Documentação de Redes Descobertas

Autor: Kassia Kellem Da Silva

Data: 24/07/2025

Módulo 1.

Diagrama de Rede

Metodologia

Foram utilizadas ferramentas de código aberto para realizar a descoberta e o escaneamento da rede.

A análise partiu de um ponto de acesso na rede de convidados para simular um cenário de "menor privilégio".

- **Ferramentas:** `nmap`, `ifconfig`, `traceroute`, `ip route`.
- **Técnicas:** Descoberta de hosts (Ping Scan), escaneamento de portas TCP, detecção de serviços e versões, e análise de rotas de rede.

Redes Identificadas

Nome Estimado	Subnet Descoberta	Finalidade Suposta

Rede de Convidados	10.10.50.0/24	Rede para visitantes e dispositivos não confiáveis
Rede Interna A	10.10.10.0/24	Rede interna (servidores ou departamentos)
Rede Interna B	10.10.30.0/24	Rede interna (servidores ou departamentos)

Dispositivos por Rede

Rede de Convidados (10.10.50.0/24)

IP	Função	Evidência
10.10.50.1	Gateway	Responde ping, porta 111/tcp (rpcbind) aberta.
10.10.50.2	Estação de Trabalho (laptop-luiz)	Responde ping, demais portas filtradas por firewall.
10.10.50.3	Estação de Análise (Sua Máquina)	-
10.10.50.4	Estação de Trabalho (macbook-aline)	Responde ping, demais portas filtradas por firewall.
10.10.50.5	Estação de Trabalho (notebook-carlos)	Responde ping, demais portas filtradas por firewall.

10.10.50.6	Estação de Trabalho (analyst)	Responde ping, demais portas filtradas por firewall.

Rede Interna A (10.10.10.0/24)

IP	Função	Evidência
10.10.10.1	Gateway	Responde ping, porta 111/tcp (rpcbind) aberta.
Outros hosts	*N/A*	Nenhum outro host foi descoberto nesta rede.

Rede Interna B (10.10.30.0/24)

IP	Função	Evidência
10.10.30.1	Gateway	Responde ping, porta 111/tcp (rpcbind) aberta.
Outros hosts	*N/A*	Nenhum outro host foi descoberto nesta rede.

Observações de Risco e Conclusão

- **Risco Crítico:** Falha de Segmentação de Rede
  A Rede de Convidados não está isolada das redes internas.

  Foi possível escanear e identificar os gateways das Redes Internas A e B a partir dela.

  Isso representa uma falha grave de segurança, pois permite a movimentação lateral de um atacante da rede menos segura para as mais críticas.

- **Risco Médio:** Exposição de Serviços nos Gateways
  Os gateways de todas as redes expõem o serviço **rpcbind**, que pode ser usado para enumerar mais informações sobre a infraestrutura.
- **Boa Prática Identificada:** Firewall nas Estações de Trabalho
  As estações de trabalho na rede de convidados possuem firewall ativo.

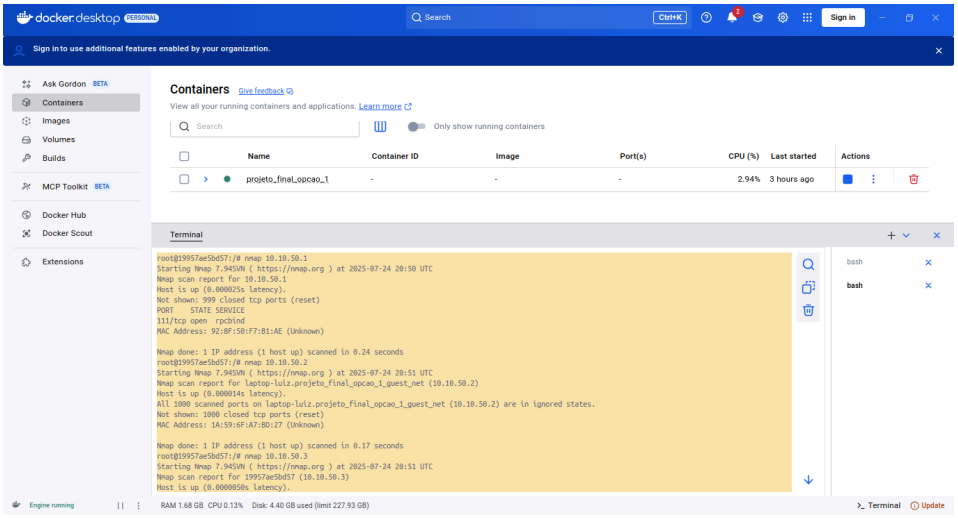
  No entanto, seu benefício é severamente reduzido pela falha de segmentação da rede.

