Documentação de Redes Descobertas

Autor: Dalila Salvatierra
Data: 25/07/2026
Versão: Desafio final Modulo 1
Formação CyberSec

Redes identificadas:

Nome	Subnet descobertas	Finalidade Suposta
Rede 1 (corp_net)	10.10.10.0/24	Rede principal de estações corporativas
Rede 2 (guest_net)	10.10.50.0/24	Rede de visitantes/dispositivos pessoais
Rede 3 (infra_net)	10.10.30.0/24	Rede de infraestrutura / servidores

Dispositivos por rede:

Rede 1 (corp_net) – Rede principal

IP	Função	Evidência
10.10.10.1	Roteador/Gateway virtual	Host ativo, porta aberta 111/TCP
10.10.10.2	Host/container	Porta 58884 aberta
10.10.10.10	Estação de trabalho (WS-001)	Responde a ping, sem portas abertas,
10.10.10.101	Estação de trabalho (WS-002)	Responde a ping, sem portas abertas,
10.10.10.127	Estação de trabalho (WS-003)	Responde a ping, sem portas abertas,
10.10.10.222	Estação de trabalho (WS-004)	Responde a ping, sem portas abertas

Rede 2 (Guest_net) - Rede de Visitantes

IP	Função	Evidência
10.10.50.1	Roteador/Gateway virtual	Host ativo, porta aberta 111/TCP
10.10.50.2	Dispositivo pessoal (laptop-vastro)	Host ativo, sem evidências de portas abertas, DNS resolvido
10.10.50.3	Dispositivo pessoal (laptop-luiz)	Host ativo; sem evidência de portas abertas; DNS resolvido
10.10.50.4	Dispositivo pessoal (macbook-aline)	Host ativo; sem evidência de portas abertas; DNS resolvido
10.10.50.5	Dispositivo pessoal (notebook-carlos)	Host ativo; sem evidência de portas abertas; DNS resolvido
10.10.50.6	host	Porta 40148 TCP aberta (possível dispositivo extra)

Rede 3 (infra_net) — Rede de Infraestrutura

IP	Função	Evidência
10.10.30.1	Roteador/Gateway virtual	Host ativo, porta aberta 111/TCP
10.10.30.10	Servidor FTP	Porta 21 aberta, serviço FTP ativo
10.10.30.11	Banco de dados (MySQL)	Portas 3306 e 33060 abertas, usuários com senha vazia
10.10.30.15	Servidor Samba (Arquivos)	Portas 139 e 445 abertas , SMB ativo, possíveis compartilhamentos
10.10.30.17	Diretório LDAP	Porta 389 aberta, versão do OpenLDAP desatualizada.
10.10.30.117	Monitoramento Zabbix (zabbix-server)	Portas 80 e 10051 abertas, ativo, PHP obsoleto
10.10.30.227	Servidor legado(legacy-server)	Host ativo, 65.535 portas TCP estão fechadas

Observações de risco:

- Vários serviços estão visíveis e não deveriam estar expostos, como o FTP e MySQL, podem ser acessados sem uma senha forte.

- O mysql-server (10.10.30.11) responde na porta 3306, o que indica que o banco de dados está acessível pela rede.

- O samba-server (10.10.30.15) está com portas abertas que podem ser exploradas por vírus e ataques antigos.

- O zabbix-server (10.10.30.117) está com portas abertas, o que pode representar riscos se não estiverem atualizadas.

- O ftp-server (10.10.30.10) responde na porta 21, que não é criptografado e pode expor senhas em texto claro, sendo recomendado desativar.

- Nenhum dos Hosts parece ter **Firewall** visível ou ativo.

Relatório Técnico
Lab Segmentação de Rede

Autor: Dalila Salvatierra
Data: 25/07/2026
Versão: Desafio final Modulo 1
Formação CyberSec

Sumario executivo:

Foi realizada uma análise em um ambiente de laboratório com várias redes segmentadas usando Docker. Foram encontradas máquinas com serviços desatualizados e inseguros. Algumas estão expostas demais e sem a proteção, como firewall. Há máquinas com funções antigas que podem ser um ponto fraco na segurança.

Objetivo:

Analisar as redes criadas no laboratório para entender quais serviços estão rodando, se há riscos e se a separação das redes está funcionando bem.

Escopo:

Esse ambiente é um laboratório criado com Docker. Ele simula uma empresa com três redes separadas: **corp_net**, **guest_net** e **infra_net**. Cada rede tem seus próprios dispositivos e servidores.

