KENSEI

Relatório Técnico – Rede Corporativa-Lab Docker(Projeto 1)

Autor: Jonathan Alex Caetano Coelho
Data: 25/07/2025.
versão: 2.0

Sumário

Sumário Executivo **3**
Objetivo **5**
Escopo **6**
Metodologia **7**
Diagrama de Rede **8**
Diagnóstico (Achados) **9**
Recomendações **10**
Classificação de Riscos e Métricas 10
Revarredura Pós-Mitigações 10
Boas Práticas de Hardening e Monitoramento 10
Plano de Ação (80/20) **11**
Tabela Resumo dos Riscos Identificados 11
Conclusão **12**
Anexos **13**
Prints **23**

Sumário Executivo

Este relatório apresenta os principais achados da análise de segmentação de rede realizada em um ambiente Docker simulado, contendo as redes corp_net (Corporação, a empresa em si), guest_net (Área exclusiva destinada a convidados) e infra_net (Área exclusiva destinada a setores da empresa e suas funcionalidades).
Foram utilizados scanners como Nmap e Rustscan, além de ferramentas auxiliares para reconhecimento de rede.
Foram identificadas diversas exposições de serviços, com recomendações específicas para sanar possíveis vulnerabilidades.

Durante a análise, observou-se a ausência de controles eficazes de segmentação entre as redes, permitindo a comunicação entre zonas que deveriam estar isoladas.
Foram encontrados serviços expostos na rede guest_net que possibilitam o acesso a recursos sensíveis da corp_net, comprometendo a confidencialidade da informação.
Identificou-se também a presença de portas abertas sem justificativa operacional, facilitando ataques de enumeração e exploração por agentes mal-intencionados.

Além disso, não foram observados mecanismos de monitoramento de tráfego entre redes, dificultando a detecção de atividades suspeitas em tempo real.
Recomenda-se a implementação de regras de firewall mais restritivas, com base no princípio do menor privilégio.

Também é aconselhado o uso de VLANs e firewalls internos para garantir que o tráfego entre redes sensíveis seja devidamente controlado e monitorado.
A segregação lógica e física das redes é essencial para evitar movimentos laterais de possíveis atacantes.

Sugere-se a aplicação imediata de atualizações e patches em sistemas e bibliotecas identificadas como desatualizadas.
A utilização de ferramentas de análise contínua de vulnerabilidades deve ser incorporada à rotina da equipe de segurança.

A estrutura atual permite que um usuário mal-intencionado da guest_net acesse informações da infra_net, o que demonstra falhas graves de design na arquitetura de rede.
Em suma, o ambiente analisado apresenta riscos relevantes que podem ser explorados por agentes internos ou externos.

A implementação das recomendações deste relatório é urgente para mitigar vulnerabilidades e elevar o nível de segurança cibernética da organização.

Objetivo

Analisar a rede da empresa Analyst que foi simulada para identificar exposição, segmentação e riscos operacionais.

Rede	Subnet	Descrição
corp_net	10.10.10.0/24	Rede corporativa (estações e web server)
guest_net	10.10.30.0/24	Rede de visitantes e dispositivos pessoais
infra_net	10.10.50.0/24	Rede de infraestrutura crítica (servidores)

Com o intuito de mostrar tais vulnerabilidades dos setores apresentados, suas possíveis correções e listar boas práticas para poder deixar o ambiente mais seguro.

Identificar Todas as Máquinas Acessíveis.

Determinar as Sub-redes Existentes e seus propósitos.

Criar um inventário técnico com IPs, Nomes e Sistemas detectados.

Elaborar relatório com diagnóstico, recomendações e plano de ação 80/20.

Escopo

Ambiente docker simulado com múltiplos hosts e redes segmentadas.
Avaliar a segmentação de rede e identificar vulnerabilidades em um ambiente Docker simulado, composto pelas redes:

- **corp_net** (rede interna da corporação)
- **guest_net** (acesso para convidados)
- **infra_net** (serviços internos da infraestrutura da empresa)
- Utilização de ferramentas como **Nmap**, **Rustscan** e outras para varredura e reconhecimento de rede
- Inspeção de serviços expostos, portas abertas e controles de acesso
- Falhas de segmentação entre redes (acesso indevido entre zonas)
- Portas abertas sem justificativa operacional
- Falta de monitoramento de tráfego entre redes
- Implementação de **firewalls internos e regras restritivas**
- Adoção de **VLANs e segregação lógica/física de redes**
- Atualização de sistemas e aplicação de **patches**
- Implantação de ferramentas de **análise contínua de vulnerabilidades**
- Desenvolvimento de um **plano de resposta a incidentes**

