

Relatório Técnico - Lab. de Segmentação de Rede

Autor: Douglas Corrêa

Data: 28/07/2025

Sumário Executivo

A rede simulada de escritório é composta por três sub-redes (Corporativa, Convidados e Infraestrutura) interconectadas, totalizando 20 ativos identificados, incluindo estações de trabalho e servidores de infraestrutura crítica como FTP, MySQL, Samba, LDAP e Zabbix. As varreduras revelaram a exposição de serviços essenciais e, mais preocupante, a possível permissão de **login anônimo em um servidor de transferência de arquivos (FTP)**, a operação de uma versão **desatualizada da Plataforma de monitoramento da rede(Zabbix)** e a presença de um **servidor legado** não identificado. As recomendações focam na redução das vulnerabilidades desses serviços críticos e na investigação de portas desconhecidas para mitigar os riscos de maior impacto com agilidade.

Objetivo

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

Escopo

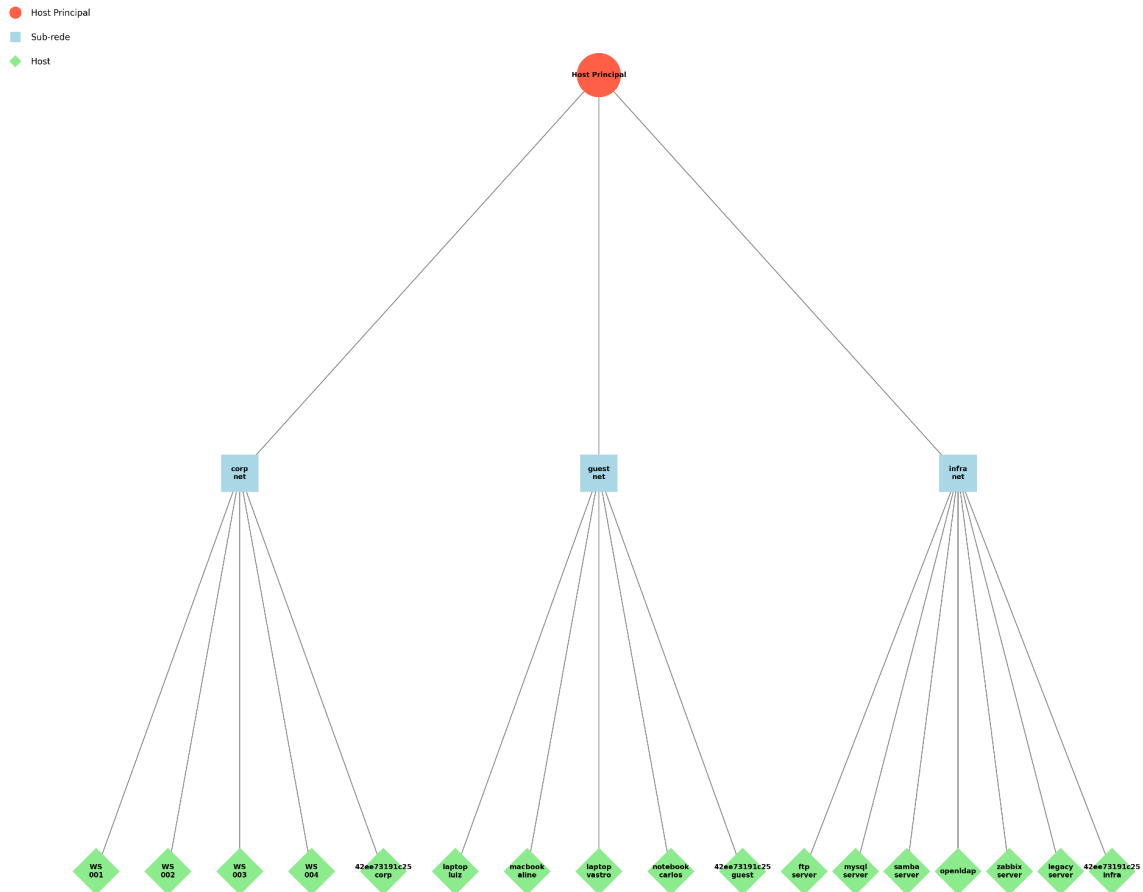
Ambiente docker simulado com múltiplos hosts e redes segmentadas:

