Relatório Técnico

Análise de Segmentação de Rede

Autor: Rairan Barbosa
Cargo: Analista de Sistemas
Data: 25/07/2025

Sumário Executivo

O ambiente analisado representa uma rede corporativa separada em três sub-redes: corp_net (usuários), infra_net (servidores) e guest_net (dispositivos convidados). Durante a auditoria, foram identificados serviços expostos desnecessariamente, (como Servidores e bancos de dados com portas de acesso abertas) e a falta de políticas de controle de acesso entre as sub-redes.

Recomenda-se segmentar corretamente dispositivos críticos, como servidores, além de desabilitar serviços não utilizados (como FTP). A correção dessas falhas reduzirá significativamente os riscos de movimentação lateral e ataques de escalonamento de privilégios.

Objetivo

Analisar a rede simulada para identificar exposições, falhas de segmentação e riscos operacionais de segurança.

Escopo

Ambiente em Docker Simulado

A simulação foi realizada em um ambiente controlado utilizando **containers Docker**, que representam servidores, estações de trabalho, dispositivos de rede e serviços expostos. Esse tipo de ambiente é ideal para testes, pois permite a replicação de cenários reais com segurança, isolamento e reprodutibilidade.

- Cada container simula um host em uma sub-rede distinta.
- O roteamento entre redes é controlado manualmente, permitindo análise da segmentação.

Três Redes Segmentadas

Foram identificadas e analisadas três sub-redes distintas no ambiente:

- `corp_net` **(ex: 10.10.10.0/24)**:
  Rede corporativa principal, utilizada por estações de trabalho e dispositivos de uso cotidiano.
- `infra_net` **(ex: 192.168.30.0/24)**:
  Rede voltada para servidores e dispositivos críticos de infraestrutura (ex: web server, banco de dados).
- `guest_net` **(ex: 172.16.50.0/24)**:
  Rede isolada para visitantes ou dispositivos não confiáveis.

Metodologia

Ferramentas Utilizadas

- **`nmap`**:
  Usado para descobrir hosts ativos, portas abertas, sistemas operacionais e serviços. Com scripts NSE (Nmap Scripting Engine), também foi possível identificar versões e possíveis vulnerabilidades conhecidas.

- **`rustscan`**:
  Ferramenta moderna e muito rápida para escaneamento de portas. Foi usada para acelerar a descoberta de portas abertas, que depois foram analisadas em profundidade com o `nmap`.

- **`arp-scan`** / **`arp -a`**:
  Utilizadas para identificar dispositivos conectados à rede local através da tabela ARP (Address Resolution Protocol), revelando IPs e MACs mesmo sem serviços escutando em portas padrão.

- **`curl`**:
  Executado para testar manualmente respostas HTTP de servidores web, confirmando status, banners, headers e comportamentos suspeitos (ex: redirecionamentos, respostas não autenticadas, etc.).

Procedimentos Adotados

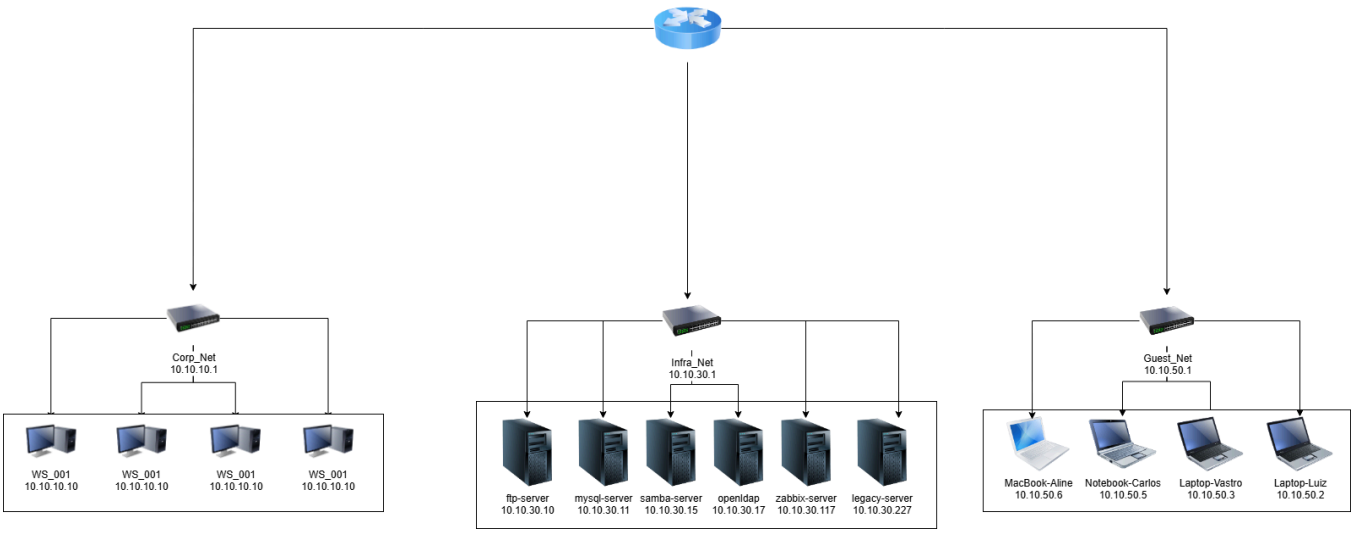
1. **Coleta Ativa**
   Scans foram realizados com `nmap`, `rustscan` e `arp-scan` para mapear o ambiente com base em resposta de serviços.