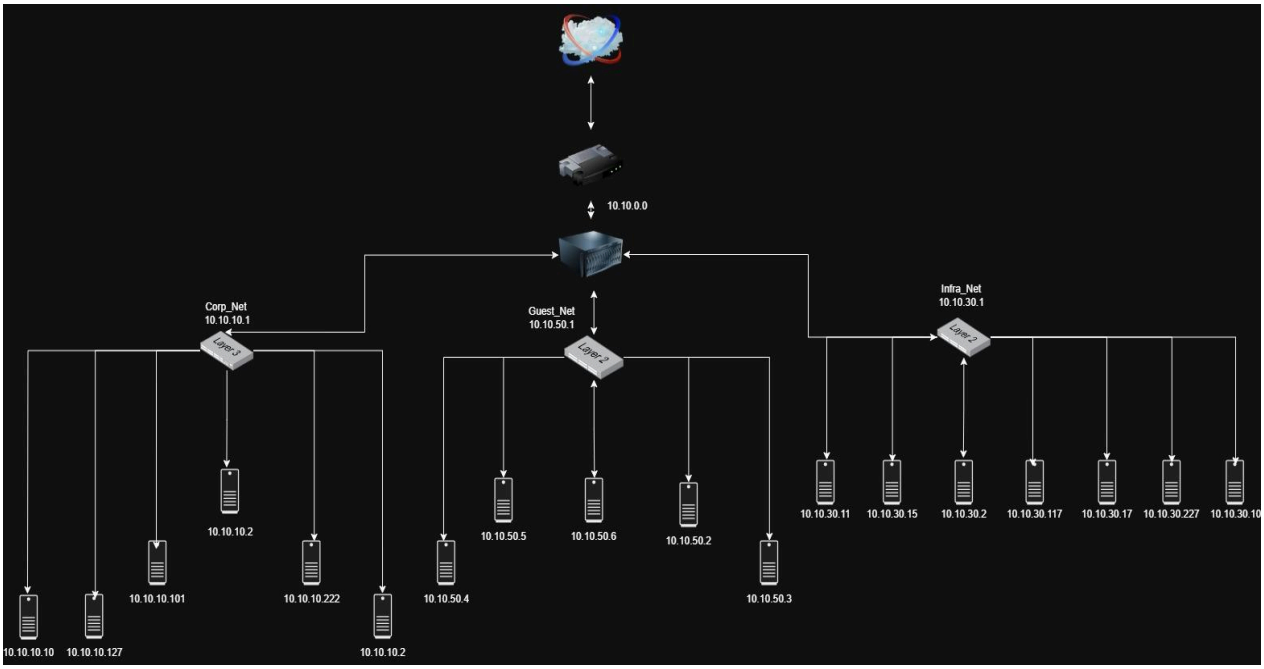
Metodologia

- Coleta ativa de dados de rede
- Análise manual e documentada
- Ferramentas:

Resumo Explicativo dos Comandos e sua Função no Diagnóstico

Ferramenta / Comando	Função	Aplicação no relatório
nmap	Varredura completa de portas e serviços	Detectar serviços ativos e vulneráveis
rustscan	Varredura rápida de portas	Pré-varredura para alimentar o Nmap
netdiscover	Descoberta de dispositivos na rede	Identificar IPs e hosts ativos
ping	Teste de conectividade entre hosts	Validar se os hosts estão acessíveis
ftp	Acesso ao serviço FTP (verificar anonimato)	Verificação de FTP anônimo
ldapsearch	Enumeração do diretório LDAP	Obter informações de RootDSE
mysql	Acesso ao MySQL e banner grabbing	Confirmar exposição do banco MySQL
smbclient	Listar compartilhamentos SMB acessíveis	Detectar recursos expostos via SMB
curl / navegador	Testar serviços web (ex: painel Zabbix)	Verificar exposição de serviços web

Diagrama de Rede



Diagnóstico (Achados)

- 10.10.30.10 - FTP - Porta 21
- Risco identificado: FTP anônimo habilitado.
- Evidência: Ver arquivo 'infra_net_servico_ftp-anon.txt'.

- 10.10.30.17 - LDAP - Porta 389
- Risco identificado: Enumeração via RootDSE habilitada.
- Evidência: Ver arquivo 'infra_net_servico_ldap-rootdse.txt'.

- 10.10.30.11 - MySQL - Porta 3306
- Risco identificado: MySQL exposto com banner.
- Evidência: Ver arquivo 'infra_net_servico_mysql-info.txt'.

- 10.10.30.15 - SMB - Porta 445
- Risco identificado: Compartilhamentos SMB acessíveis.
- Evidência: Ver arquivo 'infra_net_servico_smb.txt'.

- 10.10.30.117 - HTTP - Porta 80
- Risco identificado: Web server Zabbix exposto.
- Evidência: Ver arquivo 'infra_net_servico_zabbix.txt'.

Recomendações

- Isolar serviços de infraestrutura em redes privadas.
- Desativar FTP anônimo ou restringir por IP.
- Restringir acessos ao MySQL e SMB apenas a IPs confiáveis.
- Implementar autenticação e controle de acesso ao Zabbix.
- Utilizar firewall entre redes guest, corp e infra.

Classificação de Riscos e Métricas

Adotar classificações de risco baseadas em CVSS (Common Vulnerability Scoring System) ajuda a priorizar vulnerabilidades de forma objetiva. Sempre que possível, relacione as vulnerabilidades aos IDs do banco de dados CVEs (Common Vulnerabilities and Exposures).