- **Rede Corporativa:** 10.10.10.0/24
- **Rede de Convidados:** 10.10.50.0/24
- **Rede de Infraestrutura:** 10.10.30.0/24

Metodologia

- Ferramentas: ip, ping, rustscan, nmap, arp
- Coleta ativa de dados de rede
- Análise manual e documentada

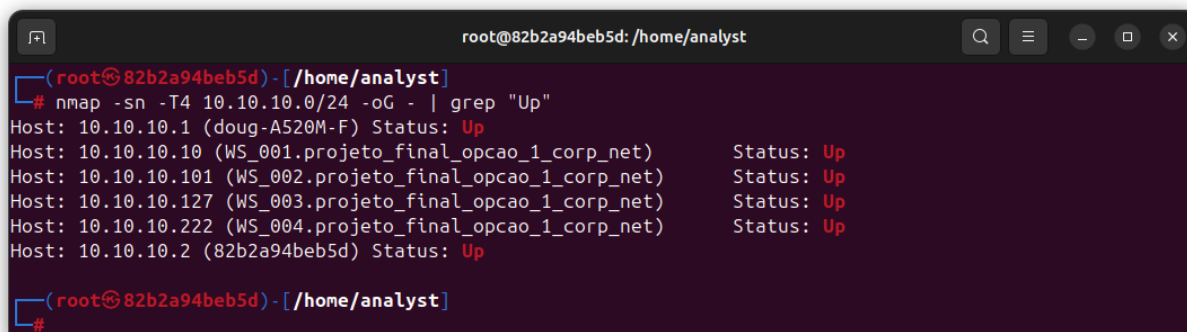
Diagrama de Rede



Diagnóstico (Achados)

No total, foram encontradas 3 subredes, sendo que a rede corporativa e a de convidados contém 6 hosts cada uma, e a rede de infraestrutura contém 8.

Rede Corporativa (10.10.10.0/24)

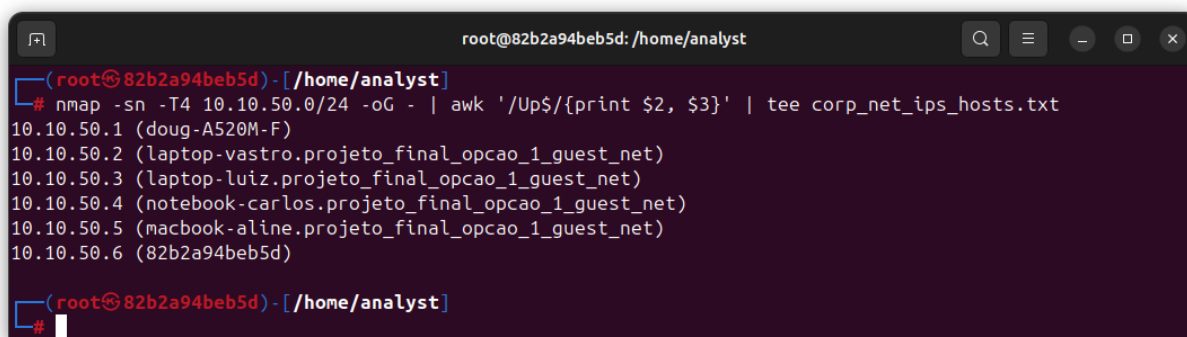


```
root@82b2a94beb5d: /home/analyst
# nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
Host: 10.10.10.1 (doug-A520M-F) Status: Up
Host: 10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.2 (82b2a94beb5d) Status: Up
```

