Relatório Técnico – Mapeamento da Rede Corporativa (Lab Docker)

Analista: Patricia Paes **Ambiente:** Kensei-cybersec-lab-docker **Ferramentas utilizadas:** nmap, rustscan, ping **Data da análise:** 23/07/2025

Sumário Executivo

Este relatório apresenta os principais achados da análise técnica conduzida sobre a rede corporativa atualmente em operação. A infraestrutura está segmentada em três sub-redes funcionais:

- **corp_net** – estações de trabalho e web server
- **guest_net** – dispositivos pessoais e visitantes
- **infra_net** – servidores críticos

A avaliação identificou ativos responsivos com portas TCP filtradas, evidenciando políticas eficazes de segurança. A limitação na visibilidade externa sugere a necessidade de testes autenticados para validar configurações internas e detectar vulnerabilidades ocultas.

Também foi observada a ausência de um inventário técnico consolidado, limitando o monitoramento eficiente e a resposta estratégica. O relatório propõe ações prioritárias para reforçar a postura defensiva, ampliar a observabilidade interna e garantir governança dos ativos.

Objetivo

Identificar os ativos conectados à rede corporativa, mapear áreas com visibilidade externa e avaliar o nível de exposição dos serviços. A análise foi feita a partir de uma perspectiva interna, sem privilégios elevados, oferecendo base técnica para decisões em segurança cibernética.

Escopo e Contexto

Esta análise foi realizada sobre uma rede segmentada em três sub-redes:

Sub-rede	Descrição	Exemplos de IPs
corp_net	Estações de trabalho e web server	192.168.10.10, 192.168.10.20, 192.168.10.30
guest_net	Dispositivos pessoais e visitantes	192.168.20.254, 192.168.20.255
infra_net	Servidores críticos (DB, L DAP, Monitoramento)	192.168.30.10, 192.168.30.11

O container **analyst** foi utilizado como ponto de partida para análise, com acesso confirmado às três redes através de ferramentas como **ping, nmap** e **rustscan**. A abordagem se concentrou em escaneamento passivo e ativo, sem acesso autenticado, com o objetivo de entender a superfície de exposição a partir de uma perspectiva de rede interna sem privilégios elevados.

O escopo da análise inclui:

● Identificação de ativos acessíveis
● Reconhecimento da arquitetura de rede
● Catalogação de sub-redes funcionais
● Diagnóstico preliminar da exposição dos hosts

Não foram realizadas ações invasivas, modificações em configurações nem exploração de vulnerabilidades — o foco foi exclusivamente no reconhecimento.

Metodologia

A análise de reconhecimento foi conduzida utilizando o container analyst, posicionado estrategicamente na rede corp_net com acesso confirmado às demais sub-redes do ambiente Docker.

Ferramentas utilizadas

- ping: conectividade básica
- nmap: descoberta de hosts -sn e detecção de serviços -sV
- rustscan: escaneamento rápido de portas TCP
- net-tools: suporte com netstat e ifconfi

Estratégia de Reconhecimento

● Passiva: coleta de IPs e análise de visibilidade da rede via ping sweep.
● Ativa: escaneamento de portas com e rustscan nos IPs identificados
● teste realizados em todas as sub-redes identificadas (corp_net, guest_net, infra_net)
● acesso não autenticado (sem credenciais), simulando perspectiva de analista em ponto de partida neutro.

Sequência de Execução

1. Validação de conectividade com ping em IPs específicos
2. Descoberta de hosts ativos com nmap -sn, identificando IPs em corp_net, guest_net e infra_net.
3. Escaneamento de portas com TCP com foco em velocidade e profundidade:

rustscan -b 1500 -a -- -A

nmap -p 80, 443 -sV <ip>
curl -I <ip>

4.Comparação entre sub-redes quanto à exposição e resposta aos escaneamentos
Todos os comandos foram executados a partir do terminal dentro do container analyst sob ambiente isolado e controlado. Diagrama de Rede Corporativa (Descrição) O ambiente de rede está segmentado em três sub-redes principais:
● corp_net – 192.168.10.0/24 Contém estações de trabalho, web server e o container analyst. Exemplo de ativos: 192.168.10.10, 192.168.10.20, 192.168.10.30
● guest_net – 192.168.20.0/24 Rede destinada a dispositivos pessoais e visitantes. Exemplo de ativos: 192.168.20.254, 192.168.20.255
● infra_net – 192.168.30.0/24 Rede crítica para servidores essenciais como banco de dados, LDAP e monitoramento.
Exemplo de ativos: 192.168.30.10, 192.168.30.11

Diagnóstico Técnico

A análise técnica revelou comportamento consistente entre os ativos das sub-redes corp_net, guest_net e infra_net, todas acessíveis a partir do ponto de observação interno.

