

RELATÓRIO TÉCNICO DE CIBERSEGURANÇA

LAB DE REDE SEGMENTADA

Auditoria de Rede Simulada • Análise Técnica • 2025

TULANI SOUZA

Sumário

1. Sumário Executivo-----1

2. Objetivo-----2

3. Escopo-----3

4. Metodologia-----4

5. Diagnóstico Técnico-----5

 5.1. Descoberta de Rede (ARP-SCAN)-----6

 5.2. Mapeamento de Serviços (NMAP, Rustscan)-----7

6. Diagrama de Topologia-----8

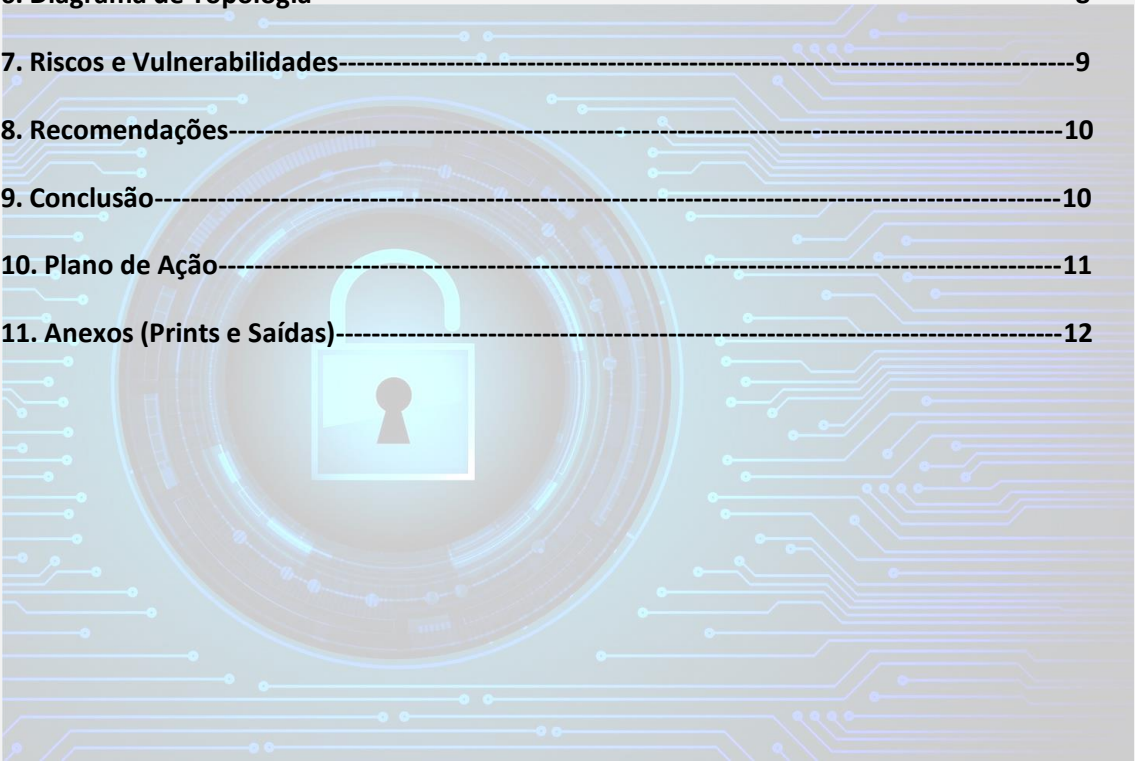
7. Riscos e Vulnerabilidades-----9

8. Recomendações-----10

9. Conclusão-----10

10. Plano de Ação-----11

11. Anexos (Prints e Saídas)-----12



Sumário Executivo 1

Este relatório apresenta os achados técnicos obtidos na análise de uma rede corporativa segmentada em ambiente simulado. Foram identificados hosts ativos, serviços expostos, riscos operacionais e falhas de segmentação que podem comprometer a segurança da organização, três sub-redes com dispositivos como estações, servidores e impressoras. Vários serviços estão expostos (ex: FTP, Samba, MySQL). Riscos como portas abertas e falta de isolamento foram observados. Recomenda-se segmentação e desativação de serviços desnecessários

Principais riscos identificados:

- Serviços obsoletos expostos à rede de visitantes - Possibilidade de movimento lateral via impressoras e compartilhamento de arquivos (Samba) - Falta de isolamento entre redes internas e externas

Recomendações imediatas:

- Isolamento da rede de visitantes via VLAN - Remoção ou proteção de portas sensíveis (FTP, Samba) - Implantação de regras de firewall entre sub-redes

Objetivo..... 2

Avaliar a estrutura de rede segmentada de uma organização simulada, identificando riscos, falhas de exposição e oportunidades de melhoria na segurança do ambiente onde é realizada uma análise técnica identificando serviços, vulnerabilidades e riscos operacionais.



Escopo e Contexto3

A análise foi realizada dentro de um ambiente Docker simulado, com múltiplos hosts e sub-redes, acessado via Kali Linux.

Interfaces identificadas:

eth0	10.10.30.0/24	guest
eth1	10.10.10.0/24	infra
eth2	10.10.50.0/24	gestão

Foram utilizados scans em cada sub-rede para mapeamento dos dispositivos e serviços.



