Autor: Diogo Nogueira de Sousa
Data: 28/07/2025
Versão: [1.0]

RELATÓRIO DE MAPEAMENTO DE REDE CORPORATIVA – LAB DOCKER

Índice

Sumário Executivo

A presente análise de segurança foi conduzida no ambiente de rede corporativo simulado, queSumário Executivo éSumário Executivo dividido em três segmentos: a rede corporativa (`corp_net`), a rede de visitantes (`guest_net`) e a rede de infraestrutura (`infra_net`). O objetivo foi avaliar a eficácia da segmentação e identificar riscos de exposição de serviços.SumárioSumário Executivo Executivo

A análise revelou que, enquanto as redes corporativa e de visitantes demonstram uma boa postura de segurança ao não exporem serviços, a **rede de infraestrutura apresenta um risco de segurança crítico**. Foi identificado que servidores essenciais para a operação, como o de autenticação (LDAP), banco de dados (MySQL) e compartilhamento de arquivos (Samba), coexistem na mesma rede sem segmentação interna.

O principal risco associado a essa arquitetura plana é a **facilidade de movimentação lateral**: uma violação em um serviço menos seguro, como o servidor de FTP (que transmite dados em texto claro), pode servir como ponto de partida para um ataque direto aos ativos mais críticos da empresa.

Diante disso, a recomendação mais urgente é a **micro-segmentação da rede de infraestrutura**, criando zonas isoladas para os diferentes tipos de servidores e aplicando regras de firewall estritas entre elas. A implementação desta e de outras medidas detalhadas neste relatório irá mitigar significativamente o risco de um comprometimento em cascata e proteger os dados e serviços vitais da organização.

Objetivo

O objetivo deste relatório é apresentar os resultados de uma análise de segurança conduzida na rede corporativa simulada. O trabalho buscou:

- Identificar e inventariar todos os ativos digitais presentes nas sub-redes `corp_net`, `infra_net` e `guest_net`.
- Mapear os serviços e portas expostas em cada ativo para determinar a superfície de ataque da rede.
- Diagnosticar falhas na política de segmentação e identificar riscos de segurança decorrentes da configuração atual.
- Propor recomendações técnicas e um plano de ação para mitigar as vulnerabilidades encontradas e fortalecer a postura de segurança da organização.

Escopo

A análise de segurança foi estritamente limitada ao ambiente de laboratório simulado, orquestrado via Docker e Docker Compose, conforme fornecido no desafio do projeto.

O escopo do trabalho abrangeu todos os ativos contidos nas três sub-redes pré-definidas:

- **Rede Corporativa (`corp_net`):** O segmento de rede `10.10.10.0/24`, contendo as estações de trabalho dos funcionários.

- **Rede de Infraestrutura (`infra_net`):** O segmento de rede `10.10.30.0/24`, onde residem os servidores de serviços críticos como FTP, MySQL, Samba e LDAP.
- **Rede de Visitantes (`guest_net`):** O segmento de rede `10.10.50.0/24`, destinado a dispositivos de convidados.

A análise incluiu a varredura de todos os hosts ativos descobertos dentro desses três segmentos. Quaisquer sistemas ou redes fora desses limites não fizeram parte desta avaliação.

