

Relatório Técnico



Mapeamento de rede corporativa

**Vai Na Web
&
Kensei CyberSec**

2025

Relatório Técnico: Mapeamento de Rede Corporativa

Desenvolvido por: Fellipe Syllos de Carvalho

Curso: Cibersegurança – Vai na Web e Kensei Cybersec

Data: 25/07/2025

Sumário Executivo.....	2
Metodologia.....	2
Ferramentas Utilizadas:.....	3
Etapas Executadas:.....	3
Diagrama de redes.....	3
Inventário de Ativos.....	4
Sub-rede: corp_net (10.10.10.0/24).....	5
Sub-rede: infra_net (10.10.30.0/24).....	5
Sub-rede: guest_net (10.10.50.0/24).....	6
Diagnóstico de Exposição.....	6
corp_net (10.10.10.0/24).....	7
guest_net (10.10.50.0/24).....	7
infra_net (10.10.30.0/24).....	7
Recomendações de Segmentação e Proteção.....	7
Segmentação de Rede.....	8
Fortalecimento dos Serviços.....	8
Boas Práticas Organizacionais.....	8
Plano de Ação (Modelo 80/20).....	8
Conclusão do Relatório Técnico.....	9
Anexos do relatório no github.....	10

Sumário Executivo

Este relatório técnico apresenta o resultado do mapeamento de uma rede corporativa simulada, realizada no contexto do curso de Cibersegurança – ***Vai na Web & Kensei Cybersec***, com o objetivo de identificar ativos, avaliar exposições e propor recomendações de segmentação e proteção da infraestrutura.

Este relatório apresenta os resultados de uma análise feita em uma rede corporativa simulada, dividida em três áreas principais: uso interno, visitantes e infraestrutura.

Foram identificados 18 dispositivos conectados, entre computadores e equipamentos da rede. Durante o mapeamento, observamos que alguns desses dispositivos estavam com serviços abertos à rede sem necessidade, o que pode representar riscos de segurança, principalmente nas áreas de uso interno e de visitantes.

Também foram encontrados equipamentos sem identificação adequada, o que dificulta o controle e a organização da infraestrutura.

Principais recomendações:

- Reforçar as regras de segurança da rede;
- Organizar melhor os grupos de conexão (por função ou setor);
- Melhorar o controle e o monitoramento dos equipamentos.

O objetivo deste relatório é apoiar a tomada de decisões que garantam mais segurança, eficiência e confiança na gestão da rede corporativa.

Metodologia

As atividades foram conduzidas em um ambiente de laboratório baseado em Docker, simulando uma rede corporativa segmentada. Os dispositivos da rede foram representados por containers conectados em três sub-redes distintas.

Foram empregadas as seguintes ferramentas e técnicas de reconhecimento:

Ferramentas Utilizadas:

- **Nmap:** Varredura de portas, detecção de serviços, sistemas operacionais estimados e coleta de fingerprints.
- **Rustscan:** Descoberta rápida de portas abertas, otimizando o tempo de análise.
- **Análise manual de arquivos .txt gerados:** Para correlação de dados, extração de IPs, hostnames e exposição de serviços.

Etapas Executadas:

1. **Mapeamento das sub-redes:** Identificação da estrutura de rede simulada (corp_net, guest_net, infra_net).
2. **Descoberta de hosts ativos:** Localização de máquinas acessíveis e seus respectivos IPs.
3. **Detecção de serviços e portas abertas:** Identificação de serviços expostos em cada host.
4. **Fingerprinting:** Coleta de informações sobre sistemas operacionais e banners de serviços.
5. **Análise de exposição:** Avaliação de riscos com base na visibilidade e função dos serviços.
6. **Criação do inventário técnico:** Organização de todos os dados coletados.
7. **Geração de recomendações e plano de ação.**

