Práctica BRS
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.
- **hexdump**: Para sistemas GNU/Linux, como Debian, amosa o contido dun ficheiro en formato hexadecimal, xunto con unha representación ASCII dos bytes imprimibles.
- **xxd**: Para sistemas GNU/Linux, como Debian, permite converter entre formato hexadecimal e binario, así como realizar parches binarios. Tamén ofrece máis opcións de formato para a saída e mostra os valores ASCII correspondentes aos bytes hexadecimais.

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?

   Os hashes non son idénticos aínda que o contido si o é. Isto é debido a que GNU/Linux e MS Windows interpretan os Intro ⏎ como caracteres distintos. Así, se copiamos f2.txt ao sistema operativo baseado en Debian podémolo comprobar do seguinte xeito:

```
$ sudo apt update
$ sudo apt -y install hexdump xxd
$ hexdump f1.txt
0000000 3231 3433 000a
0000005
$ hexdump f2.txt
0000000 3231 3433 0d20 000a
0000007
$ xxd f1.txt
00000000: 3132 3334 0a                           1234.
$ xxd f2.txt
00000000: 3132 3334 200d 0a                      1234 ..
$ ascii | grep -iE '0a|0d|20|31|32|33|34'
$ man 7 ascii #Buscar 0a, 0d, 20, 31, 32, 33, 34 onde:
0A é LF '\n' (new line)
OD é CR '\r' (carriage ret)
20 é SPACE
31 é 1
32 é 2
33 é 3
34 é 4
```

   Así, interpretamos que ó comando hexdump amosa o contido dos ficheiros en hexadecimal en formato Little Endian, polo cal os caracteres:
   - 3231 3433 representan os números 1234
   - 000a representa o carácter nova liña
   - 0d20 representa o caracter espazo é retorno de carro

   Entón:
   - MS Windows representa os Intro como 0a0d, é dicir, \r\n
   - GNU/Linux represena os Intro cono 0a, é dicir \n

   Por iso os hashes son distintos aínda que o contido sexa o mesmo.

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 SHA256SUMS e SHA512SUMS

7. Se os "hash" coinciden: a descarga foi corrupta? Por que?

   SE COINCIDEN NON É CORRUPTA porque eses ficheiros conteñen os hashes oficiais das descargas, polo que se os hashes coinciden cos dos ficheiros o arquivo descargado era o esperado.

Ricardo Feijoo Costa