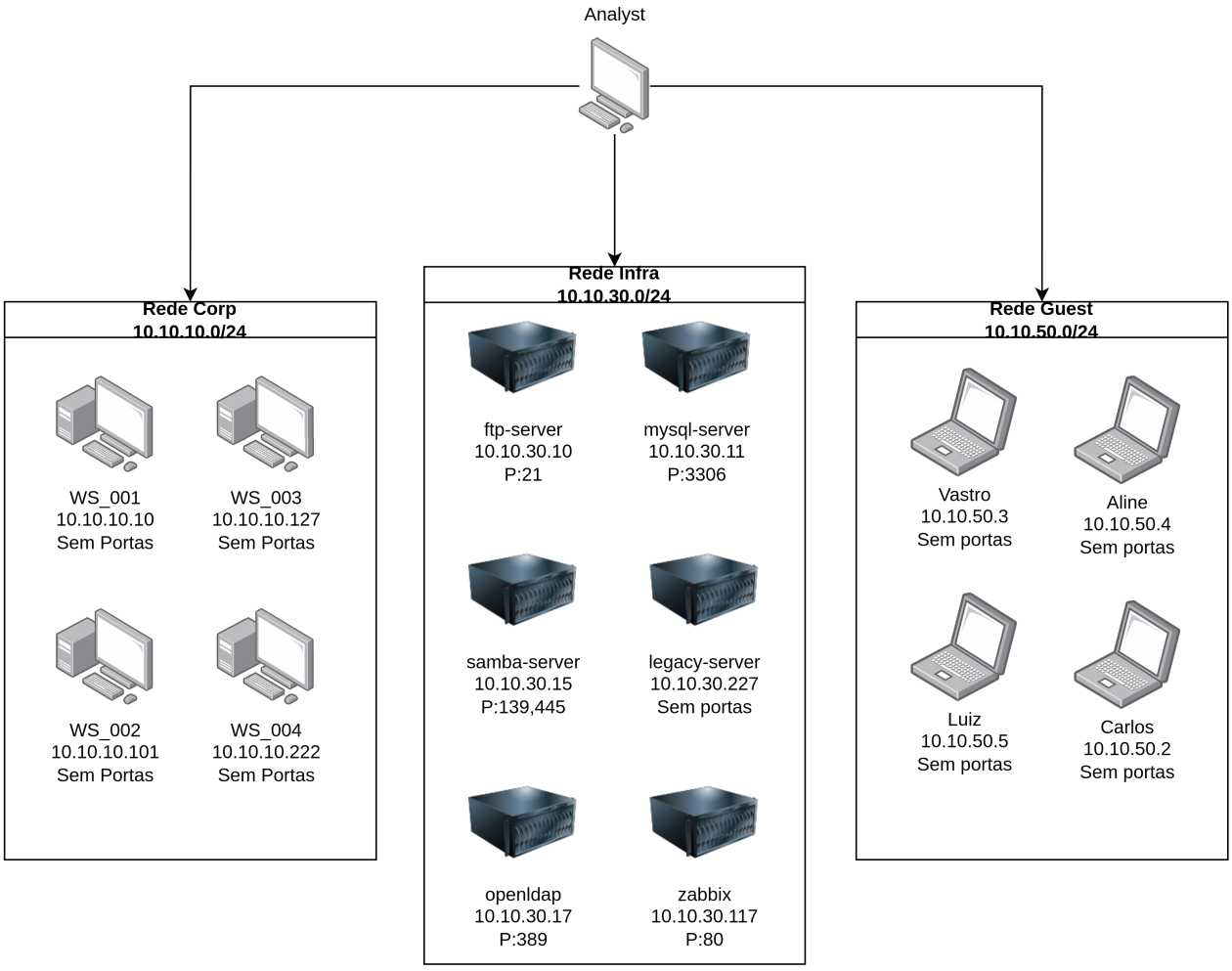
Metodologia

A análise da rede foi conduzida seguindo uma metodologia de reconhecimento ativo em fases, com o objetivo de construir um inventário completo dos ativos e identificar suas exposições de forma eficiente e confiável.

O processo foi dividido nas seguintes etapas:

1. **Descoberta de Hosts (Host Discovery):** A primeira fase consistiu em identificar os hosts ativos em cada uma das três sub-redes (`10.10.10.0/24`, `10.10.30.0/24`, `10.10.50.0/24`). Para esta tarefa, foi utilizada a ferramenta **Nmap** com a técnica de "Ping Scan" (`-sn`), que permite mapear rapidamente os dispositivos responsivos na rede sem realizar uma varredura de portas invasiva.
2. **Varredura de Portas e Serviços (Service Scanning):** Com a lista de hosts ativos em mãos, a segunda fase focou em uma análise detalhada de cada alvo. Foi empregada novamente a ferramenta **Nmap** para realizar uma varredura completa de portas, com os seguintes parâmetros:
    - **-sV:** Para detectar as versões dos serviços em execução em cada porta aberta.
    - **-sC:** Para utilizar scripts padrão de enumeração e coletar informações contextuais sobre os serviços.
    - **-T4:** Para otimizar o tempo de varredura, mantendo um equilíbrio entre velocidade e confiabilidade.
3. **Análise Manual e Documentação:** Os resultados de todas as varreduras foram salvos e consolidados. A etapa final consistiu na análise manual desses dados para correlacionar informações, identificar riscos de segurança, avaliar a eficácia da segmentação da rede e, por fim, compilar os achados, recomendações e conclusões apresentadas neste relatório.

Diagrama de Rede



Diagnóstico

Achado 1: Servidor de Autenticação (LDAP) Exposto na Rede de Infraestrutura

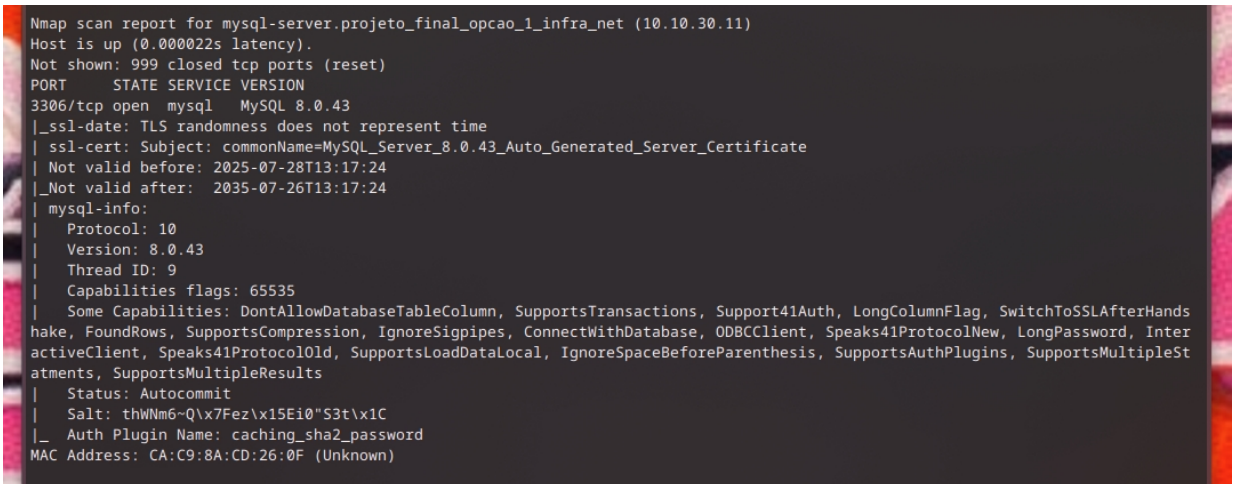
- **Descrição:** O servidor OpenLDAP (`10.10.30.17`), que gerencia a autenticação central de usuários, está diretamente acessível por todos os outros servidores na mesma sub-rede.
- **Evidência:**

```
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000024s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp open  ldapssl?
MAC Address: 6A:4F:3B:C5:3B:AF (Unknown)
```