Revarredura Pós-Mitigações

Após a implementação das medidas corretivas, é essencial realizar uma nova varredura utilizando as mesmas ferramentas para garantir que os riscos foram efetivamente mitigados.

Boas Práticas de Hardening e Monitoramento

Recomenda-se as seguintes práticas complementares:

• Desativar serviços desnecessários ou inseguros.
• Aplicar o princípio do menor privilégio.
• Manter sistemas atualizados com patches de segurança.
• Implementar monitoração contínua de tráfego entre redes.
• Fazer auditorias de segurança regularmente.
• Utilizar ferramentas SIEM e IDS/IPS.

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Isolar serviços da infra_net	Alto	Média	Alta
Desabilitar FTP anônimo	Médio	Alta	Alta
Restringir MySQL/Samba a IPs internos	Alto	Média	Alta
Habilitar autenticação no Zabbix	Alto	Alta	Alta

Tabela Resumo dos Riscos Identificados

IP	Serviço	Porta	Vunerabilidade	Nível de Risco	Status
10.10.30.10	FTP	21	FTP anônimo habilitado	Alto	Pendente
10.10.30.17	LDAP	389	Enumeração RootDSE	Médio	Pendente
10.10.30.11	MySQL	3306	Banner de versão exposto	Alto	Pendente
10.10.30.15	SMB	445	Compartilhamentos abertos	Alto	Pendente
10.10.30.117	HTTP	80	Zabbix exposto sem autenticação	Alto	Pendente

Conclusão

Foram identificadas diversas exposições de serviços nas redes **`infra_net`**, **`corp_net`** e **`guest_net`**, com destaque para a ausência de mecanismos eficazes de isolamento e controle de acesso entre zonas que deveriam ser segregadas logicamente.

Os riscos levantados, como o acesso anônimo ao FTP, a enumeração LDAP sem autenticação, o banco de dados MySQL com informações de banner públicas e compartilhamentos SMB expostos, colocam em risco direto a confidencialidade, integridade e disponibilidade dos ativos da organização. A presença de um painel de monitoramento Zabbix acessível sem autenticação reforça a urgência na aplicação de medidas corretivas.

A comunicação entre redes deveria ser estritamente controlada por regras baseadas no princípio do menor privilégio, complementadas por firewalls internos e segregação via VLANs. No entanto, observou-se ausência de filtros eficientes e monitoramento de tráfego, o que permite movimentações laterais por agentes mal-intencionados.

Diante disso, recomenda-se a implementação imediata do **plano de ação 80/20** proposto, priorizando:

- O isolamento total da **`infra_net`**;
- A desativação ou controle de serviços inseguros (FTP anônimo, SMB aberto);
- A restrição de serviços como MySQL e Zabbix a IPs confiáveis e usuários autenticados.

Adicionalmente, é altamente recomendável que a organização:

- Realize uma **varredura de validação** após as correções;
- Implemente um processo contínuo de **gerenciamento de vulnerabilidades**;
- Adote práticas de **hardening** em seus serviços e sistemas;
- Estabeleça um plano robusto de **resposta a incidentes**.

Anexos

Corp_net_ips.txt

10.10.10.1

10.10.10.10

10.10.10.101

10.10.10.127

10.10.10.222

10.10.10.2

Corp_net_ips_hosts.txt

10.10.10.1 (HpVictus15)

10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net)

10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net)

10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net)

10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net)

10.10.10.2 (f609ce277032)

Corp_net_ips_ports.txt

Open 10.10.10.2:38078

Open 10.10.10.2:42298

Guest_net_ips.txt

10.10.50.1

10.10.50.2

10.10.50.3

10.10.50.4

10.10.50.5

10.10.50.6

Guest_net_ips_hosts.txt

10.10.50.1 (HpVictus15)

10.10.50.2 (laptop-luiz.projeto_final_opcao_1_guest_net)

10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)

10.10.50.4 (notebook-carlos.projeto_final_opcao_1_guest_net)

10.10.50.5 (laptop-vastro.projeto_final_opcao_1_guest_net)

10.10.50.6 (f609ce277032)

Guest_net_ips_ports.txt

Open 10.10.50.6:57510

Infra_net_ips.txt

10.10.30.1

10.10.30.10

10.10.30.11

10.10.30.15

10.10.30.17

10.10.30.117

10.10.30.227

10.10.30.2

Infra_net_ips_hosts.txt

10.10.30.1 (HpVictus15)

10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)

10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)

10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)

10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)

10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)

10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)

10.10.30.2 (f609ce277032)

Infra_net_ips_ports.txt

Open 10.10.30.10:21

Open 10.10.30.117:80

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 10.10.30.11:33060

Infra_net_servico_ftp-anon.txt

Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:00 UTC

Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)

Host is up (0.000066s latency).

