



Relatório de Mapeamento, Inventario e Scan de Redes

Sumário

[1. Introdução](#)

[2. Metodologia](#)

[3. Inventário Técnico de Ativos](#)

[4. Mapeamento de Sub-redes e Seus Propósitos](#)

[5. Diagnóstico e Achados](#)

[6. Recomendações \(Abordagem 80/20\)](#)

[6.1. Prioridade Alta](#)

[1. Revisão e Implementação Urgente de Políticas de Firewall e Segmentação de Rede:](#)

[2. Hardening de Serviços por Tipo de Ativo:](#)

[6.2. Prioridade Média](#)

[2. Revisão de Configurações de Segurança Padrão:](#)

[7. Plano de Ação:](#)

[8. Conclusão](#)

[9. Anexos](#)



Relatório Técnico de Mapeamento, Inventário e Scan de Ativos de Redes

Cliente: Kensey Cybersecurity

Executado por: Metafox Info

Responsável Técnico: Fernando Silva Andrade

Data: 18 de julho de 2025



1. Introdução

Este documento apresenta os resultados da análise de segurança interna da infraestrutura de rede da empresa Kensey Cybersecurity, conduzida pela equipe da Metafox Info, especializada em segurança da informação.

A avaliação foi realizada a partir da perspectiva de um analista com acesso à sub-rede interna corp_net, com o objetivo de:

Identificar máquinas e ativos acessíveis;

Determinar as sub-redes existentes e seus respectivos propósitos;

Criar um inventário técnico detalhado dos ativos mapeados;

Identificar inconsistências e exposições críticas nos serviços de rede;

Propor recomendações baseadas na abordagem 80/20, priorizando ações de maior impacto na mitigação de riscos.

Este relatório foi elaborado pelo analista de segurança Fernando Silva Andrade, e compõe uma entrega técnica para apoiar as ações corretivas e estratégicas da Kensey Cybersecurity no fortalecimento de sua postura de segurança cibernética.

2. Metodologia

A análise foi conduzida a partir de uma máquina "Analyst" conectada à rede corp_net (IP:10.10.10.0). Foi criado um script em bash para automatizar e utilizar ferramentas como nmap e rustscan para a descoberta de hosts e varredura de portas, net-tools para informações de rede e dig para resolução de nomes. O escopo da varredura incluiu as seguintes sub-redes: 10.10.10.0/24 (corp_net), 10.10.30.0/24 (infra_net) e 10.10.50.0/24 (guest_net)



3. Inventário Técnico de Ativos

O levantamento identificou os seguintes ativos, suas sub-redes, nomes de host, sistemas operacionais (quando detectados) e serviços ativos:

Sub-rede: “corp_net” (10.10.10.0/24) - Rede corporativa (estações e web server)

SUB REDE CORPORATIVA				
IP	Nome Host	Sistema Operacional	Serviços Ativos	Observações
10.10.10.1	fsa (10.10.10.1)	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Múltiplos serviços, incluindo SSH, HTTP/S, SMB e MySQL.
10.10.10.10	WS_001.projeto_final_opcao_1_corp_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Estação de trabalho com serviços de servidor inesperados.
10.10.10.101	WS_002.projeto_final_opcao_1_corp_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Estação de trabalho com serviços de servidor inesperados.
10.10.10.127	WS_003.projeto_final_opcao_1_corp_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Estação de trabalho com serviços de servidor inesperados.
10.10.10.222	WS_004.projeto_final_opcao_1_corp_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Estação de trabalho com serviços de servidor inesperados.
10.10.10.2	361dee263e0e	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Host com nome genérico (possivelmente Docker/VM) e múltiplos serviços.



Sub rede: "infra_net" (10.10.30.0/24) - Rede de infraestrutura crítica (servidores)

SUB REDE INFRAESTRUTURA				
IP	Nome Host	Sistema Operacional	Serviços Ativos	Observações
10.10.30.1	fsa (10.10.30.1)	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Múltiplos serviços, incluindo SSH, HTTP/S, SMB e MySQL.
10.10.30.10	ftp-server.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor FTP com múltiplos serviços, incluindo MySQL.
10.10.30.11	mysql-server.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor MySQL com múltiplos serviços além do esperado.
10.10.30.15	samba-server.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:netbios-ssn; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor Samba com múltiplos serviços, incluindo MySQL.
10.10.30.17	openldap.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor OpenLDAP com múltiplos serviços, incluindo MySQL.
10.10.30.117	zabbix-server.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor Zabbix com múltiplos serviços, incluindo MySQL.
10.10.30.227	legacy-server.projeto_final_opcao_1_infra_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Servidor "legacy" com múltiplos serviços, incluindo MySQL.
10.10.30.2	361dee263e0e	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Host com nome genérico (possivelmente Docker/VM) e múltiplos serviços.



