



Projeto Técnico

Mapeamento de Rede Corporativa – Lab Docker

Autora: Bianca Pacheco Baptista
Instituição: VaiNaWeb
Local: Rio de Janeiro
Data: 28/06/2025

Objectivo

Analisar a rede simulada para identificar exposição, segmentação e riscos operacionais.

Escopo

Ambiente docker simulado com múltiplos hosts e redes segmentadas.


Sumario Executivo

O trabalho de identificação da rede gerou a lista de dispositivos abaixo.

IP	Name	Port	OS details
10.10.10.1	router	111	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
10.10.10.10	WS_001	-	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)

IP	Name	Port	OS details
10.10.10.101	WS_002	-	
10.10.10.127	WS_003	-	
10.10.10.222	WS_004	-	
10.10.10.2		-	
10.10.30.1	router	111	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
10.10.30.10	ftp-server	21	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
10.10.30.11	mysql-server	3306	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
10.10.30.15	samba-server	139/445	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
10.10.30.17	openldap	389/636	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
10.10.30.117	zabbix-server	80	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
10.10.30.227	legacy-server		
10.10.30.2		-	
10.10.50.1	router	111	Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
10.10.50.2	laptop-vastro	-	
10.10.50.3	notebook-carlos	-	
10.10.50.4	macbook-aline	-	
10.10.50.5	laptop-luiz	-	
10.10.50.6		-	

Diagrama da Rede

A partir do que foi encontrado, foi gerado o diagrama de rede abaixo. Diagrama de Rede

Diagnóstico (Achados)

Rede CORP_NET

- Identificado o switch IP 10.10.10.1, respondendo pela porta 111 TCP;
- Identificado 05 servidores que não possuem portas abertas e que não foi possível identificar o sistema operacional e serviços ativos;

Rede GUEST_NET

- Identificado o switch IP 10.10.30.1, respondendo pela porta 111 TCP;
- Foram encontrados 07 servidores:
- 06 servidores possuem portas abertas, sistema operacional e serviços identificáveis;
- 02 servidores não possuem portas abertas e não foi possível identificar o sistema operacional e serviços ativos

Rede INFRA_NET

- Identificado o switch IP 10.10.50.1, respondendo pela porta 111 TCP;
- Foram encontrados 04 dispositivos que aparentam ser notebooks de usuários. Como a rede se chama INFRA_NET, acredito se tratar da subrede de gerência e os notebooks são do time de infra. Nenhum dos dispositivos apresenta portas abertas, e não foi possível identificar o sistema operacional e serviços ativos;
- Identificado 01 servidor que não possuem portas abertas e que não foi possível identificar o sistema operacional e serviços ativos;

Recomendações

- Os servidores identificados na rede GUEST_NET, possuem serviços considerados críticos, como o servidor de Banco de dados, o servidor de LDAP e o de monitoramento "ZABBIX", além de um servidor com o nome de LEGACY-SERVER, que pode conter informações não públicas. Sugiro fortemente que estes servidores estejam em subredes privadas em uma rede não "GUEST", como o nome atual da rede sugere;
- Em todas as redes notam-se servidores com uptime de milhares de dias. É importante validar se todos os sistemas operacionais e serviços possuem as atualizações de segurança mais recentes;

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Isolar servidores críticos	Alto	Média	Alta
Migrar de FTP para SFTP	Médio	Media	Alta
Atualização de SO	Alto	Baixa	Alta
Atualização de Serviços	Medio	Baixa	Alta

Conclusão

O trabado preliminar de identificação gerou resultados que pedem atenção imediata no quisito de segurança, como servidores e serviços com possível defazagem nos processos de atualização o que leva a riscos de invasão. É importante isolar servidores e serviços críticos como Bancos de Dados e Servidores de

Monitoramento e de autenticação, por exporem dados da empresa, de usuários e da infraestrutura, os quais podem ser usados para causar prejuízos, para a empresa e para os seus clientes. Seguem imagens do que foi encontrado e relatórios mais detalhados podem ser gerados para apoiar nas sugestões listadas.