- **Impacto: CRÍTICO**. Este é o maior risco. Se qualquer outro servidor na rede for comprometido (como o de FTP), um invasor pode lançar ataques diretos para roubar senhas, criar usuários ou paralisar o acesso a todos os sistemas da empresa.

Achado 2: Servidor de Banco de Dados (MySQL) Exposto na Rede de Infraestrutura

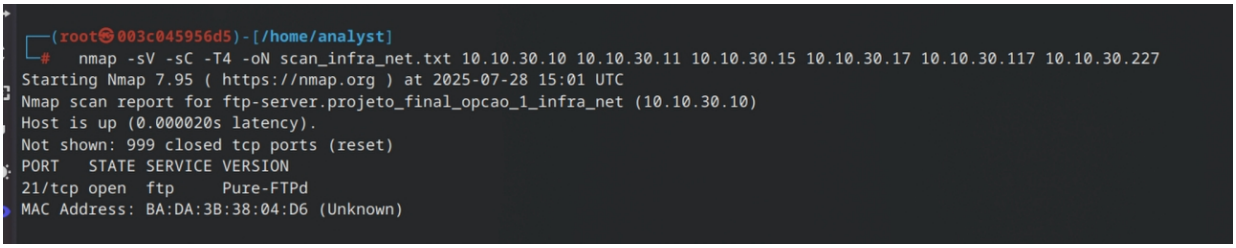
- **Descrição:** O servidor de banco de dados MySQL (`10.10.30.11`), que armazena dados críticos, está diretamente acessível na rede.
- **Evidência:**



- **Impacto: ALTO**. A exposição direta do banco de dados aumenta o risco de vazamento ou sequestro (ransomware) de dados, além de ataques de força bruta para adivinhar senhas. Um invasor pode acessar, modificar ou destruir informações vitais para o negócio.

Achado 3: Uso de Protocolo Inseguro para Transferência de Arquivos (FTP)

- **Descrição:** Um servidor FTP (`10.10.30.10`) está em operação, utilizando um protocolo que não criptografa a comunicação.
- **Evidência:**

