linux seguridad

setup

- PAM
  - su: crear un grupo tipo **permitsu** y añadir a los usuarios que pueden usar **su**
  - passwd: crear reglas fuertes de contraseña
- sudo:
  - restringido per grups usuaris
  - noexec
- sudoreplay
- sshd
  - crear un grupo tipo «permitssh» y añadir a los usuarios que se pueden conectar por **ssh**
  - restricción **AllowGroups**, **AllowUsers**
  - denedar acceso ssh a **root**
- NTP
- firewall
- fail2ban
- logs centralizados

system

- checklist server hacked
- routersploit
- secure boot
- conexiones TCP/UDP:

```
sudo ss -plunt
```

pass

- hastopolis
- fcrackzip

linux

- https://noticiasseguridad.com/tutoriales/herramienta-para-romper-contrasenas-linux-todo-en-menos-de-un-minuto/
  -
```
git clone https://github.com/huntergregal/mimipenguin
```

passwords

- https://www.redeszone.net/tutoriales/seguridad/tiempo-hackear-contrasena/

ca-certificates

Para actualizar los certificados de una debian 9 (strech) fuera de su ciclo de vida, he:

1. descargado el paquete de certificados → https://packages.debian.org/sid/all/ca-certificates/download
2. descomprimido el paquete con `ar` ← `sudo apt install binutils`
3. descomprimido el archivo **data.tar.xz**
4. hacer copia seguridad del directorio **/usr/share/ca-certificates/mozilla** original
5. mover el directorio **mozilla** del tar extraído a **/usr/share/ca-certificates/**
6. `sudo update-ca-certificates -f`

```
dpkg -c <paquete> # mira contenido de ficheros
ar vx <paquete> # extrae el contenido del paquete
tar xvf <fichero.tar.xz>
```

/más: https://www.cyberciti.biz/faq/update-ca-certificates-command-examples-in-linux-to-ssl-ca-certificates/

otros ficheros

- Main configuration file: **/etc/ca-certificates.conf**
- A single-file version of CA certificates holds all CA certificates you activated in /etc/ca-certificates.conf file: **/etc/ssl/certs/ca-certificates.crt**
- Linux directory of CA certificates: **/usr/share/ca-certificates**
- Directory of local CA certificates (with .crt extension): **/usr/local/share/ca-certificates**