Metodologia:

Ferramentas usadas:

Nmap, RustScan, netdiscover, Ping, Curl, Arp

O que foi feito:

- Foram feitas varreduras para descobrir quais IPs e serviços estavam ativos, identificando várias vulneridades e filtrando por sub-redes.
- Teste de conectividade entre redes.
- Análise detalhado das portas e de serviços específicos como FTP, MySQL, LDAP, SMB e HTTP.
- Comparação de resultados com o que seria esperado em uma rede segura.
-
- Tudo foi anotado, analisado e organizado.

Diagnóstico(Achados):

IP	Serviço	Porta	Risco Identificado	Evidência
10.10.30.10	FTP	21	Serviço inseguro, sem criptografia	nmap mostrou porta 21 aberta
10.10.30.11	MySQL	3306	Banco de dados pode estar acessível sem autenticação forte	nmap detectou MySQL na porta 3306
10.10.30.15	Samba/SMB	445	Pode ser explorado	portas 139 e 445 abertas
10.10.30.17	OpenLDAP	389	Serviço de autenticação exposto	serviço LDAP detectado
10.10.30.117	Zabbix	10051	Painel de monitoramento acessível	nmap detectou Zabbix agent ativo
10.10.30.227	Vários (legacy)	Várias	Softwares antigos e vulneráveis	Muitos serviços expostos

Recomendações:

- Desligar serviços não utilizados, como FTP.
- Instalar firewall em todas as máquinas para bloquear acessos indevidos.
- Monitorar o samba-server e, se possível, restringir o acesso a pastas compartilhadas.
- Configurar autenticação forte no MySQL e LDAP.

Plano de ação (80/20):

Ação	Impacto	Facilidade	Prioridade
Desativar serviços inseguros (FTP)	Alto	Alta	Alta
Isolar legacy-server	Alto	Média	Alta
Configurar firewall em todos os hosts	Médio	Alta	Alta
Restringir portas SMB	Médio	Média	Média
Atualizar sistema do samba-server	Alto	Média	Alta

Conclusão:

Durante a análise, percebe-se que várias máquinas estão com serviços antigos ou sem proteção. Isso pode abrir portas para ataques, mesmo sendo um ambiente de teste.

É importante revisar os serviços expostos, configurar e desativar o que não está sendo usado e proteger o que está ativo. Assim, a rede fica mais segura e difícil de invadir.

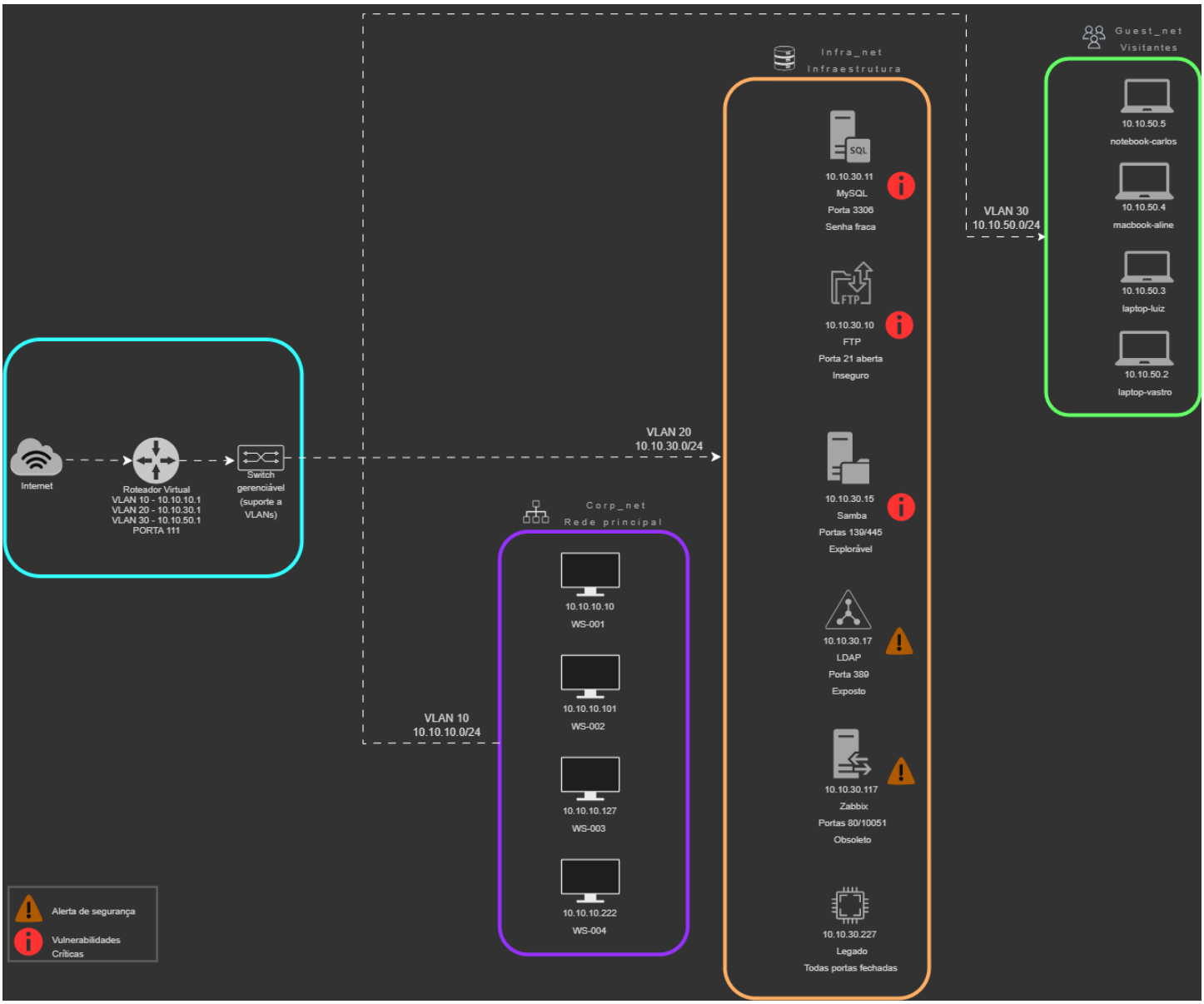
Outro ponto importante é que nenhum dos dispositivos parece utilizar Firewall, deixando todos os serviços totalmente acessíveis e visíveis na rede , o que os torna **extremamente vulneráveis** a ataques e acessos não autorizados.