PORT   STATE SERVICE

21/tcp open ftp

MAC Address: D6:8E:03:51:F6:0D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Infra_net_servico_ldap-rootdse.txt

Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:03 UTC

Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)

Host is up (0.000074s 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: GS2-IAKERB

| supportedSASLMechanisms: GS2-KRB5

| supportedSASLMechanisms: SCRAM-SHA-1

| supportedSASLMechanisms: SCRAM-SHA-256

| supportedSASLMechanisms: GSSAPI

| supportedSASLMechanisms: GSS-SPNEGO

| supportedSASLMechanisms: DIGEST-MD5

| supportedSASLMechanisms: OTP

| supportedSASLMechanisms: CRAM-MD5

| supportedSASLMechanisms: NTLM

|_ subschemaSubentry: cn=Subschema

MAC Address: B2:BD:99:48:71:22 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

Infra_net_servico_mysql-info.txt

Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:02 UTC

Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)

Host is up (0.000074s latency).

PORT STATE SERVICE

3306/tcp open mysql

| mysql-info:

| Protocol: 10

| Version: 8.0.42

| Thread ID: 11

| Capabilities flags: 65535

| Some Capabilities: SupportsLoadDataLocal, IgnoreSigpipes, Speaks41ProtocolOld, SupportsTransactions, Support41Auth, DontAllowDatabaseTableColumn, ConnectWithDatabase, FoundRows, InteractiveClient, SupportsCompression, Speaks41ProtocolNew, LongPassword, IgnoreSpaceBeforeParenthesis, ODBCClient, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins

| Status: Autocommit

| Salt: i{v2`\x14y,82QS]6\x18.-5}P

|_ Auth Plugin Name: caching_sha2_password

MAC Address: 2A:E1:09:CC:EA:5D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

Infra_net_servico_smb.txt

Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:04 UTC

Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)

Host is up (0.000071s latency).

PORT   STATE SERVICE

445/tcp open microsoft-ds

MAC Address: CE:D4:F1:E1:31:B6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds

Infra_net_servico_webserver.txt

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Jul 2025 14:06:14 GMT

Content-Type: text/html; charset=UTF-8

Connection: keep-alive

Keep-Alive: timeout=20

X-Powered-By: PHP/7.3.14

Set-Cookie: PHPSESSID=dcaacf845d70593bceccf797f57ee6d8; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: SAMEORIGIN

Infra_net_servico_zabbix.txt

<!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</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> Zabbix docker <form method="post" action="index.php" accept-charset="utf-8" aria-label="Sign in">
<label for="name">Username</label><input type="text" id="name" name="name" value="" maxlength="255" autofocus="autofocus">
<label for="password">Password</label><input type="password" id="password" name="password" value="" maxlength="255">
<input type="checkbox" id="autologin" name="autologin" value="1" class="checkbox-radio" checked="checked"><label for="autologin">Remember me for 30 days</label>
<button type="submit" id="enter" name="enter" value="Sign in">Sign in</button>
</form> Help • Support </main><footer role="contentinfo">© 2001–2020, Zabbix SIA</footer></body>

Recon_ip_maps.txt

samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) at ce:d4:f1:e1:31:b6 [ether] on eth1

HpVictus15 (10.10.50.1) at 2a:88:e2:d0:57:e7 [ether] on eth0

WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) at ba:f2:6c:32:97:e7 [ether] on eth2

WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) at d6:97:f9:c8:1b:2b [ether] on eth2

macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3) at e2:0a:7f:00:a3:3f [ether] on eth0

ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10) at d6:8e:03:51:f6:0d [ether] on eth1

laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.2) at 02:f6:24:35:9c:aa [ether] on eth0

legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227) at 96:29:1e:eb:47:52 [ether] on eth1

mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11) at 2a:e1:09:cc:ea:5d [ether] on eth1

laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5) at 5a:0f:69:20:84:b1 [ether] on eth0

WS_001.projeto_final_opcao_1_corp_net (10.10.10.10) at ba:c0:0a:45:fc:cb [ether] on eth2

openldap.projeto_final_opcao_1_infra_net (10.10.30.17) at b2:bd:99:48:71:22 [ether] on eth1

notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.4) at 12:3b:15:1a:c6:cf [ether] on eth0

zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117) at f2:18:c6:67:b6:ff [ether] on eth1

HpVictus15 (10.10.30.1) at 2e:80:81:86:dd:ff [ether] on eth1

WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) at 0a:9e:1b:72:a2:06 [ether] on eth2

