CYBERSECURITY REPORT

Relatório Técnico – Lab Segmentação de Rede

Autor: Marlon Souto

Data: 28/07/2025

Versão: 1.0

Sumário Executivo

Durante o reconhecimento da rede simulada via Docker, foi possível identificar dispositivos em diferentes sub-redes, serviços expostos e possíveis riscos de segurança. A análise se concentrou em entender como os hosts estão organizados, quais serviços estão acessíveis e onde há falhas de configuração, como o uso de portas abertas sem necessidade clara ou acessos anônimos. Algumas evidências sugerem riscos potenciais que podem ser explorados por agentes maliciosos, exigindo atenção imediata.

Objetivo

Mapear os dispositivos da rede, identificando IPs, portas abertas, serviços ativos e potenciais vulnerabilidades. Avaliar falhas de segmentação e riscos de exposição indevida de serviços.

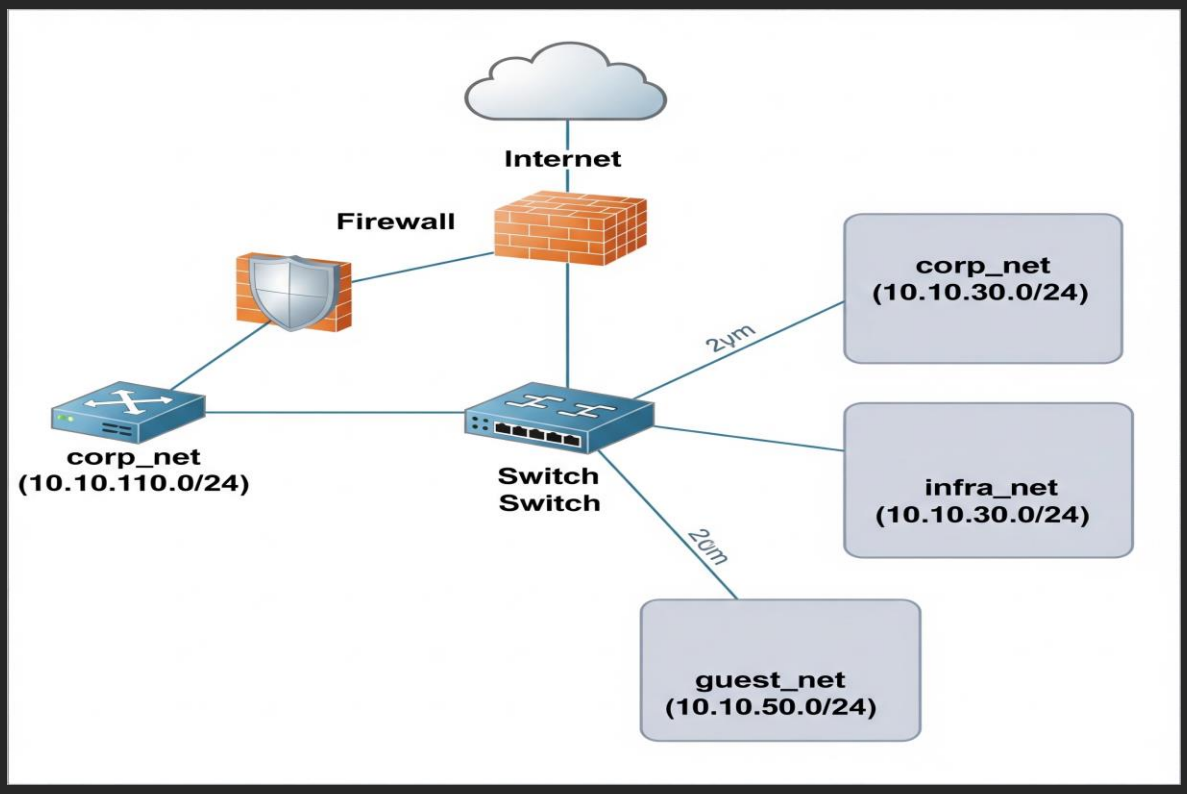
Escopo

Ambiente Docker com múltiplos contêineres em sub-redes diferentes (ex: 10.10.10.0/24, 10.10.30.0/24). As análises foram feitas diretamente de dentro dos contêineres e também da máquina host local.

