MODELO DE RELATÓRIO TÉCNICO – LAB SEGMENTAÇÃO DE REDE

Aluno(a): Pâmela Daniele Pereira Costa
Data: 28/07/2025
Versão: 1.0

OBJETIVO

Analisar a rede simulada para identificar exposição de ativos, falhas na segmentação de rede e riscos operacionais que possam comprometer a segurança da organização.

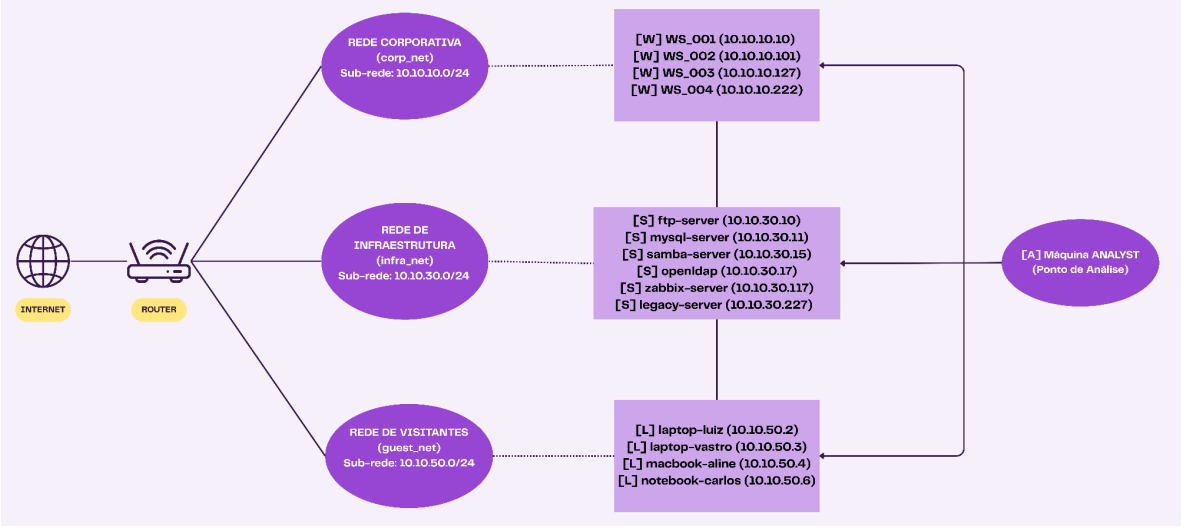
ESCOPO

O escopo da análise compreende o ambiente Docker simulado com seus múltiplos hosts e as seguintes redes segmentadas: *corp_net (10.10.10.0/24), infra_net (10.10.30.0/24) e guest_net (10.10.50.0/24).*

METODOLOGIA

- Ferramentas: *nmap* para descoberta de hosts e enumeração de serviços; *arp-scan* para validação de ativos.
- Técnicas: Descoberta de hosts ativos em cada sub-rede; Varredura completa de portas para cada host; Identificação de versões de serviços (Banners) e uso de scripts padrão do Nmap (-sC); Análise manual e documentada

DIAGRAMA DE REDE



DIAGNÓSTICO (ACHADOS)

As ferramentas confirmaram o mesmo conjunto de hosts ativos. A seguir uma tabela do inventário de ativos descobertos:

Rede	IP do Ativo	Nome Identificado
corp_net	10.10.10.10	WS_001
	10.10.10.101	WS_002
	10.10.10.127	WS_003
	10.10.10.222	WS_004
infra_net	10.10.30.10	ftp-server
	10.10.30.11	mysql-server
	10.10.30.15	samba-server
	10.10.30.17	openldap.projeto
	10.10.30.117	zabbix-server
	10.10.30.227	legacy-server
guest_net	10.10.50.2	laptop-luiz
	10.10.50.3	laptop-vastro
	10.10.50.4	macbook-aline
	10.10.50.6	notebook-carlos

Achado 1: Falha na segmentação da rede

[Host/IP] - [Serviço] - [Porta]: Todos os hosts da infra_net - Múltiplos - Múltiplas

Risco: A ausência de isolamento entre as redes permite que um atacante com acesso a uma rede de baixo privilégio, os “visitantes”, possam se comunicar e atacar diretamente os servidores mais críticos da empresa, anulando o propósito da segmentação.