HpVictus15 (10.10.10.1) at 02:05:90:d9:c6:b1 [ether] on eth2

Recon-redes.txt

inet 127.0.0.1/8 scope host lo

inet6 ::1/128 scope host proto kernel_lo

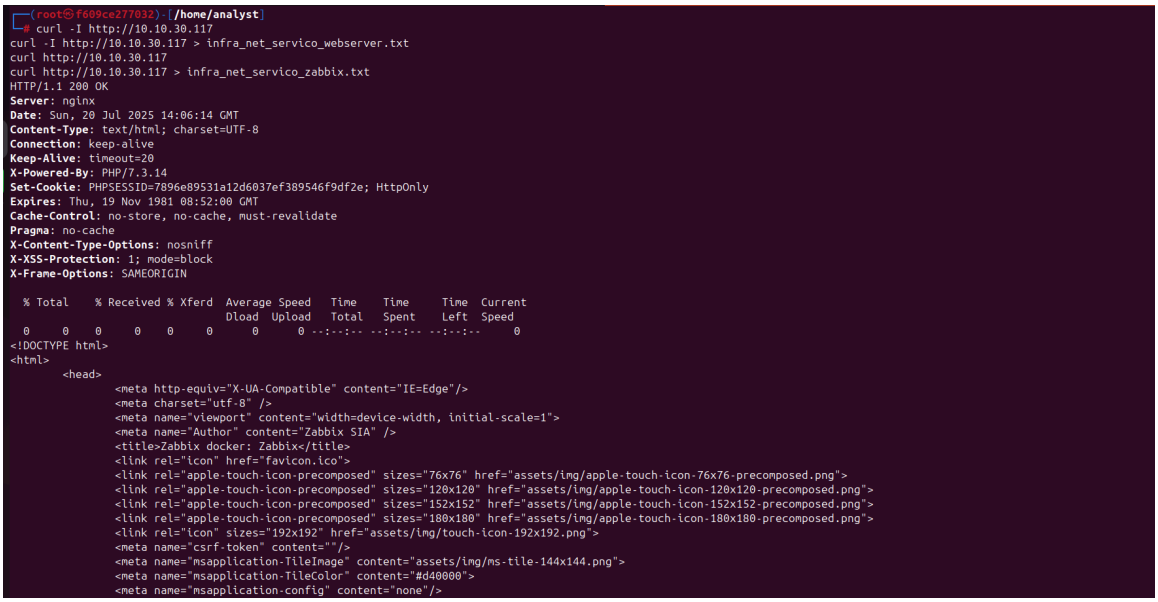
inet 10.10.50.6/24 brd 10.10.50.255 scope global eth0

inet 10.10.30.2/24 brd 10.10.30.255 scope global eth1

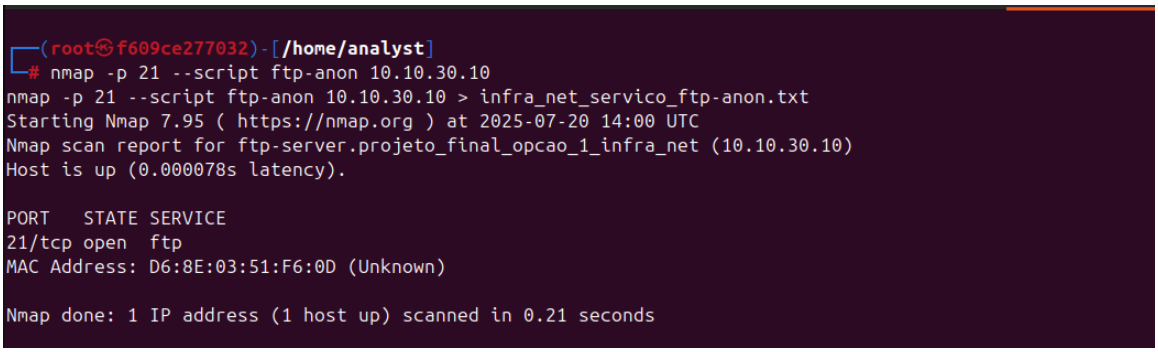
inet 10.10.10.2/24 brd 10.10.10.255 scope global eth2

Prints


<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> Zabbix docker <form method="post" action="index.php" accept-charset="utf-8" aria-label="Sign in">
<label for="name">Username</label><input type="text" id="name" name="name" value="" maxlength="255" autofocus="autofocus">
<label for="password">Password</label><input type="password" id="password" name="password" value="" maxlength="255">
<input type="checkbox" id="autologin" name="autologin" value="1" class="checkbox-radio" checked="checked"><label for="autologin">Remember me for 30 days</label>
<button type="submit" id="enter" name="enter" value="Sign in">Sign in</button>
</form> Help • Support </main><footer role="contentinfo">© 2001–2020, Zabbix SIA</footer></body>
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 3412 0 3412 0 0 60162 0 --:--:-- --:--:-- --:--:-- 60928


┌──(root㉿f609ce277032)-[/home/analyst]
└─# curl -I http://10.10.30.117
curl -I http://10.10.30.117 > infra_net_servico_webserver.txt
curl http://10.10.30.117
curl http://10.10.30.117 > infra_net_servico_zabbix.txt
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 20 Jul 2025 14:06:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Keep-Alive: timeout=20
X-Powered-By: PHP/7.3.14
Set-Cookie: PHPSESSID=7896e89531a12d6037ef389546f9df2e; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
<!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</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"/>


┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_net_servico_smb.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:04 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.000094s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: CE:D4:F1:E1:31:B6 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds


┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -p 21 --script ftp-anon 10.10.30.10
nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-07-20 14:00 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000078s latency).
PORT STATE SERVICE
21/tcp open ftp
MAC Address: D6:8E:03:51:F6:0D (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17
nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootdse.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 14:03 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000084s 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: GS2-IAKERB
|       supportedSASLMechanisms: GS2-KRB5
|       supportedSASLMechanisms: SCRAM-SHA-1
|       supportedSASLMechanisms: SCRAM-SHA-256
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: OTP
|       supportedSASLMechanisms: CRAM-MD5
|       supportedSASLMechanisms: NTLM
|_      subschemaSubentry: cn=Subschema
MAC Address: B2:BD:99:48:71:22 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11
nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 14:02 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000079s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 10
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolOld, LongPassword, Support41Auth, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, DontAllowDatabaseTableColumn, SupportsTransactions, ODBCClient, InteractiveClient, FoundRows, IgnoreSigpipes, SwitchToSSLAfterHandshake, SupportsCompression, Speaks41ProtocolNew, SupportsLoadDataLocal, LongColumnFlag, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ?@\x07JV-\x0DIEKlIrkOx\x0Fqxj
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 2A:E1:09:CC:EA:5D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
Host: 10.10.10.1 (HpVictus15)   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 (f609ce277032) Status: Up
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2}' | tee corp_net_ips.txt
10.10.10.1
10.10.10.10
10.10.10.101
10.10.10.127
10.10.10.222
10.10.10.2
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.
10.10.10.1 (HpVictus15)
10.10.10.10 (WS_001.projeto_final_opcao_1_corp_net)
10.10.10.101 (WS_002.projeto_final_opcao_1_corp_net)
10.10.10.127 (WS_003.projeto_final_opcao_1_corp_net)
10.10.10.222 (WS_004.projeto_final_opcao_1_corp_net)
10.10.10.2 (f609ce277032)
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2}' | tee guest_net_ips.txt
10.10.50.1
10.10.50.2
10.10.50.3
10.10.50.4
10.10.50.5
10.10.50.6
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee guest_net_ips_hosts.txt
10.10.50.1 (HpVictus15)
10.10.50.2 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.4 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.5 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.6 (f609ce277032)
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
Host: 10.10.50.1 (HpVictus15)   Status: Up
Host: 10.10.50.2 (laptop-luiz.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 (notebook-carlos.projeto_final_opcao_1_guest_net)      Status: Up
Host: 10.10.50.5 (laptop-vastro.projeto_final_opcao_1_guest_net)        Status: Up
Host: 10.10.50.6 (f609ce277032) Status: Up
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2}' | tee infra_net_ips.txt
10.10.30.1
10.10.30.10
10.10.30.11
10.10.30.15
10.10.30.17
10.10.30.117
10.10.30.227
10.10.30.2
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee infra_net_ips_hosts.txt
10.10.30.1 (HpVictus15)
10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)
10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)
10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)
10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)
10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)
10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)
10.10.30.2 (f609ce277032)
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
Host: 10.10.30.1 (HpVictus15)   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 (f609ce277032) Status: Up
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2}' | tee infra_net_ips.txt
10.10.30.1
10.10.30.10
10.10.30.11
10.10.30.15
10.10.30.17
10.10.30.117
10.10.30.227
10.10.30.2
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee infra_net_ips_hosts.txt
10.10.30.1 (HpVictus15)
10.10.30.10 (ftp-server.projeto_final_opcao_1_infra_net)
10.10.30.11 (mysql-server.projeto_final_opcao_1_infra_net)
10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)
10.10.30.17 (openldap.projeto_final_opcao_1_infra_net)
10.10.30.117 (zabbix-server.projeto_final_opcao_1_infra_net)
10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)
10.10.30.2 (f609ce277032)
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
Host: 10.10.30.1 (HpVictus15)   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 (f609ce277032) Status: Up
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# ls -la
total 96
drwx------ 1 analyst analyst  4096 Jul 20 13:44 .
drwxr-xr-x 1 root    root     4096 Jul 18 15:38 ..
-rw-r--r-- 1 root    root     2892 Jul 18 15:38 .ANOTACAO-ULTIMO-SCAN.TXT
-rw-r--r-- 1 analyst analyst   220 Jun 22 17:05 .bash_logout
-rw-r--r-- 1 analyst analyst  5551 Jul 13 04:02 .bashrc
-rw-r--r-- 1 analyst analyst  3526 Jun 22 17:05 .bashrc.original
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .config
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .java
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .local
-rw-r--r-- 1 analyst analyst   807 Jun 22 17:05 .profile
-rw-r--r-- 1 analyst analyst   336 Jun 24 08:51 .zprofile
-rw-r--r-- 1 analyst analyst 10856 Jun 24 08:51 .zshrc
-rw-r--r-- 1 root    root       73 Jul 20 13:38 corp_net_ips.txt
-rw-r--r-- 1 root    root      261 Jul 20 13:39 corp_net_ips_hosts.txt
-rw-r--r-- 1 root    root       44 Jul 20 13:47 corp_net_ips_ports.txt
-rw-r--r-- 1 root    root       66 Jul 20 13:43 guest_net_ips.txt
-rw-r--r-- 1 root    root      286 Jul 20 13:43 guest_net_ips_hosts.txt
-rw-r--r-- 1 root    root       96 Jul 20 13:41 infra_net_ips.txt
-rw-r--r-- 1 root    root      402 Jul 20 13:41 infra_net_ips_hosts.txt
-rw-r--r-- 1 root    root      255 Jul 20 13:33 recon-redes.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# cat corp_net_ips_ports.txt
Open 10.10.10.2:38078
Open 10.10.10.2:42298
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# ls -la
total 100
drwx------ 1 analyst analyst  4096 Jul 20 13:50 .
drwxr-xr-x 1 root    root     4096 Jul 18 15:38 ..
-rw-r--r-- 1 root    root     2892 Jul 18 15:38 .ANOTACAO-ULTIMO-SCAN.TXT
-rw-r--r-- 1 analyst analyst   220 Jun 22 17:05 .bash_logout
-rw-r--r-- 1 analyst analyst  5551 Jul 13 04:02 .bashrc
-rw-r--r-- 1 analyst analyst  3526 Jun 22 17:05 .bashrc.original
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .config
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .java
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .local
-rw-r--r-- 1 analyst analyst   807 Jun 22 17:05 .profile
-rw-r--r-- 1 analyst analyst   336 Jun 24 08:51 .zprofile
-rw-r--r-- 1 analyst analyst 10856 Jun 24 08:51 .zshrc
-rw-r--r-- 1 root    root       73 Jul 20 13:38 corp_net_ips.txt
-rw-r--r-- 1 root    root      261 Jul 20 13:39 corp_net_ips_hosts.txt
-rw-r--r-- 1 root    root       44 Jul 20 13:47 corp_net_ips_ports.txt
-rw-r--r-- 1 root    root       66 Jul 20 13:43 guest_net_ips.txt
-rw-r--r-- 1 root    root      286 Jul 20 13:43 guest_net_ips_hosts.txt
-rw-r--r-- 1 root    root        0 Jul 20 13:54 guest_net_ips_ports.txt
-rw-r--r-- 1 root    root       96 Jul 20 13:41 infra_net_ips.txt
-rw-r--r-- 1 root    root      402 Jul 20 13:41 infra_net_ips_hosts.txt
-rw-r--r-- 1 root    root      218 Jul 20 13:50 infra_net_ips_ports.txt
-rw-r--r-- 1 root    root      255 Jul 20 13:33 recon-redes.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# cat guest_net_ips_ports.txt
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# ls -la
total 100
drwx------ 1 analyst analyst  4096 Jul 20 13:49 .
drwxr-xr-x 1 root    root     4096 Jul 18 15:38 ..
-rw-r--r-- 1 root    root     2892 Jul 18 15:38 .ANOTACAO-ULTIMO-SCAN.TXT
-rw-r--r-- 1 analyst analyst   220 Jun 22 17:05 .bash_logout
-rw-r--r-- 1 analyst analyst  5551 Jul 13 04:02 .bashrc
-rw-r--r-- 1 analyst analyst  3526 Jun 22 17:05 .bashrc.original
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .config
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .java
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .local
-rw-r--r-- 1 analyst analyst   807 Jun 22 17:05 .profile
-rw-r--r-- 1 analyst analyst   336 Jun 24 08:51 .zprofile
-rw-r--r-- 1 analyst analyst 10856 Jun 24 08:51 .zshrc
-rw-r--r-- 1 root    root       73 Jul 20 13:38 corp_net_ips.txt
-rw-r--r-- 1 root    root      261 Jul 20 13:39 corp_net_ips_hosts.txt
-rw-r--r-- 1 root    root       44 Jul 20 13:47 corp_net_ips_ports.txt
-rw-r--r-- 1 root    root       66 Jul 20 13:43 guest_net_ips.txt
-rw-r--r-- 1 root    root      286 Jul 20 13:43 guest_net_ips_hosts.txt
-rw-r--r-- 1 root    root       96 Jul 20 13:41 infra_net_ips.txt
-rw-r--r-- 1 root    root      402 Jul 20 13:41 infra_net_ips_hosts.txt
-rw-r--r-- 1 root    root      218 Jul 20 13:50 infra_net_ips_ports.txt
-rw-r--r-- 1 root    root      255 Jul 20 13:33 recon-redes.txt