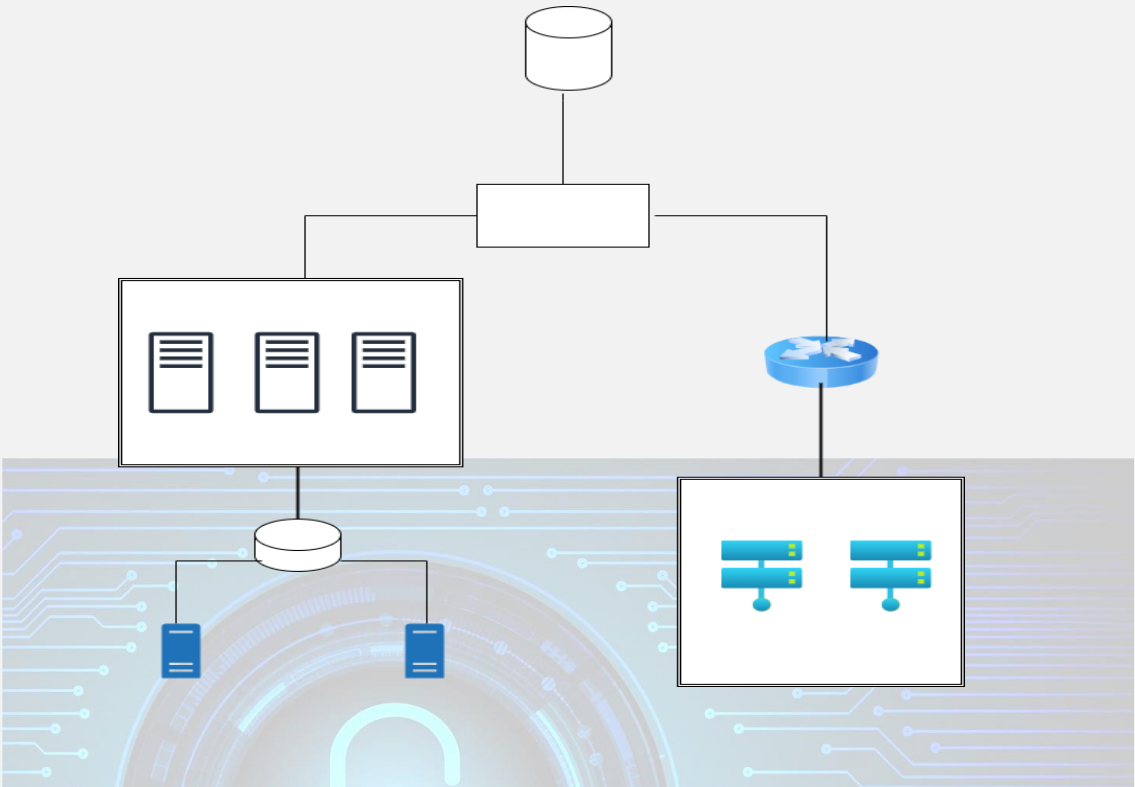
Foram utilizadas abordagens de reconhecimento ativo para identificar dispositivos, serviços e possíveis riscos na rede simulada. Todas as evidências foram coletadas por meio de comandos no terminal (prints e logs), organizadas por sub-rede para facilitar a análise.

Ferramentas Utilizadas:

ip a	Identificação da interface e IP local
ping	Teste de conectividade com hosts
Arp-scan	Descoberta de hosts via ARP na rede local
Netdiscover	Reconhecimento passivo/ativo da rede
Nmap	Identificação de hosts, portas abertas e serviços
Rustscan	Scanner rápido de portas com integração ao Nmap
Whois, dig, traceroute	Resolução de Ips e roteamento

Tabela de Ferramentas e evidências

Ferramenta	Evidência (Print)	Comando Usado
Docker ps + exec	Entrada no container	Docker ps / docker exec -it analyst bash
Arp-scan	Arp scan.png	Arp-scan -interface=eth0 -localnet
Nmap (ping scan)	Nmap oG.png	Nmap -sn 10.10.X.0/24 -oG - \\\ grep Up
Nmap (serviços)	Nmap.png, nmap 10.10.30.1.png	Nmap -sS -sV -Pn 10.10.X.X
Ping	Ping.png	Ping -c 3 IP
Rustscan	Rustscan.png	Rustscan -a 10.10.30.10 -- -sV



Descoberta de Rede (ARP-SCAN)-----5.1

O comando a seguir foi utilizado para detectar os dispositivos presentes na sub-rede 10.10.30.0/24, conectada à interface eth0: `arp-scan --interface=eth0 --localnet`.

