Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

1. Seguridad en Sistemas Operativos
   - UNIX
   - Windows
2. Ataques contra contraseñas
   - Tipos de ataques
   - Herramientas
   - Defensas

Cuentas de usuarios

- Cada usuario tiene una cuenta en el sistema operativo.
- Existen cuentas de usuarios del sistema y de usuarios reales.
- Cada proceso se ejecuta con los permisos de una determinada cuenta.
- La base de usuarios se almacena en el archivo `/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:daemon:*:2:2:daemon:/sbin:
ftp:*:14:50:FTP User:/home/ftp:
nobody:*:99:99:Nobody:/:
juan:$1$hwqqWPmr$TNL0UManaI/v0coS6yvM21:501:501:
    Juan Perez:/home/juan:/bin/bash
```

- El usuario `root` tiene todos los privilegios.

Cuentas de usuarios

Formato /etc/passwd

- **username:** es el nombre que va a tener la cuenta de usuario en el sistema. No debe contener letras mayúsculas.
- **password:** contraseña cifrada del usuario. Este campo puede también contener un asterisco, lo cual significa que el usuario está bloqueado; o la letra "x", que indica que la contraseña está almacenada en el archivo `/etc/shadow`.
- **UID:** una identificación numérica única para el usuario.
- **GID:** una identificación numérica única para el grupo primario del usuario.
- **full name:** en este campo se coloca el nombre completo del usuario real o algún comentario que se quiera agregar.
- **home directory:** indica el home directory del usuario en cuestión.
- **shell:** aquí se indica el comando que se va a ejecutar en el momento que el usuario inicie una sesión. Usualmente es el shell.

Cuentas de usuarios

Archivo /etc/shadow

- El archivo `/etc/passwd` es legible por todo el mundo.
- Los sistemas UNIX modernos utilizan `/etc/shadow` para guardar las contraseñas.
- `/etc/shadow` es sólo legible por `root`.

```
root:$1$bed128365216c019988915ed3add75fb:
   14729:0:99999:7:::
daemon:*:14728:0:99999:7:::
bin:*:14728:0:99999:7:::
```

Cuentas de grupos

- Los grupos simplifican la administración de permisos de usuarios.
- Linux y UNIX soportan la creación de grupos de usuarios.
- Los grupos se almacenan en el archivo `/etc/group`

```
root:x:0:
daemon:x:2:root,bin
desarrollo:x:25:juan
```

Representación de contraseñas

- Los primeros UNIX utilizaban la función `crypt(3)` con un algoritmo criptográfico sumamente débil.
- Luego se pasó al algoritmo de cifrado DES y a la función de hash MD5.
- Actualmente existen implementaciones basadas en Blowfish, MD5 y SHA (SHA-256 y SHA-512).
- El formato de la contraseña en el campo correspondiente de `/etc/shadow` es como sigue:

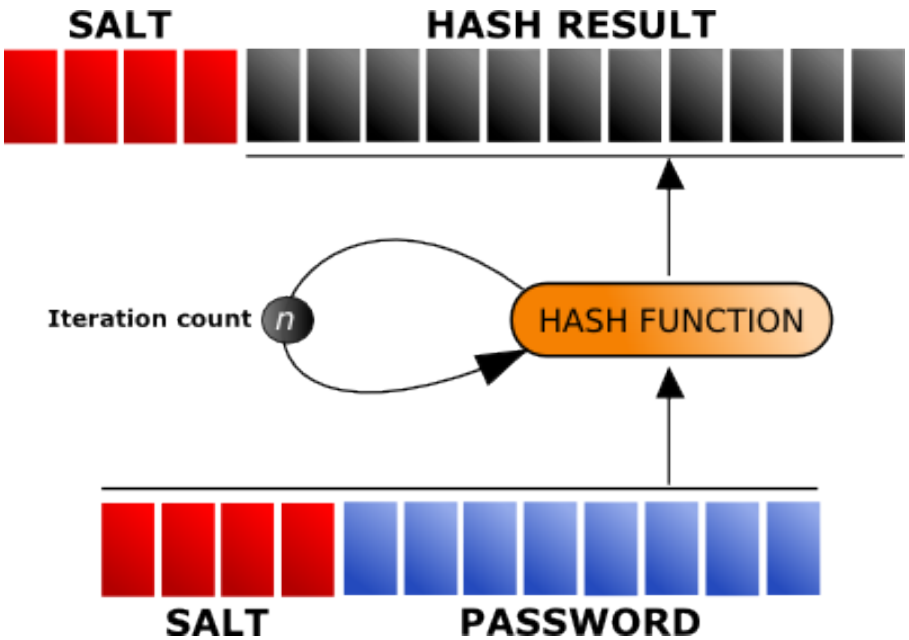
`$<ID>$<SALT>$<PWD>`

ID	Método
1	MD5
2b	Blowfish
5	SHA-256
6	SHA-512

Representación de contraseñas

Password salting

- Los algoritmos de cifrado y hashing son públicamente conocidos.