2. **Reconhecimento de IPs e Serviços**
   A partir dos IPs descobertos, foi possível identificar os serviços ativos, como HTTP, SSH, SNMP, FTP e serviços web específicos de dispositivos.

3. **Documentação Manual**
   Cada resultado foi analisado manualmente, e os dados relevantes (função do host, tipo de serviço, evidência da vulnerabilidade) foram documentados em tabelas.

4. **Análise de Evidências e Diagrama**
   As informações coletadas foram consolidadas em um **diagrama de rede lógico**, representando topologia, IPs e dispositivos, o que facilita a visualização de falhas de segmentação ou rotas cruzadas não autorizadas.

Diagrama de Rede



Inventário de Hosts e Serviços

corp_net

IP	Hostname	Portas Abertas	Observações
10.10.10.1	(Gateway)	111, 60779	Host desconhecido
10.10.10.10	WS_001	-	Estação de trabalho
10.10.10.101	WS_002	-	Estação de trabalho
10.10.10.127	WS_003	-	Estação de trabalho
10.10.10.222	WS_004	-	Estação de trabalho
10.10.10.2	(Host local)	58746	Interface da auditoria

infra_net

IP	Hostname	Portas Abertas	Serviços
10.10.30.1	(Gateway)	111, 60779	Host desconhecido
10.10.30.10	ftp-server	21	FTP anônimo ativado
10.10.30.11	mysql-server	3306, 33060	MySQL 8.0.42
10.10.30.15	samba-server	139, 445	SMB, compartilhamentos
10.10.30.17	openldap	389, 636	LDAP, sem autenticação
10.10.30.117	zabbix-server	80, 10051, 10052	Painel web Zabbix exposto
10.10.30.227	legacy-server	-	Serviço desconhecido
10.10.30.2	(Host local)	-	Interface da auditoria

guest_net

IP	Hostname	Portas Abertas	Observações
10.10.50.1	(Gateway)	111, 60779	Host desconhecido
10.10.50.2	notebook-carlos	-	Dispositivo de visitante
10.10.50.3	macbook-aline	-	Dispositivo de visitante
10.10.50.4	laptop-luiz	-	Dispositivo de visitante
10.10.50.5	laptop-vastro	-	Dispositivo de visitante
10.10.50.6	(Host local)	-	Interface da auditoria

Diagnóstico de Segurança

Pontos de Risco Identificados

- FTP anônimo (10.10.30.10): pode permitir upload/download de arquivos sensíveis sem autenticação.
- MySQL exposto (10.10.30.11): versão detectada, possibilidade de ataque por brute-force.
- LDAP aberto (10.10.30.17): informações sensíveis do diretório visíveis sem autenticação.
- SMB com shares visíveis (10.10.30.15): risco de vazamento de arquivos internos.
- Zabbix Web (10.10.30.117): painel administrativo exposto publicamente.

Recomendações

1. **Desativar FTP e migrar para SFTP.**

O FTP transmite dados e senhas em texto plano e estava acessível anonimamente, o que representa alto risco de vazamento de arquivos. A migração para SFTP garante criptografia e autenticação segura.

2. **Restringir acesso à porta do MySQL por firewall ou ACLs.**

A exposição da porta 3306 permite ataques externos, especialmente brute-force. Limitar acesso apenas a hosts autorizados e usar autenticação forte reduz drasticamente esse vetor de ataque.

3. **Proteger o LDAP com autenticação e limitar escopo de consulta.**

LDAP aberto permite enumeração de usuários e vazamento de dados sensíveis. Autenticação e TLS garantem sigilo na comunicação, e escopo limitado evita coleta em massa.