Essa análise ajudou a compreender melhor como pequenas falhas podem abrir portas para invasores. Além disso, foi muito útil para treinar a identificação de problemas, falhas e vulnerabilidades em geral, bem como entender quais ferramentas usar em cada situação, sempre buscando soluções simples.

Com pequenas mudanças no ambiente de rede, é possível reduzir significativamente os riscos, fortalecer a segurança e proteger melhor as informações.

Diagrama de rede:

Desenvolvido no aplicativo draw.io



Anexos:

Conforme as instruções, seguem os prints de ferramentas e saída dos scans.

Identificação e localização de dispositivos dentro da rede:

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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@if19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether da:ad:74:1b:1a:59 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
3: eth1@if23: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether e6:e0:ad:33:af:b2 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
4: eth2@if24: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default
    link/ether be:24:1b:b0:26:8e 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

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host proto kernel_lo
    inet 10.10.10.2/24 brd 10.10.10.255 scope global eth0
    inet 10.10.50.6/24 brd 10.10.50.255 scope global eth1
    inet 10.10.30.2/24 brd 10.10.30.255 scope global eth2

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# ip a | grep inet > recon-redes.txt
```

Teste de conexão entre dispositivos na rede:

```
┌──(root㉿623f19706c0c)-[/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=0.689 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.095 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.124 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2096ms
rtt min/avg/max/mdev = 0.095/0.302/0.689/0.273 ms

┌──(root㉿623f19706c0c)-[/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=0.866 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.140 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.120 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2088ms
rtt min/avg/max/mdev = 0.120/0.375/0.866/0.347 ms

┌──(root㉿623f19706c0c)-[/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=1.23 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.086 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2086ms
rtt min/avg/max/mdev = 0.086/0.482/1.230/0.529 ms
```

Hosts que estão ativos na rede:

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | grep "Up"
Host: 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 (623f19706c0c) Status: Up

┌──(root㉿623f19706c0c)-[/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㉿623f19706c0c)-[/home/analyst]
└─# nmap -sn -T4 10.10.10.0/24 -oG - | awk '/Up$/{print $2, $3}' | tee corp_net_
ips_hosts.txt
10.10.10.1 ()
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 (623f19706c0c)
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -sn -T4 10.10.30.0/24 -oG - | grep "Up"
Host: 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:U
p
Host: 10.10.30.15 (samba-server.projeto_final_opcao_1_infra_net)        Status:U
p
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:U
p
Host: 10.10.30.227 (legacy-server.projeto_final_opcao_1_infra_net)      Status:U
p
Host: 10.10.30.2 (623f19706c0c) Status: Up

┌──(root㉿623f19706c0c)-[/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㉿623f19706c0c)-[/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 ()
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 (623f19706c0c)
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -sn -T4 10.10.50.0/24 -oG - | grep "Up"
Host: 10.10.50.1 ()     Status: Up
Host: 10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net)        Status:U
p
Host: 10.10.50.3 (laptop-luiz.projeto_final_opcao_1_guest_net)  Status: Up
Host: 10.10.50.4 (notebook-carlos.projeto_final_opcao_1_guest_net)      Status:U
p
Host: 10.10.50.5 (macbook-aline.projeto_final_opcao_1_guest_net)        Status:U
p
Host: 10.10.50.6 (623f19706c0c) Status: Up

┌──(root㉿623f19706c0c)-[/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㉿623f19706c0c)-[/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 ()
10.10.50.2 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.3 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.4 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.5 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.6 (623f19706c0c)
```