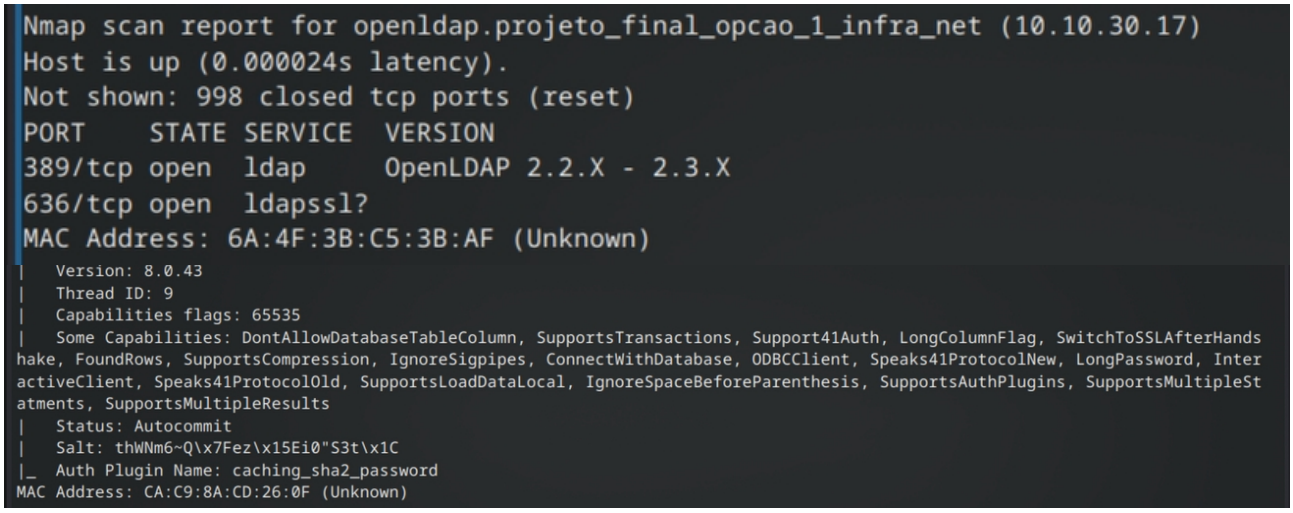


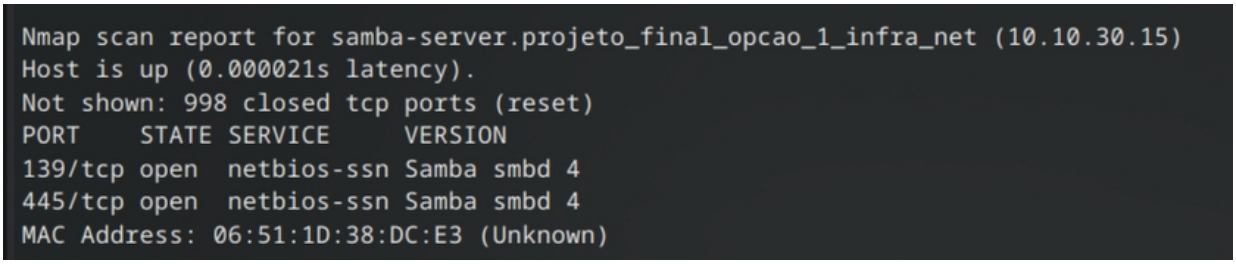
- **Impacto: MÉDIO**. O protocolo FTP transmite senhas e arquivos em texto claro. Qualquer pessoa na rede pode capturar essas informações. As credenciais roubadas do FTP podem ser as mesmas usadas em outros sistemas, servindo como porta de entrada para ataques mais graves.

Achado 4: Ausência de Segmentação na Rede de Infraestrutura

- **Descrição:** A própria arquitetura da rede `infra_net` é uma vulnerabilidade. Servidores com funções e níveis de criticidade completamente diferentes (autenticação, banco de dados, arquivos, monitoramento) coexistem na mesma rede, sem isolamento entre si.

- **Evidência:** A saída combinada do scan da rede `10.10.30.0/24`, que mostra múltiplos serviços críticos (LDAP, MySQL, Samba) na mesma sub-rede.





- **Impacto: ALTO**. Essa "rede plana" facilita a **movimentação lateral**. Se um invasor comprometer o servidor menos seguro (como o Zabbix na porta 80), ele tem um caminho livre para atacar os alvos mais valiosos (LDAP e MySQL) sem nenhuma barreira de rede.

Recomendações

Recomendação 1: Desativar o serviço FTP e substituí-lo por SFTP.

- **Ação Concreta:** Desativar permanentemente o serviço Pure-FTPd no servidor `10.10.30.10` e implementar um serviço de SFTP (Secure File Transfer Protocol), que opera sobre o protocolo SSH.
- **Justificativa:** O protocolo FTP, operando na porta 21, é inerentemente inseguro, pois transmite credenciais de acesso e dados em texto claro. Isso permite que qualquer ator mal-intencionado na mesma rede possa capturar essas informações sensíveis. A substituição por SFTP garante que toda a comunicação seja criptografada, protegendo a confidencialidade e a integridade dos dados em trânsito.

Recomendação 2: Implementar micro-segmentação na rede de infraestrutura.

- **Ação Concreta:** Dividir a rede `infra_net` (`10.10.30.0/24`) em múltiplas sub-redes menores e isoladas (VLANs), agrupando os servidores por função. Sugere-se a criação de, no mínimo, as seguintes zonas:

    - **Zona de Bancos de Dados:** Contendo apenas o `mysql-server` (10.10.30.11).
    - **Zona de Autenticação:** Contendo apenas o `openldap` (10.10.30.17).
    - **Zona de Serviços Gerais:** Contendo os demais servidores como Samba e Zabbix.
- **Justificativa:** A arquitetura atual da `infra_net` é plana, o que facilita a movimentação lateral. Caso um servidor seja comprometido, o invasor tem acesso direto para atacar todos os outros na mesma rede. A micro-segmentação cria barreiras, de modo que uma violação no servidor Zabbix, por exemplo, não permitiria acesso direto ao servidor de banco de dados, limitando o impacto de um incidente.

Recomendação 3: Aplicar uma política de firewall com regras restritivas (Default Deny).

- **Ação Concreta:** Configurar um firewall para controlar o tráfego entre as novas sub-redes e entre a rede corporativa e a de infraestrutura. A política deve ser "negar tudo por padrão" (`default deny`), e devem ser criadas regras explícitas apenas para as comunicações estritamente necessárias. (Ex: Permitir que apenas o servidor de aplicação acesse a porta 3306 do `mysql-server`).
- **Justificativa:** Atualmente, a falta de um firewall interno permite que qualquer máquina na rede tente se comunicar com os serviços críticos. Uma política de `default deny` garante que apenas comunicações legítimas e autorizadas sejam permitidas, aplicando o princípio do menor privilégio e reduzindo drasticamente a superfície de ataque.