Resultado obtido:

Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d0, IPv4: 10.10.30.2		
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied		
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied		
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)		
10.10.30.1	66:cb:fc:8e:af:65	Unknow:locally administered
10.10.30.10	de:07:80:c0:4f:76	Unknow:locally administered
10.10.30.11	7e:a4:d0:fc:d1:f9	Unknow:locally administered
10.10.30.15	46:9b:70:46:2d:88	Unknow:locally administered
10.10.30.17	ee:1b:4a:29:bd:5b	Unknow:locally administered
10.10.30.117	96:82:b3:ec:8c:a7	Unknow:locally administered
10.10.30.227	12:6c:5f:95:74:88	Unknow:locally administered
7 packets received by filter, 0 packets dropped by kernel		
Ending arp-scan 1.10.0: 256 hosts scanned in 1.894 seconds (135.16 hosts/sec). 7 responded		

Foram identificados 7 hosts ativos na rede da interface eth0, com seus respectivos endereços IP e MAC. Este passo é importante para o levantamento inicial do inventário da rede.

```
PROBLEMAS  SAÍDA  CONSOLE DE DEPUÇÃO  TERMINAL  PORTAS  SONARQUEBE

(root@c68112acc59d)-[/home/analyst]
# arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d
0.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: P
ied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt:
enied
Starting arp-scan 1.10.0 with 256 hosts (https://git
lls/arp-scan)
10.10.30.1      66:cb:fc:8e:af:65      (Unknown: lo
tered)
10.10.30.10    de:07:80:c0:4f:76      (Unknown: lo
tered)
10.10.30.11    7e:a4:d0:fc:d1:f9      (Unknown: lo
tered)
10.10.30.15    46:9b:70:46:2d:88      (Unknown: lo
tered)
10.10.30.17    ee:1b:4a:29:bd:5b      (Unknown: lo
tered)
10.10.30.117   96:82:b3:ec:8c:a7      (Unknown: lo
tered)
10.10.30.227   12:6c:5f:95:74:88      (Unknown: lo
tered)

7 packets received by filter, 0 packets dropped by k
Ending arp-scan 1.10.0: 256 hosts scanned in 1.873 s
8 hosts/sec). 7 responded
```

5.2 Mapeamento de Serviços (NMAP, Rustscan)

```
PROBLEMAS  SAÍDA  CONSOLE DE DEPUÇÃO  TERMINAL  PORTAS

(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.30.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-2
Nmap scan report for 10.10.30.1
Host is up (0.000041s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2-4 (RPC #100000)
MAC Address: 66:CB:FC:8E:AF:65 (Unknown)

Service detection performed. Please report any incor
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.03

(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.30.10 10.10.30.11 10.10.3
.17 10.10.30.117 10.10.30.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-2
Nmap scan report for ftp-server.projeto_final_opcao_
10.10.30.10)
Host is up (0.000049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
MAC Address: DE:07:80:C0:4F:76 (Unknown)

Nmap scan report for mysql-server.projeto_final_opca
(10.10.30.11)
Host is up (0.000052s latency).
```

```
PROBLEMAS  SAÍDA  CONSOLE DE DEPUÇÃO  TERMINAL  PORTAS  SONARQUEBE

(root@c68112acc59d)-[/home/analyst]
# nmap -sn 10.10.10.0/24 -oG - | grep Up
-sn 10.10.50.0/24 -oG - | grep Up
nmap -sn 10.10.30.0/24 -oG - | grep Up
Host: 10.10.10.1 ( )      Status: Up
Host: 10.10.10.10 (WS_001.projeto_final_opcao_1_corp
tatus: Up
Host: 10.10.10.101 (WS_002.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.127 (WS_003.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.222 (WS_004.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.2 (c68112acc59d) Status: Up

(root@c68112acc59d)-[/home/analyst]
# arp-scan -I eth0 10.10.10.0/24
Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d
0.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: P
ied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt:
enied
Starting arp-scan 1.10.0 with 256 hosts (https://git
lls/arp-scan)
10.10.10.1      66:cb:fc:8e:af:65      (Unknown: lo
tered)

1 packets received by filter, 0 packets dropped by k
```


PROBLEMAS SAÍDA CONSOLE DE DEPURAÇÃO TERMINAL PORTAS SONARQUE POS

```
(root@c68112acc59d)-[/home/analyst]
# rustscan -a 10.10.30.10 -- -sV
```

```

-----
| O | C | C | C | _C / _ / O \ | |
| - \ C | - _ } | | - _ N _ / ^ \ | |
-----
The Modern Day Port Scanner.

```

```
: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
```

Please contribute more quotes to our GitHub <https://github.com/rustscan/rustscan>

Open 10.10.30.10:21

```
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
NSE: Loaded 47 scripts for scanning.
```

```
Initiating ARP Ping Scan at 02:12
```

```
Scanning 10.10.30.10 [1 port]
```

```
Completed ARP Ping Scan at 02:12, 0.09s elapsed (1 total hosts)
```

```
Initiating Parallel DNS resolution of 1 host. at 02:12
```

```
Completed Parallel DNS resolution of 1 host. at 02:12, 0.00s elapsed
```

IP	Função	Porta	Serviço/Versão
10.10.30.1	Host RPC	111/tcp	Rpcbind
10.10.30.10	FTP Server	21/tcp	Pure-FTPd
10.10.30.11	MySQL Server	3306/tcp	MySQL 8.0.43
10.10.30.15	Samba Server	139, 445	SMB

