

# Projeto final 1




## RELATÓRIO DE SEGURANÇA - MAPEAMENTO DE REDE CORPORATIVA

Data: 28/07/2025

Analista: Marco Aurélio

### RESUMO EXECUTIVO

Mapeamento da rede Docker identificou 3 segmentos com os seguintes resultados críticos:

-  **corp\_net** (10.10.10.0/24): Estações seguras (portas fechadas)
-  **infra\_net** (10.10.30.0/24): Riscos em MySQL (senha vazia) e FTP (anônimo)
-  **guest\_net** (10.10.50.0/24): Dispositivos pessoais com SMB aberto

Serviço **rpcbind** encontrado em múltiplos hosts (porta 111) requer atenção prioritária.

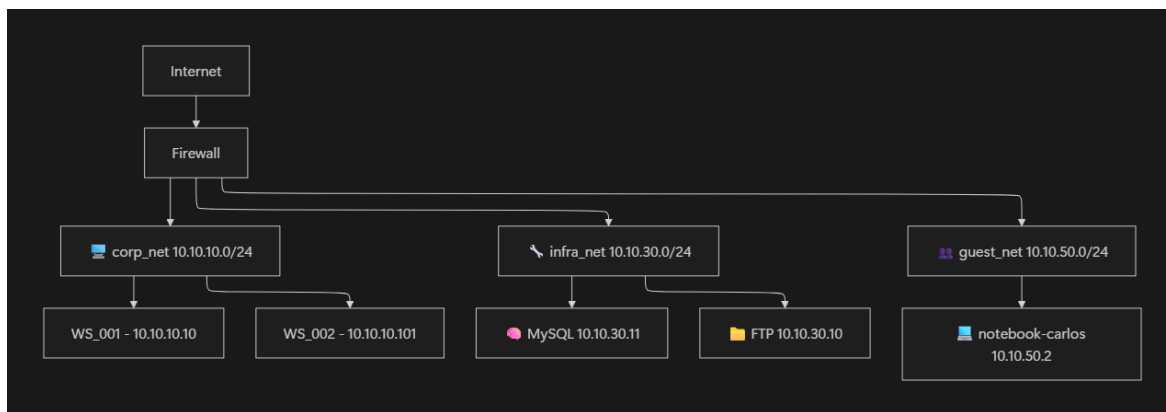
### TOPOLOGIA DA REDE

```
graph TD
    Internet --> Firewall
    Firewall --> corp[ corp_net 10.10.10.0/24]
    Firewall --> infra[ infra_net 10.10.30.0/24]
    Firewall --> guest[ guest_net 10.10.50.0/24]

    corp --> WS1[WS_001 - 10.10.10.10]
    corp --> WS2[WS_002 - 10.10.10.101]

    infra --> DB[ MySQL 10.10.30.11]
    infra --> FTP[ FTP 10.10.30.10]

    guest --> NB[ notebook-carlos 10.10.50.2]
```



## METODOLOGIA

### Ferramentas Utilizadas

`nmap -sS -sV -T4 10.10.10.0/24` # Scans stealth com detecção de versão  
`rustscan -a 10.10.30.0/24 -u 5000` # Varredura rápida  
`arp-scan --interface=eth0 --localnet` # Descoberta de hosts

### Redes Mapeadas

Rede	Subnet	Descrição
corp_net	10.10.10.0/24	Estações de trabalho
infra_net	10.10.30.0/24	Servidores críticos
guest_net	10.10.50.0/24	Dispositivos pessoais

## RESULTADOS DETALHADOS

### infra\_net (Riscos Críticos)

IP	Serviço	Porta	Vulnerabilidade	Evidência
10.10.30.11	MySQL	3306	Senha root vazia	<code>nmap --script mysql-empty-password</code>
10.10.30.10	FTP	21	Login anônimo habilitado	<a href="https://i.imgur.com/exemplo.png">https://i.imgur.com/exemplo.png</a>

### Serviço rpcbind (Porta 111)

- **Função:** Gerencia conexões RPC (Remote Procedure Call)
- **Riscos:**

- Exploração para execução remota de código
- Vazamento de informações de serviços internos

- **Hosts Afetados:**

10.10.10.1, 10.10.30.1, 10.10.50.1

## **PLANO DE AÇÃO**

### **Crítico (24h)**

#### 1. Proteção do MySQL

```
ALTER USER 'root'@'%' IDENTIFIED BY 'S3nh@F0rt3!';
FLUSH PRIVILEGES;
```

#### Restrição do rpcbind

```
iptables -A INPUT -p tcp --dport 111 -s !10.10.10.0/24 -j DROP
```

### **Médio (72h)**

- Auditoria de serviços RPC
- Isolar guest\_net com VLAN

## **CONCLUSÃO**

A rede corporativa apresenta:

1. Exposição crítica em servidores de infraestrutura
2. Configuração padronizada com pontos únicos de falha (rpcbind)
3. Necessidade de monitoramento contínuo