Analise de serviços específicos como FTP, MySQL, LDAP, SMB, HTTP (web):

```
Host is up (0.000054s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: DA:8C:05:43:59:BC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:23 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000067s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 12
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSigpipes, LongPassword, Support41Auth, LongColumnFl
ag, Speaks41ProtocolOld, ODBCClient, SupportsTransactions, SupportsLoadDataLocal
, SwitchToSSLAfterHandshake, ConnectWithDatabase, DontAllowDatabaseTableColumn,
Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, SupportsCompression, Interact
iveClient, FoundRows, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMu
ltipleResults
|   Status: Autocommit
|   Salt: ..3_'\x07H\x1BAv!?YCQ\x1E2\x0B\x12>
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 1A:4B:A0:EB:ED:C4 (Unknown)

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

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.
txt
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:23 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.000079s 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: GSS-SPNEGO
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: OTP
|       supportedSASLMechanisms: CRAM-MD5
|       supportedSASLMechanisms: NTLM
|_      subschemaSubentry: cn=Subschema
MAC Address: E6:B6:48:D3:AE:FD (Unknown)

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

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootd
se.txt
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:23 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.00011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: AA:E8:95:A2:DB:FA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_ne
t_servico_smb.txt
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# curl -I http://10.10.30.117
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 23 Jul 2025 19:24:19 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=d0bc3d09dd00474d0d719217972d8e15; 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


┌──(root㉿623f19706c0c)-[/home/analyst]
└─# curl -I http://10.10.30.117 > infra_net_servico_webserver.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# curl http://10.10.30.117
<!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="ass
ets/img/apple-touch-icon-76x76-precomposed.png">
                <link rel="apple-touch-icon-precomposed" sizes="120x120" href="a
ssets/img/apple-touch-icon-120x120-precomposed.png">
                <link rel="apple-touch-icon-precomposed" sizes="152x152" href="a
ssets/img/apple-touch-icon-152x152-precomposed.png">
                <link rel="apple-touch-icon-precomposed" sizes="180x180" href="a
ssets/img/apple-touch-icon-180x180-precomposed.png">
                <link rel="icon" sizes="192x192" href="assets/img/touch-icon-192
x192.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-b
g:before, .flh-na-bg, .status-na-bg { background-color: #97AAB3 }
.info-bg, .info-bg input[type="radio"]:checked + label, .info-bg:before, .flh-in
fo-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-hi
gh-bg, .status-high-bg { background-color: #E97659 }
.disaster-bg, .disaster-bg input[type="radio"]:checked + label, .disaster-bg:bef
ore, .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-cha
rset="utf-8" aria-label="Sign in"><ul><li><label for="name">Username</label><inp
ut type="text" id="name" name="name" value="" maxlength="255" autofocus="autofoc
us"></li><li><label for="password">Password</label><input type="password" id="pa
ssword" name="password" value="" maxlength="255"></li><li><input type="checkbox"
 id="autologin" name="autologin" value="1" class="checkbox-radio" checked="check
ed"><label for="autologin"><span></span>Remember me for 30 days</label></li><li>
<button type="submit" id="enter" name="enter" value="Sign in">Sign in</button></
li></ul></form></div><div class="signin-links"><a target="_blank" class="grey li
nk-alt" href="https://www.zabbix.com/documentation/4.4/">Help</a>  •&n
bsp; <a target="_blank" class="grey link-alt" href="https://www.zabbix.com/
support">Support</a></div></main><footer role="contentinfo">&copy; 2001&ndash;20
20, <a class="grey link-alt" target="_blank" href="https://www.zabbix.com/">Zabb
ix SIA</a></footer></body>

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# curl http://10.10.30.117 > infra_net_servico_zabbix.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3412    0  3412    0     0  97773      0 --:--:-- --:--:-- --:--:--   98k
```

