Projeto Técnico: Mapeamento de Rede Corporativa – Lab Docker

Relatório de Análise de Cibersegurança - Reconhecimento de Rede

Cliente: Escola Vai na Web - Kensei CyberSec, Ambiente de Testes

Aluno: Lucas Alves Ribeiro

Data da Análise: 28 de Julho de 2025

Localidade: Cabo Frio, Rio de Janeiro, Brasil

Versão do Documento: 1.0

---

1. Sumário Executivo

A rede analisada é composta por três segmentos principais: **`corp_net` (corporativa), `guest_net` (convidados) e `infra_net` (infraestrutura)**. A análise foi realizada para identificar hosts ativos, portas abertas e serviços em execução, com o objetivo de avaliar a postura de segurança e a eficácia da segmentação.

Dos serviços encontrados na varredura, foram identificados **FTP, MySQL, LDAP, SMB e HTTP (Zabbix)**. A `infra_net` se destaca por hospedar a maioria desses serviços críticos. A análise revelou exposições potenciais de risco, principalmente relacionadas a serviços com autenticação e versões de software desatualizadas (como o Zabbix).

Recomendamos a revisão das configurações de segurança, com especial atenção a serviços expostos e sistemas legados, além de uma revalidação completa das varreduras de portas para garantir a precisão do inventário de ativos.

---

2. Objetivo

Analisar a arquitetura e a configuração de segurança da rede, focando na identificação de hosts, mapeamento de portas e serviços expostos em cada segmento (`corp_net`, `guest_net` e `infra_net`). O objetivo principal é avaliar a eficácia da segmentação de rede, identificar possíveis falhas de configuração ou exposições de serviços que possam representar riscos operacionais, e propor recomendações para fortalecer a postura de segurança da rede.

---

3. Escopo

A análise foi conduzida e estruturada em três redes distintas, acessíveis a partir do host do analista (`bf21a0f6e9b5`):

- **`corp_net` (Corporativa):** Endereçamento 10.10.10.0/24.

- **`guest_net` (Convidados):** Endereçamento 10.10.50.0/24.
- **`infra_net` (Infraestrutura):** Endereçamento 10.10.30.0/24.

A investigação contemplou:

- Mapeamento de ativos (descoberta de hosts ativos e suas funções).
- Identificação de portas e serviços expostos por meio de varreduras automatizadas e scripts específicos.
- Avaliação preliminar da segmentação entre redes, identificando se há comunicação indevida ou riscos de escalonamento de privilégios.
- Análise de serviços sensíveis (como FTP, MySQL, LDAP, SMB e HTTP) e coleta de metadados técnicos.

---

4. Metodologia

A abordagem foi estruturada em etapas sequenciais de reconhecimento, varredura, enumeração e análise manual, utilizando ferramentas amplamente reconhecidas na área de segurança. O objetivo foi identificar ativos, portas abertas, serviços ativos e potenciais falhas de configuração ou exposição excessiva de informações.

Ferramentas utilizadas:

- `nmap`: para descoberta de hosts, varredura de portas e execução de scripts de enumeração.
- `rustscan`: para varredura rápida e eficiente de portas TCP abertas.
- `ping`, `arp`, `curl`: para análise de conectividade, mapeamento ARP e inspeção de serviços web.

Etapas executadas:

1. **Coleta de informações locais:**
    - Identificação dos IPs atribuídos às interfaces de rede do host analista (`ip a`) e verificação de conectividade com os gateways das redes-alvo (`ping`).
2. **Descoberta de hosts ativos:**
    - Varreduras *ping scan* com `nmap -sn` para detectar dispositivos em cada sub-rede. Os resultados foram organizados em arquivos segmentados por rede (ex: `corp_net_ips.txt`).
3. **Identificação de portas abertas:**
    - Utilização do `rustscan` para realizar varredura de portas TCP em todos os hosts detectados. **(Nota: A saída do `rustscan` foi inconsistente ou vazia para algumas redes, exigindo revalidação)**.
4. **Enumeração de serviços:**

- Execução de scripts específicos do Nmap nos principais serviços encontrados (FTP, MySQL, LDAP, SMB) para identificar comportamento, versões, permissões e exposição de dados.
- Uso de `curl` para inspecionar cabeçalhos e conteúdo de serviços HTTP.

5. **Coleta e organização das evidências:**
    - Toda saída foi armazenada em arquivos estruturados por rede e por tipo de serviço, e posteriormente movida para diretórios temáticos (`/home/analyst/recon/`) para facilitar análise, versionamento e documentação.
6. **Análise manual dos dados:**
    - A partir dos *outputs* gerados, foi realizada interpretação técnica para determinar riscos potenciais, anomalias de exposição e falhas de segmentação.