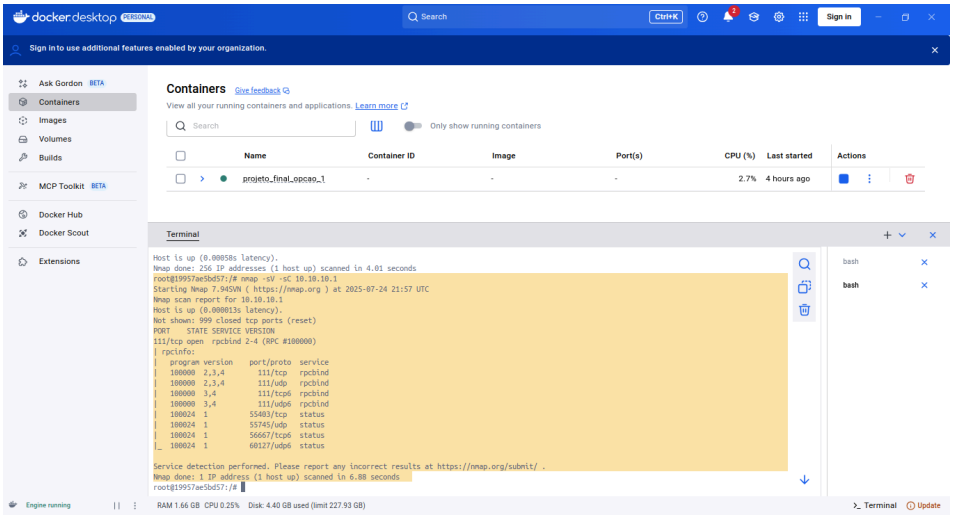
Conclusão Final: A rede apresenta uma falha fundamental de segmentação que representa o risco mais significativo ao ambiente.

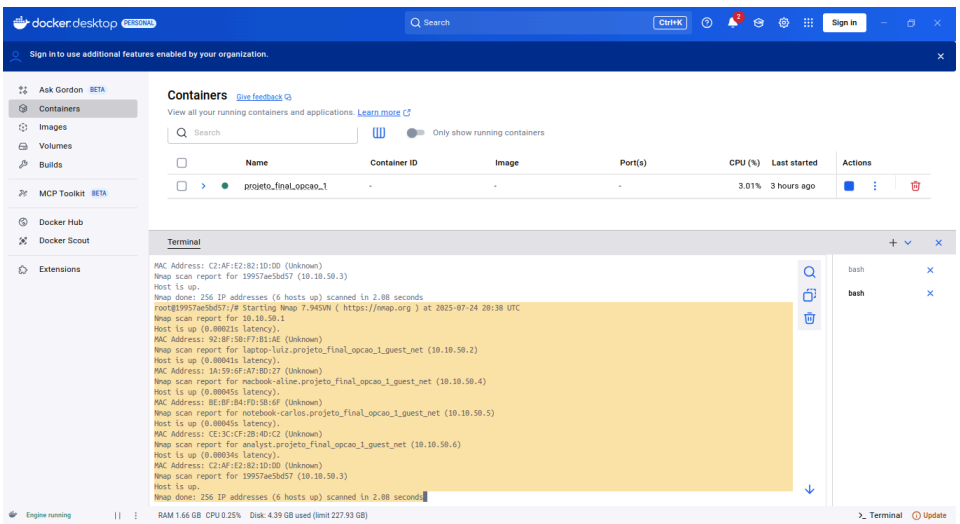
A correção da regra de isolamento da rede de convidados é o passo mais urgente e de maior impacto para melhorar a postura de segurança geral.

As demais boas práticas observadas, como o uso de firewalls em estações de trabalho, são eficazes, mas seu benefício é reduzido pela falha de segmentação.