Recomendação 4: Realizar uma auditoria de configuração e hardening nos serviços expostos.

- **Ação Concreta:** Realizar uma revisão de segurança detalhada nas configurações dos serviços `samba-server`, `openldap` e `zabbix-server`. Isso inclui verificar senhas padrão, permissões de compartilhamento anônimas, e garantir que apenas os módulos e funcionalidades essenciais estejam habilitados.
- **Justificativa:** Embora os serviços estejam operacionais, suas configurações padrão podem conter fraquezas. Uma auditoria (hardening) garante que eles estejam configurados para operar de forma segura, desabilitando funcionalidades de risco e aplicando as melhores práticas de segurança para cada tecnologia, prevenindo exposições desnecessárias.
-

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Substituir FTP inseguro por SFTP	Alto	Alta	Alta
Micro-segmentar a rede de infraestrutura	Alto	Média	Alta
Aplicar política de firewall Default Deny	Alto	Média	Alta
Realizar	Médio	Média	Média

hardening nos
serviços expostos

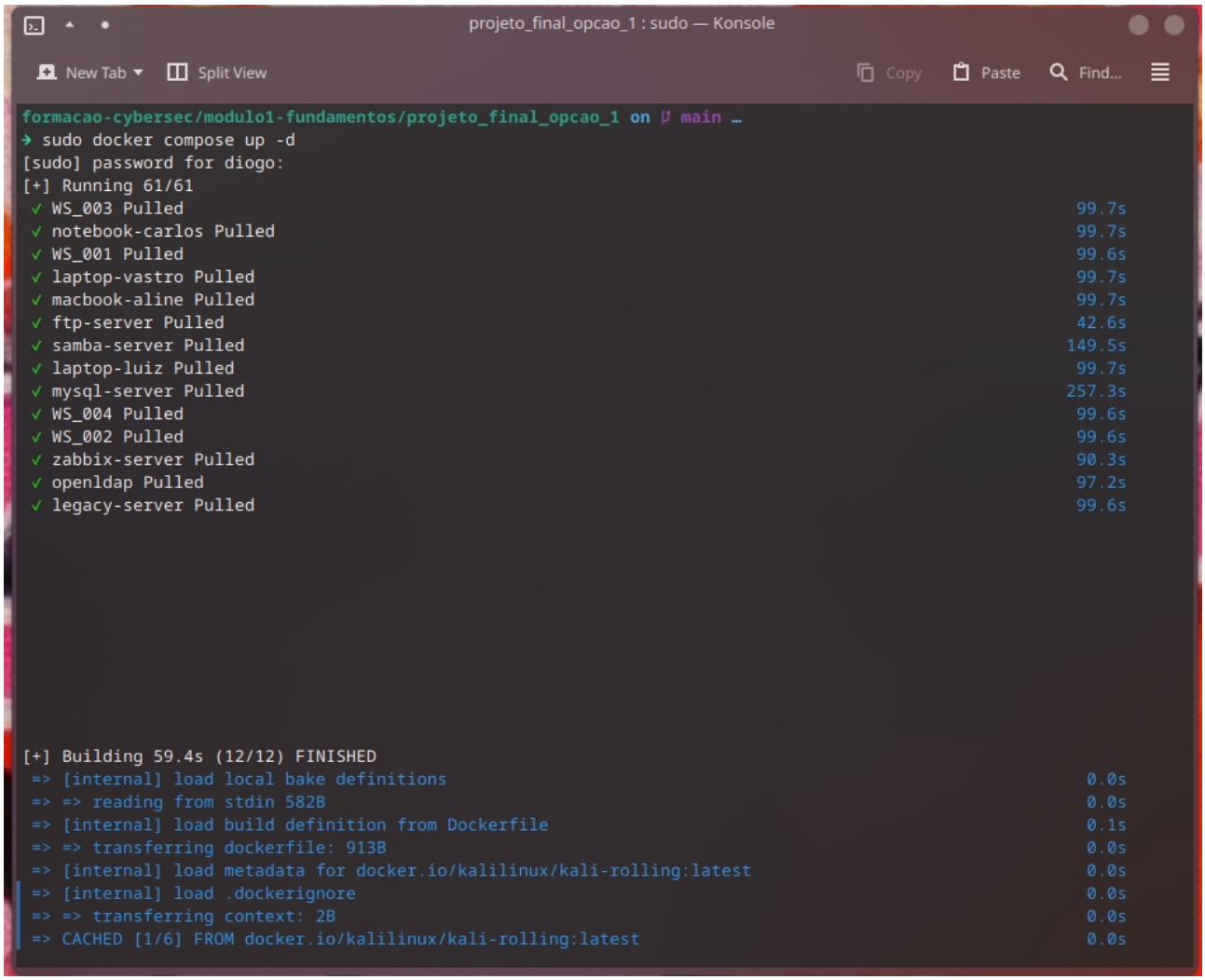
Conclusão

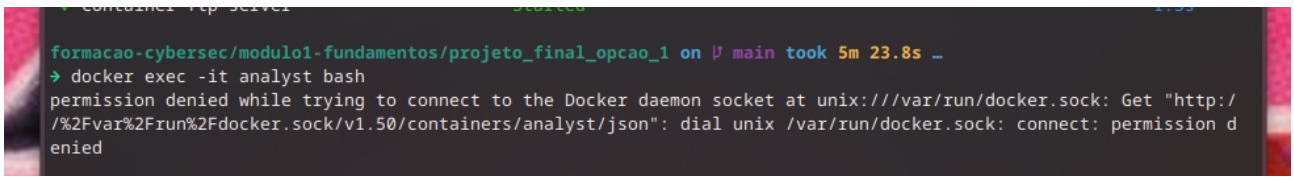
