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-10.6.0-amd64-netinst.iso

```
$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-10.6.0-amd64-netinst.iso #Descargar a ISO debian-10.6.0-amd64-netinst.iso
```

Comparar "hash"

3. Comparar os "hash" da imaxe ISO anterior co que aparece dentro dos ficheiros MD5SUMS, SHA256SUMS e SHA512SUMS:

```
$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/MD5SUMS #Descargar o ficheiro MD5SUMS que contén os "hash" das ISO debian

$ md5sum debian-10.6.0-amd64-netinst.iso | cut -d' ' -f1 > 1.md5.txt #Gardar soamente o hash MD5 no ficheiro 1.md5.txt, é dicir, executar o comando md5sum 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-10.6.0-amd64-netinst.iso MD5SUMS | cut -d' ' -f1 > 2.md5.txt #Gardar soamente o hash MD5 no ficheiro 2.md5.txt, é dicir, executar o comando grep sobre o ficheiro MD5SUMS 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.md5.txt 2.md5.txt #Comparar os ficheiros 1.md5.txt e 2.md5.txt, é dicir, comparar o hash MD5 do ficheiro descargado co gardado no ficheiro MD5SUMS

$ 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-10.6.0-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-10.6.0-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-10.6.0-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-10.6.0-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 (MD5SUMS, SHA256SUMS e SHA512SUMS)? Por que?

Importar clave pública de Debian

6. Importar ao noso anel de claves a clave pública de Debian para logo poder verificar os ficheiros asinados coa clave privada de Debian (MD5SUMS.sign, SHA256SUMS.sign e SHA512SUMS.sign):

$ gpg --keyserver keyring.debian.org --recv-keys 0x64E6EA7D #Importar ao noso anel a chave pública de Debian que se atopa no servidor keyring.debian.org

Verificar sinaturas

7. Verificar as sinaturas dos ficheiros MD5SUMS, SHA256SUMS e SHA512SUMS:

$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/MD5SUMS.sign #Descargar o ficheiro MD5SUMS.sign, sinatura do ficheiro MD5SUMS

$ gpg --verify MD5SUMS.sign MD5SUMS #Verificar a sinatura do ficheiro MD5SUMS mediante o ficheiro asinado MD5SUMS.sign

$ gpg --keyserver keyring.debian.org --recv-keys 0x6294BE9B #Importar ao noso anel outra chave pública de Debian que se atopa no servidor keyring.debian.org

$ gpg --verify MD5SUMS.sign MD5SUMS #Verificar a sinatura do ficheiro MD5SUMS mediante o ficheiro asinado MD5SUMS.sign

$ 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

$ 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

8. Se as sinaturas verificadas son auténticas pódese deducir que os ficheiros MD5SUMS, SHA256SUMS e SHA512SUMS son pertencentes a Debian? Por que?

9. Teño que confiar nos ficheiros que conteñen as sinaturas na páxina oficial de Debian (MD5SUMS.sign, SHA256SUMS.sign e SHA512SUMS.sign)? Por que? Ten algo que ver o servidor keyring.debian.org

---

Ricardo Feijoo Costa

This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**