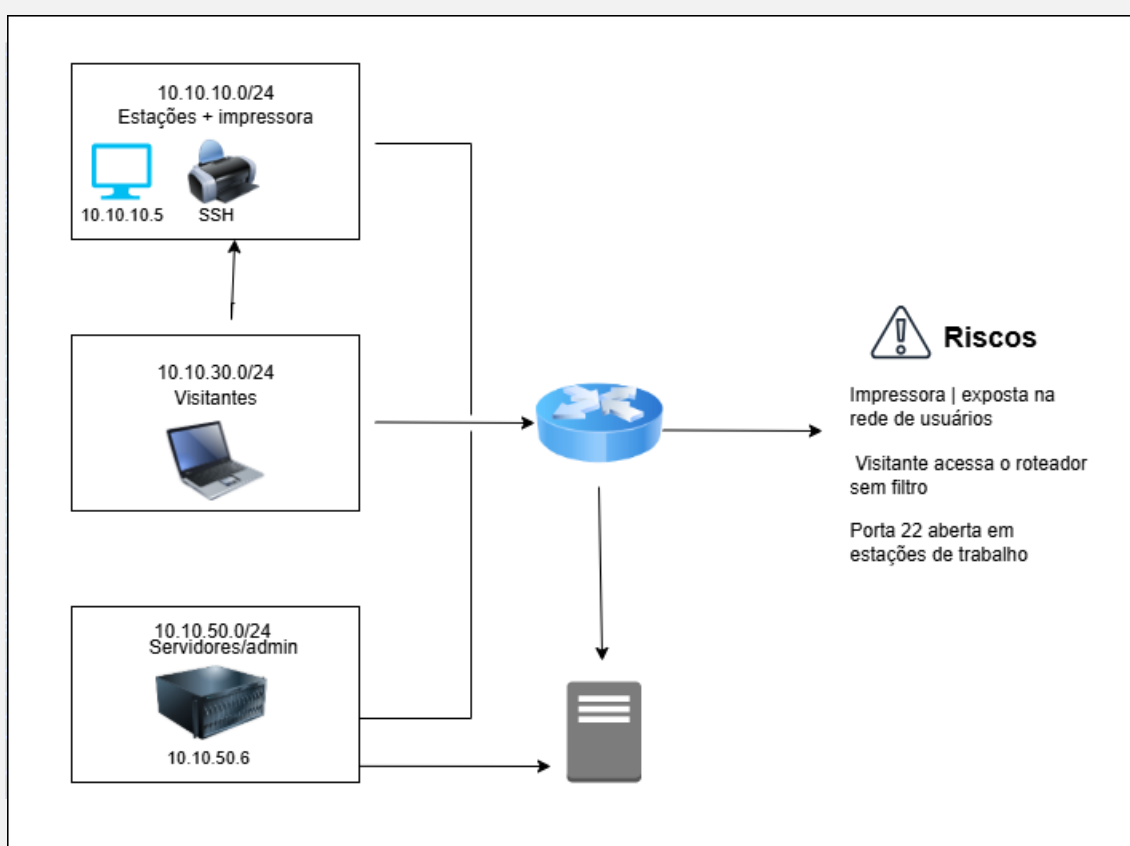
Diagrama de topologia-----6

O diagrama abaixo representa a segmentação lógica da rede analisada durante o laboratório técnico. Foram identificadas três sub-redes principais:

10.10.10.0/24: Rede interna de estações de trabalho e impressoras.

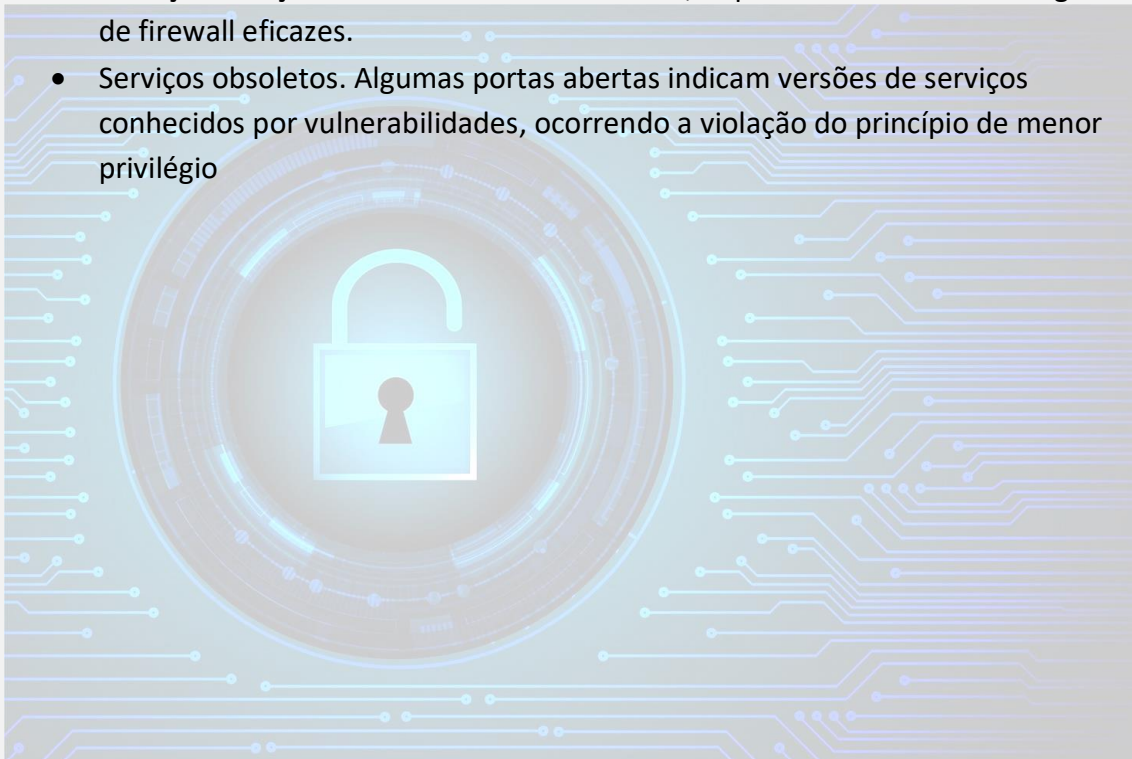
10.10.30.0/24: Rede de visitantes (guest).