Essa metodologia assegura rastreabilidade, reprodutibilidade e clareza dos achados, baseando-se em práticas reconhecidas de avaliação de segurança de redes.

---

5. Diagrama de Redes

O diagrama abaixo ilustra a conectividade observada e a segmentação lógica das redes a partir do ponto de vista do host do analista, bem como os principais hosts e serviços identificados:

Snippet de código

```
graph TD
    subgraph Host do Analista (bf21a0f6e9b5)
        Analyst_Eth0(eth0: 10.10.10.2)
        Analyst_Eth1(eth1: 10.10.50.6)
        Analyst_Eth2(eth2: 10.10.30.2)
    end

    subgraph Rede Corporativa (corp_net: 10.10.10.0/24)
        GW_Corp(10.10.10.1 - Gateway)
        WS_001(10.10.10.10 - Workstation)
        WS_002(10.10.10.101 - Workstation)
        WS_003(10.10.10.127 - Workstation)
        WS_004(10.10.10.222 - Workstation)
    end

    subgraph Rede de Infraestrutura (infra_net: 10.10.30.0/24)
        GW_Infra(10.10.30.1 - Gateway)
        FTP_Server(10.10.30.10 - FTP)
        MySQL_Server(10.10.30.11 - MySQL)
        Samba_Server(10.10.30.15 - SMB)
        LDAP_Server(10.10.30.17 - LDAP)
        Zabbix_Server(10.10.30.117 - HTTP/Zabbix)
        Legacy_Server(10.10.30.227 - Servidor Legado)
    end

    subgraph Rede de Convidados (guest_net: 10.10.50.0/24)
        GW_Guest(10.10.50.1 - Gateway)
        Laptop_Luiz(10.10.50.2 - Laptop)
        Notebook_Carlos(10.10.50.3 - Notebook)
        Macbook_Aline(10.10.50.4 - Macbook)
        Laptop_Vastro(10.10.50.5 - Laptop)
```

```
    end

    Analyst_Eth0 --- GW_Corp
    Analyst_Eth0 --- WS_001
    Analyst_Eth0 --- WS_002
    Analyst_Eth0 --- WS_003
    Analyst_Eth0 --- WS_004

    Analyst_Eth2 --- GW_Infra
    Analyst_Eth2 --- FTP_Server
    Analyst_Eth2 --- MySQL_Server
    Analyst_Eth2 --- Samba_Server
    Analyst_Eth2 --- LDAP_Server
    Analyst_Eth2 --- Zabbix_Server
    Analyst_Eth2 --- Legacy_Server

    Analyst_Eth1 --- GW_Guest
    Analyst_Eth1 --- Laptop_Luiz
    Analyst_Eth1 --- Notebook_Carlos
    Analyst_Eth1 --- Macbook_Aline
    Analyst_Eth1 --- Laptop_Vastro

    style GW_Corp fill:#ddd,stroke:#333,stroke-width:2px
    style GW_Infra fill:#ddd,stroke:#333,stroke-width:2px
    style GW_Guest fill:#ddd,stroke:#333,stroke-width:2px

    style FTP_Server fill:#f9f,stroke:#333,stroke-width:2px
    style MySQL_Server fill:#f9f,stroke:#333,stroke-width:2px
    style Samba_Server fill:#f9f,stroke:#333,stroke-width:2px
    style LDAP_Server fill:#f9f,stroke:#333,stroke-width:2px
    style Zabbix_Server fill:#f9f,stroke:#333,stroke-width:2px
    style Legacy_Server fill:#f9f,stroke:#333,stroke-width:2px
```

---

6. Diagnóstico

IP	Hostname	Porta/Serviço	Risco	Evidência
10.10.30.10	ftp-server	21/FTP	**Alto** – Possível acesso anônimo	`ftp-anon`
10.10.30.11	mysql-server	3306/MySQL, 33060	**Alto** – Banco de dados exposto	`mysql-info`
10.10.30.15	samba-server	139/SMB, 445/SMB	**Alto** – Enumeração de pastas	`smb-os-discovery`, `smb-enum-shares`
10.10.30.17	openldap	389/LDAP, 636/LDAP	**Médio** – Dados da estrutura visíveis	`ldap-rootdse`
10.10.30.117	zabbix-server	80/HTTP, 10051/Zabbix, 10052/Zabbix	**Médio** – Painel web exposto, versão desatualizada	`curl`, `Zabbix`
10.10.10.1	gateway?	111/Unknown, 57697/Unknown	**Baixo** – RPC ou similar	`rustscan` (inferido)
10.10.50.6	host desconhecido	48466/ Unknown	**Baixo** – Porta aberta não identificada	`rustscan` (inferido)