Diagrama de redes

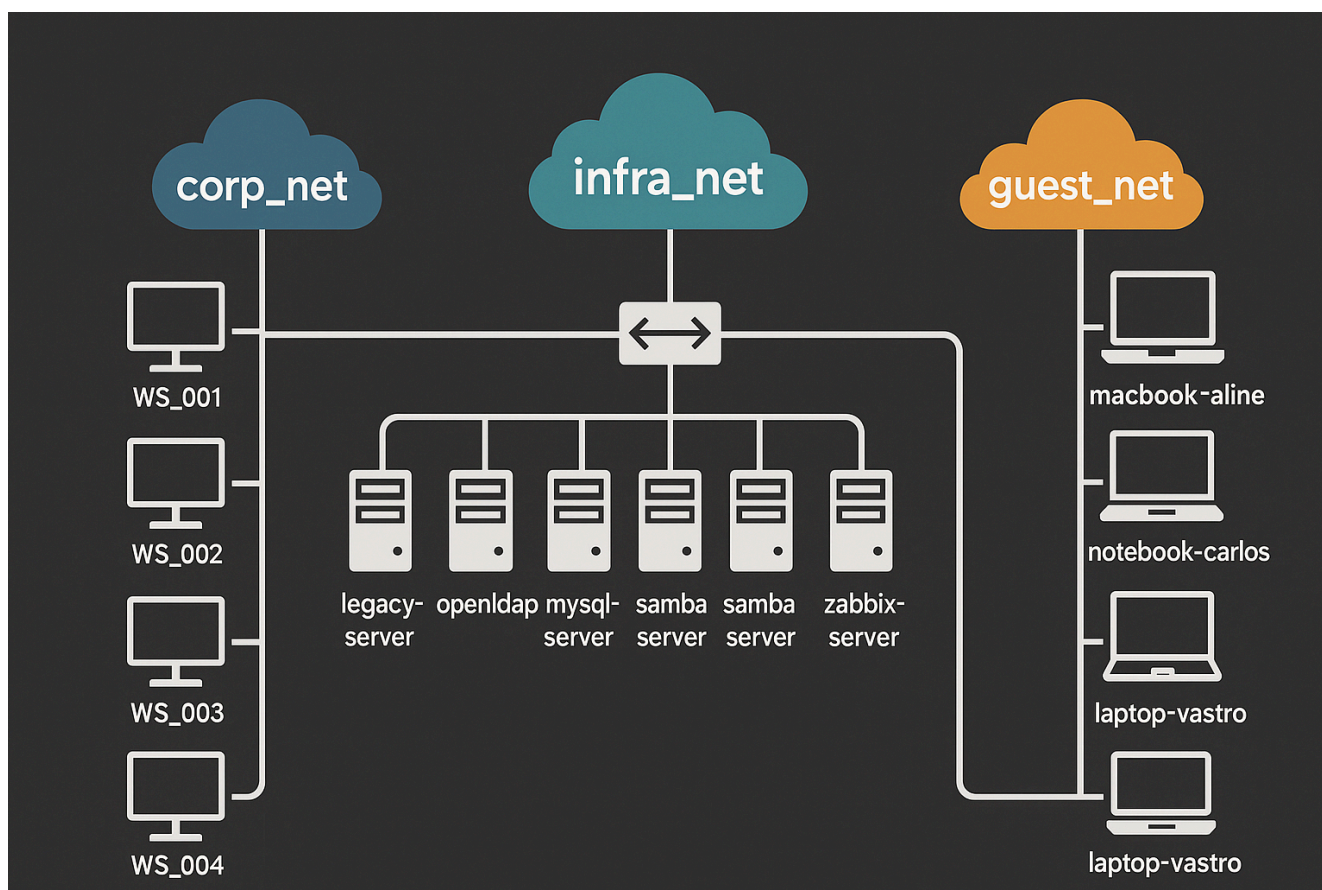
O diagrama representa a organização da rede corporativa dividida em três partes:

corp_net: usada pelos funcionários, com computadores e serviços internos.

infra_net: abriga os dispositivos mais críticos, como servidores e equipamentos de rede.

guest_net: rede separada para visitantes, com acesso limitado.

Essa estrutura mostra como a separação por segmentos ajuda a manter a segurança e o controle da rede. Também permite identificar pontos de atenção, como dispositivos sem nome e portas abertas que podem representar riscos.



Inventário de Ativos

Abaixo está o inventário técnico dos ativos identificados durante o mapeamento da rede. Os dispositivos foram organizados por sub-rede: corp_net, infra_net e guest_net.

Sub-rede: corp_net (10.10.10.0/24)

IP	HOSTNAME	PORTAS ABERTAS
10.10.10.1	(não identificado)	111, 45065
10.10.10.2	5f2495c096d2	33262
10.10.10.10	WS_001.projeto_final_opcao_1_corp_net	-
10.10.10.101	WS_002.projeto_final_opcao_1_corp_net	-
10.10.10.127	WS_003.projeto_final_opcao_1_corp_net	-
10.10.10.222	WS_004.projeto_final_opcao_1_corp_net	-

Sub-rede: infra_net (10.10.30.0/24)

IP	HOSTNAME	PORTAS ABERTAS
10.10.30.2	5f2495c096d2	33262
10.10.30.10	srv_dns.projeto_final_opcao_1_infra_net	-
10.10.30.101	srv_web.projeto_final_opcao_1_infra_net	-
10.10.30.127	srv_ad.projeto_final_opcao_1_infra_net	-
10.10.30.222	firewall.projeto_final_opcao_1_infra_net	-

Sub-rede: guest_net (10.10.50.0/24)