Anexos


docker desktop PERSONAL
Search Ctrl+K
Sign in
Sign in to use additional features enabled by your organization.
Ask Gordon BETA
Containers
Images
Volumes
Builds
MCP Toolkit BETA
Docker Hub
Docker Scout
Extensions
Containers
Give feedback
View all your running containers and applications. Learn more
Search
Only show running containers
Name
Container ID
Image
Port(s)
CPU (%)
Last started
Actions
projeto_final_opcao_1
2.94%
3 hours ago
Terminal
root@19957ae5bd57:/# nmap 10.10.50.1
Starting Nmap 7.945VN (https://nmap.org) at 2025-07-24 20:50 UTC
Nmap scan report for 10.10.50.1
Host is up (0.000025s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
111/tcp open rpcbind
MAC Address: 92:8F:50:F7:B1:AE (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@19957ae5bd57:/# nmap 10.10.50.2
Starting Nmap 7.945VN (https://nmap.org) at 2025-07-24 20:51 UTC
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.000014s latency).
All 1000 scanned ports on laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 1A:59:6F:A7:BD:27 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@19957ae5bd57:/# nmap 10.10.50.3
Starting Nmap 7.945VN (https://nmap.org) at 2025-07-24 20:51 UTC
Nmap scan report for 19957ae5bd57 (10.10.50.3)
Host is up (0.0000050s latency).
bash
bash
Engine running
RAM 1.68 GB CPU 0.13% Disk: 4.40 GB used (limit 227.93 GB)
Terminal
Update


docker desktop PERSONAL
Search Ctrl+K
Sign in
Sign in to use additional features enabled by your organization.
Ask Gordon BETA
Containers
Images
Volumes
Builds
MCP Toolkit BETA
Docker Hub
Docker Scout
Extensions
Containers
Give feedback
View all your running containers and applications. Learn more
Search
Only show running containers
Name
Container ID
Image
Port(s)
CPU (%)
Last started
Actions
projeto_final_opcao_1
2.7%
4 hours ago
Terminal
Host is up (0.00058s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 4.01 seconds
root@19957ae5bd57:/# nmap -sV -sC 10.10.10.1
Starting Nmap 7.945VN (https://nmap.org) at 2025-07-24 21:57 UTC
Nmap scan report for 10.10.10.1
Host is up (0.000013s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100000 3,4 111/tcp6 rpcbind
| 100000 3,4 111/udp6 rpcbind
| 100024 1 55403/tcp status
| 100024 1 55745/udp status
| 100024 1 56667/tcp6 status
|_ 100024 1 60127/udp6 status
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds
root@19957ae5bd57:/#
bash
bash
Engine running
RAM 1.66 GB CPU 0.25% Disk: 4.40 GB used (limit 227.93 GB)
Terminal
Update


docker desktop PERSONAL
Search Ctrl+K
Sign in
Sign in to use additional features enabled by your organization.
Ask Gordon BETA
Containers
Images
Volumes
Builds
MCP Toolkit BETA
Docker Hub
Docker Scout
Extensions
Containers
Give feedback
View all your running containers and applications. Learn more
Search
Only show running containers
Name
Container ID
Image
Port(s)
CPU (%)
Last started
Actions
projeto_final_opcao_1
3.01%
3 hours ago
Terminal
MAC Address: C2:AF:E2:82:1D:DD (Unknown)
Nmap scan report for 19957ae5bd57 (10.10.50.3)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.08 seconds
root@19957ae5bd57:/# Starting Nmap 7.945VN (https://nmap.org) at 2025-07-24 20:38 UTC
Nmap scan report for 10.10.50.1
Host is up (0.00021s latency).
MAC Address: 92:8F:50:F7:B1:AE (Unknown)
Nmap scan report for laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2)
Host is up (0.00041s latency).
MAC Address: 1A:59:6F:A7:BD:27 (Unknown)
Nmap scan report for macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.4)
Host is up (0.00045s latency).
MAC Address: BE:BF:B4:FD:5B:6F (Unknown)
Nmap scan report for notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.5)
Host is up (0.00045s latency).
MAC Address: CE:3C:CF:2B:4D:C2 (Unknown)
Nmap scan report for analyst.projeto_final_opcao_1_guest_net (10.10.50.6)
Host is up (0.00034s latency).
MAC Address: C2:AF:E2:82:1D:DD (Unknown)
Nmap scan report for 19957ae5bd57 (10.10.50.3)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.08 seconds
bash
bash
Engine running
RAM 1.66 GB CPU 0.25% Disk: 4.39 GB used (limit 227.93 GB)
Terminal
Update