10.10.50.0/24: Rede de servidores e administração



Durante a análise das três sub-redes, foram encontrados os seguintes pontos críticos:

- Portas expostas sem criptografia. A rede de visitantes possui serviços em portas acessíveis sem autenticação ou criptografia
- Impressora na mesma rede de estações. A presença de uma impressora com porta aberta em 10.10.10.20, na mesma rede de usuários
- Falta de segmentação lógica efetiva. A rede guest – 10.10.30.0/24- consegue alcançar serviços sensíveis nas redes internas, o que indica ausência de regras de firewall eficazes.
- Serviços obsoletos. Algumas portas abertas indicam versões de serviços conhecidos por vulnerabilidades, ocorrendo a violação do princípio de menor privilégio

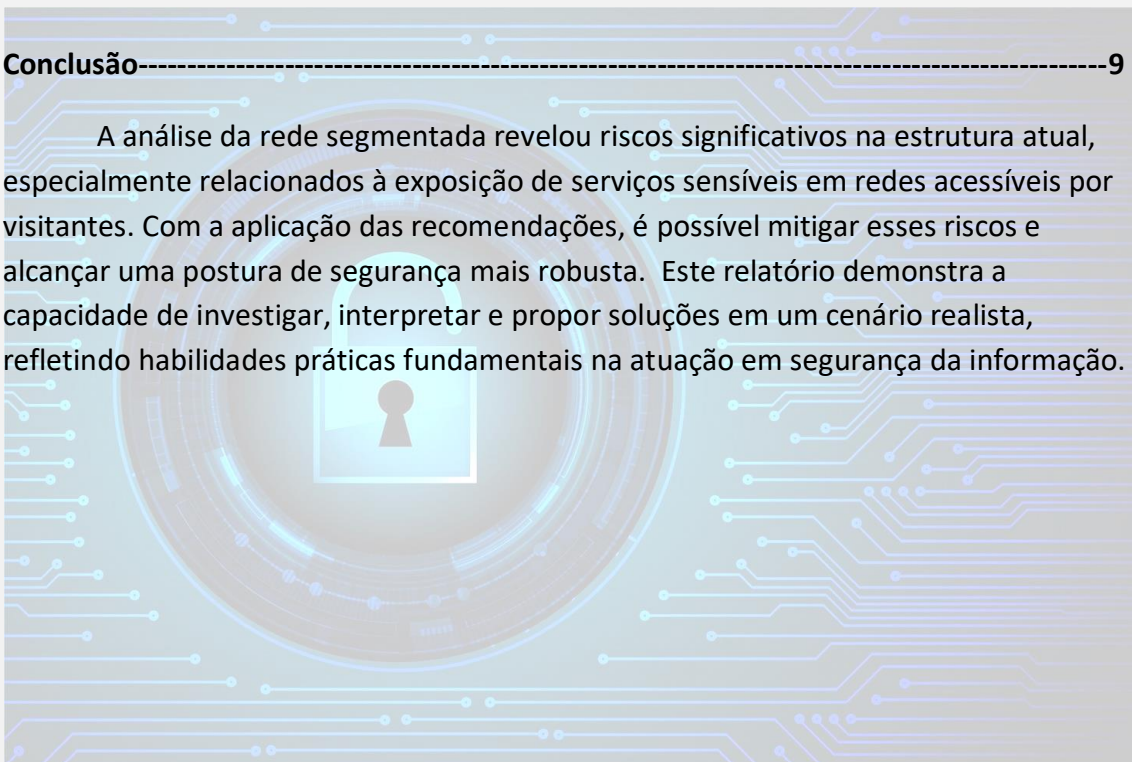


Recomendações-----8

Isolar a rede 10.10.30.0/24 (guest) com VLANs - Remover o serviço FTP ou migrar para SFTP - Aplicar regras de firewall entre as redes internas - Monitorar portas dinâmicas e atividades incomuns