Anexos

```
(root@c082dbf416ee)-[/home/analyst]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
3: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1000
    link/tunnel6 :: brd :: permaddr e6e0:32c2:829f::
37: eth0@if38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:0a:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
41: eth1@if42: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:32:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth1
        valid_lft forever preferred_lft forever
43: eth2@if44: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:0a:1e:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth2
        valid_lft forever preferred_lft forever
```

```
inet 127.0.0.1/8 scope host lo
inet 10.10.30.2/24 brd 10.10.30.255 scope global eth2
inet 10.10.10.2/24 brd 10.10.10.255 scope global eth0
inet 10.10.50.6/24 brd 10.10.50.255 scope global eth1
```

Listas de hosts CORP NET

```
(root@c082dbf416ee)-[/home/analyst]
# nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
Host: 10.10.10.1 (10.10.10.1) Status: Up
Host: 10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net) Status: Up
Host: 10.10.10.2 (c082dbf416ee) Status: Up

Host: 10.10.30.1 (10.10.30.1) Status: Up
Host: 10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.17 (openldap.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net) Status: Up
Host: 10.10.30.2 (c082dbf416ee) Status: Up

Host: 10.10.50.1 (10.10.50.1) Status: Up
Host: 10.10.50.2 (notebook-carlos.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.4 (laptop-vastro.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.6 (laptop-luiz.projeto_final_opcao_1_guest_net) Status: Up
Host: 10.10.50.5 (c082dbf416ee) Status: Up
```

Portas abertas


```
Open 10.10.10.1:111
Open 10.10.10.2:43572
Open 10.10.10.2:45116
Open 10.10.10.1:56253
Open 10.10.10.2:59358
```

```
Open 10.10.30.10:21
Open 10.10.30.117:80
Open 10.10.30.1:111
Open 10.10.30.15:139
Open 10.10.30.17:389
Open 10.10.30.15:445
Open 10.10.30.17:636
Open 10.10.30.11:3306
Open 10.10.30.117:10051
Open 10.10.30.117:10052
Open 10.10.30.2:32920
Open 10.10.30.11:33060
Open 10.10.30.1:56253
Open 10.10.30.2:59598
```

```
Open 10.10.50.1:111
Open 10.10.50.5:39804
Open 10.10.50.5:47938
Open 10.10.50.1:56253
```

Banco de dados MySQL

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 19:09 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000054s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 10
|   Capabilities Flags: 65536
|   Some Capabilities: Support41Auth, LongPassword, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, FoundRows, IgnoreSpaceBeforeParenthesis, InteractiveClient, IgnoreSigpipes, SupportsCompression, Su
|   portsTransactions, SupportsLoadDataLocal, ODBCClient, LongColumnFlag, ConnectWithDatabase, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: 5U'\x14*\v4
|   SPoV=/L?F\x1F
|   Auth Plugin Name: caching_sha2_password
MAC Address: 02:42:8A:0A:1E:0B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

LDAP

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-28 19:10 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000073s latency).

PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-rootdse:
| LDAP Results
| <ROOT>
|   namingContexts: dc=example,dc=org
|   supportedControl: 2.16.840.1.113730.3.4.18
|   supportedControl: 2.16.840.1.113730.3.4.2
|   supportedControl: 1.3.6.1.4.1.4203.1.10.1
|   supportedControl: 1.3.6.1.1.22
|   supportedControl: 1.2.840.113556.1.4.319
|   supportedControl: 1.2.826.0.1.3344810.2.3
|   supportedControl: 1.3.6.1.1.13.2
|   supportedControl: 1.3.6.1.1.13.1
|   supportedControl: 1.3.6.1.1.12
|   supportedExtension: 1.3.6.1.4.1.1466.20037
|   supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|   supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|   supportedExtension: 1.3.6.1.1.8
|   supportedLDAPVersion: 3
|   supportedSASLMechanisms: SCRAM-SHA-1
|   supportedSASLMechanisms: SCRAM-SHA-256
|   supportedSASLMechanisms: GS2-IAKERB
|   supportedSASLMechanisms: GS2-KRB5
|   supportedSASLMechanisms: GSSAPI
|   supportedSASLMechanisms: GSS-SPNEGO
|   supportedSASLMechanisms: DIGEST-MD5
|   supportedSASLMechanisms: OTP
|   supportedSASLMechanisms: NTLM
|   supportedSASLMechanisms: CRAM-MD5
|_   subschemaSubentry: cn=Subschema
MAC Address: 02:42:0A:0A:1E:11 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