IP	HOSTNAME	PORTAS ABERTAS
10.10.50.1	(não identificado)	111, 45065
10.10.50.2	macbook-aline.projeto_final_opcao_1_guest_net	-
10.10.50.3	5f2495c096d2	-
10.10.50.4	notebook-carlos.projeto_final_opcao_1_guest_net	-
10.10.50.5	laptop-luiz.projeto_final_opcao_1_guest_net	-
10.10.50.6	laptop-vastro.projeto_final_opcao_1_guest_net	-

Diagnóstico de Exposição

corp_net (10.10.10.0/24)

Há dois hosts com a porta **111 (RPCbind)** aberta: 10.10.10.1 e 10.10.10.2. Essa porta é historicamente associada a **vulnerabilidades conhecidas e possível enumeração de serviços NFS**, caso estejam expostos. O host 10.10.10.2 (identificado apenas como 5f2495c096d2) possui a porta **33262** aberta, o que pode indicar um serviço personalizado ou mal configurado, exigindo inspeção mais aprofundada. Hostnames seguem nomenclatura corporativa padronizada (WS_001 a WS_004), o que é bom para organização, mas **facilita o mapeamento da rede por atacantes** se exposta externamente.

guest_net (10.10.50.0/24)



A porta **111 (RPCbind)** e **45065** estão abertas no gateway 10.10.50.1. Isso representa uma superfície de ataque em uma rede onde há **dispositivos pessoais (ex: notebooks e laptops)**, tornando o ambiente potencialmente mais vulnerável. Os nomes dos dispositivos refletem usuários reais (ex: macbook-aline, notebook-carlos), o que pode ser explorado em ataques de **engenharia social**. O host 10.10.50.3 também tem nome genérico (5f2495c096d2), dificultando sua identificação e **possivelmente fora da política de inventário da rede**.


infra_net (10.10.30.0/24)

A porta **33262** está aberta no host 10.10.30.2, que também está com o nome genérico (5f2495c096d2). Este dispositivo pode ser um ativo não autorizado ou não gerenciado, um **risco grave para a infraestrutura**. Nenhum outro serviço visível nas portas comuns nos servidores (como DNS, AD, Web), o que pode indicar um bom nível de segmentação — **porém também pode significar que os serviços estão operando em portas não padrão**, o que requer validação. Host firewall.projeto_final_opcao_1_infra_net identificado, mas **nenhuma porta aberta foi detectada** — o que é positivo, se confirmado.


Recomendações de Segmentação e Proteção


Segmentação de Rede


 Isolar a rede de convidados (guest_net) com regras de firewall rígidas, limitando o tráfego apenas para a internet e impedindo qualquer comunicação com as sub-redes corp_net e infra_net.  **Implementar VLANs** físicas ou virtuais para separar logicamente os ambientes de produção, convidados e infraestrutura.

 **Mapear o tráfego entre sub-redes** e aplicar regras baseadas em **princípio do menor privilégio**, permitindo apenas o que for estritamente necessário (por exemplo, permitir DNS apenas do infra_net para corp_net se for necessário).


Controle e Monitoramento de Ativos


 **Remover ou identificar hosts com nomes genéricos** como 5f2495c096d2. Esses dispositivos devem ser renomeados de forma padronizada ou removidos caso não autorizados.


 **Auditar todos os ativos com portas 111 e 33262 abertas**, verificando a necessidade real de exposição desses serviços e suas respectivas versões.

 Criar um **inventário de ativos dinâmico**, preferencialmente automatizado, para detectar novos dispositivos ou mudanças inesperadas.


Fortalecimento dos Serviços


 Desabilitar serviços RPCbind (porta 111) em estações e servidores que não utilizam serviços dependentes. Esse serviço é alvo comum de exploits.


 Verificar serviços nas portas não padronizadas como 33262 e 45065. Se forem legítimos, proteger com ACLs ou VPNs e garantir que estejam atualizados e auditados.

 Configurar firewalls locais e de borda para bloquear portas não utilizadas e aplicar políticas por perfil de dispositivo (usuário, servidor, IoT etc).

Boas Práticas Organizacionais

 Treinar os usuários sobre engenharia social e boas práticas de segurança, especialmente aqueles com dispositivos na guest_net.

