PROJETO

ANÁLISE DE VULNERABILIDADES

VAI NA WEB

Relatório Técnico – Lab Segmentação de Rede

Autor: Gabriel de Aragão Araujo Oliveira

Data: 27/07/2025

Versão: 1.0

CONTEÚDO

Sumário Executivo

Foi analisado um ambiente Docker segmentado em três redes: `corp_net`, `guest_net` e `infra_net`, contendo múltiplos hosts simulando uma estrutura corporativa. A rede simulada foi analisada com foco em identificar falhas de segmentação, exposição de serviços e potenciais riscos operacionais. Foram encontrados diversos serviços em execução sem autenticação forte, como FTP anônimo, serviços SMB e LDAP abertos, além de um servidor Zabbix acessível via HTTP. A segmentação lógica está presente, mas há sobreposição de permissões entre as sub-redes. Recomenda-se o isolamento de serviços sensíveis, controle de acesso entre redes e a desativação de serviços não essenciais.

Objetivo

Analisar a rede simulada para identificar:

- Serviços e portas expostos desnecessariamente.
- Falhas de segmentação entre redes.
- Riscos operacionais envolvendo comunicação e exposição.

Escopo

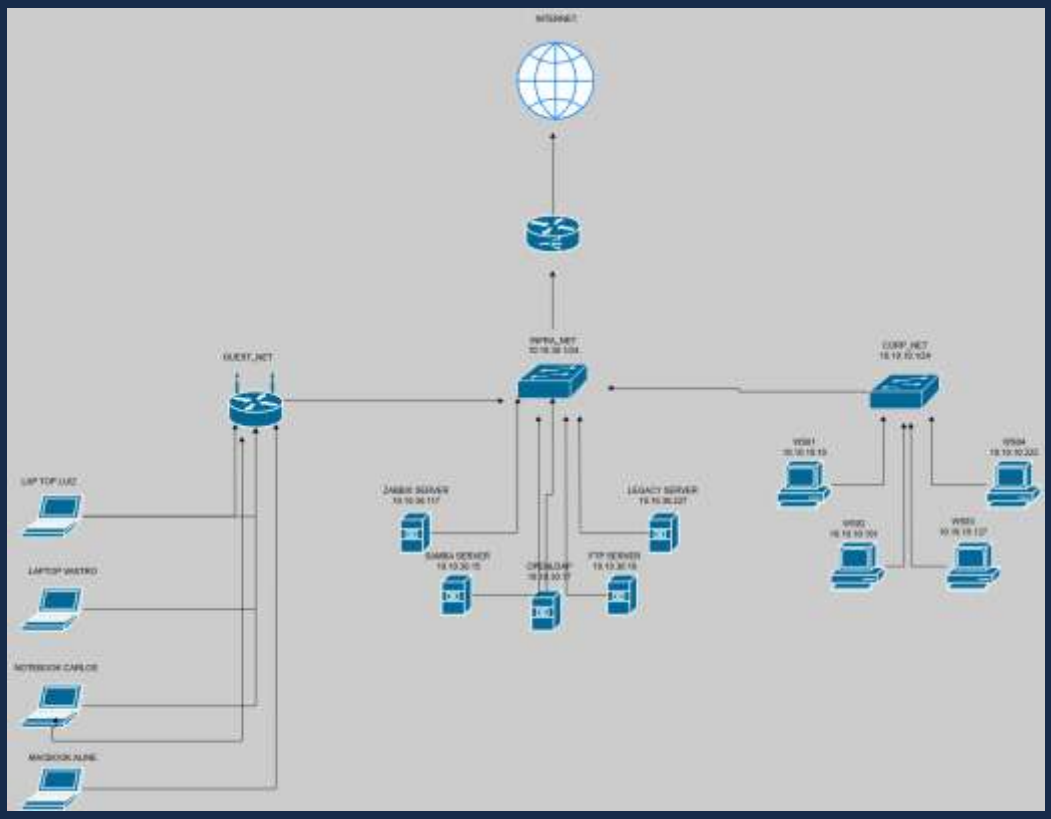
Ambiente Docker com múltiplos hosts distribuídos em três redes: corp_net, guest_net e infra_net. Cada rede possui diferentes serviços e dispositivos simulando cenários corporativos comuns.

Metodologia

Ferramentas Utilizadas:
- netdiscover: Identificação de hosts ativos e mapeamento ARP.
- nmap, rustscan: Varredura de portas e detecção de serviços.
- ping, traceroute: Testes de conectividade e segmentação entre redes.

Etapas:
1. Mapeamento de todos os dispositivos nas três redes usando netdiscover.
2. Identificação das portas abertas e serviços com nmap e rustscan.
3. Coleta de banners e versões de serviços para identificação de riscos.
4. Testes de segmentação cruzada (ex: um host da guest_net acessa serviços da infra_net?).
5. Análise dos serviços ativos, riscos, evidências e recomendações.

Diagrama de Rede



Diagnóstico (Achados)

Host/IP	Serviço	Porta	Risco Identificado	Evidência	Recomendação
WS_001/10.10.10.1	Unknown	47659	Porta alta sem identificação	Nmap mostra a porta 47659	Desligar o serviço se não for necessário ou fixar portas dinâmicas para facilitar firewall
WS_001/10.10.10.1	Portmapper	111	RCP exposto	nmap mostra porta 111 exposta	Desabilitar o serviço caso não seja essencial, ou limitar o acesso
Ftp-server/10.10.30.10	FTP	21	Serviço FTP aberto, possível FTP anônimo	nmap mostra porta 21 aberta	Desabilitar FTP ou implementar SFTP com autenticação
Mysql-server/10.10.30.11	MySQL	3306	Banco exposto na rede, pode ser explorado	nmap -sV mostra versão e salt	Restringir acesso a hosts autorizados
Samba-server/10.10.30.15	Samba/SMB	445	Compartilhamento de arquivos potencialmente aberto	nmap detecta serviço microsoft-ds	Limitar compartilhamento à rede interna
Openldap/10.10.30.17	LDAP	389	LDAP exposto, risco de enumeração	nmap com script ldap-rootdse	Habilitar autenticação e filtrar IPs
Zabbix-server/10.10.30.117	HTTP/Zabbix	80	Interface web exposta, risco de acesso indevido	Header HTTP e cookie de sessão	Proteger com autenticação, firewall ou VPN
Indefinido /10.10.50.1	Portmapper	111	RCP exposto	nmap mostra porta 111 exposta	Desabilitar o serviço caso não seja essencial, ou limitar o acesso
Container/10.10.50.6	Unknown	34030	Porta alta sem contexto	Nmap mostra a porta 34030	Desligar o serviço se não for necessário ou fixar portas dinâmicas para facilitar firewall

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Desativar FTP anônimo	Alto	Alta	Alta
Restringir acesso ao MySQL	Alto	Média	Alta
Habilitar HTTPS no Zabbix	Alto	Média	Alta
Bloquear portas SMB externamente	Médio	Alta	Média
Filtrar acesso LDAP por IP	Médio	Média	Média

Conclusão

A análise revelou que, embora exista segmentação lógica das redes, diversos serviços estão expostos e sem restrições adequadas, especialmente em infra_net. Alguns serviços utilizam protocolos não criptografados, e a exposição de interfaces administrativas representa riscos operacionais consideráveis. Recomenda-se o uso de firewalls internos, autenticação forte, e o bloqueio de portas não utilizadas. Como próximos passos, sugere-se validar o isolamento entre sub-redes e realizar testes de vulnerabilidade mais profundos.