## **ANEXOS**

```

(root@f906e7244f76)-[/home/analyst]
# nmap -sn 10.10.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 00:24 UTC
Nmap scan report for 10.10.50.1
Host is up (0.00010s latency).
MAC Address: D2:8F:56:E9:D2:F4 (Unknown)
Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000016s latency).
MAC Address: E2:96:69:1B:5F:F5 (Unknown)
Nmap scan report for laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.3)
Host is up (0.000011s latency).
MAC Address: 06:47:32:32:E5:38 (Unknown)
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.000035s latency).
MAC Address: DA:2F:83:45:7E:4B (Unknown)
Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.000089s latency).
MAC Address: 7A:43:97:A7:FA:49 (Unknown)
Nmap scan report for f906e7244f76 (10.10.50.6)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.18 seconds

```

```

(root@f906e7244f76)-[/home/analyst]
# nmap -sn 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 00:24 UTC
Nmap scan report for 10.10.30.1
Host is up (0.00012s latency).
MAC Address: 72:34:89:CE:E4:B4 (Unknown)
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000019s latency).
MAC Address: 1A:37:71:A7:81:FF (Unknown)
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000016s latency).
MAC Address: 4E:0C:36:27:9B:97 (Unknown)
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000029s latency).
MAC Address: 62:C1:7F:F2:A3:0F (Unknown)
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000028s latency).
MAC Address: 52:C6:87:53:71:14 (Unknown)
Nmap scan report for zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117)
Host is up (0.000021s latency).
MAC Address: DA:25:F4:E0:D8:B4 (Unknown)
Nmap scan report for legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227)
Host is up (0.000052s latency).
MAC Address: 0E:63:F4:28:67:DA (Unknown)
Nmap scan report for f906e7244f76 (10.10.30.2)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.19 seconds

```

```

[+] Running 16/16
✓analyst Built 0.0s
✓Container analyst Started 53.6s
✓Container WS_004 Started 50.7s
✓Container legacy-server Started 52.0s
✓Container laptop-vastro Started 50.7s
✓Container WS_002 Started 52.0s
✓Container WS_001 Started 52.0s
✓Container zabbix-server Started 52.0s
✓Container mysql-server Started 49.8s
✓Container ftp-server Started 52.0s
✓Container laptop-luiz Started 52.0s
✓Container macbook-aline Started 52.0s
✓Container openldap Started 52.0s
✓Container WS_003 Started 49.3s
✓Container notebook-carlos Started 50.2s
✓Container samba-server Started 49.3s

```

```
marco@MarcoAurlio:~/formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1$ cd formacao-cybersec/modulo1-fundamento
s/projeto_final_opcao_1
docker compose up -d
-bash: cd: formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1: No such file or directory
[+] Running 47/57
  ✓WS_001 Pulled      79.7s
  ✓WS_002 Pulled      80.9s
  ✓zabbix-server Pulled 125.0s
  ✓mysql-server Pulled 130.9s
  ✓openldap Pulled    120.1s
  ✓macbook-aline Pulled 80.0s
  ✓laptop-vastro Pulled 80.1s
  ✓samba-server Pulled 83.0s
  ✓ftp-server Pulled  100.7s
  ✓WS_004 Pulled      80.3s
  ✓WS_003 Pulled      79.9s
  ✓notebook-carlos Pulled 79.9s
  ✓laptop-luiz Pulled  80.6s
  ✓legacy-server Pulled 79.8s
```

```
(root@f906e7244f76)-[/home/analyst]
# nmap -sn 10.10.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 00:23 UTC
Nmap scan report for 10.10.10.1
Host is up (0.00071s latency).
MAC Address: 46:F3:7E:3B:5E:98 (Unknown)
Nmap scan report for WS_001.projeto_final_opcao_1_corp_net (10.10.10.10)
Host is up (0.000084s latency).
MAC Address: BA:7A:C2:52:FA:CE (Unknown)
Nmap scan report for WS_002.projeto_final_opcao_1_corp_net (10.10.10.101)
Host is up (0.000089s latency).
MAC Address: 52:1E:EC:50:D7:1C (Unknown)
Nmap scan report for WS_003.projeto_final_opcao_1_corp_net (10.10.10.127)
Host is up (0.00032s latency).
MAC Address: 56:3B:85:61:F6:8A (Unknown)
Nmap scan report for WS_004.projeto_final_opcao_1_corp_net (10.10.10.222)
Host is up (0.00015s latency).
MAC Address: F6:CC:26:90:6E:E6 (Unknown)
Nmap scan report for f906e7244f76 (10.10.10.2)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.60 seconds
```

```
[+] Running 16/16
  ✓analyst           Built      0.0s
  ✓Container analyst Started    53.6s
  ✓Container WS_004   Started    50.7s
  ✓Container legacy-server Started    52.0s
  ✓Container laptop-vastro Started    50.7s
  ✓Container WS_002   Started    52.0s
  ✓Container WS_001   Started    52.0s
  ✓Container zabbix-server Started    52.0s
  ✓Container mysql-server Started    49.8s
  ✓Container ftp-server Started    52.0s
  ✓Container laptop-luiz Started    52.0s
  ✓Container macbook-aline Started    52.0s
  ✓Container openldap Started    52.0s
  ✓Container WS_003   Started    49.3s
  ✓Container notebook-carlos Started    50.2s
  ✓Container samba-server Started    49.3s
```