- **10.10.10.1 (Main Host)** - HTTP, HTTP alternativo, HTTPS alternativo - Portas: 80, 8000, 9443
 - Sistema Operacional Estimado: Linux (baseado no hostname, comumente uma estação de trabalho ou um gateway/router)
 - Risco identificado: Exposição de serviços web sem contexto claro. Necessidade de verificar propósito e segurança (ex: uso de HTTPS).
 - Evidência: *Open 10.10.10.1:80, Open 10.10.10.1:8000, Open 10.10.10.1:9443*
- **10.10.10.2 (42ee73191c25)** - Gateway Docker - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Linux (provavelmente o host Docker, pela MAC address "42ee73191c25" que indica um contêiner ou o bridge Docker)
 - Risco identificado: N/A. Atua como gateway da sub-rede.
 - Evidência: *inet 10.10.10.2/24 brd 10.10.10.255 scope global eth0*
- **10.10.10.10 (WS_001)** - Estação de trabalho - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Windows (Workstation)
 - Risco identificado: N/A. (Bom sinal para estação de trabalho).
 - Evidência: *10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net)*
- **10.10.10.101 (WS_002)** - Estação de trabalho - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Windows (Workstation)
 - Risco identificado: N/A.
 - Evidência: *10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net)*

- **10.10.10.127 (WS_003)** - Estação de trabalho - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Windows
 - Risco identificado: N/A.
 - Evidência: *10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net)*
- **10.10.10.222 (WS_004)** - Estação de trabalho - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Windows
 - Risco identificado: N/A.
 - Evidência: *10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net)*

Rede de Convidados (10.10.50.0/24)



```

root@82b2a94beb5d: /home/analyst
# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/[print $2, $3]' | tee corp_net_ips_hosts.txt
10.10.50.1 (doug-A520M-F)
10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.3 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.4 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.5 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.6 (82b2a94beb5d)
#
  
```

- **10.10.50.1 (Main Host)** - HTTP, HTTP alternativo, HTTPS alternativo - Portas: 80, 8000, 9443
 - Sistema Operacional Estimado: Linux
 - Risco identificado: Mesmas preocupações que na rede corporativa; serviços web expostos.
 - Evidência: *Open 10.10.50.1:80, Open 10.10.50.1:8000, Open 10.10.50.1:9443*
- **10.10.50.2 (laptop-luiz)** - Laptop - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Desconhecido
 - Risco identificado: N/A.
 - Evidência: *10.10.50.2 (laptop-luiz.projeto_final_opcao_1_guest_net)*

- **10.10.50.3 (macbook-aline)** - Macbook - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: macOS (Macbook)
 - Risco identificado: N/A.
 - Evidência: *10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)*
- **10.10.50.4 (laptop-vastro)** - Laptop - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Desconhecido
 - Risco identificado: N/A.
 - Evidência: *10.10.50.4 (laptop-vastro.projeto_final_opcao_1_guest_net)*
- **10.10.50.5 (notebook-carlos)** - Notebook - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Desconhecido
 - Risco identificado: N/A.
 - Evidência: *10.10.50.5 (notebook-carlos.projeto_final_opcao_1_guest_net)*
- **10.10.50.6 (42ee73191c25)** - Gateway Docker - Porta: 51200
 - Sistema Operacional Estimado: Linux
 - Risco identificado: Porta de serviço desconhecido exposta no gateway da rede de convidados.
 - Evidência: *inet 10.10.50.6/24 brd 10.10.50.255 scope global eth1, Open 10.10.50.6:51200*

Rede de Infraestrutura (10.10.30.0/24)

```

root@82b2a94beb5d: /home/analyst
(root@82b2a94beb5d) - [ /home/analyst ]
# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.txt
10.10.30.1 (doug-A520M-F)
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 (82b2a94beb5d)