A análise de segurança revelou uma arquitetura de rede com um nível de maturidade de segurança misto. Por um lado, as redes corporativa e de visitantes apresentam uma configuração segura, com estações de trabalho e dispositivos de convidados devidamente isolados e sem exposição de serviços, o que é uma prática recomendável.

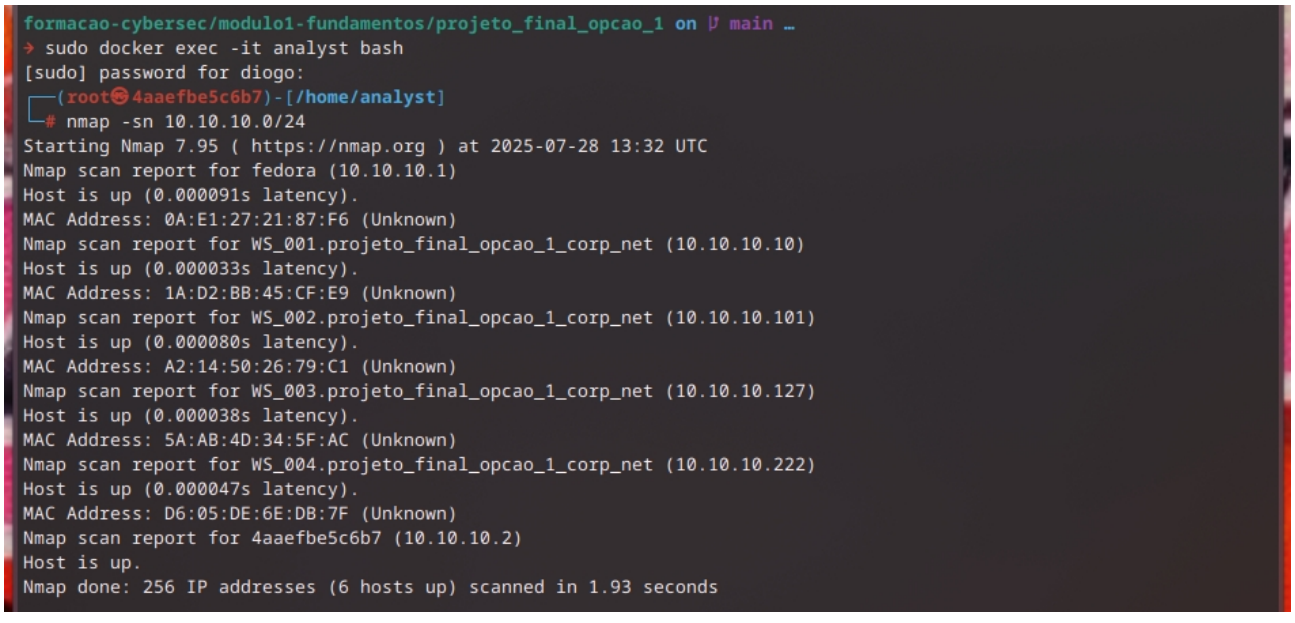
Por outro lado, a **rede de infraestrutura (`infra_net`) representa um risco significativo e imediato** para a segurança da organização. A ausência de segmentação interna (arquitetura plana) permite que servidores críticos, incluindo os de autenticação, banco de dados e arquivos, fiquem diretamente expostos a um possível ataque de movimentação lateral, originado a partir do comprometimento de um único serviço menos seguro, como o de FTP.

Recomenda-se fortemente que a organização adote as medidas propostas neste relatório, com especial urgência para a **implementação da micro-segmentação e a aplicação de políticas de firewall restritivas**, conforme detalhado no Plano de Ação. A execução dessas tarefas é fundamental para mitigar os riscos identificados e elevar a postura de segurança da infraestrutura a um nível robusto e resiliente.