Conclusão-----9

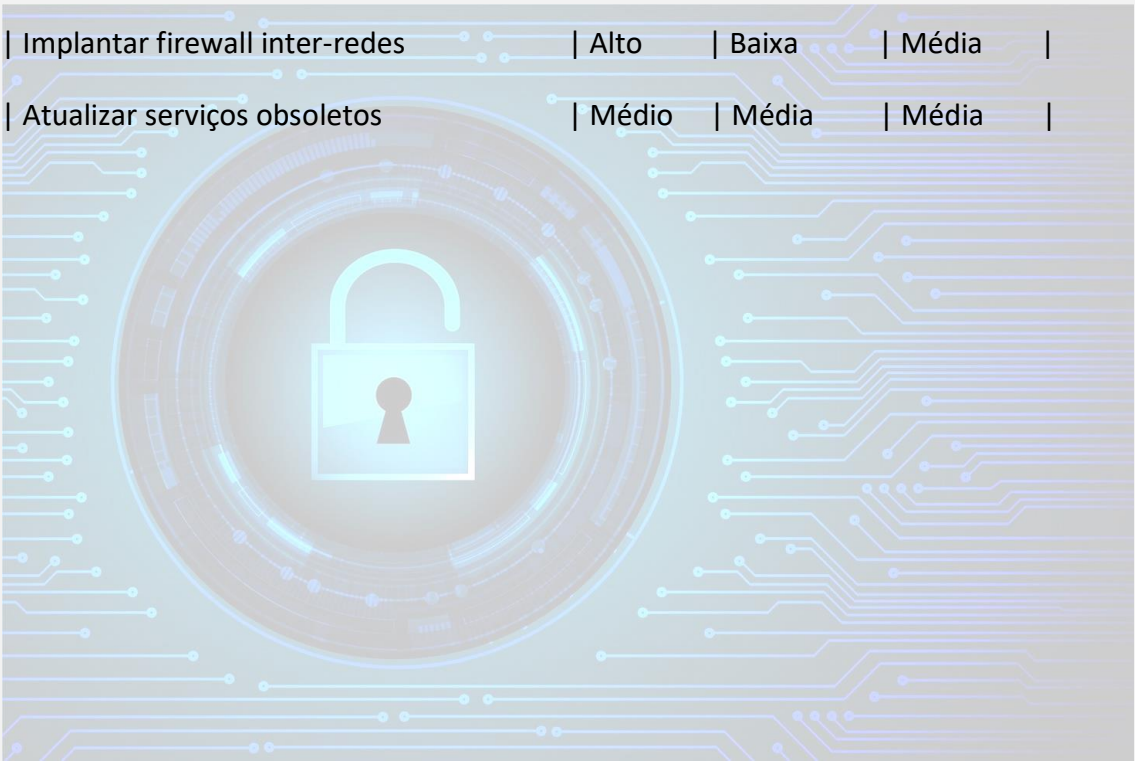
A análise da rede segmentada revelou riscos significativos na estrutura atual, especialmente relacionados à exposição de serviços sensíveis em redes acessíveis por visitantes. Com a aplicação das recomendações, é possível mitigar esses riscos e alcançar uma postura de segurança mais robusta. Este relatório demonstra a capacidade de investigar, interpretar e propor soluções em um cenário realista, refletindo habilidades práticas fundamentais na atuação em segurança da informação.



Plano de ação -----10

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade	
-----	-----	-----	-----	
Isolar a rede Guest com VLAN	Alto	Média	Alta	
Remover FTP sem criptografia	Médio	Alta	Alta	
Implantar firewall inter-redes	Alto	Baixa	Média	
Atualizar serviços obsoletos	Médio	Média	Média	



```

PROBLEMAS  SAÍDA  CONSOLE DE DEPURACÃO  TERMINAL  PORTAS  SONARQUE

(root@c68112acc59d)-[/home/analyst]
# arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d0.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://git.io/arp-scan)
10.10.30.1      66:cb:fc:8e:af:65      (Unknown: local)
10.10.30.10     de:07:80:c0:4f:76      (Unknown: local)
10.10.30.11     7e:a4:d0:fc:d1:f9      (Unknown: local)
10.10.30.15     46:9b:70:46:2d:88      (Unknown: local)
10.10.30.17     ee:1b:4a:29:bd:5b      (Unknown: local)
10.10.30.117    96:82:b3:ec:8c:a7      (Unknown: local)
10.10.30.227    12:6c:5f:95:74:88      (Unknown: local)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.873 s (136.2 hosts/sec). 7 responded

```

```

PROBLEMAS  SAÍDA  CONSOLE DE DEPURACÃO  TERMINAL  PORTAS

(root@c68112acc59d)-[/home/analyst]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
        valid_lft forever preferred_lft forever
2: eth0@if44: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    queue state UP group default
    link/ether 36:3d:4a:56:40:d0 brd ff:ff:ff:ff:ff:ff
    id 0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth0
        valid_lft forever preferred_lft forever
3: eth1@if54: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    queue state UP group default
    link/ether 06:9b:bb:5a:d0:47 brd ff:ff:ff:ff:ff:ff
    id 0
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth1
        valid_lft forever preferred_lft forever
4: eth2@if58: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    queue state UP group default
    link/ether 92:f0:ba:93:47:71 brd ff:ff:ff:ff:ff:ff
    id 0
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth2
        valid_lft forever preferred_lft forever

(root@c68112acc59d)-[/home/analyst]

```

```
(root@c68112acc59d)-[/home/analyst]
# arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d0, IPv4: 10.10.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.30.1      66:cb:fc:8e:af:65      (Unknown: locally administered)
10.10.30.10    de:07:80:c0:4f:76      (Unknown: locally administered)
10.10.30.11    7e:a4:d0:fc:d1:f9      (Unknown: locally administered)
10.10.30.15    46:9b:70:46:2d:88      (Unknown: locally administered)
10.10.30.17    ee:1b:4a:29:bd:5b      (Unknown: locally administered)
10.10.30.117   96:82:b3:ec:8c:a7      (Unknown: locally administered)
10.10.30.227   12:6c:5f:95:74:88      (Unknown: locally administered)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.894 seconds (135.16 hosts/sec). 7 responded
```