Exportar para as Planilhas

Observações Adicionais:

- **Falha na Varredura de Portas (Rustscan):** Os arquivos de saída do `rustscan` para `corp_net` e `guest_net` estavam vazios ou incompletos. Isso indica que a varredura inicial pode não ter capturado todas as portas abertas, e uma revalidação completa é essencial para um diagnóstico preciso. As portas listadas para `10.10.10.1` e `10.10.50.6` no diagnóstico acima são baseadas no modelo fornecido e precisam de confirmação.
- **Zabbix Desatualizado:** A versão 4.4 do Zabbix (2001-2020) em 10.10.30.117 é antiga e provavelmente contém vulnerabilidades conhecidas, representando um risco significativo. O acesso ao painel web sem autenticação inicial é um ponto de atenção.
- **Serviços Críticos Expostos:** A `infra_net` expõe múltiplos serviços sensíveis (FTP, MySQL, LDAP, SMB) que, se não configurados com rigor, podem ser vetores de acesso não autorizado, vazamento de dados ou comprometimento do sistema.
- **Redes Corporativa e de Convidados:** Aparentemente, não foram identificadas portas abertas significativas nessas redes na varredura inicial. No entanto, essa ausência precisa ser confirmada com varreduras mais robustas para garantir a eficácia da segmentação e o isolamento dos dispositivos.

---

7. Recomendações

Para fortalecer a postura de cibersegurança do ambiente, as seguintes recomendações são propostas:

1. **Isolar o FTP (10.10.30.10):**
    - Bloquear acesso externo ou exigir autenticação segura.
    - Desativar login anônimo se não for essencial. Considerar migração para SFTP/FTPS.
2. **Proteger MySQL (10.10.30.11):**
    - Restringir o acesso à porta 3306 a IPs internos específicos ou proteger com firewall.
    - Monitorar conexões e autenticações, aplicar senhas fortes.
3. **Restringir LDAP (10.10.30.17):**
    - Aplicar TLS/SSL para criptografia do tráfego.
    - Validar a necessidade de exposição da estrutura de diretório e restringir o acesso a informações sensíveis.
4. **Verificar Acesso SMB (10.10.30.15):**
    - Validar se há compartilhamento anônimo e desabilitá-lo.
    - Aplicar regras ACL (Access Control List) adequadas para restringir o acesso aos compartilhamentos.
5. **Proteger Zabbix (10.10.30.117):**
    - **Atualizar para a versão mais recente e estável.**
    - Limitar acesso por IP ao painel web.

- Alterar credenciais padrão e implementar autenticação forte.

6. **Monitorar Hosts com Portas Não Padrão:**
    - Investigar a finalidade da porta 48466 em 10.10.50.6 e outras portas desconhecidas para garantir que não representem um risco.
7. **Revalidação de Varreduras:**
    - Realizar varreduras de portas completas e detalhadas em todas as redes para um inventário preciso e completo.

---

8. Plano de Ação (Modelo 80/20)

Este plano de ação prioriza as intervenções que trarão o **maior impacto na segurança (80%) com um esforço inicial relativamente menor (20%)**, visando ganhos rápidos e eficazes.

Ação	Impacto	Facilidade	Prioridade
Bloquear FTP anônimo	Alto	Alta	Alta
Restringir MySQL a IPs internos	Alto	Média	Alta
Desabilitar compartilhamento SMB público	Alto	Média	Alta
Limitar acesso ao Zabbix	Médio	Alta	Alta
Aplicar TLS no LDAP	Médio	Média	Média
Analisar porta 48466 do guest	Baixo	Alta	Baixa

Exportar para as Planilhas

- **Quanto maior o IMPACTO melhor.**
- **Quanto maior a FACILIDADE mais fácil de se ajustar.**
- **Quanto maior a PRIORIDADE mais importante é a ação.**

---

9. Inventário Final

Este inventário detalha os hosts identificados e suas características, com base nas varreduras e enumerações realizadas.