- Si se consigue la base de usuarios, pueden probarse todas las combinaciones hasta encontrar las contraseñas.
- Mediante el "password salting" hacemos que este proceso sea mucho más dificultoso.



Cuentas de usuarios

- En Windows existen dos tipos de cuentas: cuentas por defecto y cuentas creadas por un administrador.
- La cuentas por defecto son “Administrator” y “Guest”.
- La cuenta Administrator tiene el mayor nivel de privilegios, y no puede borrarse ni bloquearse.
- La cuenta Guest por defecto está deshabilitada.
- El resto de cuentas son creadas por el Administrador y pueden ser para usuarios o servicios.

Cuentas de grupos

- Los grupos se utilizan para controlar accesos y privilegios.
- Existen grupos Globales y Locales.
  - Globales: no proporcionan directamente ningún acceso a ningún recurso. Se definen a nivel Dominio.
  - Locales: brindan acceso a los recursos del equipo local. Un grupo global se puede incluir en un grupo local.

Grupos Locales	**Grupos Globales**
Administrators	Domain Administrators
Account Operators	Domain Users
Server Operators	
Backup Operators	
Print Operators	
Replicators	
Users	
Guests	

Representación de contraseñas

- En un sistema Windows la información de las cuentas se almacena en una base llamada SAM (Security Accounts Manager).
- Se ubica en `\%systemroot%\system32\config\SAM`
- El archivo SAM se encuentra cifrado a nivel filesystem con una llave de 128 bits llamada SYSKEY
- Contiene las contraseñas representadas en dos formatos: LM Hash y NT Hash.

```
Administrador:500:855c3697d9979e78ac404c4ba2c66533:
   7f8fe03093cc84b267b109625f6bbf4b:::
Invitado:501:552902031bede9efaad3b435b51404ee:
   878d8014606cda29677a44efa1353fc7:::
paula:1005:4d98b75fd1dacd79aad3b435b51404ee:
   74ed32086b1317b742c3a92148df1019:::
```

Representación de contraseñas
Hash LM

- Se ajusta la longitud de la contraseña a exactamente 14 caracteres, agregando caracteres NULL al final de ser necesario.
- La cadena resultante es dividida en dos partes iguales de 7 caracteres.
- Se agrega un caracter de paridad requerido por DES.
- Cada parte se utiliza como "llave" para cifrar con DES una cadena de caracteres constante: `"KGS!@#$%"`

Debilidades:

1. Los caracteres de contraseña están limitados al conjunto de caracteres ANSI.
2. Las contraseñas mayores a 7 caracteres son divididas en dos partes que pueden ser luego atacadas por separado. Se pasa de 2^{92} posibles combinaciones a 2^{46}
3. Todas las letras minúsculas son convertidas a mayúsculas antes de ser utilizadas para cifrar. Se reducen las posiblidades a 2^{43}
4. LM no utiliza "password salting"

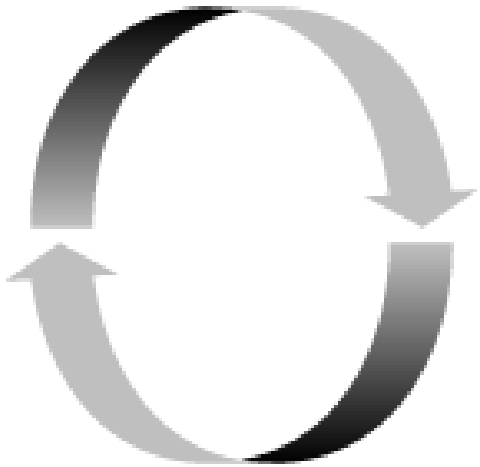
Representación de contraseñas
Hash NTLM

- Amplía el conjunto de caracteres válidos a Unicode.