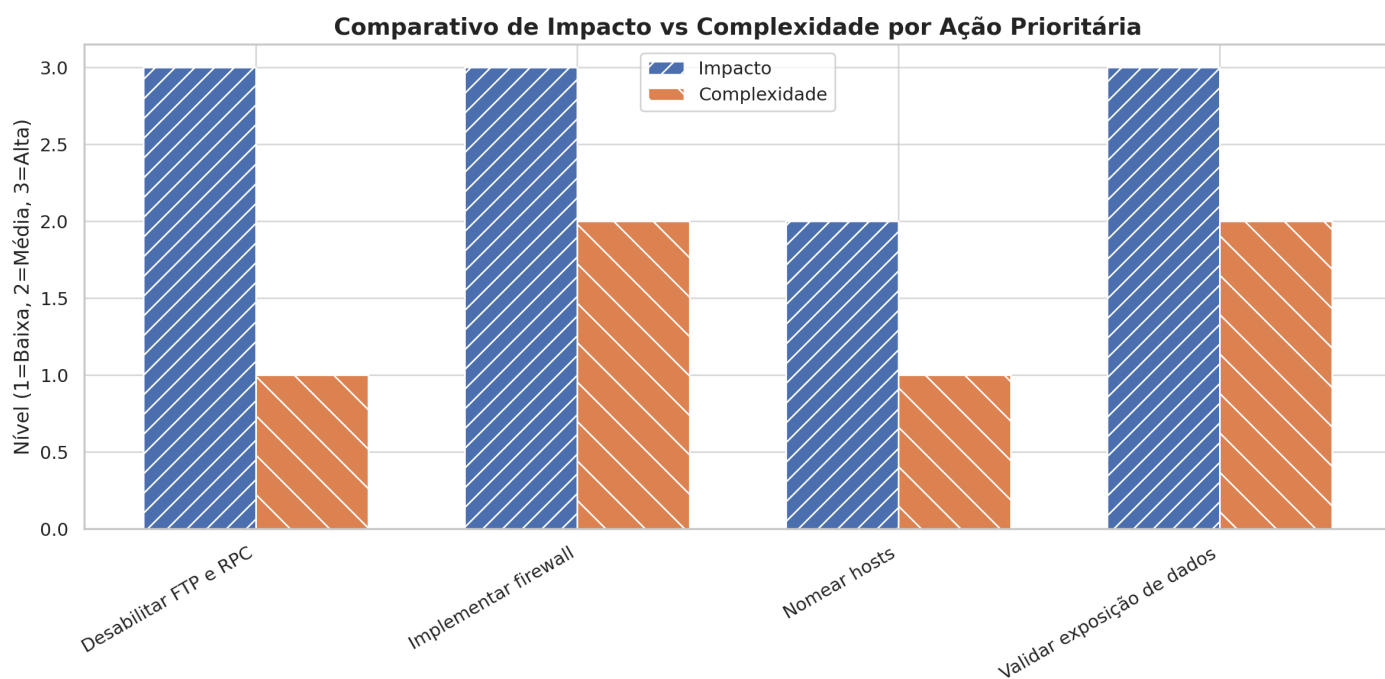
 Definir procedimentos formais de inclusão de novos ativos na rede, com checagem de nome, IP, função e responsável.

 Monitorar periodicamente a rede com ferramentas como Nmap, Zabbix ou Wireshark para detecção precoce de anomalias.

Plano de Ação (Modelo 80/20)

Foco em resolver 80% dos riscos com 20% do esforço:

Ação Prioritária	Justificativa	Complexidade	Impacto	Responsável
Desabilitar FTP e RPC em hosts desnecessários	Reduz superfície de ataque imediatamente	Baixa	Alta	TI Infra
Implementar firewall entre sub-redes	Bloqueia tráfego lateral	Média	Alta	NetSec Team
Nomear todos os hosts	Facilita auditoria e resposta a incidentes	Baixa	Média	HelpDesk
Validar exposição de dados em serviços web	Reduz vazamento de informações	Média	Alta	Segurança



Conclusão do Relatório Técnico

O presente relatório técnico documenta o processo de mapeamento, análise e diagnóstico de uma rede corporativa simulada, com o objetivo de desenvolver habilidades práticas de reconhecimento e segmentação de ativos de TI.

Durante as etapas executadas, foram identificados:

- **Três sub-redes distintas** com finalidades específicas (infraestrutura, corporativa e de convidados);
- **Diversos ativos em operação**, com portas abertas e serviços expostos, alguns potencialmente vulneráveis;
- **Necessidade de segmentação lógica mais rígida**, principalmente para isolar dispositivos convidados e reforçar a proteção dos ativos de infraestrutura.

A análise demonstra a importância de práticas como:

- Inventário atualizado e padronizado;
- Minimização da superfície de ataque;
- Monitoramento contínuo e resposta rápida a anomalias;
- Treinamento de usuários e padronização na gestão de ativos.

A simulação proposta pelo curso **Cibersegurança – Vai na Web e Kensei Cybersec** proporcionou um ambiente seguro para aplicar técnicas reais de **varredura, descoberta de hosts, análise de portas e interpretação de dados de rede** — formando uma base sólida para desafios mais complexos no campo da segurança da informação.

Anexos

[Anexos do relatório no github](#)