Metodologia

- Ferramentas: nmap, rustscan, netdiscover, ping
- Coleta ativa e passiva
- Coleta de evidências com comandos como ls -la e docker cp
- Comparação de resposta entre diferentes sub-redes
- Investigação de arquivos sensíveis e permissões

Diagrama de Rede



Diagnóstico (Achados)

Host: 10.10.10.3

- Serviço: SSH
- Porta: 22/tcp
- Risco: Possível login com credenciais fracas ou sem autenticação forte
- Evidência: Porta detectada com nmap -sS

- Serviço: MySQL
- Porta: 3306/tcp
- Risco: Banco de dados exposto a rede externa
- Evidência: Acessível via traceroute -p 3306

- Serviço: FTP
- Porta: 21/tcp
- Risco: Permite login anônimo
- Evidência: Confirmado manualmente

Por meio desse diagnostico é possivel visualizar serviços e portas abertas que representam riscos potenciais. Foram identificados os seguintes serviços críticos: SSH (porta 22/tcp), com risco de login com credenciais fracas ou sem autenticação forte, evidenciado por detecção via ferramenta nmap. O serviço MySQL (porta 3306/tcp) foi detectado como um banco de dados exposto à rede externa, com evidência de acessibilidade via traceroute -p 3306. Por fim, o serviço FTP (porta 21/tcp) também foi identificado evidenciando assim um risco aos serviços e portas.

Inventário

IP	Hostname	SO estimado	Portas abertas (exemplos)	Serviços (exemplos)	Notas
10.10.50.4	notebook-carlos.projeto_final_opcao_1_guest_net	Provável Windows/Linux (notebook)	Nenhuma porta TCP aberta detectada	Firewall bloqueando?	Host up, sem portas TCP abertas visíveis
10.10.30.10	ftp-server.projeto_final_opcao_1_infra_net	Provável Linux/Unix (servidor FTP)	21 (FTP)	FTP anônimo?	Possível FTP com login anônimo
10.10.30.17	openldap.projeto_final_opcao_1_infra_net	Linux/Unix (LDAP)	389 (LDAP), 636 (LDAPS)	Serviço LDAP	Possível serviço LDAP seguro (porta 636)
10.10.50.3	macbook-aline.projeto_final_opcao_1_guest_net	macOS (MacBook)	A definir	A definir	Cliente rede guest_net
10.10.30.117	zabbix-server.projeto_final_opcao_1_infra_net	Linux (Zabbix Docker)	80 (HTTP), 10051, 10052 (Zabbix)	Monitoramento Zabbix	Interface web Zabbix acessível
10.10.10.10	WS_001.projeto_final_opcao_1_corp_net	Provável Windows (Workstation)	A definir	A definir	Usuário corp_net
10.10.30.1	ideapad-lo	Provável laptop Lenovo	A definir	A definir	Gateway ou roteador da infra_net?
10.10.10.222	WS_004.projeto_final_opcao_1_corp_net	Provável Windows	A definir	A definir	Usuário corp_net

10.10.50.2	laptop-luiz.projeto_final_opcao_1_guest_net	Provável Windows/Linux	A definir	A definir	Cliente guest_net
10.10.30.227	legacy-server.projeto_final_opcao_1_infra_net	Provável Linux/Unix	A definir	A definir	Servidor legado infra_net
10.10.30.15	samba-server.projeto_final_opcao_1_infra_net	Linux/Unix	445 (SMB)	Samba compartilhamento de arquivos	Possível compartilhamento SMB
10.10.50.5	laptop-vastro.projeto_final_opcao_1_guest_net	Cliente guest_net	A definir	A definir	Cliente guest_net
10.10.30.11	mysql-server.projeto_final_opcao_1_infra_net	Linux (MySQL)	3306, 33060 (MySQL)	Banco de dados MySQL	Servidor DB MySQL ativo
10.10.10.101	WS_002.projeto_final_opcao_1_corp_net	Provável Windows	A definir	A definir	Usuário corp_net
10.10.10.127	WS_003.projeto_final_opcao_1_corp_net	Provável Windows	A definir	A definir	Usuário corp_net

Recomendações

- Desabilitar FTP anônimo ou restringir a usuários específicos com autenticação forte.
- Fechar a porta 3306 na rede pública se não for necessária externamente.
- Monitorar o acesso SSH e aplicar autenticação com chave pública.