Anexos


projeto_final_opcao_1 : sudo — Konsole
New Tab
Split View
Copy
Paste
Find...
formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1 on main …
sudo docker compose up -d
[sudo] password for diogo:
[+] Running 61/61
WS_003 Pulled 99.7s
notebook-carlos Pulled 99.7s
WS_001 Pulled 99.6s
laptop-vastro Pulled 99.7s
macbook-aline Pulled 99.7s
ftp-server Pulled 42.6s
samba-server Pulled 149.5s
laptop-luiz Pulled 99.7s
mysql-server Pulled 257.3s
WS_004 Pulled 99.6s
WS_002 Pulled 99.6s
zabbix-server Pulled 90.3s
openldap Pulled 97.2s
legacy-server Pulled 99.6s
[+] Building 59.4s (12/12) FINISHED
=> [internal] load local bake definitions 0.0s
=> => reading from stdin 582B 0.0s
=> [internal] load build definition from Dockerfile 0.1s
=> => transferring dockerfile: 913B 0.0s
=> [internal] load metadata for docker.io/kalilinux/kali-rolling:latest 0.0s
=> [internal] load .dockerignore 0.0s
=> => transferring context: 2B 0.0s
=> CACHED [1/6] FROM docker.io/kalilinux/kali-rolling:latest 0.0s


formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1 on main took 5m 23.8s …
docker exec -it analyst bash
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.50/containers/analyst/json": dial unix /var/run/docker.sock: connect: permission denied


formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1 on main …
sudo docker exec -it analyst bash
[sudo] password for diogo:
(root㉿4aaefbe5c6b7)-[/home/analyst]
nmap -sn 10.10.10.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-07-28 13:32 UTC
Nmap scan report for fedora (10.10.10.1)
Host is up (0.000091s latency).
MAC Address: 0A:E1:27:21:87:F6 (Unknown)
Nmap scan report for WS_001.projeto_final_opcao_1_corp_net (10.10.10.10)
Host is up (0.000033s latency).
MAC Address: 1A:D2:BB:45:CF:E9 (Unknown)
Nmap scan report for WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)
Host is up (0.000080s latency).
MAC Address: A2:14:50:26:79:C1 (Unknown)
Nmap scan report for WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)
Host is up (0.000038s latency).
MAC Address: 5A:AB:4D:34:5F:AC (Unknown)
Nmap scan report for WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)
Host is up (0.000047s latency).
MAC Address: D6:05:DE:6E:DB:7F (Unknown)
Nmap scan report for 4aaefbe5c6b7 (10.10.10.2)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.93 seconds

```
┌──(root㉿4aaefbe5c6b7)-[/home/analyst]
└─# nmap -sn 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:32 UTC
Nmap scan report for fedora (10.10.30.1)
Host is up (0.00013s latency).
MAC Address: 86:34:76:7A:E9:09 (Unknown)
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000031s latency).
MAC Address: DE:13:BD:49:93:3A (Unknown)
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000030s latency).
MAC Address: 56:01:8F:88:2C:A1 (Unknown)
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000050s latency).
MAC Address: 62:A1:46:A7:8E:BA (Unknown)
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000038s latency).
MAC Address: FA:8E:60:0B:1E:DC (Unknown)
Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000064s latency).
MAC Address: 8A:B0:68:80:24:4D (Unknown)
Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000070s latency).
MAC Address: CA:98:FE:8F:52:1A (Unknown)
Nmap scan report for 4aaefbe5c6b7 (10.10.30.2)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.05 seconds
```

```
┌──(root㉿4aaefbe5c6b7)-[/home/analyst]
└─# nmap -sn 10.10.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 13:33 UTC
Nmap scan report for fedora (10.10.50.1)
Host is up (0.000094s latency).
MAC Address: AE:81:8E:35:81:C3 (Unknown)
Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000033s latency).
MAC Address: 22:4B:E2:FE:70:41 (Unknown)
Nmap scan report for laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.3)
Host is up (0.000027s latency).
MAC Address: 9A:50:FD:7B:49:58 (Unknown)
Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000030s latency).
MAC Address: 8E:D4:E9:83:FA:1E (Unknown)
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000053s latency).
MAC Address: B2:50:70:10:CD:D7 (Unknown)
Nmap scan report for 4aaefbe5c6b7 (10.10.50.6)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.07 seconds
```

```
┌──(root㉿003c045956d5)-[/home/analyst]
└─# nmap -sV -sC -T4 -oN scan_corp_net.txt 10.10.10.10 10.10.10.101 10.10.10.127 10.10.10.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 14:35 UTC
Nmap scan report for WS_001.projeto_final_opcao_1_corp_net (10.10.10.10)
Host is up (0.000032s latency).
All 1000 scanned ports on WS_001.projeto_final_opcao_1_corp_net (10.10.10.10) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 96:D8:B4:AB:2C:C8 (Unknown)

Nmap scan report for WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)
Host is up (0.000041s latency).
All 1000 scanned ports on WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 0A:57:E3:8D:92:20 (Unknown)

Nmap scan report for WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)
Host is up (0.000036s latency).
All 1000 scanned ports on WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 62:E2:9C:5C:59:05 (Unknown)

Nmap scan report for WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)
Host is up (0.000032s latency).
All 1000 scanned ports on WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 52:20:3B:C8:20:F2 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 1.67 seconds
```

```
┌──(root㉿003c045956d5)-[/home/analyst]
└─# nmap -sV -sC -T4 -oN scan_guest_net.txt 10.10.50.2 10.10.50.3 10.10.50.4 10.10.50.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:01 UTC
Nmap scan report for 003c045956d5 (10.10.50.2)
Host is up (0.000020s latency).
All 1000 scanned ports on 003c045956d5 (10.10.50.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.3)
Host is up (0.000038s latency).
All 1000 scanned ports on laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 72:11:08:EC:F4:E6 (Unknown)

Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000036s latency).
All 1000 scanned ports on macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EE:F5:FA:07:B7:F8 (Unknown)

Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000031s latency).
All 1000 scanned ports on notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.5) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: F6:F1:BA:E5:D7:CE (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (4 hosts up) scanned in 1.05 seconds
```