```

- **10.10.30.1 (Main Host)** - HTTP, HTTP alternativo, HTTPS alternativo - Portas: 80, 8000, 9443
 - Sistema Operacional Estimado: Linux
 - Risco identificado: Mesmas preocupações com serviços web expostos.
 - Evidência: *Open 10.10.30.1:80, Open 10.10.30.1:8000, Open 10.10.30.1:9443*
- **10.10.30.2 (42ee73191c25)** - Gateway Docker - Porta: 51032
 - Sistema Operacional Estimado: Linux
 - Risco identificado: Porta de serviço desconhecido exposta no gateway da rede de infraestrutura.
 - Evidência: *inet 10.10.30.2/24 brd 10.10.30.255 scope global eth2, Open 10.10.30.2:51032*
- **10.10.30.10 (ftp-server)** - FTP - Porta: 21
 - Sistema Operacional Estimado: Linux (servidor FTP)
 - Risco identificado: Alta probabilidade de **login FTP anônimo permitido**, o que pode levar a acesso não autorizado a dados ou upload de arquivos maliciosos.
 - Evidência: *21/tcp open ftp*
- **10.10.30.11 (mysql-server)** - MySQL - Portas: 3306, 33060
 - Sistema Operacional Estimado: Linux (servidor MySQL)
 - Risco identificado: Servidor de banco de dados crítico com versão 8.0.43. Potencial para vulnerabilidades se não estiver com patches atualizados ou configurações de autenticação fracas. Contém dados sensíveis.
 - Evidência: *3306/tcp open mysql, 33060/tcp open mysql, Version: 8.0.43, Auth Plugin Name: caching_sha2_password.*
- **10.10.30.15 (samba-server)** - SMB - Portas: 139, 445
 - Sistema Operacional Estimado: Linux (servidor Samba)
 - Risco identificado: Potencial para compartilhamentos SMB acessíveis sem autenticação forte, permitindo enumeração de usuários, acesso a arquivos ou movimento lateral.
 - Evidência: *139/tcp open netbios-ssn, 445/tcp open microsoft-ds.*
- **10.10.30.17 (openldap)** - LDAP, LDAPS - Portas: 389, 636
 - Sistema Operacional Estimado: Linux (servidor OpenLDAP)
 - Risco identificado: Servidor de diretório que armazena informações críticas de autenticação. A segurança depende da configuração e força das autenticações suportadas.
 - Evidência: *389/tcp open ldap, 636/tcp open ldaps, ldap-rootdse script.*

- **10.10.30.117 (zabbix-server)** - HTTP, Zabbix Agent, Zabbix Trapper - Portas: 80, 10051, 10052
 - Sistema Operacional Estimado: Linux (servidor Zabbix)
 - Risco identificado: **Interface web do Zabbix exposta via HTTP (porta 80)** e versão potencialmente desatualizada, o que pode conter vulnerabilidades conhecidas e permitir acesso não autorizado a dados de monitoramento críticos.
 - Evidência: *Open 10.10.30.117:80, Open 10.10.30.117:10051, Open 10.10.30.117:10052, HTML com "Zabbix docker", "© 2001–2020, Zabbix SIA".*
- **10.10.30.227 (legacy-server)** - Servidor Legado - Nenhuma porta aberta explicitamente listada.
 - Sistema Operacional Estimado: Desconhecido (servidor legado)
 - Risco identificado: O nome "legacy-server" sugere que pode estar executando um sistema operacional ou software desatualizado.. Alto risco, mesmo sem portas abertas visíveis.
 - Evidência: 10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)

Recomendações

- **Servidores Web (Main Host nas 3 redes):**
 - Verificar a finalidade dos serviços HTTP/HTTPS nas portas 80, 8000 e 9443. Se forem interfaces de gerenciamento, garantir que o acesso seja restrito a IPs autorizados e que o uso de **HTTPS** seja forçado, com certificados válidos.
- **ftp-server (10.10.30.10):**
 - **Desabilitar ou restringir severamente o login FTP anônimo.** Se necessário, configurar um diretório de upload/download isolado com permissões mínimas (ex: somente escrita para upload).
- **mysql-server (10.10.30.11):**
 - Garantir que a versão 8.0.43 do MySQL esteja com **todos os patches de segurança aplicados.**
 - Implementar **políticas de senhas fortes** para todas as contas de banco de dados.
 - Configurar o firewall do host para permitir conexões ao MySQL **apenas de IPs autorizados** (ex: servidor Zabbix, aplicações específicas).