4. **Aplicar regras de compartilhamento restrito no SMB.**

Compartilhamentos amplos expõem dados e podem ser usados para movimentação lateral. A aplicação de permissões rigorosas mitiga riscos de exfiltração e acesso não autorizado.

5. **Isolar o painel Zabbix atrás de VPN e autenticação robusta.**

A interface web acessível externamente facilita ataques de força bruta ou exploração de falhas conhecidas. Proteger com VPN e autenticação reduz significativamente a superfície de ataque.

6. **Aplicar firewall entre sub-redes.**

Impede que visitantes ou usuários de menor privilégio acessem serviços críticos. Segmentação lógica com regras ACL ou firewalls fortalece o modelo de confiança mínima.

7. **Monitorar tráfego com IDS/IPS**

Sistemas de detecção identificam varreduras, comportamento suspeito e ataques em tempo real, permitindo resposta rápida e coleta de evidências.

Plano de Ação (80/20)

Ação	Impacto	Facilidade	Prioridade
Troca (FTP) para (SFTP)	Alto	Alta	Alta
Restringir porta 3306 (MySQL)	Alto	Alta	Alta
Aplicar autenticação no LDAP	Alto	Média	Alta
Restringir compartilhamento SMB	Médio	Média	Média
Proteger Zabbix	Alto	Alta	Alta
Aplicar firewall entre sub-redes	Alto	Baixa	Média
Implementar IDS/IPS	Alto	Baixa	Média

Conclusão

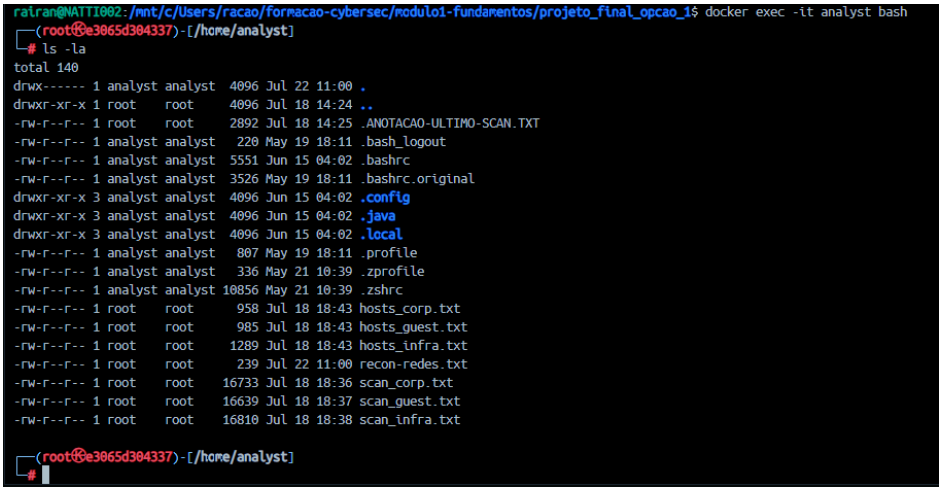
A análise revelou diversas exposições e más práticas de segmentação. A priorização imediata deve incluir a remoção de serviços inseguros (FTP), proteção de serviços expostos (MySQL, LDAP, SMB, Zabbix) e isolamento de dispositivos menos confiáveis. A aplicação de VLANs, firewalls e monitoramento contínuo irá reduzir significativamente os riscos. A próxima etapa deve incluir testes de penetração controlados e validação pós-correção.

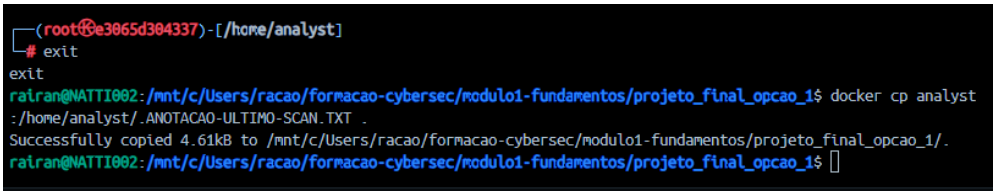
Anexos

- Saídas nmap, rustscan, arp-scan

Link para acesso as saidas com o relatório:
https://github.com/rairansb/Relatori-de-Seguimenta-o-de-rede