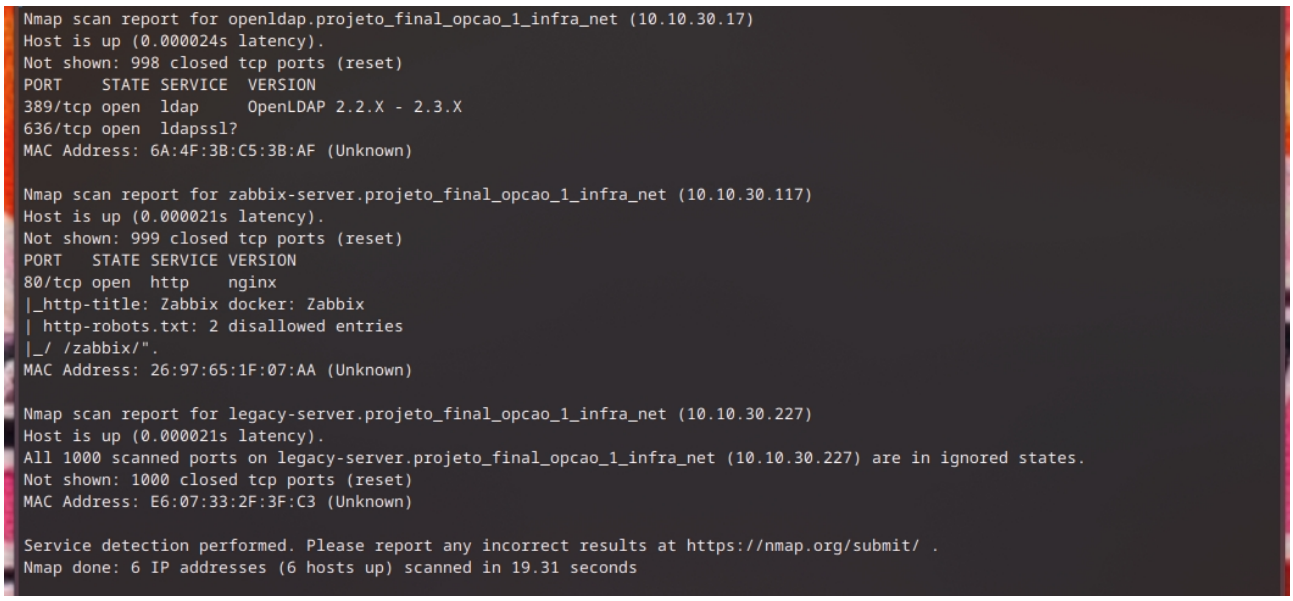
```
┌──(root㉿003c045956d5)-[/home/analyst]
└─#   nmap -sV -sC -T4 -oN scan_infra_net.txt 10.10.30.10 10.10.30.11 10.10.30.15 10.10.30.17 10.10.30.117 10.10.30.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 15:01 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd
MAC Address: BA:DA:3B:38:04:D6 (Unknown)

Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000022s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 8.0.43
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_8.0.43_Auto_Generated_Server_Certificate
| Not valid before: 2025-07-28T13:17:24
|_Not valid after:  2035-07-26T13:17:24
| mysql-info:
|   Protocol: 10
|   Version: 8.0.43
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: DontAllowDatabaseTableColumn, SupportsTransactions, Support41Auth, LongColumnFlag, SwitchToSSLAfterHands
hake, FoundRows, SupportsCompression, IgnoreSigpipes, ConnectWithDatabase, ODBCClient, Speaks41ProtocolNew, LongPassword, Inter
activeClient, Speaks41ProtocolOld, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleSt
atments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: thWNm6~Q\x7Fez\x15Ei0"S3t\x1C
|_  Auth Plugin Name: caching_sha2_password
MAC Address: CA:C9:8A:CD:26:0F (Unknown)

Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000021s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
MAC Address: 06:51:1D:38:DC:E3 (Unknown)

Host script results:
|_clock-skew: -1s
| smb2-time:
|   date: 2025-07-28T15:01:14
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000024s latency).
```



```
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000024s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp open  ldapssl?
MAC Address: 6A:4F:3B:C5:3B:AF (Unknown)

Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx
|_http-title: Zabbix docker: Zabbix
| http-robots.txt: 2 disallowed entries
|_/ /zabbix/".
MAC Address: 26:97:65:1F:07:AA (Unknown)

Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000021s latency).
All 1000 scanned ports on legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: E6:07:33:2F:3F:C3 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 6 IP addresses (6 hosts up) scanned in 19.31 seconds
```