Práctica 3. Hashing, Cifrado y Certificados

Temporalización

- Semana 5 y 6.

Parte 1

Objetivos

- Usar herramientas de creación de hashes o resúmenes.
- Conocer la aplicabilidad de las hashes o resúmenes.
- Conocer los fundamentos básicos de dos algoritmos de *hashing* muy empleados.
- Usar herramientas de *hashing* para proporcionar control de cambios de ficheros.

Plan de Trabajo

1. Familiarizarse con las herramientas md5sum y sha(*)sum.
2. Elaboración de un script de control de cambios sobre MD5 o SHA1.

Tareas a realizar

Parte 1

1. A partir de la página de manual sobre la forma de uso de **`md5sum`** y **`sha1sum`** (y documentación extra que pueda obtener sobre MD5 y SHA-*), elabora un resumen de cómo se emplean estas aplicaciones para generar *hashcodes* a partir de documentos. Discuta brevemente las debilidades conocidas y reportadas.
2. Use ambas herramientas para construir el *hash* asociado a diferentes tiras de caracteres que difieran en pocos caracteres. Analice y documente las diferencias entre ambas.

3. Elija cualquier fichero presente en tu ordenador (puedes creardo) y obtenga el *hashcode* usando ambas herramientas, describiendo la salida que se obtiene.
4. Sobre los hashes generados en el punto anterior, utiliza la herramienta **`hashid`** para tratar de obtener cuál ha sido la función de hash utilizada para crear los resúmenes anteriores.
5. A partir de la información sobre el fichero (propiedades) que se pueden obtener, por ejemplo, con la orden **`ls -l`**, genere un *hashcode*. Modifique alguna propiedad del fichero y vuelva a obtener el hashcode. ¿qué conclusiones obtienes?
6. Sobre un sistema Ubuntu 20.04.2 LTS, crea dos usuarios (**`root/toor`**), (**`admin/123456`**). Determina cuál es la función de *hash* utilizada para que las claves de los usuarios no se almacenen en texto plano y realiza un ataque de fuerza bruta sobre las contraseñas de los usuarios almacenadas por el sistema operativo en el fichero **`/etc/shadow`**. ¿Para qué puede ser útil la herramineta *John The Ripper*?
7. Construya un programa [**`buildhash`**] (*shell script* o como prefiera), que obtenga para todos y cada uno de los ficheros cuyos nombres aparecen (uno por línea) en un fichero de texto de entrada dos *hashcodes*: uno asociado al propio fichero y otro a sus propiedades. Para cada fichero, se generará una línea que contenga el nombre de fichero, el *hashcode* del fichero y el *hashcode* de sus propiedades, separados por '**`;`**'.
8. Construya un programa [**`checkhash`**] (*shell script* o como prefiera), que tome como entrada el fichero generado por el anterior y compruebe, para cada fichero, si se han producido cambios en el mismo o en sus propiedades, generando una salida en que se muestre cada fichero y se indique si se ha modificado o no.

Enlaces de interés

- Página de manual de *md5sum*.
- Página en GNU con más detalles.
- PPT de Nortwestern.
- Página de manual de sha1sum.
- Herramienta hashid.

Parte 2

En este apartado montaremos un router/firewall a través de la máquina "mallet" utilizando *iptables*.

Se pide:

1. Dibuja el diagrama de red lo más detallado posible.
2. Configura la máquina mallet para que actúe como *router*. Tendrá dos interfaces de red, la eth4 con dirección 192.168.1.3/24 para eth4 en la red interna "Privada", y la eth5 con dirección 1.0.0.1/8 en la red interna "Pública". Deberá tener habilitado el bit de enrutamiento.
3. Configura la máquina bob para que esté dentro de la red interna "Pública" y tenga como dirección IP la 1.0.0.2/8, y como puerta de enlace la 1.0.0.1/8.
4. Configura la máquina Alice para que esté dentro de la red interna "Privada" y tenga como dirección IP la 192.168.1.2, y como puerta de enlace la 192.168.1.3/24.
5. Realiza pruebas a nivel de red para comprobar que las máquinas se comunican. ¿Qué ocurre con el valor del *ttl* cuando un paquete atraviesa un *router*?
6. Indica las diferencias entre las reglas de tipo INPUT, OUTPUT y FORDWARD en iptables.
7. Configura una regla en el firewall del *router* para que sólo se puedan realizar peticiones de tipo ICMP(8) desde la red interna.
8. Configura una regla en el firewall para que sólo la máquina con IP 192.168.1.3 sea quién pueda establecer una conexión por *ssh* a la máquina 192.168.1.2.

Enlaces de interés

- Manual práctico de iptables
  - http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf
- Página del proyecto Netfilter
  - https://netfilter.org/