Práctica BRS
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-X.Y.Z-amd64-netinst.iso *(Sustituír X.Y.Z polos valores correspondentes)*

   $ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-X.Y.Z-amd64-netinst.iso #Sustituír X.Y.Z polos valores correspondentes

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? Ver **Práctica BRS Colision Hash MD5**

   $ 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-X.Y.Z-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-X.Y.Z-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-X.Y.Z-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-X.Y.Z-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?

   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.

5. Teño que confiar nos ficheiros que conteñen os "hash" na páxina oficial de Debian (SHA256SUMS e SHA512SUMS)? Por que?

   Debería, porque son os ficheiros oficiais que nos aporta Debian, é dicir, eses ficheiros son cargados no servidor, supostamente, polos administradores do/s servidor/es web de Debian. Pero, quen me asegura que eses ficheiros non foron trocados por algún ciberdelincuente? Pois imos ver se eses ficheiros están asinados dixitalmente por Debian.

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: Firmado el dom 01 sep 2024 00:01:11 CEST
   gpg:                usando RSA clave DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   gpg: Imposible comprobar la firma: No hay clave pública
   ```

   $ 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: Firmado el dom 01 sep 2024 00:01:11 CEST
   gpg:                usando RSA clave DF9B9C49EAA9298432589D76DA87E80D6294BE9B
   gpg: Imposible comprobar la firma: No hay clave pública
   ```

   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 0xDF9B9C49EAA9298432589D76DA87E80D6294BE9B #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: clave DA87E80D6294BE9B: clave pública "Debian CD signing key " importada
   gpg: Cantidad total procesada: 1
   gpg:               importadas: 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: Firmado el dom 01 sep 2024 00:01:11 CEST
gpg:                usando RSA clave DF9B9C49EAA9298432589D76DA87E80D6294BE9B
gpg: Firma correcta de "Debian CD signing key " [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 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: Firmado el dom 01 sep 2024 00:01:11 CEST
gpg:                usando RSA clave DF9B9C49EAA9298432589D76DA87E80D6294BE9B
gpg: Firma correcta de "Debian CD signing key " [desconocido]
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: DF9B 9C49 EAA9 2984 3258  9D76 DA87 E80D 6294 BE9B
```

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

NON, as sinaturas son auténticas, pero poderon ser asinadas dixitalmente por un ciberdelicuente con acceso aos arquivos. Así, a mensaxe anterior indica que:

- **A sinatura é válida**: Isto significa que os ficheiros SHA256SUM e SHA512SUMS foron asinados correctamente pola clave pública asociada coa pegada dixital(fingerprint) DF9B 9C49 EAA9 2984 3258 9D76 DA87 E80D 6294 BE9B, que se atribúe a "Debian CD signing key".
- **A clave non está certificada**: Isto quere dicir que non hai unha cadea de confianza que conecte esta clave cunha autoridade de certificación(AC) coñecida. Noutras palabras, non hai unha forma independente de comprobar que esta clave realmente pertence a Debian.

  O anterior non garante ao 100% que o ficheiro sexa de Debian, pois poderían darse os seguintes casos:

  - **Suplantación de identidade**: En teoría, alguén podería ter obtido a clave privada correspondente á pegada dixital(fingerprint) e usala para asinar un ficheiro falso. Aínda que isto é pouco probable, non se pode descartar completamente.
  - **Ataque de home no medio(MITM)**: Un atacante podería interceptar a comunicación e modificar tanto os ficheiros como as sinaturas, facendo que penses que estás a comprobar un ficheiro auténtico cando en realidade é unha falsificación.

  Aínda así, proporciona unha forte evidencia debido a:
  - **Alta probabilidade**: A probabilidade de que alguén teña obtido a clave privada de Debian e estea a realizar ataques a gran escala é moi baixa.
  - **Verificación independente**: Podes verificar a pegada dixital(fingerprint) da clave pública coa publicada oficialmente por Debian para asegurarte de que coincide.
  - **Prácticas de seguridade de Debian**: Debian ten un historial de boas prácticas de seguridade e é pouco probable que comprometa a integridade dos seus sistemas.

En resumo:

- Aínda que a sinatura é válida, sempre existe un pequeno risco de que alguén nos intente enganar. Pero, en xeral, esta comprobación danos unha boa indicación de que o ficheiro é auténtico.

- Para poder garantir as sinaturas estas deberían estar certificadas por unha Autoridade de Certificación(CA), igualmente que no noso DNIe os certificados dixitais están emitidos e autorizados polo Goberno de España - Ministerio do Interior - Dirección Xeral da Policía(DGP).

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

Polo comentado anteriormente a resposta curta é SI, pero con certas reservas.

Xa tivemos en conta que a verificación das sinaturas do arquivos SHA256SUMS e SHA512SUMS en Debian proporciona unha forte evidencia da súa autenticidade. Pero, é importante comprender os matices e os riscos involucrados.

Por qué confiar (en xeral)?

- **Cadea de confianza**: O sistema de sinaturas de Debian básase nunha cadea de confianza. Ao verificar a sinatura do arquivo, estás confiando en que a clave pública empregada para asinar é a clave pública correcta de Debian. Esta clave pública se almacena en servidores como **keyring.debian.org** e distribúese de forma segura.
- **Prácticas de seguridad sólidas**: Debian ten un historial de boas prácticas de seguridade e implementa medidas para protexer os seus sistemas de firma.
- **Comunidade activa**: A comunidade de Debian é grande e vixiante. Calquer intento de comprometer a integridade dos paquetes sería rapidamente detectado e denunciado.

Por que non confiar ao 100%?

- **Ataques sofisticados**: Aínda que pouco probable, sempre existe a posibilidade de ataques moi sofisticados que poidan comprometer a infraestructura de firma de Debian.
- **Errores humáns**: Incluso os sistemas mais seguros poden ser vulnerables a errores humáns.
- **Falta de verificación independente**: Se ben podes verificar a pegada dixital(fingerprint) da clave pública, non sempre é posible realizar unha verificación independente completa da cadea de confianza.

Que papel xoga keyring.debian.org?

- **Almacenamento de claves públicas**: Este servidor almacena a clave pública utilizada para firmar os paquetes de Debian.
- **Punto de referencia**: Ao descargar a clave pública dende este servidor, estableces un punto de referencia para verificar as firmas.
- **Risco de compromiso**: Se este servidor fora comprometido, un atacante podería sustituir a clave pública por unha falsa, o que permitiría firmar paquetes maliciosos.

Ricardo Feijoo Costa