- Prints do terminal





```
┌──(root㉿e3065d304337)-[/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
       valid_lft forever preferred_lft forever
2: eth0@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether ca:bf:df:8f:fb:2e 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 de:b2:75:15:c5:6e 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 5e:89:18:9e:f0:f8 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㉿e3065d304337)-[/home/analyst]
└─#
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    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㉿e3065d304337)-[/home/analyst]
└─# 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
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=0.671 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.048 ms

--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2287ms
rtt min/avg/max/mdev = 0.046/0.255/0.671/0.294 ms
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=0.506 ms
64 bytes from 10.10.30.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 10.10.30.1: icmp_seq=3 ttl=64 time=0.041 ms

--- 10.10.30.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2309ms
rtt min/avg/max/mdev = 0.041/0.196/0.506/0.218 ms
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=0.319 ms
64 bytes from 10.10.50.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 10.10.50.1: icmp_seq=3 ttl=64 time=0.051 ms

--- 10.10.50.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2309ms
rtt min/avg/max/mdev = 0.043/0.137/0.319/0.128 ms

┌──(root㉿e3065d304337)-[/home/analyst]
└─#
```

```
┌──(root㉿e3065d304337)-[/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 (e3065d304337) Status: Up

┌──(root㉿e3065d304337)-[/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㉿e3065d304337)-[/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 (e3065d304337)

┌──(root㉿e3065d304337)-[/home/analyst]
└─#
```

```
┌──(root㉿e3065d304337)-[/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: 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 (e3065d304337) Status: Up

┌──(root㉿e3065d304337)-[/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㉿e3065d304337)-[/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 (e3065d304337)
```

```
┌──(root㉿e3065d304337)-[/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 (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-luiz.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 (e3065d304337) Status: Up

┌──(root㉿e3065d304337)-[/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㉿e3065d304337)-[/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 (notebook-carlos.projeto_final_opcao_1_guest_net)
10.10.50.3 (macbook-aline.projeto_final_opcao_1_guest_net)
10.10.50.4 (laptop-luiz.projeto_final_opcao_1_guest_net)
10.10.50.5 (laptop-vastro.projeto_final_opcao_1_guest_net)
10.10.50.6 (e3065d304337)

┌──(root㉿e3065d304337)-[/home/analyst]
└─#
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# rustscan -a 'corp_net_ips.txt' | grep Open > corp_net_ips_ports.txt

┌──(root㉿e3065d304337)-[/home/analyst]
└─# rustscan -a 'infra_net_ips.txt' | grep Open > infra_net_ips_ports.txt

┌──(root㉿e3065d304337)-[/home/analyst]
└─# rustscan -a 'guest_net_ips.txt' | grep Open > guest_net_ips_ports.txt
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 21 --script ftp-anon 10.10.30.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 18:14 UTC
Nmap scan report for ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10)
Host is up (0.00012s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 2E:7E:B9:6C:F6:C2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 21 --script ftp-anon 10.10.30.10 > infra_net_servico_ftp-anon.txt
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 18:15 UTC
Nmap scan report for mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11)
Host is up (0.000063s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.42
|   Thread ID: 10
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolNew, Support41Auth, IgnoreSigpipes, DontAllowDatabaseTableColumn, LongColumnFlag, ConnectWithDatabase, SupportsLoadDataLocal, FoundRows, ODBCClient, Speaks41Protocol
old, SupportsTransactions, InteractiveClient, LongPassword, IgnoreSpaceBeforeParenthesis, SwitchToSSLAfterHandshake, SupportsCompression, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleSt
atments
|   Status: Autocommit
|   Salt: dC0}\x13c?1\x10A0x<   ZY'}b`
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 92:79:19:F8:81:43 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 3306 --script mysql-info 10.10.30.11 > infra_net_servico_mysql-info.txt
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 18:15 UTC
Nmap scan report for openldap.projeto_final_opcao_1_infra_net (10.10.30.17)