┌──(root㉿f609ce277032)-[/home/analyst]
└─# cat infra_net_ips_ports.txt
Open 10.10.30.10:21
Open 10.10.30.117:80
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 10.10.30.11:33060
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# ls -la
total 64
drwx------ 1 analyst analyst  4096 Jul 18 15:38 .
drwxr-xr-x 1 root    root     4096 Jul 18 15:38 ..
-rw-r--r-- 1 root    root     2892 Jul 18 15:38 .ANOTACAO-ULTIMO-SCAN.TXT
-rw-r--r-- 1 analyst analyst   220 Jun 22 17:05 .bash_logout
-rw-r--r-- 1 analyst analyst  5551 Jul 13 04:02 .bashrc
-rw-r--r-- 1 analyst analyst  3526 Jun 22 17:05 .bashrc.original
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .config
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .java
drwxr-xr-x 3 analyst analyst  4096 Jul 13 04:02 .local
-rw-r--r-- 1 analyst analyst   807 Jun 22 17:05 .profile
-rw-r--r-- 1 analyst analyst   336 Jun 24 08:51 .zprofile
-rw-r--r-- 1 analyst analyst 10856 Jun 24 08:51 .zshrc
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# cat .ANOTACAO-ULTIMO-SCAN.TXT
# NÃO APAGAR