Evidência (scan output): A capacidade de executar com sucesso os scans nmap e arp-scan nos alvos da infra_net (10.10.30.0/24) a partir da máquina analyst é uma evidência da falha que foi encontrada.

Achado 2: Servidor de autenticação desatualizado

[Host/IP] - [Serviço] - [Porta]: openldap (10.10.30.17) - ldap - 389/tcp

Risco: O servidor executa uma versão do OpenLDAP (2.2.X - 2.3.X) com mais de 15 anos, e este possui múltiplas vulnerabilidades públicas conhecidas. Isso pode

levar ao roubo de credenciais, senhas e comprometimento total do sistema de autenticação da empresa.

Evidência (scan output):

```
# Nmap 7.95 scan initiated Tue Jul 29 00:18:57 2025 as: /usr/lib/nmap/nmap -sV
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.0000050s latency).
Not shown: 65533 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: 36:1D:36:6D:5C:7A (Unknown)
```

Achado 3: Exposição de Banco de Dados

[Host/IP] - [Serviço] - [Porta]: mysql-server (10.10.30.11) - mysql - 3306/tcp

Risco: O acesso direto ao servidor de banco de dados a partir de redes não autorizadas aumenta o risco de vazamento de dados e de ataques de força bruta.

Evidência (scan output):

```
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.0000050s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql   MySQL 8.0.43
```

Achado 4: O uso de protocolo inseguro para transferência de arquivos

[Host/IP] - [Serviço] - [Porta]: ftp-server (10.10.30.10) - ftp - 21/tcp

Risco: O protocolo FTP transmite credenciais e dados em texto claro (sem criptografia), o que permite que um atacante na mesma rede capture facilmente as senhas de acesso com um ataque de "sniffing".

Evidência (scan output):

```
# Nmap 7.95 scan initiated Tue Jul 29 00:18:03 2025 as: /usr/lib/nmap/nmap -sV
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.0000050s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd
MAC Address: 0A:3B:D3:7C:52:B5 (Unknown)
```

Achado 5: Configuração de risco em servidor de arquivos

[Host/IP] - [Serviço] - [Porta]: samba-server (10.10.30.15) - netbios-ssn - 139/tcp, 445/tcp

Risco: O serviço de compartilhamento de arquivos Samba não exige assinatura de mensagens (Message signing enabled but not required). Isso torna a comunicação

vulnerável a ataques onde um atacante pode interceptar e modificar os dados em trânsito.

Evidência (scan output):

```
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-29T00:18:50
|_  start_date: N/A
```

RECOMENDAÇÕES

Implementar segmentação de rede efetiva: Criar regras de firewall (ACLs) para bloquear todo o tráfego entre as sub-redes por padrão, permitindo apenas as comunicações estritamente necessárias e autorizadas.

Atualizar o servidor OpenLDAP: Dada a idade crítica do software, o servidor openldap deve ser atualizado para uma versão recente e com suporte ou ser substituído. O acesso ao serviço deve ser restrito.

Restringir acesso ao banco de dados: O acesso ao mysql-server na porta 3306 deve ser limitado apenas aos IPs dos servidores de aplicação que necessitam se conectar a ele.

Desativar o servidor FTP: O protocolo FTP deve ser desativado e substituído por uma alternativa segura, como SFTP (que opera sobre SSH na porta 22).

Fortalecer a configuração do samba: A assinatura de mensagens (SMB signing) deve ser configurada como "obrigatória" no servidor samba-server para prevenir ataques MitM.

PLANO DE AÇÃO BASEADO EM IMPACTO E FACILIDADE

A tabela a seguir mostra as seguintes recomendações:

Ação Corretiva	Impacto na Segurança	Facilidade de Implementação	Prioridade
Isolar a infra_net com regras de firewall	Crítico	Média	Crítica
Atualizar ou desativar o servidor OpenLDAP	Crítico	Difícil	Crítica
Restringir acesso de rede ao mysql-server	Alto	Média	Alta
Substituir FTP por SFTP e restringir acesso	Alto	Média	Alta
Exigir assinatura de pacotes no Samba	Médio	Alta	Média

CONCLUSÃO

Portanto, essa análise de segurança conclui que a rede da organização possui uma postura de segurança deficiente. As falhas de segmentação e a presença de software criticamente desatualizado criam um risco para o comprometimento de dados e dos sistemas. A implementação das ações corretivas citadas anteriormente, é fundamental e necessária para proteger os ativos da organização.