- Utiliza el algoritmo de hashing MD4 para producir un resumen de la contraseña expresada en codificación UTF-16-LE: MD4(UTF-16-LE(password))
- No utiliza "password salting".

Ejemplos de hash de contraseñas:
`http://openwall.info/wiki/john/sample-hashes`

Ataques contra contraseñas

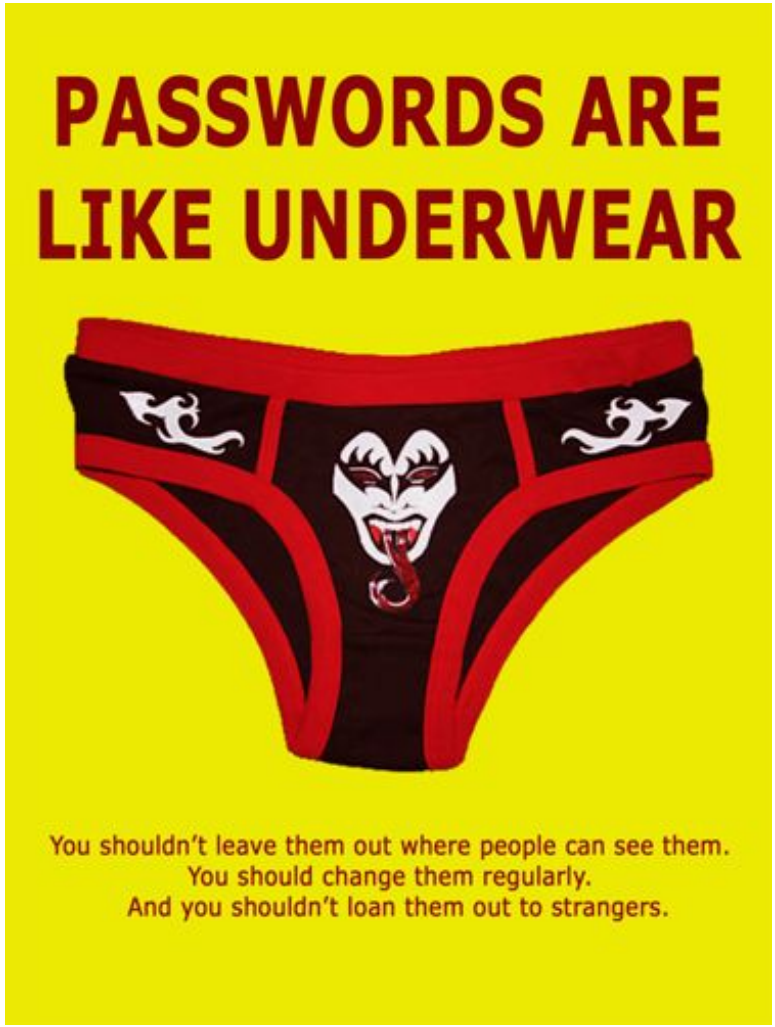
- Las contraseñas son la herramienta más utilizada en el mundo de la seguridad de la información.
- Contraseñas fáciles de deducir son normalmente el eslabón más débil en la seguridad de los sistemas.
- Por qué se siguen utilizando? Porque son el mecanismo de autenticación más "barato".



- Create a password guess
- Encrypt the guess
- Compare encrypted guess with encrypted value from the stolen password file
- If match, you've got the password! Else, loop back to the top.

