Práctica Seguridade Informática
Funcións Resumo (Funcións Hash)

ESCENARIO

Máquina virtual ou física:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Sistema operativo instalado: Microsoft Windows 64bits
Rede: DHCP (NAT)
ISO/CD/DVD/USB: Live amd64 - Calquera distribución baseada en Debian
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:

- **usuario**: O usuario que accede ao sistema operativo Microsoft Windows posúe de nome: usuario
- **md5sum, sha1sum, sha256sum, sha512sum**: Para sistemas GNU/Linux, como Debian, podedes empregar comandos como md5sum e sha256sum para verificar os "hash" dos arquivos.
- **certutil**: Para sistemas Microsoft Windows, coma Windows 10, podedes empregar o comando certutil para verificar os "hash" dos arquivos.

Práctica

Arrancar coa distro Live amd64 baseada en Debian

1. Abrir un terminal e executar:
   $ echo 1234 > f1.txt #Crear o ficheiro f1.txt co contido 1234
   $ md5sum f1.txt #Crear hash MD5 do ficheiro f1.txt
   $ sha256sum f1.txt #Crear hash SHA256 do ficheiro f1.txt

Arrancar co sistema operativo instalado Microsoft Windows 64 bits

2. Abrir unha consola de comandos **cmd** e executar:
   C:\Users\usuario> echo 1234 > f2.txt #Crear o ficheiro f2.txt co contido 1234
   C:\Users\usuario> certutil -hashfile f2.txt MD5 #Crear hash MD5 do ficheiro f2.txt
   C:\Users\usuario> certutil -hashfile f2.txt SHA256 #Crear hash SHA256 do ficheiro f2.txt
3. Compara os "hash" dos ficheiros f1.txt e f2.txt anteriores. Que acontece? Por que?
4. Visitar **https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/**
5. Descargar unha imaxe
6. Verificar o "hash" da imaxe anterior co que aparece dentro do ficheiro MD5SUMS e SHA256SUMS
7. Se os "hash" coinciden: a descarga foi corrupta? Por que?

Ricardo Feijoo Costa