Principais achados:

- Os IPs em cada sub-rede responderam positivamente aos testes de conectividade (ping) e descoberta de ativos (nmap -sn).
- A maioria dos hosts apresentou **filtragem total de portas TCP**, evidenciando mecanismos de proteção como firewalls ou regras restritivas de acesso.
- Foram detectadas respostas específicas de serviços:
    - **MySQL (porta 3306)**: acesso externo permitido e script mysql-info executado com sucesso.
    - **FTP (21)**, **SMB (445)**, **LDAP (389)** e **HTTP/HTTPS (80/443)**: portas filtradas, sem retorno dos scripts aplicados.
- Não foram identificados serviços inseguros ou abertos, como **Telnet**, **FTP anônimo**, ou **SMB sem autenticação**.
- IPs de broadcast (*.255) responderam aos escaneamentos, mas foram descartados do inventário por serem endereços reservados.

Recomendações Técnicas

Realizar escaneamentos autenticados via SSH ou credenciais administrativas para obter visibilidade aprofundada dos serviços internos.

Validar configurações de firewall nos ativos que apresentaram portas filtradas, garantindo consistência e conformidade.

Implantar monitoramento contínuo nos servidores da sub-rede infra_net, preferencialmente utilizando Zabbix ou solução equivalente.

Consolidar e manter um inventário técnico atualizado, com dados de IP, sistema operacional e função de cada host, visando suporte a auditorias e resposta a incidentes.

Plano de ação 80/20

Ação Prioritária	Impacto	Esforço	Justificativa
Mapear serviços via SSH/credenciais	Alto	Médio	Pode Revelar ativos críticos e aplicações vulneráveis
Verificar configuração dos firewalls locais	Alto	Baixo	Garante proteção constante
Consolidar inventário técnico dos hosts	Médio	Baixo	Suporte para auditorias e correções futuras

Conclusão

A análise realizada permitiu identificar e documentar as principais características da rede corporativa simulada, composta por três sub-redes segmentadas e ativos distribuídos por diferentes funções. O ambiente apresenta visibilidade controlada, ausência de serviços inseguros e resposta adequada aos testes de escaneamento, sugerindo uma configuração defensiva satisfatória.

A identificação de ativos com portas filtradas reforça a presença de políticas de firewall, e a visibilidade integral via container analyst permite a continuidade das avaliações com escopos mais avançados, incluindo testes autenticados e auditoria de serviços internos. As recomendações propostas e o plano de ação 80/20 visam fortalecer a postura defensiva, aprimorar o inventário técnico e garantir que possíveis superfícies de ataque ocultas sejam devidamente monitoradas.

Este relatório consolida os achados iniciais e serve como base estratégica para investigações futuras, reforçando a abordagem proativa na segurança cibernética corporativa.

Anexos

A1. Comandos utilizados

docker exec -it analyst bash
ping nmap -sn
rustscan -b 1500 -a -- -A

A2. IPs ativos detectados

● 192.168.10.20
● 192.168.10.30
● 192.168.20.254
● 192.168.30.10
● 192.168.30.11
●192.168.10.46

A3. Ferramentas disponíveis no container analyst

- nmap
- rustscan
- net-tools
- dig

A4. Ambiente de simulação

● Repositório: https://github.com/kensei-sec/kensei-cybersec-lab-docker
● Comando de inicialização: docker compose up –d

Teste Complementar – Recon-Backup

Durante a análise, foi conduzido o módulo recon-backup como complemento ao mapeamento principal. Essa etapa teve como objetivo reforçar a confiabilidade dos dados coletados, registrar a sequência técnica dos comandos aplicados e validar a consistência dos serviços ativos em horários distintos. As evidências e registros foram organizados e salvos com controle de versão, incluindo:

- recon_ip_maps.txt Arquivo com o mapeamento consolidado dos IPs ativos nas sub-redes corp_net, guest_net e infra_net. Inclui resultado dos testes ping e escaneamentos básicos com nmap.
- reconn_rede.txt Registro cronológico dos comandos executados, organizado como um diário técnico com todos os testes aplicados durante a etapa de reconhecimento.
- /prints/ Capturas de tela dos resultados obtidos com as ferramentas nmap, rustscan, curl, entre outras. Cada imagem está nomeada e datada para facilitar a rastreabilidade.
- /scripts/ Scripts utilizados na execução dos testes, com comentários explicando parâmetros e objetivos técnicos.

Repositório de Evidências – GitHub

Todas as evidências e arquivos estão disponíveis para consulta pública no repositório:

https://github.com/Patriciapaes88/Relatorio-Tecnico.git

Estrutura do repositório:

- /recon-backup/ → testes complementares e arquivos reconn_rede.txt, recon_ip_maps.txt
- /mapeamento/ → prints e evidências do reconhecimento principal
- /scripts/ → comandos utilizados com observações técnicas