at 52:fb:85:dd:8a:5a [ether] on eth2
ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10) at 7a:ac:ef:1e:4e:77 [ether] on eth0
WS_001.projeto_final_opcao_1_corp_net (10.10.10.10) at ea:e3:6c:f1:93:04 [ether] on eth1
zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117) at 8a:2e:08:ba:9f:5a [ether] on eth0
samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) at 0a:28:c4:21:d5:71 [ether] on eth0
WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) at 16:13:12:06:a1:ef [ether] on eth1
? (10.10.50.1) at 4a:3e:90:d2:b6:f1 [ether] on eth2
? (10.10.30.1) at 56:8a:dc:04:af:f9 [ether] on eth0
WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) at f2:b4:87:49:33:00 [ether] on eth1
(root㉿ffccf25e99e8)-[/home/analyst]
arp -a > recon_ip_maps.txt
(root㉿ffccf25e99e8)-[/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

]


JavaScript
VARIABLES
WATCH
CALL STACK
BREAKPOINTS
inicial.for
program inicial
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.5) at 02:48:87:42:d6:e2 [ether] on eth2
mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11) at ba:ce:ed:9d:85:64 [ether] on eth0
WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) at 66:1f:92:28:b4:d7 [ether] on eth1
macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4) at 52:fb:85:dd:8a:5a [ether] on eth2
ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10) at 7a:ac:ef:1e:4e:77 [ether] on eth0
WS_001.projeto_final_opcao_1_corp_net (10.10.10.10) at ea:e3:6c:f1:93:04 [ether] on eth1
zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117) at 8a:2e:08:ba:9f:5a [ether] on eth0
samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) at 0a:28:c4:21:d5:71 [ether] on eth0
WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) at 16:13:12:06:a1:ef [ether] on eth1
? (10.10.50.1) at 4a:3e:90:d2:b6:f1 [ether] on eth2
? (10.10.30.1) at 56:8a:dc:04:af:f9 [ether] on eth0
WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) at f2:b4:87:49:33:00 [ether] on eth1
(root㉿ffccf25e99e8)-[/home/analyst]
arp -a > recon_ip_maps.txt
(root㉿ffccf25e99e8)-[/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



Sigla / Termo	Significado
Autocommit	Modo em que alterações no banco de dados são automaticamente confirmadas.
caching_sha2_password	Plugin de autenticação usado em MySQL para criptografar senhas.
Firewall	Sistema que controla o tráfego de entrada e saída em uma rede.
FTP	File Transfer Protocol – Protocolo de transferência de arquivos.
Host	Equipamento (servidor, computador, etc.) conectado à rede.
Interface Web	Página acessada via navegador para administrar serviços.
LDAP	Lightweight Directory Access Protocol – Protocolo para diretórios organizacionais.
MySQL	Sistema de gerenciamento de banco de dados relacional (RDBMS).
Netdiscover	Ferramenta de detecção de dispositivos ativos na rede. (ARP)
Nmap	Network Mapper – Ferramenta de varredura e descoberta de redes.
Ping	Ferramenta de teste de conectividade baseada em ICMP.
RootDSE	Entry especial em servidores LDAP contendo informações básicas da estrutura.
RPC	Remote Procedure Call – Chamada de procedimento remoto entre sistemas.
Rustscan	Scanner de portas rápido e eficiente baseado em Rust.
Segmentação de Rede	Divisão da rede em sub-redes para segurança e performance.
SFTP -	Secure File Transfer Protocol – Variante segura do FTP com criptografia.
SMB	Server Message Block – Protocolo de compartilhamento de arquivos e impressoras.
VLAN	Virtual LAN – Segmentação lógica de redes dentro de uma infraestrutura física.
Zabbix	Ferramenta de monitoramento de redes, servidores e aplicações.