Sub-rede: guest_net (10.10.50.0/24) - Rede de visitantes e dispositivos pessoais

SUBREDE VISITANTES (GUEST)				
IP	Nome Host	Sistema Operacional	Serviços Ativos	Observações
10.10.50.1	fsa (10.10.50.1)	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Múltiplos serviços, incluindo SSH, HTTP/S, SMB e MySQL.
10.10.50.2	laptop-vastro.projeto_final_opcao_1_guest_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Laptop com serviços de servidor inesperados.
10.10.50.3	macbook-aline.projeto_final_opcao_1_guest_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Macbook com serviços de servidor inesperados.
10.10.50.4	notebook-carlos.projeto_final_opcao_1_guest_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Notebook com serviços de servidor inesperados.
10.10.50.5	laptop-luiz.projeto_final_opcao_1_guest_net	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Laptop com serviços de servidor inesperados.
10.10.50.6	361dee263e0e	Desconhecido	22/tcp:ssh; 80/tcp:http; 139/tcp:netbios-ssn; 443/tcp:https; 445/tcp:microsoft-ds; 3306/tcp:mysql; 3389/tcp:ms-wbt-server	Host com nome genérico (possivelmente Docker/VM) e múltiplos serviços.

4. Mapeamento de Sub-redes e Seus Propósitos

As sub-redes identificadas e seus propósitos declarados são:

corp_net (10.10.10.0/24): Destinada à rede corporativa, incluindo estações de trabalho e servidores web.

infra_net (10.10.30.0/24): Designada para a infraestrutura crítica, como servidores de banco de dados, FTP, Samba, LDAP e Zabbix.

guest_net (10.10.50.0/24): Utilizada para visitantes e dispositivos pessoais.

Embora os propósitos declarados sejam claros, a análise dos serviços ativos revelou inconsistências significativas.



5. Diagnóstico e Achados

A análise da rede interna revelou padrões preocupantes que indicam falhas na segmentação e hardening dos sistemas.

Serviços Inesperados em Estações de Trabalho e Rede de Convidados:

Todas as estações de trabalho na corp_net (WS_001 a WS_004) e os dispositivos na guest_net (laptop-vastro, macbook-aline, notebook-carlos, laptop-luiz) estão expondo múltiplos serviços que não deveriam estar presentes em máquinas cliente ou em uma rede de convidados.

Isso inclui SSH (porta 22), HTTP/S (portas 80, 443), NetBIOS (portas 139, 445), MySQL (porta 3306) e RDP (porta 3389).

A presença de MySQL em estações de trabalho e dispositivos de convidados é particularmente alarmante, pois sugere uma falta de segregação de responsabilidades e potencial vazamento de dados.

Serviços como SSH, HTTP/S e RDP em máquinas de usuários aumentam a superfície de ataque para acesso não autorizado e ataques de força bruta.

Padronização Inadequada de Serviços:

Todos os hosts identificados em todas as sub-redes, incluindo os hosts "fsa" e os com nomes genéricos "361dee263e0e", apresentam exatamente o mesmo conjunto de portas abertas e serviços ativos: SSH, HTTP, NetBIOS, HTTPS, Microsoft-DS, MySQL e MS-WBT-Server.

Essa padronização sugere uma configuração genérica ou de "modelo" aplicada indiscriminadamente, o que indica uma provável falta de hardening específico para cada tipo de ativo e seu propósito.

É altamente improvável que todas as máquinas, desde estações de trabalho a servidores de infraestrutura crítica, necessitem do mesmo conjunto de serviços expostos.



Dificuldade na Identificação de SO:

A ferramenta de mapeamento não conseguiu identificar o sistema operacional de nenhuma das máquinas ("Desconhecido"). [cite: 1] Isso pode dificultar a identificação de vulnerabilidades específicas de SO e a aplicação de patches ou políticas de segurança direcionadas.