- **samba-server (10.10.30.15):**
 - Auditar e **restringir as permissões dos compartilhamentos SMB**, removendo acessos anônimos ou de convidado.
 - Forçar a **autenticação forte** para todos os acessos aos compartilhamentos.
- **openldap (10.10.30.17):**
 - Sempre que possível, configurar aplicações e clientes para utilizar **LDAPS (porta 636)** para proteger o tráfego de credenciais e dados.
 - Implementar políticas de senhas complexas para contas LDAP.
- **zabbix-server (10.10.30.117):**
 - **Atualizar o servidor Zabbix para a versão mais recente e suportada.** Versões de 2020 são consideravelmente desatualizadas.
 - **Redirecionar todo o tráfego da porta 80 para HTTPS (porta 443)** para proteger as credenciais de login e os dados de monitoramento.
 - Implementar **políticas de senhas fortes** e considerar autenticação de dois fatores (MFA) se o Zabbix for acessível remotamente.
- **legacy-server (10.10.30.227):**
 - Realizar uma **avaliação de risco aprofundada** para determinar a criticidade dos serviços e dados.
 - Priorizar a **migração** dos serviços e dados para uma plataforma moderna e suportada.
 - Enquanto não migrado, **isolar o servidor em uma VLAN separada** com regras de firewall restritivas, permitindo apenas o tráfego estritamente essencial.
- **Portas Desconhecidas (10.10.50.6:51200, 10.10.30.2:51032):**
 - **Investigar a origem e a finalidade desses serviços.** Identificar o processo que está ouvindo nessas portas.
 - Se não forem essenciais para a operação do laboratório, **fechá-las (firewall) ou desabilitar os serviços** associados para reduzir a superfície de ataque.

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Desabilitar/Restringir FTP Anônimo (10.10.30.10)	Alto	Alta	Alta
Atualizar Zabbix (10.10.30.117)	Alto	Média	Alta
Investigar e Bloquear Portas Desconhecidas (51200, 51032)	Alto	Média	Alta
Auditoria Rápida SMB (10.10.30.15)	Médio	Média	Média
Isolar/Migrar Legacy Server (10.10.30.227)	Alto	Média	Média
Forçar HTTPS no Zabbix (10.10.30.117)	Médio	Média	Média
Hardening do MySQL (10.10.30.11)	Alto	Média	Média

Conclusão

A rede simulada apresenta uma arquitetura segmentada, o que é um bom ponto de partida para a segurança. No entanto, a presença de serviços desatualizados ou com configurações subótimas, como o FTP anônimo e o Zabbix antigo, e a existência de um "legacy server", introduzem riscos significativos. Focar no plano de ação 80/20 permitirá uma melhoria substancial na postura de segurança do ambiente com um esforço concentrado. Os próximos passos devem incluir a execução das ações prioritárias, seguidas por varreduras de vulnerabilidades mais aprofundadas e testes de penetração para validar a eficácia das mitigações implementadas.

Anexos

Scans da rede corporativa:

https://github.com/doougg26/desafio_final_cybersec-mod1/tree/ba1a45256c51aac5ffa5b923f5c7784bd352be1/corp_net

Scans da rede convidados:

https://github.com/doougg26/desafio_final_cybersec-mod1/tree/ba1a45256c51aac5ffa5b923f5c7784bd352be1/guest_net

Scans da rede de infraestrutura:

https://github.com/doougg26/desafio_final_cybersec-mod1/tree/ba1a45256c51aac5ffa5b923f5c7784bd352be1/infra_net

Registro de reconhecimento de redes:

https://github.com/doougg26/desafio_final_cybersec-mod1/blob/ba1a45256c51aac5ffa5b923f5c7784bd352be1/recon-redes.txt

Registro de mapeamento de ips:

https://github.com/doougg26/desafio_final_cybersec-mod1/blob/ba1a45256c51aac5ffa5b923f5c7784bd352be1/recon_ip_maps.txt

Diagrama de redes:

https://github.com/doougg26/desafio_final_cybersec-mod1/blob/b380f3e6257d7f8a32d653d10ab465a4c2702ba6/diagrama%20de%20rede.png