WEB

```
l = curl http://10.10.30.17/
<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="Author" content="Zabbix SIA" />
    <title>Zabbix docker: Zabbix SIA</title>
    <link rel="icon" href="/favicon.ico">
    <link rel="apple-touch-icon-precomposed" sizes="76x76" href="/assets/img/apple-touch-icon-76x76-precomposed.png">
    <link rel="apple-touch-icon-precomposed" sizes="120x120" href="/assets/img/apple-touch-icon-120x120-precomposed.png">
    <link rel="apple-touch-icon-precomposed" sizes="152x152" href="/assets/img/apple-touch-icon-152x152-precomposed.png">
    <link rel="apple-touch-icon-precomposed" sizes="180x180" href="/assets/img/apple-touch-icon-180x180-precomposed.png">
    <link rel="icon" sizes="192x192" href="/assets/img/touch-icon-192x192.png">
    <meta name="csrf-token" content="" />
    <meta name="msapplication-tileimage" content="/assets/img/ms-tile-144x144.png">
    <meta name="msapplication-tilecolor" content="#d40000">
    <meta name="msapplication-config" content="none"/>
    <link rel="stylesheet" type="text/css" href="/assets/styles/blue-theme.css" />
    <style type="text/css">.na-bg, .na-bg input[type="radio"]:checked + label, .na-bg:before, .flh-na-bg, .status-na-bg { background-color: #97AAB3 }
    .info-bg, .info-bg input[type="radio"]:checked + label, .info-bg:before, .flh-info-bg, .status-info-bg { background-color: #7499FF }
    .warning-bg, .warning-bg input[type="radio"]:checked + label, .warning-bg:before, .flh-warning-bg, .status-warning-bg { background-color: #FFC859 }
    .average-bg, .average-bg input[type="radio"]:checked + label, .average-bg:before, .flh-average-bg, .status-average-bg { background-color: #FFA059 }
    .high-bg, .high-bg input[type="radio"]:checked + label, .high-bg:before, .flh-high-bg, .status-high-bg { background-color: #E97659 }
    .disaster-bg, .disaster-bg input[type="radio"]:checked + label, .disaster-bg:before, .flh-disaster-bg, .status-disaster-bg { background-color: #E45959 }
    </style><script>var PHP_TZ_OFFSET = 10800,PHP_ZBX_FULL_DATE_TIME = "Y-m-d H:i:s";</script><script src="/js/browsers.js"></script>
  </head>
  <body lang="en">
    <output class="msg-global-footer msg-warning" id="msg-global-footer"></output>
    <main><div class="server-name">Zabbix docker</div><div class="signin-container"><div class="signin-logo"></div><form method="post" action="index.php" accept-charset="utf-8" aria-label="Sign in"><ul><li><label form="name">Username</label><input type="text" id="name" name="name" value="" maxlength="255" autofocus="autofocus"></li><li><label for="password">Password</label><input type="password" id="password" name="password" value="" maxlength="255"></li><li><input type="checkbox" id="autologin" name="autologin" value="1" class="checkbox"><label for="autologin">Remember me for 30 days</li></ul><input type="submit" id="enter" name="enter" value="Sign in"></div><div class="signin-links"><a target="_blank" class="grey link-alt" href="https://www.zabbix.com/documentation/4.4/en/doc/>Help</a><a href="#">Support</a></div></div></main><div class="contentinfo">&copy; 2001-2025, <a class="grey link-alt" target="_blank" href="https://www.zabbix.com/>Zabbix SIA</a></div></div></body>
```

Local de armazenamento dos dados capturados

```
(root@c082dbf416ee)-[/home/analyst/recon]  
[ # ls -ls  
total 20  
4 drwxr-xr-x 2 root root 4096 Jul 28 19:14 corp_net  
4 drwxr-xr-x 2 root root 4096 Jul 28 19:15 guest_net  
4 drwxr-xr-x 2 root root 4096 Jul 28 19:15 infra_net  
4 -rw-r--r-- 1 root root 209 Jul 27 21:10 recon-redes.txt  
4 -rw-r--r-- 1 root root 1473 Jul 28 19:14 recon_ip_maps.txt
```