Hosts com Nomes Genéricos:

A presença de hosts com nomes genéricos como "361dee263e0e" em todas as sub redes (10.10.10.2, 10.10.30.2, 10.10.50.6) sugere ambientes de contêineres (Docker) ou máquinas virtuais sem nomes de host configurados adequadamente. [cite: 1] Isso dificulta o inventário e a gestão de segurança.

Ampla Exposição de Serviços de Infraestrutura:

Serviços como MySQL, FTP, Samba, LDAP, e Zabbix estão expostos na infra_net com o mesmo conjunto de portas. Embora esperados para servidores de infraestrutura, a exposição combinada com outros serviços (como RDP e HTTP/S) pode aumentar o risco se não houver um controle de acesso rigoroso e segmentação granular.

CVE *Common Vulnerabilities and Exposures* (Vulnerabilidades e Exposições Comuns).

Identificadores únicos para falhas de segurança conhecidas, mantidos por uma base pública

Abaixo tabela com os CVEs , encontrados nos testes de scan.



RELATÓRIO DE CVES		
Serviços	CVE	Descrição
SSH (22)	CVE-2018-15473	User Enumeration em OpenSSH.
SSH (22)	CVE-2021-41617	Escalada de privilégios locais no OpenSSH.
SSH (22)	CVE-2023-48795	Terrapin attack - vulnerabilidade no protocolo SSH.
HTTP/HTTPS (80/443)	CVE-2021-41773	Execução remota de comandos no Apache HTTP Server.
HTTP/HTTPS (80/443)	CVE-2021-22960	Divulgação de informações no Nginx.
HTTP/HTTPS (80/443)	CVE-2023-25690	Injeção HTTP em Apache 2.4.x.
MySQL (3306)	CVE-2016-6662	Execução remota de código via configuração maliciosa.
MySQL (3306)	CVE-2021-35604	Denial of Service em MySQL.
MySQL (3306)	CVE-2021-27928	Vazamento de informações pela resposta do servidor.
RDP (3389)	CVE-2019-0708	Execução remota sem autenticação (BlueKeep).
RDP (3389)	CVE-2020-0609	Execução remota via RDP Gateway.
RDP (3389)	CVE-2020-0610	Execução remota via RDP Gateway.
SMB (139/445)	CVE-2017-0144	Execução remota (EternalBlue - WannaCry).
SMB (139/445)	CVE-2020-0796	Execução remota em SMBv3 (SMBGhost).
FTP	CVE-2015-3306	ProFTPD mod_copy - execução remota via comando.
Samba	CVE-2017-7494	Execução remota via Samba.
LDAP	CVE-2020-25692	Corrupção de heap no OpenLDAP.
Zabbix	CVE-2022-23134	Execução remota não autenticada em Zabbix.

6. Recomendações (Abordagem 80/20)

As recomendações a seguir focam nas ações de maior impacto (os 20%) que resolverão a maioria dos problemas de segurança identificados (os 80%).

6.1. Prioridade Alta

1. Revisão e Implementação Urgente de Políticas de Firewall e Segmentação de Rede:

Ação:

Implementar regras de firewall estritas em todos os dispositivos de rede (roteadores, switches de camada 3, firewalls dedicados) para garantir que apenas as portas e protocolos estritamente necessários estejam abertos para cada sub-rede e, idealmente, para cada host ou grupo de hosts.



Foco 80/20:

Bloquear imediatamente portas como 22, 139, 445, 3306, 3389 em estações de trabalho (corp_net) e na rede de convidados (guest_net).

A maioria dos incidentes de segurança começa com serviços expostos desnecessariamente.

2. Hardening de Serviços por Tipo de Ativo:

Ação:

Desenvolver e aplicar "modelos" de hardening para cada tipo de ativo (estações de trabalho, servidores web, servidores de banco de dados, etc.), garantindo que apenas os serviços essenciais para a função do ativo estejam ativos e acessíveis.

Foco 80/20:

Desabilitar ou remover serviços desnecessários (SSH, MySQL, RDP, SMB) das estações de trabalho e dispositivos de convidados.

Isso reduz drasticamente a superfície de ataque.

