**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 Cibersecurity  
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 Cibersecurity, 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 Cibersecurity 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: “infra\_net” (10.10.30.0/24) - Rede de infraestrutura crítica (servidores)**



**Sub-rede: guest\_net (10.10.50.0/24) - Rede de visitantes e dispositivos pessoais**



**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.**



**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**



### ****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](https://github.com/FSA-1606/desafio_kensey/tree/main/evidencias)

B) [📁 Planilhas de Sub-redes e Inventário](https://github.com/FSA-1606/desafio_kensey/tree/main/planilhas)

C) [📸 Imagens de Evidências Nmap/Rustscan](https://github.com/FSA-1606/desafio_kensey/tree/main/imagens)

D) [📊 CVEs Recomendadas (XLSX)](https://github.com/FSA-1606/desafio_kensey/blob/main/cves/CVEs_recomendadas_relatorio_pentest.xlsx?raw=true)