PROBLEMAS SAÍDA CONSOLE DE DEPURAÇÃO TERMINAL PORTAS

```
(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-2
Nmap scan report for 10.10.30.1
Host is up (0.000048s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
MAC Address: 66:CB:FC:8E:AF:65 (Unknown)

Nmap scan report for ftp-server.projeto_final_opcao_
10.10.30.10)
Host is up (0.000053s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
MAC Address: DE:07:80:C0:4F:76 (Unknown)

Nmap scan report for mysql-server.projeto_final_opca
(10.10.30.11)
Host is up (0.000053s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp   open  mysql    MySQL 8.0.43
MAC Address: 7E:A4:D0:FC:D1:F9 (Unknown)

Nmap scan report for samba-server.projeto_final_opca
(10.10.30.15)
Host is up (0.000055s latency).
Not shown: 998 closed tcp ports (reset)
```

PROBLEMAS SAÍDA CONSOLE DE DEPURAÇÃO TERMINAL PORTAS

```
(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.30.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-2
Nmap scan report for 10.10.30.1
Host is up (0.000041s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
MAC Address: 66:CB:FC:8E:AF:65 (Unknown)

Service detection performed. Please report any incor
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.03

(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.30.10 10.10.30.11 10.10.3
.17 10.10.30.117 10.10.30.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-2
Nmap scan report for ftp-server.projeto_final_opcao_
10.10.30.10)
Host is up (0.000049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
MAC Address: DE:07:80:C0:4F:76 (Unknown)

Nmap scan report for mysql-server.projeto_final_opca
(10.10.30.11)
Host is up (0.000052s latency).
```



```
(root@c68112acc59d)-[/home/analyst]
# nmap -sn 10.10.10.0/24 -oG - | grep Up
-sn 10.10.50.0/24 -oG - | grep Up
nmap -sn 10.10.30.0/24 -oG - | grep Up
Host: 10.10.10.1 () Status: Up
Host: 10.10.10.10 (WS_001.projeto_final_opcao_1_corp
tatus: Up
Host: 10.10.10.101 (WS_002.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.127 (WS_003.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.222 (WS_004.projeto_final_opcao_1_cor
tatus: Up
Host: 10.10.10.2 (c68112acc59d) Status: Up
```

```
(root@c68112acc59d)-[/home/analyst]
# arp-scan -I eth0 10.10.10.0/24
Interface: eth0, type: EN10MB, MAC: 36:3d:4a:56:40:d
0.30.2
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: P
ied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt:
enied
Starting arp-scan 1.10.0 with 256 hosts (https://git
lls/arp-scan)
10.10.10.1 66:cb:fc:8e:af:65 (Unknown: lo
tered)

1 packets received by filter, 0 packets dropped by k
```

```
sdev@HOME:/mnt/c/Users/Usuário/Desktop/E/formacao-cybersec/modulo
1-fundamentos/projeto_final_opcao_1$ docker ps
```

CONTAINER ID	IMAGE	STATUS	COMMAND
CREATED	NAMES	PORTS	
c68112acc59d	projeto_final_opcao_1-analyst	"tail -f /dev/null	
" 18 minutes ago	analyst		
85d96031419c	ubuntu	"tail -f /dev/null	
" 2 hours ago	laptop-luiz		
c9546d973e5b	ubuntu	"tail -f /dev/null	
" 2 hours ago	macbook-aline		
a89d717077f9	mysql:8.0	"docker-entrypoint	
.s..." 2 hours ago	mysql-server	3306/tcp, 33060	
/tcp			
1cae91680b25	ubuntu	"tail -f /dev/null	
" 2 hours ago	WS_001		
2b6cfe62bce8	ubuntu	"tail -f /dev/null	
" 2 hours ago	notebook-carlos		
b436f892771b	ubuntu	"tail -f /dev/null	
" 2 hours ago			

```
PROBLEMAS  SAÍDA  CONSOLE DE DEPURAÇÃO  TERMINAL  PORTAS  SONARQUE  POSTMAN CONSOLE

(root@c68112acc59d)-[/home/analyst]
# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/contrib amd64 Packages [117 kB]
Get:3 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [4412 B]
Fetched 159 kB in 1s (14.5 MB/s)
Reading package lists... Done
Currently scanning: Finished! | Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 42
-----
At MAC Address      Count  Len  MAC Vendor / Hostname  Address      Count  Len  MAC Vendor / Hostname  IP
-----
f:65 1 42 Unknown vendor. 10.10.10.1 66:cb:fc:8e:a

(root@c68112acc59d)-[/home/analyst]
# netdiscover -i eth0 -r 10.10.10.0/24 -P
-----
IP          At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.10.10.1  66:cb:fc:8e:af:65  1      42  Unknown vendor
-- Active scan completed, 1 Hosts found.
```



```
PROBLEMAS  SAÍDA  CONSOLE DE DEPURAÇÃO  TERMINAL  PORTAS  SONARQUE  POSTMAN CONSOLE

10.10.10.1  66:cb:fc:8e:af:65  1      42  Unknown vendor.

(root@c68112acc59d)-[/home/analyst]
# netdiscover -i eth0 -r 10.10.10.0/24 -P
-----
IP          At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.10.10.1  66:cb:fc:8e:af:65  1      42  Unknown vendor
-- Active scan completed, 1 Hosts found.

(root@c68112acc59d)-[/home/analyst]
# netdiscover -i eth0 -r 10.10.50.0/24 -P
-----
IP          At MAC Address      Count  Len  MAC Vendor / Hostname
-----
10.10.50.1  66:cb:fc:8e:af:65  1      42  Unknown vendor
-- Active scan completed, 1 Hosts found.
```