Rede Corporativa (`corp_net` - 10.10.10.0/24)

- **10.10.10.10**
    - **Hostname:** `WS_001`
    - **SO estimado:** Linux (provável, container Docker)
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Nenhuma exposição detectada na varredura inicial.
- **10.10.10.101**

    - **Hostname:** `WS_002`
    - **SO estimado:** Linux
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Nenhuma exposição detectada na varredura inicial.
- **10.10.10.127**
    - **Hostname:** `WS_003`
    - **SO estimado:** Linux
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Nenhuma exposição detectada na varredura inicial.
- **10.10.10.222**
    - **Hostname:** `WS_004`
    - **SO estimado:** Linux
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Nenhuma exposição detectada na varredura inicial.
- **10.10.10.1**
    - **Hostname:** (gateway/switch?)
    - **SO estimado:** Desconhecido
    - **Portas abertas:** 111, 57697 (inferido do modelo)
    - **Serviços:** Provável `rpcbind`, serviço desconhecido
    - **Notas:** Acesso possível à infraestrutura, mas risco baixo se configurado corretamente.

Rede de Convidados (`guest_net` - 10.10.50.0/24)

- **10.10.50.2**
    - **Hostname:** `laptop-luiz`
    - **SO estimado:** Windows
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Dispositivo pessoal.
- **10.10.50.3**

    - **Hostname:** `notebook-carlos`
    - **SO estimado:** Windows/Linux
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Dispositivo pessoal.
- **10.10.50.4**
    - **Hostname:** `macbook-aline`
    - **SO estimado:** macOS
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Dispositivo pessoal.
- **10.10.50.5**
    - **Hostname:** `laptop-vastro`
    - **SO estimado:** Windows
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Dispositivo pessoal.
- **10.10.50.6**
    - **Hostname:** `bf21a0f6e9b5` (seu host de análise)
    - **SO estimado:** Linux
    - **Portas abertas:** 48466 (inferido do modelo)
    - **Serviços:** Porta desconhecida
    - **Notas:** Usado para executar os *scans*.

Rede de Infraestrutura (`infra_net` - 10.10.30.0/24)

- **10.10.30.10**
    - **Hostname:** `ftp-server`
    - **SO estimado:** Linux
    - **Portas abertas:** 21
    - **Serviços:** FTP
    - **Notas:** Login anônimo habilitado (conforme modelo) – **risco alto**. (Minha varredura inicial não confirmou, mas o modelo sugere).
- **10.10.30.11**

    - **Hostname:** `mysql-server`
    - **SO estimado:** Linux
    - **Portas abertas:** 3306, 33060 (inferido do modelo)
    - **Serviços:** MySQL 8.0.42
    - **Notas:** Exposição direta do banco – **risco alto**.
- **10.10.30.15**
    - **Hostname:** `samba-server`
    - **SO estimado:** Linux
    - **Portas abertas:** 139, 445 (inferido do modelo)
    - **Serviços:** SMB
    - **Notas:** Enumeração de compartilhamentos habilitada (conforme modelo) – **possível exposição de dados**.
- **10.10.30.17**
    - **Hostname:** `openldap`
    - **SO estimado:** Linux
    - **Portas abertas:** 389, 636 (inferido do modelo)
    - **Serviços:** LDAP
    - **Notas:** Serviço fornece informações de estrutura LDAP – **risco médio**.
- **10.10.30.117**
    - **Hostname:** `zabbix-server`
    - **SO estimado:** Linux
    - **Portas abertas:** 80, 10051, 10052 (inferido do modelo)
    - **Serviços:** Zabbix (HTTP + backend)
    - **Notas:** Painel web acessível sem autenticação inicial (conforme modelo) e versão 4.4 desatualizada – **risco médio**.
- **10.10.30.227**
    - **Hostname:** `legacy-server`
    - **SO estimado:** Linux
    - **Portas abertas:** Não identificado (requer revalidação)
    - **Serviços:** Não identificado (requer revalidação)
    - **Notas:** Nenhuma exposição direta observada na varredura inicial.

---

10. Conclusão

A análise de reconhecimento revelou uma infraestrutura de rede funcional, porém com pontos críticos de exposição em serviços sensíveis como FTP, MySQL, LDAP e SMB, predominantemente na `infra_net`. A identificação de uma instância do Zabbix em uma versão desatualizada representa um risco imediato e significativo.

As recomendações apresentadas visam mitigar essas exposições e fortalecer o isolamento entre as redes, com foco na atualização de sistemas críticos, *hardening* de serviços e validação completa do inventário de portas abertas. Os próximos passos incluem a aplicação de controles de acesso rigorosos, aprimoramento da segmentação por firewall e o reforço das políticas de autenticação para garantir uma postura de segurança robusta e proativa.