A exposição de serviços como FTP, MySQL e SSH sem as devidas configurações de segurança representa uma ameaça real à integridade de sistemas em rede. Em um cenário onde ataques automatizados são frequentes, a adoção de boas práticas de segurança é essencial.

O uso de **FTP anônimo**, por exemplo, deve ser evitado, pois permite acesso irrestrito a arquivos do servidor. A Red Hat (2023) recomenda a desativação dessa funcionalidade ou sua restrição a usuários com autenticação forte. Da mesma forma, a **porta 3306**, padrão do MySQL, não deve estar aberta à internet, pois facilita ataques automatizados. Segundo Bazzell (2021), em *OSINT Techniques*, ferramentas simples já são capazes de localizar essas portas abertas rapidamente.

No caso do SSH, a autenticação por senha é considerada insegura. A Red Hat (2022) reforça a importância da **autenticação por chave pública**, além do uso de ferramentas como Fail2Ban para bloqueio de acessos suspeitos.

Além dessas medidas, o uso de **firewalls** para controle de portas e **monitoramento contínuo** com IDS como Wazuh são indispensáveis. Tais práticas formam a base da defesa em profundidade, como orienta o NIST (2021).

Em resumo, garantir a segurança dos serviços expostos é uma responsabilidade contínua. Medidas simples, quando bem aplicadas, podem evitar prejuízos sérios.

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Desabilitar login anônimo FTP	Alto	Alta	Alta
Restringir porta 3306	Alto	Média	Alta
Auditar arquivos sensíveis	Médio	Média	Média
Reforçar SSH com chaves	Médio	Alta	Alta

Conclusão

A análise realizada no ambiente simulado demonstrou a importância de uma segmentação de rede bem estruturada para garantir a segurança e a organização dos ativos digitais. Através do reconhecimento ativo e da análise dos segmentos, foi possível identificar dispositivos com serviços expostos, fora de seu segmento, portas abertas desnecessárias (como a 21 – FTP), e configurações que podem representar potenciais vetores de ataque.

O mapeamento evidenciou ainda a necessidade de reforçar políticas de isolamento de dispositivos por função e criticidade. A presença de serviços

acessíveis em múltiplos segmentos representa um risco à confidencialidade, integridade e disponibilidade dos sistemas, especialmente em ambientes produtivos.

Recomenda-se que as ações propostas sejam implementadas com base na priorização apresentada, focando primeiro nos pontos de maior risco e maior facilidade de mitigação. Além disso, é fundamental adotar uma abordagem contínua de monitoramento da rede, realizando revisões periódicas e testes de intrusão controlados para garantir que a postura de segurança seja mantida ao longo do tempo.

Por fim, este relatório contribui não apenas para a identificação de falhas técnicas, mas também para a conscientização organizacional sobre a importância da arquitetura de rede segura, defendendo a aplicação dos princípios de menor privilégio, segmentação por função e revisão constante da exposição dos ativos.

Anexos

Link do gitHub :

https://github.com/Marlonsouto/Relatorio_de_Rede_Corporativa-Lab_Docker

Referência

RED HAT. *Securing FTP services*. Red Hat Customer Portal, 2023. Disponível em: https://access.redhat.com/solutions/70021. Acesso em: 31 jul. 2025.

RED HAT. *Using public key authentication with SSH*. Red Hat Documentation, 2022. Disponível em: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/using-ssh-key-based-authentication_security-hardening. Acesso em: 31 jul. 2025.

BAZZELL, Michael. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. 10. ed. United States: IntelTechniques, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Zero Trust Architecture: NIST Special Publication 800-207*. Gaithersburg, MD: NIST, 2021.

Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Acesso em: 31 jul. 2025.