



SMTP

Simple Mail Transfer Protocol



SMTP

Simple Mail Transfer Protocol

Karen Ruver Mentges

karen_ruvermentges@hotmail.com

Autor

Luiz Paulo Grafetti Terres

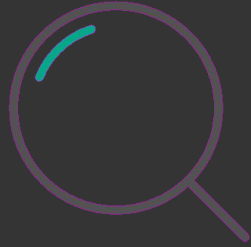
luiz.paulus51@gmail.com

Autor

Winicius Eduardo Girardi

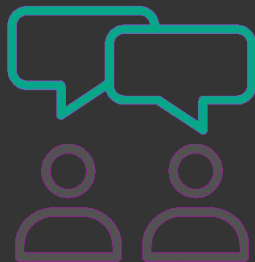
wgirardi541@gmail.com

Autor



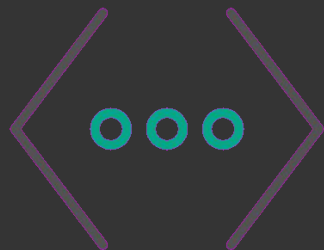
Análise do protocolo

Simple Mail Transfer Protocol



O que é o SMTP?

Análise do protocolo



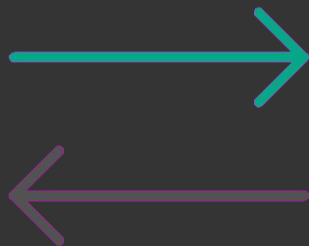
Como surgiu?

Análise do protocolo



Como funciona?

Análise do protocolo



Qual porta o SMTP usa?

Análise do protocolo

Qual porta o SMTP usa?

- ⤵ Porta 25
- ⤵ Porta 465
- ⤵ Porta 587
- ⤵ Porta 2525



Aspectos de segurança

Simple Mail Transfer Protocol

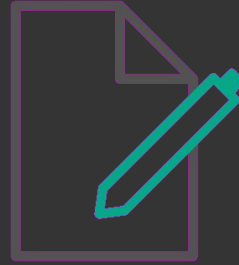
- ⑤ Transport Layer Security - TLS
- ⑤ Secure Sockets Layer - SSL
- ⑤ Filtragem de Spam e Malware
- ⑤ SMTPS - SMTP + TLS

➤ SMTP AUTH

➤ Sender Policy Framework (SPF) - Valida o domínio

➤ DomainKeys Identified Mail (DKIM) - Integridade

➤ Domain-based Message Authentication (DMARC) - SPF + DKIM



Ataques

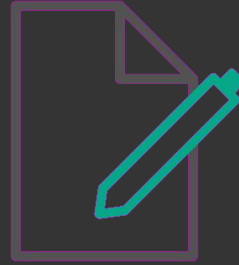
Simple Mail Transfer Protocol

➤ Man in the Middle

➤ Phishing

➤ Spam

➤ Spoofing



Curiosidades e aspectos relevantes

Simple Mail Transfer Protocol

SMTP é um protocolo que possui várias extensões:

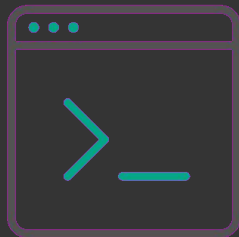
➤ SMTP AUTH

➤ STARTTLS

➤ SMTPS

④ SMTP vs. IMAP(Internet Message Access Protocol)/POP3(Post Office Protocol)

④ RFC 821 - 1982



Demonstração do serviço

Simple Mail Transfer Protocol

Instalação do Docker: <https://docs.docker.com/engine/install/>

Supported platforms

Platform	x86_64 / amd64	arm64 / aarch64	arm (32-bit)	ppc64le	s390x
CentOS	✓	✓		✓	
Debian	✓	✓	✓	✓	
Fedora	✓	✓		✓	
Raspberry Pi OS (32-bit)			✓		
RHEL (s390x)					✓
SLES					✓
Ubuntu	✓	✓	✓	✓	✓
Binaries	✓	✓	✓		

Criando um container Ubuntu:

<https://docs.docker.com/get-started/overview/#example-docker-run-command>

```
$ docker run -i -t ubuntu /bin/bash
```

Atualizando lista de pacotes no container

```
# apt update
```

A instalação do postfix: *

```
# apt install postfix
```

* Postfix em várias distribuições linux: <https://www.postfix.org/packages.html>

Durante a instalação do postfix, escolha a configuração inicial **5 (Local Only)**.

```
root@cd334cbe8cf3: /
debconf: falling back to frontend: Readline
debconf: unable to initialize frontend: Readline
debconf: (Can't locate Term/ReadLine.pm in @INC (you may need to install the Term::ReadLine module)
(@INC contains: /etc/perl /usr/local/lib/x86_64-linux-gnu/perl/5.34.0 /usr/local/share/perl/5.34.0 /
usr/lib/x86_64-linux-gnu/perl5/5.34 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl-base /usr/lib/x8
6_64-linux-gnu/perl/5.34 /usr/share/perl/5.34 /usr/local/lib/site_perl) at /usr/share/perl5/Debconf/
FrontEnd/Readline.pm line 7.)
debconf: falling back to frontend: Teletype
Postfix Configuration
-----

Please select the mail server configuration type that best meets your needs.

No configuration:
  Should be chosen to leave the current configuration unchanged.
Internet site:
  Mail is sent and received directly using SMTP.
Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
  delivery.
Local only:
  The only delivered mail is the mail for local users. There is no
  network.

1. No configuration    3. Internet with smarthost    5. Local only
2. Internet Site       4. Satellite system

General mail configuration type: 5
Progress: [ 53%] [#####.....]
```

Escolha do **system mail name** pode ser arbitrária (para nosso caso):

```
root@cd334cbe8cf3: /

No configuration:
  Should be chosen to leave the current configuration unchanged.
Internet site:
  Mail is sent and received directly using SMTP.
Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
  delivery.
Local only:
  The only delivered mail is the mail for local users. There is no
  network.

  1. No configuration   3. Internet with smarthost   5. Local only
  2. Internet Site     4. Satellite system

General mail configuration type: 5

The 'mail name' is the domain name used to 'qualify' _ALL_ mail addresses without a domain name.
This includes mail to and from <root>: please do not make your machine send out mail from
root@example.org unless root@example.org has told you to.

This name will also be used by other programs. It should be the single, fully qualified domain name
(FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option
would be example.org.

System mail name: atomicbomb.project
Progress: [ 53%] [#####.....]
```

Por estarmos em um Docker, alguns ajustes devem ser feitos em */etc/hosts*:

Remover a linha:

```
::1    localhost ip6-localhost ip6-loopback
```

Adicionar o **system mail name** como equivalente ao localhost:

```
127.0.0.1    atomicbomb.project
```

Configurações do postfix em */etc/postfix/main.cf*:

```
myhostname = atomicbomb.project  
inet_interfaces = $myhostname, localhost  
mynetworks_style = host  
home_mailbox = Maildir/
```

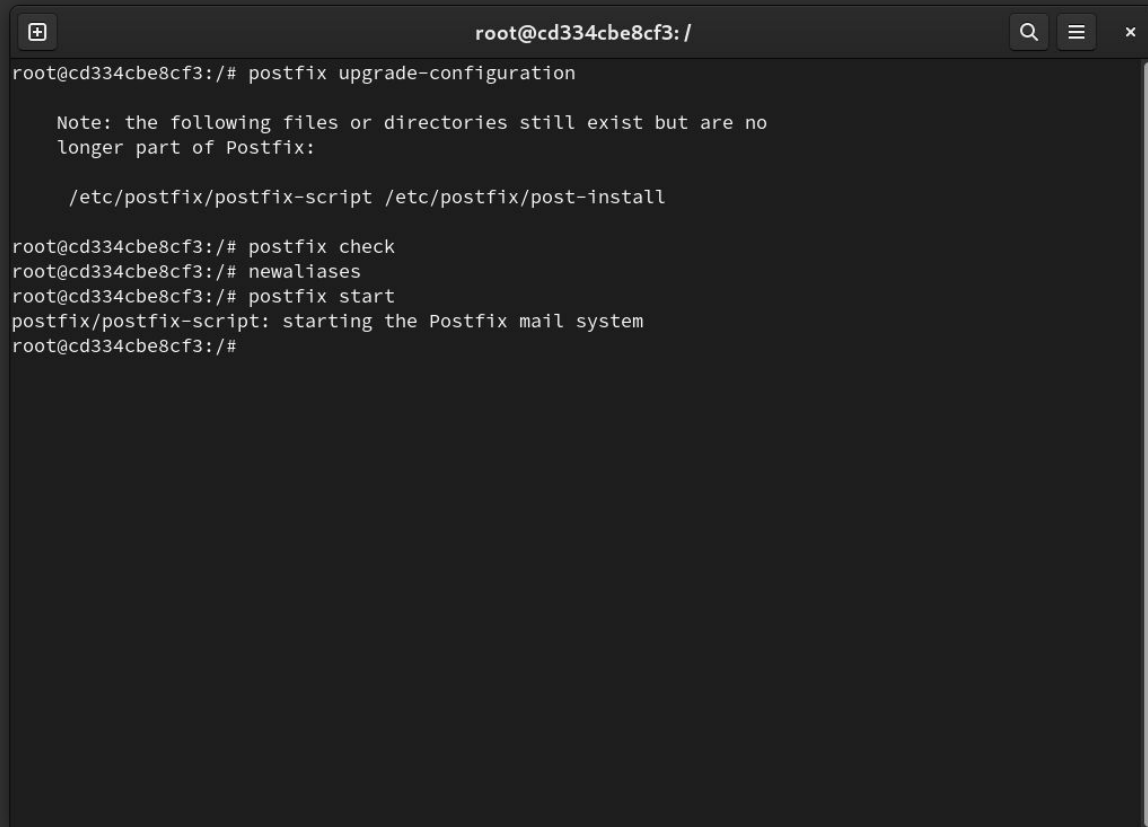
Para verificar a validade das alterações:

```
# postfix upgrade-configuration  
# postfix check
```

E aplicar newaliases, e iniciar serviço do postfix:

```
# newaliases  
# postfix start
```

Você deve esperar um resultado similar:



```
root@cd334cbe8cf3: /  
root@cd334cbe8cf3:/# postfix upgrade-configuration  
  
    Note: the following files or directories still exist but are no  
    longer part of Postfix:  
  
    /etc/postfix/postfix-script /etc/postfix/post-install  
  
root@cd334cbe8cf3:/# postfix check  
root@cd334cbe8cf3:/# newaliases  
root@cd334cbe8cf3:/# postfix start  
postfix/postfix-script: starting the Postfix mail system  
root@cd334cbe8cf3:/#
```


Podemos agora instalar o **mail-client**, será usado o **s-nail**:

Primeiro, precisamos colocar em uma variável de ambiente o nosso diretório de Inbox (escolhido em */etc/postfix/main.cf*):

```
# echo 'export MAIL=~/.Maildir' | tee -a /etc/bash.bashrc | tee -a /etc/profile.d/mail.sh
```

Aplicamos a variável de ambiente na nossa sessão atual:

```
# source /etc/profile.d/mail.sh
```

Podemos fazer a instalação do pacote:

```
# apt install s-nail
```

Configurações do s-nail:

```
# echo set emptystart >> /etc/s-nail.rc  
# echo set folder=Maildir >> /etc/s-nail.rc  
# echo set record=+sent >> /etc/s-nail.rc
```

Criar novo usuário, para que seja possível comunicar para ele por email:

```
# adduser boom
```

A primeira mensagem do **s-nail** para um usuário precisa conter a opção **"Snorecord"**, então enviando uma primeira mensagem:

```
# echo 'atomic' | s-nail -s 'bomb' -Snorecord root  
# echo 'atomic' | s-nail -s 'bomb' -Snorecord boom
```

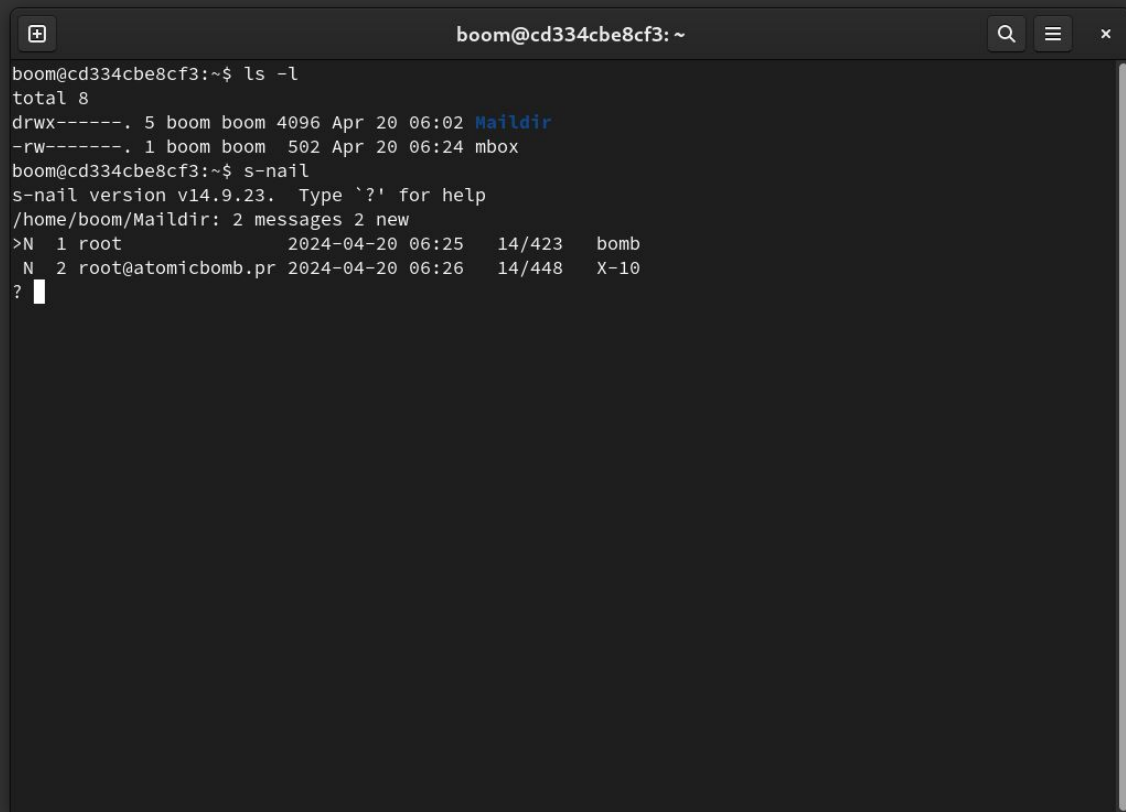
Enviando novas mensagens ao recém criado usuário:



```
root@cd334cbe8cf3: /  
root@cd334cbe8cf3:/# s-nail -s "X-10" -r root@atomicbomb.project boom@atomicbomb.project  
To: boom@atomicbomb.project  
Subject: X-10  
  
We need more Pu-94 !  
^D  
-----  
(Preliminary) Envelope contains:  
From: root@atomicbomb.project  
To: boom@atomicbomb.project  
Subject: X-10  
Send this message [yes/no, empty: recompose]? yes
```

Podemos (como usuário boom), acessar aos e-mails usando:

s-nail

A terminal window titled 'boom@cd334cbe8cf3: ~' with search, menu, and close icons in the title bar. The terminal shows the following commands and output:

```
boom@cd334cbe8cf3:~$ ls -l
total 8
drwx-----, 5 boom boom 4096 Apr 20 06:02 Maildir
-rw-----, 1 boom boom 502 Apr 20 06:24 mbox
boom@cd334cbe8cf3:~$ s-nail
s-nail version v14.9.23. Type '?' for help
/home/boom/Maildir: 2 messages 2 new
>N 1 root 2024-04-20 06:25 14/423 bomb
N 2 root@atomicbomb.pr 2024-04-20 06:26 14/448 X-10
? █
```

Ao pressionar “Enter”, é possível visualizar os emails do Inbox em ordem:

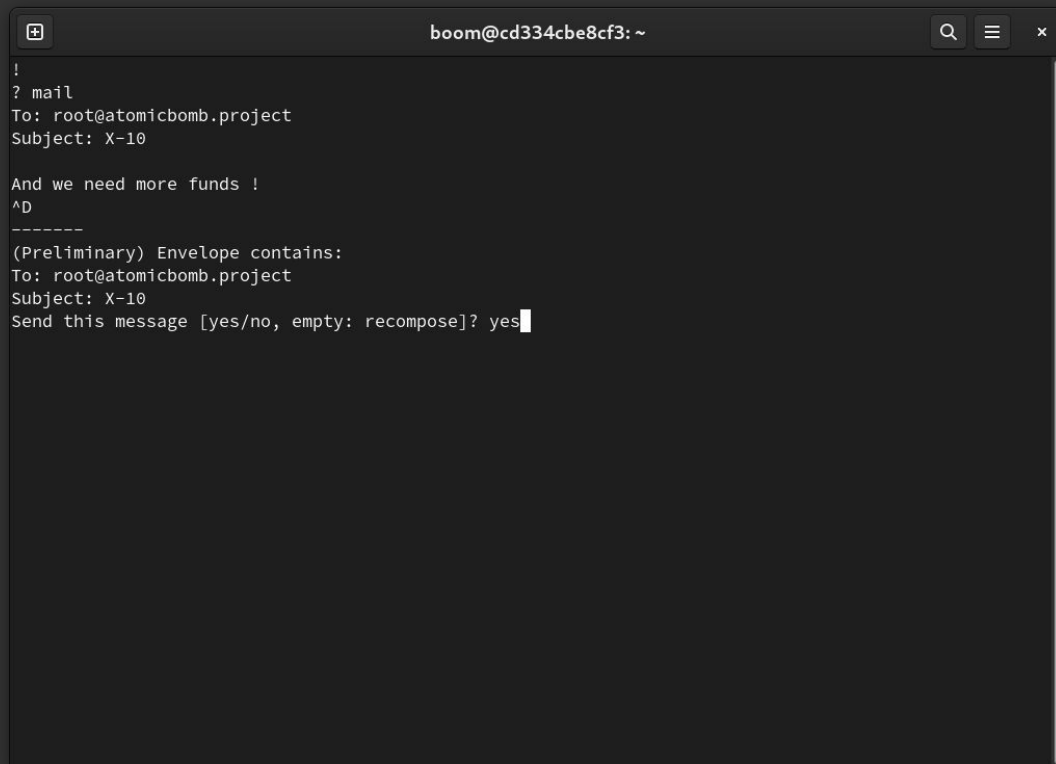
```
boom@cd334cbe8cf3: ~  
boom@cd334cbe8cf3:~$ ls -l  
total 8  
drwx-----, 5 boom boom 4096 Apr 20 06:02 Maildir  
-rw-----, 1 boom boom 502 Apr 20 06:24 mbox  
boom@cd334cbe8cf3:~$ s-nail  
s-nail version v14.9.23. Type `?' for help  
/home/boom/Maildir: 2 messages 2 new  
>N 1 root 2024-04-20 06:25 14/423 bomb  
N 2 root@atomicbomb.pr 2024-04-20 06:26 14/448 X-10  
?  
[-- Message 1 -- 14 lines, 423 bytes --]:  
Date: Sat, 20 Apr 2024 06:25:19 +0000  
To: boom@atomicbomb.project  
Subject: bomb  
Message-Id: <20240420062519.DE2A53A3D63@atomicbomb.project>  
From: root <root@atomicbomb.project>  
  
atomic  
  
?  
[-- Message 2 -- 14 lines, 448 bytes --]:  
Date: Sat, 20 Apr 2024 06:26:27 +0000  
From: root@atomicbomb.project  
To: boom@atomicbomb.project  
Subject: X-10  
Message-ID: <20240420062627.-mgUY%root@atomicbomb.project>  
  
We need more Pu-94 !  
  
? █
```

Para listar comandos úteis do **s-nail**: “?” + Enter

Para enviar e-mail usando o cliente: “**mail**” + Enter

Visualizar mensagens enviadas pelo usuário: “**file +sent**” + Enter

Listar mensagens recebidas: “**h**” + Enter

A terminal window with a dark background and light gray text. The window title bar shows 'boom@cd334cbe8cf3: ~' and standard window controls. The terminal output shows the s-nail mail client interface. It starts with a prompt '!', followed by the user entering '? mail'. The output shows the email headers: 'To: root@atomicbomb.project' and 'Subject: X-10'. The body of the email is displayed, starting with 'And we need more funds !' and a signature block. The prompt 'Send this message [yes/no, empty: recompose]? yes' is shown at the bottom with a cursor.

```
boom@cd334cbe8cf3: ~
!  
? mail  
To: root@atomicbomb.project  
Subject: X-10  
  
And we need more funds !  
^D  
-----  
(Preliminary) Envelope contains:  
To: root@atomicbomb.project  
Subject: X-10  
Send this message [yes/no, empty: recompose]? yes
```

REFERÊNCIAS do Tutorial:

Mais exemplos de Configurações e Links Úteis:

http://cafim.sssup.it/~giulio/other/Postfix_Setup_for_Local_Mail_Only.html

<https://ubuntu.com/server/docs/install-and-configure-postfix>

<https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-22-04>

Documentação das ferramentas utilizadas:

<https://www.postfix.org/documentation.html>

<https://manpages.debian.org/stretch/s-nail/s-nail.1.en.html>