Verificação de portas estão abertas:

```
PORT      STATE SERVICE REASON
111/tcp   open  rpcbind syn-ack ttl 64
53735/tcp open  unknown syn-ack ttl 64
MAC Address: 36:59:0D:A6:8D:1A (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)

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

[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:21 UTC
Initiating ARP Ping Scan at 19:21
Scanning 10.10.30.15 [1 port]
Completed ARP Ping Scan at 19:21, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:21
Completed Parallel DNS resolution of 1 host. at 19:21, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:21
Scanning samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) [2 ports]
Discovered open port 139/tcp on 10.10.30.15
Discovered open port 445/tcp on 10.10.30.15
Completed SYN Stealth Scan at 19:21, 0.02s elapsed (2 total ports)
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up, received arp-response (0.000079s latency).
Scanned at 2025-07-23 19:21:32 UTC for 0s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
MAC Address: AA:E8:95:A2:DB:FA (Unknown)
```

```
PORT      STATE SERVICE        REASON
80/tcp    open  http           syn-ack ttl 64
10051/tcp open  zabbix-trapper syn-ack ttl 64
10052/tcp open  unknown        syn-ack ttl 64
MAC Address: CA:BB:D6:5B:48:EB (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
           Raw packets sent: 4 (160B) | Rcvd: 4 (160B)

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

[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:21 UTC
Initiating ARP Ping Scan at 19:21
Scanning 10.10.30.10 [1 port]
Completed ARP Ping Scan at 19:21, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:21
Completed Parallel DNS resolution of 1 host. at 19:21, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR:
Initiating SYN Stealth Scan at 19:21
Scanning ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10) [1 port]
Discovered open port 21/tcp on 10.10.30.10
Completed SYN Stealth Scan at 19:21, 0.02s elapsed (1 total ports)
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up, received arp-response (0.000070s latency).
Scanned at 2025-07-23 19:21:32 UTC for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
MAC Address: DA:8C:05:43:59:BC (Unknown)
```

```
PORT      STATE SERVICE REASON
111/tcp   open  rpcbind syn-ack ttl 64
53735/tcp open  unknown syn-ack ttl 64
MAC Address: 4E:7E:74:65:CE:E4 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)


┌──(root㉿623f19706c0c)-[/home/analyst]
└─# rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# rustscan -a 'infra_net_ips.txt'
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
```

```
PORT      STATE SERVICE REASON
111/tcp   open  rpcbind syn-ack ttl 64
53735/tcp open  unknown syn-ack ttl 64
MAC Address: 22:B7:3A:C8:66:FD (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)


┌──(root㉿623f19706c0c)-[/home/analyst]
└─# rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 21 --script ftp-anon 10.10.30.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:22 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.000054s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: DA:8C:05:43:59:BC (Unknown)
```

```
PORT    STATE SERVICE REASON
389/tcp open  ldap    syn-ack ttl 64
636/tcp open  ldapssl syn-ack ttl 64
MAC Address: E6:B6:48:D3:AE:FD (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)


┌──(root㉿623f19706c0c)-[/home/analyst]
└─# rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

┌──(root㉿623f19706c0c)-[/home/analyst]
└─# rustscan -a 'guest_net_ips.txt'
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com
```

```
PORT      STATE SERVICE REASON
3306/tcp  open  mysql   syn-ack ttl 64
33060/tcp open  mysqlx  syn-ack ttl 64
MAC Address: 1A:4B:A0:EB:ED:C4 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)

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

[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:21 UTC
Initiating SYN Stealth Scan at 19:21
Scanning 623f19706c0c (10.10.30.2) [1 port]
Completed SYN Stealth Scan at 19:21, 0.03s elapsed (1 total ports)
Nmap scan report for 623f19706c0c (10.10.30.2)
Host is up, received localhost-response (0.000054s latency).
Scanned at 2025-07-23 19:21:32 UTC for 0s
```

```
┌──(root㉿623f19706c0c)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:23 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000067s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 12
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSigpipes, LongPassword, Support41Auth, LongColumnFlag, Speaks41ProtocolOld, (
SupportsTransactions, SupportsLoadDataLocal, SwitchToSSLAfterHandshake, ConnectWithDatabase,
DontAllowDatabaseTableColumn, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, SupportsCompression,
InteractiveClient, FoundRows, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ..3_'\x07H\x1BAv!?YCQ\x1E2\x0B\x12>
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 1A:4B:A0:EB:ED:C4 (Unknown)

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