Tomb – the crypto undertaker

Ovvero: il becchino che seppellisce i vostri segreti

Appunti di Gabriele Tettamanzi

Tomb – the crypto undertaker

Cosa è Tomb?

- Semplice strumento CLI per creare un contenitore criptato (LUKS) in cui riporre file ed una chiave per chiuderlo
- Il contenitore si monta come un dispositivo a blocchi (analogo ad un hd)
- La chiave crittografica può essere nascosta in una foto (formato jpeg) oppure memorizzata come QR code

Tomb – the crypto undertaker

A chi è utile Tomb?

Tre condizioni:

- hai qualche segreto in forma di file
- hai desiderio (o hai necessità) di rendere difficile l'accesso ad occhi indiscreti al tuo segreto
- utilizzi Linux

Tomb – the crypto undertaker

Linux? Ma c'è nella mia distribuzione?

Tomb è uno script che usa strumenti Linux comuni e presenti in molte distribuzioni.

Ho provato Tomb con Archlinux e **openSUSE**.

Ho verificato la presenza dei pacchetti necessari e opzionali in Debian, Ubuntu, Fedora.

...Controllate le vostre distro preferite...

Tomb – the crypto undertaker

Pacchetti indispensabili:

- **zsh**
- **gnupg**
- **cryptsetup**
- **pinentry-curses** (o -gtk o -qt)

Ho inoltre installato i pacchetti opzionali:

- **dcfldd**, mostra l'avanzamento delle operazioni
- **steghide**, per nascondere la chiave in una immagine
- **qrencode**, per generare un QR code contente la chiave

Tomb – the crypto undertaker

Installazione di Tomb

1.Scaricate l'ultima versione da
https://files.dyne.org/tomb/
(click su Tomb-<versione>.tar.gz e download del file omonimo)
2.Decomprimete il file scaricato con:
tar xvfz Tomb-<versione>.tar.gz
3.Viene creata una cartella Tomb-<versione>, posizionatevi in essa ed eseguite:
sudo make install
4.per assicurarvi che Tomb funzioni provate:
tomb -h

Tomb – the crypto undertaker

Creazione di un contenitore e della sua chiave

Comandi da terminale:

1.creo un contenitore da 50M (“-f” se avete una partizione di swap attiva):
tomb dig -f -s 50 segretoGT

2.creo la chiave (seguire le istruzioni):
tomb forge -f segretoGT.tomb.key

3.chiudo il contenitore con la chiave:
tomb lock segretoGT.tomb -k segretoGT.tomb.key

Tomb – the crypto undertaker

Aprire e chiudere il contenitore

Comandi da terminale:

1.apro il contenitore e lo monto (“-f” se avete una partizione di swap attiva)

tomb open -f segretoGT.tomb -k segretoGT.tomb.key

[opero sui dati nel contenitore, ad esempio da file manager]

2.chiudo il contenitore:

tomb close segretoGT

Tomb – the crypto undertaker

Nascondere/riprendere la chiave in/da una immagine
(necessario steghide)

Comandi da terminale:

1.nascondo la chiave nell'immagine:

tomb bury -k segretoGT.tomb.key paesaggio.jpg

[attenzione: non cancella la chiave]

2.recupero la chiave dall'immagine:

tomb exhume -k segretoGT.tomb.key paesaggio.jpg

Tomb – the crypto undertaker

Conservare la chiave come QRCode (necessario qrencode)

1.preparo un immagine png del qrcode, comando da terminale:
tomb engrave -k segretoGT.tomb.key
[attenzione: non cancella la chiave]

2.stampo il file immagine segretoGT.tomb.key.qr.png e lo conservo

3.per aprire il contenitore leggo il file immagine con un qr scanner, il file di testo che si ottiene è la chiave.

Tomb – the crypto undertaker

Risorse

Sito: https://www.dyne.org/software/tomb/

Wiki: https://github.com/dyne/Tomb/wiki

Download: https://files.dyne.org/tomb/

Consiglio: hai paura della CLI? Frequenta i corsi Linux.

GRAZIE!!