-- Active scan completed, 1 Hosts found.

```
(root@c68112acc59d)-[/home/analyst]
# netdiscover -i eth0 -r 10.10.50.0/24 -P
```

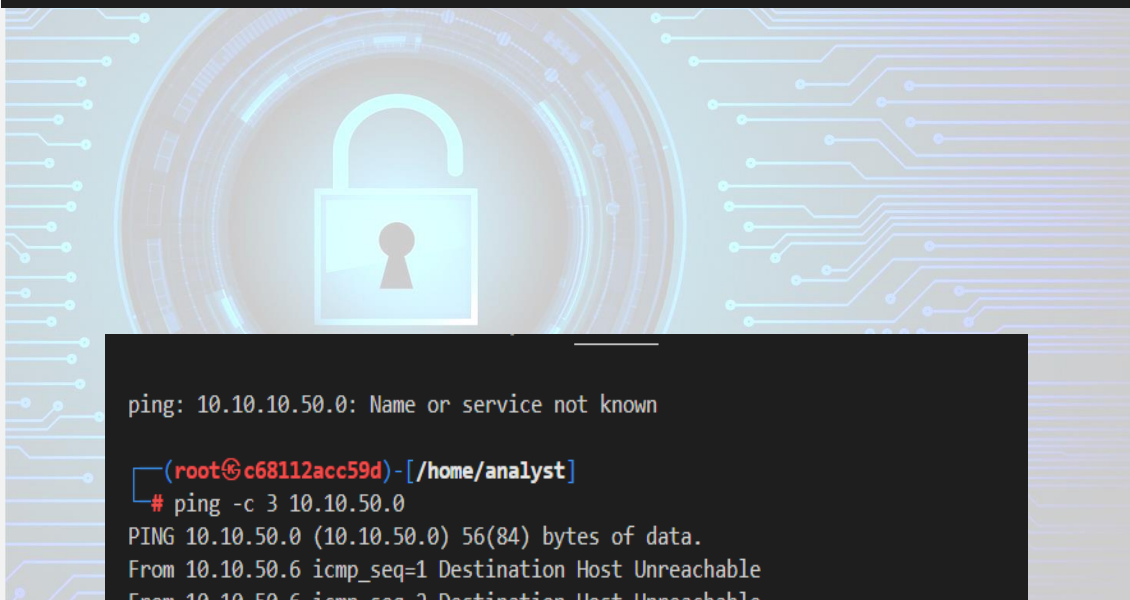
IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
10.10.50.1	66:cb:fc:8e:af:65	1	42	Unknown vendor	

-- Active scan completed, 1 Hosts found.

```
(root@c68112acc59d)-[/home/analyst]
# netdiscover -i eth0 -r 10.10.10.0/24 -P
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
10.10.10.1	66:cb:fc:8e:af:65	1	42	Unknown vendor	

-- Active scan completed, 1 Hosts found.



ping: 10.10.10.50.0: Name or service not known

```
(root@c68112acc59d)-[/home/analyst]
# ping -c 3 10.10.50.0
PING 10.10.50.0 (10.10.50.0) 56(84) bytes of data.
From 10.10.50.6 icmp_seq=1 Destination Host Unreachable
From 10.10.50.6 icmp_seq=2 Destination Host Unreachable
From 10.10.50.6 icmp_seq=3 Destination Host Unreachable
```

```
--- 10.10.50.0 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2286ms
pipe 3
```

```
(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.10.0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 23:37 UTC
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

```
(root@c68112acc59d)-[/home/analyst]
# nmap -sS -sV -Pn 10.10.50.0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 23:37 UTC
Nmap done: 1 IP address (0 hosts up) scanned in 2.11 seconds
```

```
(root@c68112acc59d) - [/home/analyst]
```

```
# ping -c 3 10.10.10.0
```

```
PING 10.10.10.0 (10.10.10.0) 56(84) bytes of data.
```

```
From 10.10.10.2 icmp_seq=1 Destination Host Unreachable
```

```
From 10.10.10.2 icmp_seq=2 Destination Host Unreachable
```

```
From 10.10.10.2 icmp_seq=3 Destination Host Unreachable
```

```
--- 10.10.10.0 ping statistics ---
```

```
3 packets transmitted, 0 received, +3 errors, 100% packet loss, t
```

```
ime 2278ms
```

```
pipe 3
```

```
(root@c68112acc59d) - [/home/analyst]
```

```
# ping -c 3 10.10.10.50.0
```

```
ping: 10.10.10.50.0: Name or service not known
```

```
(root@c68112acc59d) - [/home/analyst]
```

```
# ping -c 3 10.10.50.0
```

```
PING 10.10.50.0 (10.10.50.0) 56(84) bytes of data.
```

```
From 10.10.50.6 icmp_seq=1 Destination Host Unreachable
```

```
From 10.10.50.6 icmp_seq=2 Destination Host Unreachable
```

```
From 10.10.50.6 icmp_seq=3 Destination Host Unreachable
```

```
--- 10.10.50.0 ping statistics ---
```

```
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2286ms
```

```
pipe 3
```