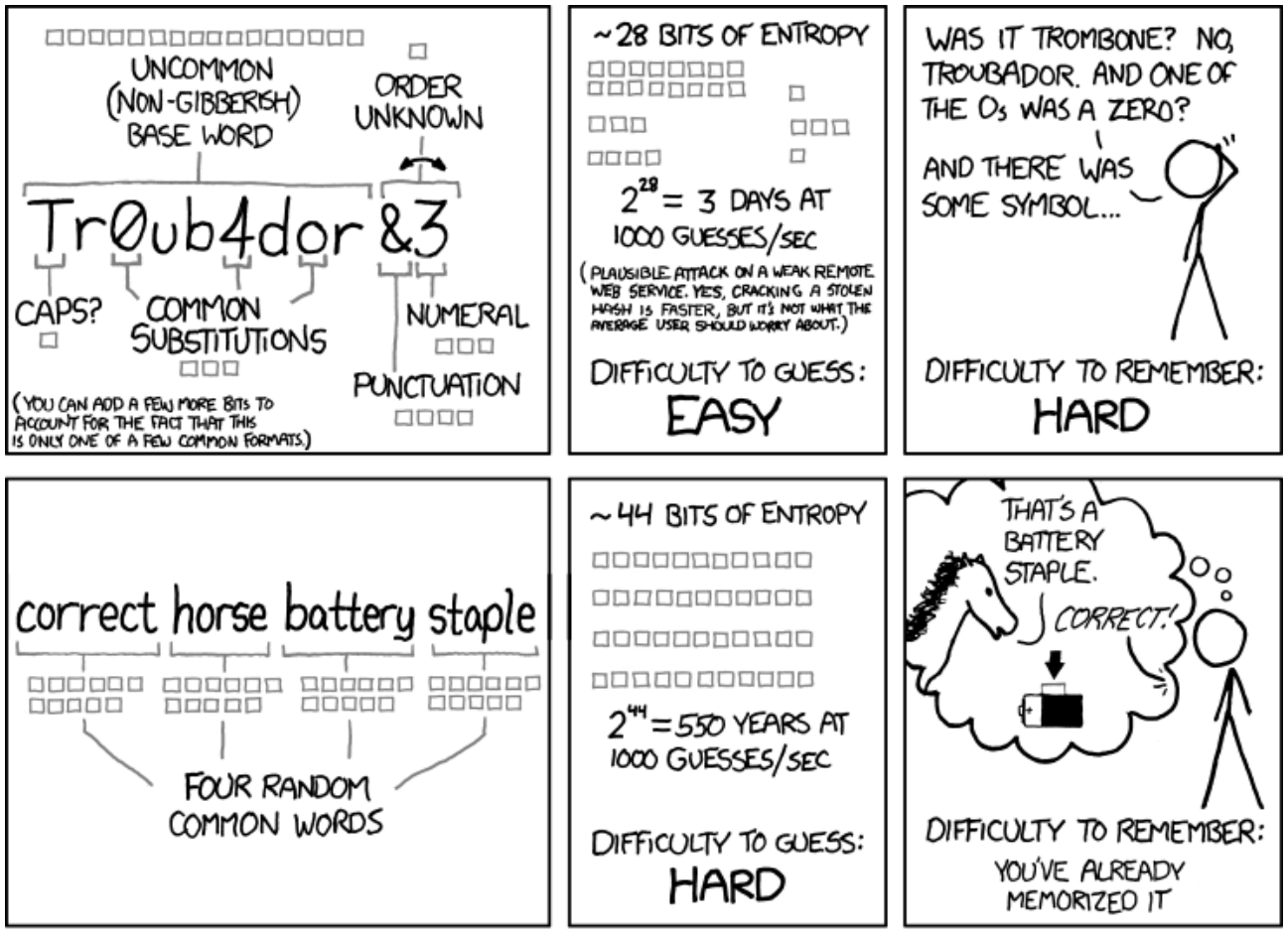
Ataques contra contraseñas

- Buenas prácticas:



Ataques contra contraseñas

- Buenas prácticas:



Tipos de ataques
Password Guessing

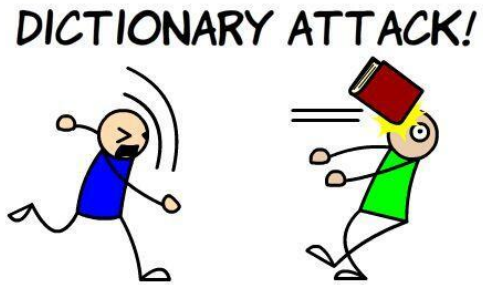
Password Guessing: consiste en adivinar la contraseña en función de conocer alguna información respecto del usuario o del servicio.

Ejemplos:

- En blanco.
- Contraseñas por defecto (se puede usar una Default Password List como `http://www.phenoelit.org/dpl/dpl.html`).
- Las palabras "password", "passcode", "admin", etc.