3.Implementação de Naming Convention e Gestão de Ativos:

Padronizar a nomenclatura de hosts e garantir que todos os dispositivos na rede tenham um nome de host significativo e configurado corretamente. Integrar isso a um sistema de gestão de ativos.

Foco 80/20: Identificar e renomear os hosts genéricos ("361dee263e0e", "fsa") para facilitar o gerenciamento, monitoramento e resposta a incidentes.

6.2. Prioridade Média

1.Detecção e Inventário de Sistemas Operacionais:

Ação:

Implementar ferramentas de descoberta de ativos mais robustas que possam identificar com precisão os sistemas operacionais e versões de software.



Foco 80/20:

Melhorar a visibilidade sobre a base de sistemas operacionais permitirá priorizar patches e atualizações de segurança para os ativos mais críticos ou vulneráveis.

2. Revisão de Configurações de Segurança Padrão:

Ação:

Auditar e revisar as configurações padrão de todos os softwares e sistemas operacionais instalados na rede, removendo funcionalidades não essenciais e aplicando as melhores práticas de segurança.

Foco 80/20:

Muitos dos serviços abertos podem ser resultado de configurações padrão inseguras. A revisão minuciosa dessas configurações pode mitigar grande parte dos riscos identificados.

7. Plano de Ação

ID	Ação	Responsável	Prazo	Status	Observações
PA01	Definir e implementar regras de firewall para corp_net e guest_net bloqueando serviços desnecessários (SSH, SMB, MySQL, RDP).	Equipe de Infraestrutura/Redes	1 semana	Pendente	Prioridade Alta: Foco em estações de trabalho e rede de convidados.
PA02	Desabilitar/Remover serviços de servidor (SSH, MySQL, RDP, SMB) das estações de trabalho na corp_net.	Equipe de TI/Suporte	2 semanas	Pendente	Prioridade Alta: Reduzir superfície de ataque.
PA03	Desabilitar/Remover serviços de servidor (SSH, MySQL, RDP, SMB) dos dispositivos na guest_net.	Equipe de TI/Suporte	2 semanas	Pendente	Prioridade Alta: Reduzir superfície de ataque na rede de visitantes.
PA04	Implementar e fazer cumprir uma política de nomenclatura para todos os novos hosts.	Equipe de TI/Infraestrutura	Contínuo	Pendente	Incluir treinamento para equipes de provisionamento.
PA05	Identificar e renomear hosts com nomes genéricos (ex: "361dee263e0e", "fsa") em todas as sub-redes.	Equipe de TI/Infraestrutura	3 semanas	Pendente	Melhorar a rastreabilidade e gestão de ativos.
PA06	Adquirir/Configurar ferramenta de análise de rede para identificação precisa de SO e serviços.	Equipe de Segurança/TI	4 semanas	Pendente	Apoiar futuras auditorias de segurança.
PA07	Desenvolver padrões de hardening para cada tipo de ativo (estações, servidores web, DBs, etc.).	Equipe de Segurança/TI	6 semanas	Pendente	Base para futuras configurações e auditorias.
PA08	Auditar e aplicar as melhores práticas de segurança às configurações padrão de todos os serviços críticos.	Equipe de Segurança/TI	8 semanas	Pendente	Foco inicial em HTTP/S, MySQL, SSH.







Justificativa para o Plano

"O bloqueio imediato das portas 22, 3389 e 3306 (Prioridade Alta) reduzirá em 80% a superfície de ataque, conforme demonstrado nos scans do Anexo A. Já as ações de médio prazo (ex.: hardening) previnem explorações futuras de vulnerabilidades conhecidas."

8. Conclusão

A auditoria de mapeamento de ativos revelou um cenário de segurança que requer atenção imediata. A presença de múltiplos serviços expostos em todas as sub-redes, incluindo estações de trabalho e rede de convidados, demonstra uma falta crítica de segmentação e hardening. A implementação das recomendações propostas, com foco na abordagem 80/20, será fundamental para mitigar os riscos mais significativos e estabelecer uma base de segurança mais robusta para a empresa. A continuidade do monitoramento e auditorias periódicas serão essenciais para manter a postura de segurança.

9. Anexos

- A)  Arquivos de Logs e Scans
- B)  Planilhas de Sub-redes e Inventário
- C)  Imagens de Evidências Nmap/Rustscan
- D)  CVEs Recomendadas (XLSX)