UP02 – Criptografía

Prueba práctica 2

Desde *Terraformadores* estamos trabajando con datos relevantes de todas nuestras plataformas en los diferentes satélites de Venus. Necesitamos tener la información replicada y a salvo en varias terminales remotas, así que hemos pensado en vosotros para que os encarguéis de esta tarea.

Como siempre hay espías de la competencia al acecho, hemos tenido que utilizar criptografía para despistar un poco a los atacantes y, sobre todo, para securizar las transferencias de datos.

Para todo el proceso deberás escribir un documento Markdown en tu GitHub/GitLab explicando lo que haces y mostrando capturas.

Paso 1

A cada uno de vosotros se os habilitado una carpeta en el servidor web del PC del profesor. Dentro de ella tenéis 3 mensajes firmados con la clave privada del profesor, así como 3 ficheros *zip*. Deberéis descargar el fichero *zip* que se indique en el mensaje correcto (hay dos mensaje falsos).

Paso 2

Debéis descomprimir dicho fichero y realizar una copia con *rsync* a la máquina remota con la dirección IP que estará indicada en la pizarra. Cada uno de vosotros tiene un usuario en dicha máquina con la contraseña idéntica al nombre de usuario. La copia deberá cumplir lo siguiente:

- La almacenaréis en una carpeta del equipo remoto llamada `/sincro/usuario/` siendo `usuario` vuestro nombre de usuario.
- Se copiará todo el contenido que había dentro de la carpeta `Data` pero no dicha carpeta.
- Deberá mantener siempre exactamente el mismo contenido del origen.
- Se guaradará un **backup** en la carpeta `/backups/usuario/` de manera que tengamos acceso a los datos que se modificaron o borraron en el último *rsync* por si hubiera que recuperarlos.

Paso 3

Para asegurarnos de que todo funciona correctamente, elimina el fichero llamado `old_data.txt` y modifica el fichero llamado `modme.txt` (cambia el texto interno) y vuelve a ejecutar el comando

rsync con las mismas opciones que antes.

Paso 4

Como hemos visto que los usuarios y contraseñas que tenéis no son seguros, vais a crear un par de claves asimétricas para que el acceso por **ssh** se valide mediante esas claves y no por usuario/contraseña.

Debéis crear las claves y copiar la clave pública en la máquina remota.

Paso 5

Una vez configurado lo anterior y, para asegurarnos de que todo funciona correctamente, elimina el fichero llamado `old_data2.txt` y modifica el fichero `modme2.txt` y vuelve a ejecutar el comando rsync con las mismas opciones que antes. Debería realizarse correctamente sin solicitar contraseña.

Paso 6

Añade un fichero llamado `superimportantedelamuerte.txt` en la carpeta `Data` cuyo contenido debe ser la palabra clave que pondrá el profesor en la pizarra.

Paso 7

Espera instrucciones…

Paso 8

Crea un fichero de texto con el enlace al Markdown de tu repositorio GitHub/GitLab donde has redactado toda la memoria. Firma ese documento en modo ASCII y encriptalo, también en modo ASCII, con la clave pública del profesor. Sube ese fichero como entrega en *Aules*.