# SE VOCÊ ACHOU ISSO E ESTÁ FAZENDO O DESAFIO DO PROJETO FINAL OPÇÃO 1 SE DEU BEM ;-) ...

# comandos que eu executei a ultima vez que estava aqui... deixar anotado pq pode salvar tempo da próxima vez.

## Primeiro pegar info das redes
ip a
ip a | grep inet
ip a | grep inet > recon-redes.txt

## Testar se tem conectividade com as redes
ping -c 3 10.10.10.1  # corp_net
ping -c 3 10.10.30.1  # guest_net
ping -c 3 10.10.50.1  # infra_net

## 1. descobrir os hosts com Nmap ping scan
nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2}' | tee corp_net_ips.txt
nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_ips_hosts.txt

nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2}' | tee infra_net_ips.txt
nmap -sn -T4 10.10.30.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee infra_net_ips_hosts.txt

nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2}' | tee guest_net_ips.txt
nmap -sn -T4 10.10.50.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee guest_net_ips_hosts.txt

## 2. Scan rápido com Rustscan para pegar as portas abertas
rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt
rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt
rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

## 3. Analisar os serviços especificos
### FTP
nmap -p 21 --script ftp-anon 10.10.30.10
nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
```

```
### MySQL
nmap -p 3306 --script mysql-info 10.10.30.11
nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt

### LDAP
nmap -p 389 --script ldap-rootdse 10.10.30.17
nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootdse.txt

### SMB
nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_net_servico_smb.txt

### HTTP (web)
curl -I http://10.10.30.117
curl -I http://10.10.30.117 > infra_net_servico_webserver.txt
curl http://10.10.30.117
curl http://10.10.30.117 > infra_net_servico_zabbix.txt

## Extras úteis
arp -a
arp -a > recon_ip_maps.txt
cat /etc/resolv.conf

## Organizar os resultados (manter tudo limpinho)
mkdir -p /home/analyst/recon/{corp_net,guest_net,infra_net}
mv *corp*.txt /home/analyst/recon/corp_net/
mv *guest*.txt /home/analyst/recon/guest_net/
mv *infra*.txt /home/analyst/recon/infra_net/
mv *recon*.txt /home/analyst/recon/

## Copiar depois pro host local - tem que sair do docker e rodar da maquina local
docker cp analyst:/home/analyst/recon ./recon-backup

## Inventário final (manual mesmo, preenche depois)
# IP:
# Hostname:
# SO estimado:
# Portas abertas:
# Serviços:
# Notas: login anônimo? dados sensíveis? falhas visíveis?
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host proto kernel_lo
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth1
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth2
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# cat recon-redes.txt
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host proto kernel_lo
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth1
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth2
```

```
┌──(root㉿f609ce277032)-[/home/analyst]
└─# ping -c 3 10.10.10.1  # corp_net
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.129 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.127 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.118 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.118/0.124/0.129/0.004 ms

┌──(root㉿f609ce277032)-[/home/analyst]
└─# ping -c 3 10.10.30.1  # guest_net
PING 10.10.30.1 (10.10.30.1) 56(84) bytes of data.
64 bytes from 10.10.30.1: icmp_seq=1 ttl=64 time=0.197 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.069 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2082ms
rtt min/avg/max/mdev = 0.069/0.115/0.197/0.057 ms

┌──(root㉿f609ce277032)-[/home/analyst]
└─# ping -c 3 10.10.50.1  # infra_net
PING 10.10.50.1 (10.10.50.1) 56(84) bytes of data.
64 bytes from 10.10.50.1: icmp_seq=1 ttl=64 time=0.281 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.120 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.142 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2080ms
rtt min/avg/max/mdev = 0.120/0.181/0.281/0.071 ms
```

```
jonataahh@HpVictus15:~/formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1$ docker exec -it analyst bash
┌──(root㉿f609ce277032)-[/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
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0@if57: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 52:bc:2a:b3:98:00 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth0
       valid_lft forever preferred_lft forever
3: eth1@if60: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 0e:ea:7a:d8:39:e1 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth1
       valid_lft forever preferred_lft forever
4: eth2@if61: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether b2:0d:08:6a:50:63 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth2
       valid_lft forever preferred_lft forever
```