- Una fila de teclas del teclado: qwerty, asdf, etc.
- El nombre del usuario o algún conocido suyo.
- El número de teléfono, dirección, DNI, etc.

Tipos de ataques
Ataques de Diccionario

Ataque de diccionario: aprovecha el hecho de que los usuarios normalmente utilizan contraseñas débiles (como palabras que pueden encontrarse en un diccionario), para probar sucesivamente con todas las palabras de una lista extensiva (llamada "diccionario") hasta hallar la contraseña.



- Este ataque se enfoca en probar sólo las combinaciones que tienen mayor probabilidad de ocurrir.
- Suele tener un gran porcentaje de efectividad.
- Es más rápido que otro tipo de ataques.

Tipos de ataques
Ataques de Fuerza Bruta

Ataque Fuerza Bruta: consiste en probar "todas" las posibles contraseñas hasta hallar la buscada. En teoría, si no hay un límite en el número de intentos, un ataque de fuerza bruta va a encontrar siempre la contraseña buscada.

- A medida que la longitud de la clave aumenta, también la cantidad de intentos necesarios para hallarla.
- En la práctica es difícil utilizar este método por el poder computacional y tiempo que demandan: puede llevar de horas a siglos!
- Existen técnicas llamadas "*smart brute force*" o "*hybrid password cracking*" que comienzan probando con palabras de diccionario, luego con variaciones de estas palabras y finalmente con el resto de combinaciones.

Tipos de ataques

Ataques de Pre-cómputo

Ataque Pre-Cómputo: consiste básicamente en pre-calcular todas las posibles combinaciones de un algoritmo determinado y almacenarlas en una base de datos key-value que pueda ser luego consultada rápidamente. Utiliza las llamadas Tablas Rainbow.

- Calcule 1 vez, use N veces.
- Tiempo de éxito de varios órdenes de magnitud menos que la fuerza bruta.
- Pueden bajarse tablas Rainbow en forma gratuita de la web:
  - `http://ophcrack.sourceforge.net/tables.php`
  - `https://freerainbowtables.com/`
  - `http://project-rainbowcrack.com/table.htm`
- Sitios con tablas Rainbow on-line:
  - `http://www.onlinehashcrack.com/`
  - `http://crackstation.net/`
  - `http://online.crackmyhash.com/`

Herramientas

- **THC Hydra:** cracker de mecanismos de autenticación de red, tales como telnet, ftp, http, smtp, etc.
- **Medusa:** un network login brute-forcer paralelo para distintos servicios de red (HTTP, FTP, IMAP, SMB, etc.)
- **John the Ripper:** una herramienta potente para UNIX/Linux que realiza cracking con contraseñas simples, listas de palabras, fuerza bruta y/o smart brute force.
- **RainbowCrack:** un cracker de contraseñas de fuerza bruta que utiliza tablas Rainbow.
- **Brutus:** utilidad de password guessing remota para Windows. Soporta todo tipo de servicios de red: HTTP, POP3, SMTP, IMAP, etc.

Defensas

1. NO usar contraseñas :)
2. Definir políticas de contraseñas fuertes: longitud mínima, no utilizar una palabra de diccionario, cambiarlas cada 30 o 60 días, etc.
3. Utilizar "passphrases" en vez de "passwords", o las primeras letras de una frase recordable.
4. Utilizar herramientas que eviten la utilización de contraseñas débiles.
5. EDUCAR a los usuarios.

Más información

- **DREPPER, Ulrich.** *Unix crypt using SHA-256 and SHA-512.* `http://people.redhat.com/drepper/SHA-crypt.txt`
- **JASYPT.** *How to encrypt user passwords.* `http://www.jasypt.org/howtoencryptuserpasswords.html`
- **SKOUDIS - LISTON.** *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Capítulos 3, 4 y 7.
- **PRITCHETT - DE SMET.** *BackTrack 5 Cookbook.* Capítulo 9.
- **WIKIPEDIA.** *crypt (Unix).* `http://en.wikipedia.org/wiki/Crypt_(Unix)`
- **WIKIPEDIA.** *Password Cracking.* `http://en.wikipedia.org/wiki/Password_cracking`
- **WIKIPEDIA.** *Security Accounts Manager.* `http://en.wikipedia.org/wiki/Security_Accounts_Manager`