Host is up (0.00011s 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: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedSASLMechanisms: OTP
|       supportedSASLMechanisms: CRAM-MD5
|       supportedSASLMechanisms: NTLM
|_      subschemaSubentry: cn=Subschema
MAC Address: EA:6C:68:83:6C:77 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 389 --script ldap-rootdse 10.10.30.17 > infra_net_servico_ldap-rootdse.txt
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 18:16 UTC
Nmap scan report for samba-server.projeto_final_opcao_1_infra_net (10.10.30.15)
Host is up (0.00010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 6A:EF:11:E5:18:68 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

┌──(root㉿e3065d304337)-[/home/analyst]
└─# nmap -p 445 --script smb-os-discovery,smb-enum-shares 10.10.30.15 > infra_net_servico_smb.txt
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# curl -I http://10.10.30.117
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 25 Jul 2025 18:17:59 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=74c3030dc261012de94c160ff813a13e; 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㉿e3065d304337)-[/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㉿e3065d304337)-[/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="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 for="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-radio" checked="checked"><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 link-alt" href
="https://www.zabbix.com/documentation/4.4/">Help</a>  •  <a target="_blank" class="grey link-alt" href="https://www.zabbix.com/support">Support</a></div></main><footer role="contentI
nfo">&copy; 2001&ndash;2020, <a class="grey link-alt" target="_blank" href="https://www.zabbix.com/">Zabbix SIA</a></footer></body>

┌──(root㉿e3065d304337)-[/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   110k      0 --:--:-- --:--:-- --:--:--  111k
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# arp -a
legacy-server.projeto_final_opcao_1_infra_net (10.10.30.227) at 8e:2b:36:b1:ad:d8 [ether] on eth2
ftp-server.projeto_final_opcao_1_infra_net (10.10.30.10) at 2e:7e:b9:6c:f6:c2 [ether] on eth2
mysql-server.projeto_final_opcao_1_infra_net (10.10.30.11) at 92:79:19:f0:81:43 [ether] on eth2
samba-server.projeto_final_opcao_1_infra_net (10.10.30.15) at 6a:ef:11:e5:18:68 [ether] on eth2
? (10.10.30.1) at c2:f5:0d:69:e6:e0 [ether] on eth2
? (10.10.10.1) at ae:22:36:a8:5d:8d [ether] on eth0
laptop-luiz.projeto_final_opcao_1_guest_net (10.10.50.4) at fe:00:d0:ab:44:7f [ether] on eth1
laptop-vastro.projeto_final_opcao_1_guest_net (10.10.50.5) at 36:77:6c:9d:7b:d9 [ether] on eth1
notebook-carlos.projeto_final_opcao_1_guest_net (10.10.50.2) at e6:45:ac:5f:a2:10 [ether] on eth1
macbook-aline.projeto_final_opcao_1_guest_net (10.10.50.3) at ee:df:4b:c4:1c:3d [ether] on eth1
? (10.10.50.1) at d6:7c:5e:ec:f7:ec [ether] on eth1
WS_001.projeto_final_opcao_1_corp_net (10.10.10.10) at 76:b4:a6:1c:85:dc [ether] on eth0
zabbix-server.projeto_final_opcao_1_infra_net (10.10.30.117) at 72:e6:84:dd:1d:33 [ether] on eth2
WS_004.projeto_final_opcao_1_corp_net (10.10.10.222) at 9a:98:72:22:44:11 [ether] on eth0
WS_003.projeto_final_opcao_1_corp_net (10.10.10.127) at c6:36:be:34:40:38 [ether] on eth0
WS_002.projeto_final_opcao_1_corp_net (10.10.10.101) at 2e:95:77:af:d3:4a [ether] on eth0
openldap.projeto_final_opcao_1_infra_net (10.10.30.17) at ea:6c:68:83:6c:77 [ether] on eth2
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# arp -a > recon_ip_maps.txt

┌──(root㉿e3065d304337)-[/home/analyst]
└─# cat /etc/resolv.conf
# Generated by Docker Engine.
# This file can be edited; Docker Engine will not make further changes once it
# has been modified.

nameserver 127.0.0.11
options ndots:0

# Based on host file: '/etc/resolv.conf' (internal resolver)
# ExtServers: [host(192.168.65.7)]
# Overrides: []
# Option ndots from: internal
```

```
┌──(root㉿e3065d304337)-[/home/analyst]
└─# mkdir -p /home/analyst/recon/{corp_net,guest_net,infra_net}

┌──(root㉿e3065d304337)-[/home/analyst]
└─# mv *corp*.txt /home/analyst/recon/corp_net/

┌──(root㉿e3065d304337)-[/home/analyst]
└─# mv *guest*.txt /home/analyst/recon/guest_net/

┌──(root㉿e3065d304337)-[/home/analyst]
└─# mv *infra*.txt /home/analyst/recon/infra_net/

┌──(root㉿e3065d304337)-[/home/analyst]
└─# mv *recon*.txt /home/analyst/recon/
```

```
ratran@NATTI002:/mnt/c/Users/racao/formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1$ docker cp analyst:/home/analyst/recon ./recon-backup
Successfully copied 83.5kB to /mnt/c/Users/racao/formacao-cybersec/modulo1-fundamentos/projeto_final_opcao_1/recon-backup
```

- Diagrama da rede: