

Práctica BRS

Xestor de correo: Cifrado e Sinatura Dixital

ESCENARIO

Máquina virtual ou física:

RAM \leq 2048MB CPU \leq 2 PAE/NX habilitado

ISO/CD/DVD/USB: Live amd64 - Calquera distribución baseada en Debian

REDE: DHCP (NAT)

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **gpg**
- **OpenPGP**
- **Philip Zimmermann**
- **Firma digital y cifrado de mensajes**
- **De interese: TALLER SR – PRÁCTICA 71 – Cliente de correo electrónico: Mozilla Thunderbird + cabeceiras**
- **De interese: TALLER SR – PRÁCTICA 72 – Mozilla Thunderbird + combinación de correo (Mail Merge)**

Práctica

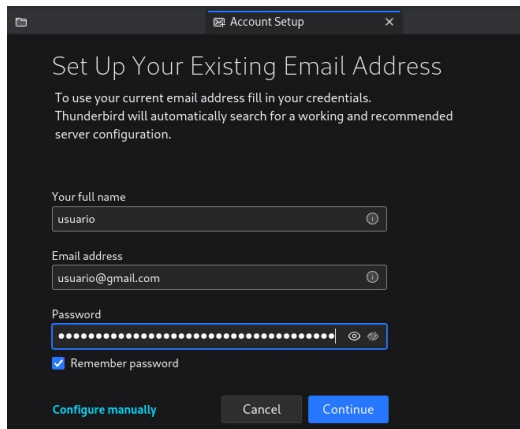
1. Instalar xestor de correo Thunderbird:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando
sudo (/etc/sudoers, visudo)
root@kali:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list,
/etc/apt/sources.list.d/)
root@kali:~# apt search thunderbird #Buscar calquera paquete que coincida co patrón de búsqueda
thunderbird
root@kali:~# apt -y install thunderbird thunderbird-l10n-gl #Instalar o paquete thunderbird(xestor
de correo) e o paquete thunderbird-l10n-gl(idioma galego para o xestor de correo thunderbird). Co parámetro -y
automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
root@kali:~# exit #Saír da consola do usuario root, para voltar á consola do usuario kali sen permisos de root
kali@kali:~$
```

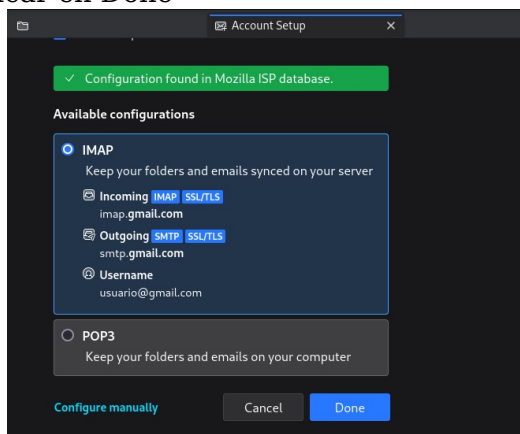
2. Configurar Thunderbird

kali@kali:~\$ thunderbird & #Executar thunderbird en segundo plano, devolveéndose o prompt da consola

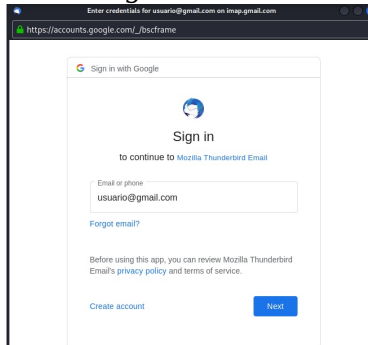
- A. Cubrir os campos do formulario solicitado para configurar a conta de correo, e picar en Continue:



- B. Picar en Done



C. Acceder a gmail

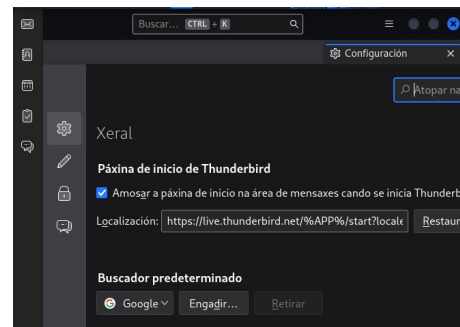
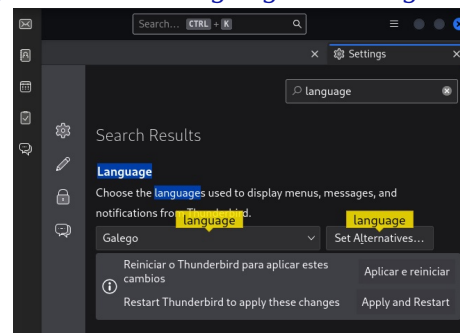
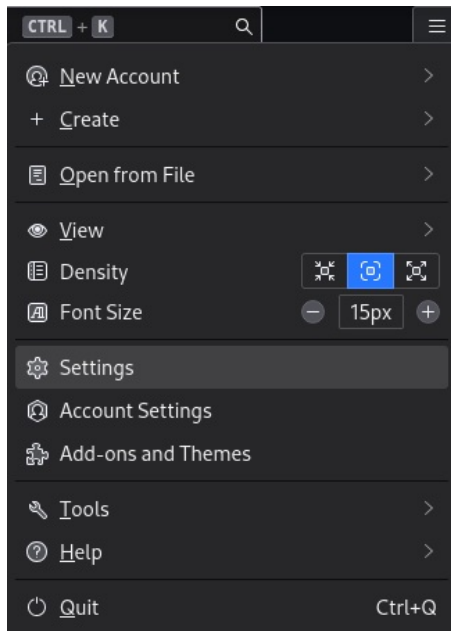


D. Permitir acceso a thunderbird

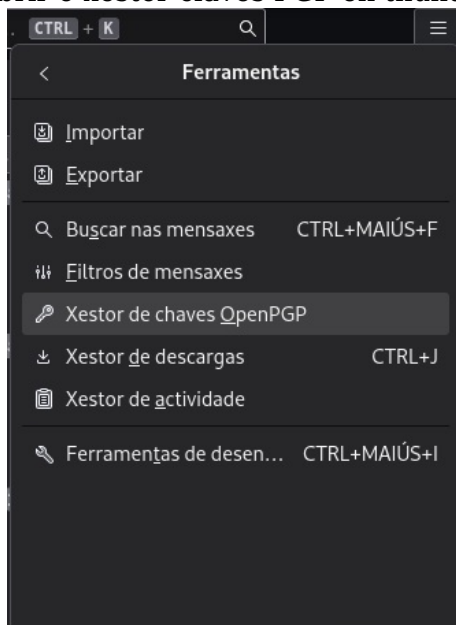


Mozilla Thunderbird Email quiere acceder a tu cuenta de Google

E. Cambiar o idioma da interface a Galego: Settings → Buscar language → Galego → Cambiado



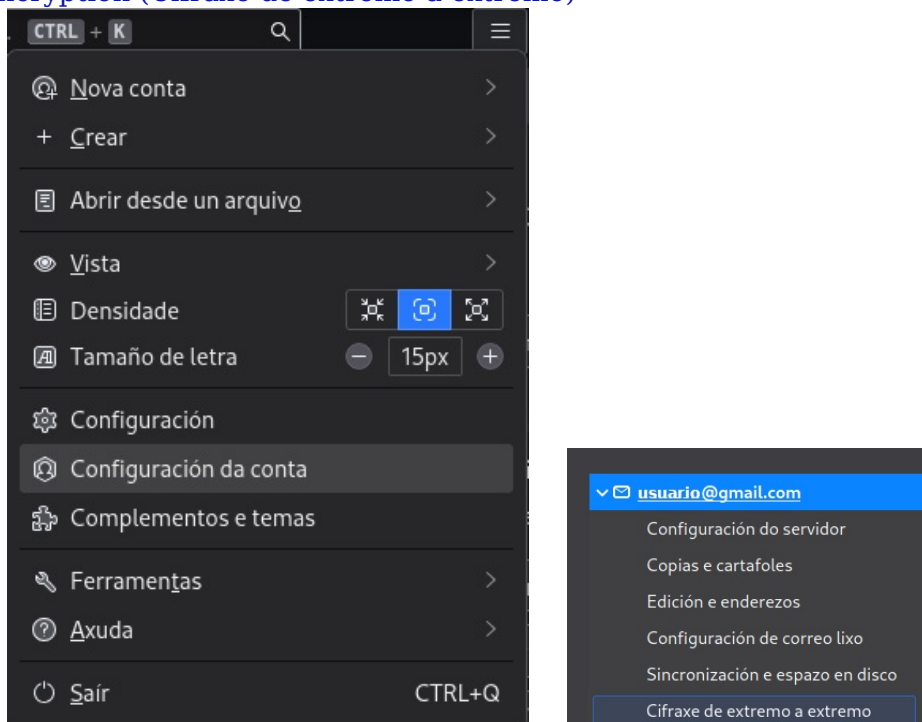
F. Abrir o xestor claves PGP en thunderbird: Ferramentas → Xestor de chaves OpenPGP



- G. Crear un novo par de claves: [Xerar](#) → [Nova par de claves](#) → [Xerar unha chave OpenPGP](#) → [Xerar a chave](#) → [Confirmar](#)

The image shows two screenshots of the 'Xestor de claves OpenPGP' application. The top screenshot shows the application window with the 'Xerar' menu item highlighted. The bottom screenshot shows the 'Xerar unha chave OpenPGP' dialog box. The dialog box has a title bar 'Xerar unha chave OpenPGP'. It contains a 'Identidade' field with the value 'usuario < usuario@gmail.com > - usuario@gmail.com'. Below this is a section for 'Caducidade da chave' (Key expiration) with a description: 'Defina o tempo de caducidade da chave acabada de xerar. Máis tarde pode modificar a data para a se o precisa.' There are two radio buttons: 'A chave caduca en' (selected) and 'A chave non caduca'. The 'A chave caduca en' option has a numeric input field set to '3' and a unit dropdown set to 'anos'. Below this is a section for 'Configuración avanzada' (Advanced configuration) with a description: 'Controlar a configuración avanzada da súa chave OpenPGP.' It has two dropdown menus: 'Tipo de chave:' set to 'RSA' and 'Tamaño da chave:' set to '3072'. At the bottom, there is a warning message: 'A xeración de claves pode tardar varios minutos en completarse. Non saia da aplicación mentres a xeración de claves estea en curso. Navegar activamente ou realizar operacións intensivas en disco durante a xeración de claves reabastecerá o «cantidade de aleatoriedade» e acelerará o proceso. Recibirá un aviso cando remate a xeración de claves.' Below the warning is a question: 'Quere xerar unha chave pública e secreta para usuario "usuario@gmail.com"?'. At the bottom are two buttons: 'Cancelar' and 'Confirmar'.

- H. Configurar a conta para permitir cifrar(clave pública destinatario), descifrar(clave privada propia) e asinar correos(clave privada propia): [Configuración da conta](#) → [End-To-End Encryption \(Cifraxa de extremo a extremo\)](#) →



Caixa de entrada

Configuración da conta X

usuario@gmail.com

Configuración do servidor

Copias e cartafolios

Edición e enderezos

Configuración de correo lixo

Sincronización e espazo en disco

End-To-End Encryption

Avisos de recepción

Local Folders

Configuración de correo lixo

Espazo no disco

Servidor de correo de saída (SMTP)

Accións da conta

End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. [Learn more](#)

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with usuario@gmail.com

Add Key...

✓ Your current configuration uses key ID 0x74A069132AEC15E7 [Learn more](#)

None

Do not use OpenPGP for this identity.

0x74A069132AEC15E7

Expires on: 10/23/2024

Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

Caixa de entrada

Configuración da conta X

usuario@gmail.com

Configuración do servidor

Copias e cartafolios

Edición e enderezos

Configuración de correo lixo

Sincronización e espazo en disco

End-To-End Encryption

Avisos de recepción

Local Folders

Personal certificate for encryption:

Seleccionar...

Borrar (M)

Manage S/MIME Certificates

S/MIME Security Devices

Default settings for sending messages

Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

Do not enable encryption by default

Require encryption by default

If you require encryption, to send a message you must have the public key or certificate of every recipient.

Caixa de entrada

Configuración da conta X

usuario@gmail.com

Configuración do servidor

Copias e cartafolios

Edición e enderezos

Configuración de correo lixo

Sincronización e espazo en disco

End-To-End Encryption

Avisos de recepción

Local Folders

Configuración de correo lixo

Espazo no disco

Servidor de correo de saída (SMTP)

Personal certificate for encryption:

Manage S/MIME Certificates

S/MIME Security Devices

Default settings for sending messages

Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

Do not enable encryption by default

Require encryption by default

If you require encryption, to send a message you must have the public key or certificate of every recipient.

A digital signature allows recipients to verify the message has not been changed.

Add my digital signature by default

3. **Enviar correo cifrado/asinado:** Escribir → Seguranza → Escoller a/s opción/s que interesen

