Práctica Seguridade Informática
Verificar ISO Debian

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:

- **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.
- **gpg**
- **OpenPGP**
- **Philip Zimmermann**
- **Verificar la autenticidad de los CD de Debian**
- **Firmado de claves**

Práctica

Descargar ISO Debian

1. Visitar **https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/**
2. Descargar unha imaxe, por exemplo: debian-11.1.0-amd64-netinst.iso

```
$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.1.0-amd64-netinst.iso #debian-11.1.0-amd64-netinst.iso
```

Comparar "hash"

3. Comparar os "hash" da imaxe ISO anterior co que aparece dentro dos ficheiros SHA256SUMS e SHA512SUMS:

Non existe o ficheiro MD5SUMS. A que será debido?

```
$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA256SUMS #Descargar o ficheiro SHA256SUMS que contén os "hash" das ISO debian

$ sha256sum debian-11.1.0-amd64-netinst.iso | cut -d' ' -f1 > 1.sha256.txt #Gardar soamente o hash SHA256 no ficheiro 1.sha256.txt, é dicir, executar o comando sha256sum sobre a ISO de debian e desa saida quedarse soamente coa primeira columna (-f1), entendendo que as columnas son tidas en conta co caracter espazo (-d ' ') como separador

$ grep debian-11.1.0-amd64-netinst.iso SHA256SUMS | cut -d' ' -f1 > 2.sha256.txt #Gardar soamente o hash SHA256 no ficheiro 2.sha256.txt, é dicir, executar o comando grep sobre o ficheiro SHA256SUMS e desa saida quedarse soamente coa primeira columna (-f1), entendendo que as columnas son tidas en conta co caracter espazo (-d ' ') como separador

$ diff 1.sha256.txt 2.sha256.txt #Comparar os ficheiros 1.sha256.txt e 2.sha256.txt, é dicir, comparar o hash SHA256 do ficheiro descargado co gardado no ficheiro SHA256SUMS

$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA512SUMS #Descargar o ficheiro SHA512SUMS que contén os "hash" das ISO debian

$ sha512sum debian-11.1.0-amd64-netinst.iso | cut -d' ' -f1 > 1.sha512.txt #Gardar soamente o hash SHA512 no ficheiro 1.sha512.txt, é dicir, executar o comando sha512sum sobre a ISO de debian e desa saida quedarse soamente coa primeira columna (-f1), entendendo que as columnas son tidas en conta co caracter espazo (-d ' ') como separador

$ grep debian-11.1.0-amd64-netinst.iso SHA512SUMS | cut -d' ' -f1 > 2.sha512.txt #Gardar soamente o hash SHA512 no ficheiro 2.sha512.txt, é dicir, executar o comando grep sobre o ficheiro SHA512SUMS e desa saida quedarse soamente coa primeira columna (-f1), entendendo que as columnas son tidas en conta co caracter espazo (-d ' ') como separador

$ diff 1.sha512.txt 2.sha512.txt #Comparar os ficheiros 1.sha512.txt e 2.sha512.txt, é dicir, comparar o hash SHA512 do ficheiro descargado co gardado no ficheiro SHA512SUMS
```

4. Se os "hash" coinciden: a descarga foi corrupta? Por que?
5. Teño que confiar nos ficheiros que conteñen os "hash" na páxina oficial de Debian (SHA256SUMS e SHA512SUMS)? Por que?

Verificar sinaturas

6. Verificar as sinaturas dos ficheiros SHA256SUMS e SHA512SUMS:

   $ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA256SUMS.sign #Descargar o ficheiro SHA256SUMS.sign, sinatura do ficheiro SHA256SUMS

   $ gpg --verify SHA256SUMS.sign SHA256SUMS #Verificar a sinatura do ficheiro SHA256SUMS mediante o ficheiro asinado SHA256SUMS.sign

   ```
   gpg: Signature made Sat 09 Oct 2021 04:53:47 PM EDT
   gpg:                using RSA key DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   gpg: Can't check signature: No public key
   ```

   $ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/SHA512SUMS.sign #Descargar o ficheiro SHA512SUMS.sign, sinatura do ficheiro SHA512SUMS

   $ gpg --verify SHA512SUMS.sign SHA512SUMS #Verificar a sinatura do ficheiro SHA512SUMS mediante o ficheiro asinado SHA512SUMS.sign

   ```
   gpg: Signature made Sat 09 Oct 2021 04:53:48 PM EDT
   gpg:                using RSA key DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   gpg: Can't check signature: No public key
   ```

   As sinaturas non se poden verificar. Debemos importar a clave pública de Debian para poder verificalas.
   Fixarse na saída dos comandos anteriores para recoller o fingerprint. Así:

   SHA256SUMS → DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   SHA512SUMS → DF9B9C49EAA9298432589D76DA87E80D6294BE9B

   Co cal o fingerprint é:

   DF9B9C49EAA9298432589D76DA87E80D6294BE9B

   

   Firmado de claves

Importar clave pública de Debian

7. Importar ao noso anel de claves a clave pública de Debian para logo poder verificar os ficheiros asinados coa clave privada de Debian (SHA256SUMS.sign e SHA512SUMS.sign):

   $ gpg --keyserver keyring.debian.org --recv-keys 0xDF9B9C49EA #Importar ao noso anel a chave pública de Debian que se atopa no servidor keyring.debian.org Non é necesario escribir o todo o fingerprint, soamente o número de caracteres hexadecimal co que sexa identificativo e unívoco.

   ```
   gpg: key DA87E80D6294BE9B: public key "Debian CD signing key " imported
   gpg: Total number processed: 1
   gpg:               imported: 1
   ```

Verificar de novo as sinaturas

8. Verificar de novo as sinaturas dos ficheiros SHA256SUMS e SHA512SUMS:

   $ gpg --verify SHA256SUMS.sign SHA256SUMS #Verificar a sinatura do ficheiro SHA256SUMS mediante o ficheiro asinado SHA256SUMS.sign

   ```
   gpg: Signature made Sat 09 Oct 2021 04:53:47 PM EDT
   gpg:                using RSA key DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   gpg: Good signature from "Debian CD signing key " [unknown]
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: DF9B 9C49 EAA9 2984 3258  9D76 DA87 E80D 6294 BE9B
   ```

```
$ gpg --verify SHA512SUMS.sign SHA512SUMS #Verificar a sinatura do ficheiro SHA512SUMS mediante o ficheiro asinado SHA512SUMS.sign

gpg: Signature made Sat 09 Oct 2021 04:53:48 PM EDT
gpg:                using RSA key DF9B9C49EAA9298432589D76DA87E80D6294BE9B
gpg: Good signature from "Debian CD signing key " [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DF9B 9C49 EAA9 2984 3258  9D76 DA87 E80D 6294 BE9B
```

9. Se as sinaturas verificadas son auténticas ***(Good Signature)*** pódese deducir que os ficheiros SHA256SUMS e SHA512SUMS son pertencentes a Debian? Por que?

10. Teño que confiar nos ficheiros que conteñen as sinaturas na páxina oficial de Debian (SHA256SUMS.sign e SHA512SUMS.sign)? Por que? Ten algo que ver o servidor keyring.debian.org

---

Ricardo Feijoo Costa