TEMA

Tema 4. Seguridad Lógica

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 4: Seguridad Lógica

¿Qué aprenderás?

- La Regla Básica de la Seguridad
- La diferencia entre SSO y MFA
- Qué ha de tener una contraseña robusta
- Cómo nos pueden robar las contraseñas

¿Sabías que…?

- El PIN más común en un cajero automático es 8520

4.1. Introducción

Definimos la **Seguridad Lógica** como el conjunto de pasos cuyo objetivo es garantizar la seguridad en el uso de los sistemas y los programas que gestionan los datos y procesos en cualquier empresa.

También se responsabiliza de gestionar el acceso autorizado y ordenador de los usuarios a la información almacenada en el sistema informático. Cualquier vulneración de esta seguridad tiene un gran problema, solo nos enteramos cuando ha pasado.

Por lo tanto, con las medidas que vamos a tomar buscamos:

- Controlar el acceso a los programas y datos
- Garantizar que el usuario no pueda modificar programas y datos que no le competen
- El asegurar que cada proceso utilice los archivos, recursos y aplicaciones que le corresponda
- Verificar que la información compartida llegue al receptor autorizado
- Asegurar la integridad de la información
- Asegurar medidas de contingencia para la transmisión de datos

Como punto de referencia sobre el que vamos a trabajar a partir de ahora, nos vamos a fijar en las CINCO LEYES DE LA CIBERSEGURIDAD:

1ª. Si hay una vulnerabilidad (física, lógica o humana) será explotada

2ª. Todo sistema es vulnerable de alguna forma y en algún momento

3ª. Los humanos creen cosas que deberían creer

4ª. Junto con las nuevas tecnologías vienen nuevas vulnerabilidades

5ª. En cado de duda, nos regimos por la Ley 1ª.

Fuente: https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity?/language=es

4.2. La gestión de la información en la seguridad lógica

La Seguridad Lógica garantiza estos cuatro principios:

- **Confidencialidad**: Este principio busca la no divulgación desautorizada de la información de la empresa. La misma solo es accesible al personal autorizado y competente
- **Integridad**: La información, aunque se comparta, no se altera y no pierde credibilidad
- **Disponibilidad**: La información se mantiene siempre a punto para ser utilizada, sin problema de rendimiento o de acceso.
- **Confirmación**: Toda la información compartida lleva la firma del emisor y del receptor, el cual confirma su recibo.

"Todo lo que no está permitido debe estar prohibido"

4.3. El control de acceso

El acceso a un sistema informático se basa en cumplir una serie de requisitos:

3.3.1. Identificación y Autentificación

Nos identificamos en un sistema en el que introducimos nuestro usuario y contraseña, y el sistema nos autentifica cuando realiza la verificación de que la información es correcta.

Desde el punto de vista de la eficacia, conviene realizar este proceso solamente una vez. Os podéis imaginar lo incómodo que es el tener que introducir el usuario y contraseña cada vez que cambias de página web, o cada ver que cambias de pantalla en una aplicación. A este proceso se le denomina "**Single login**" o sincronización de contraseña.

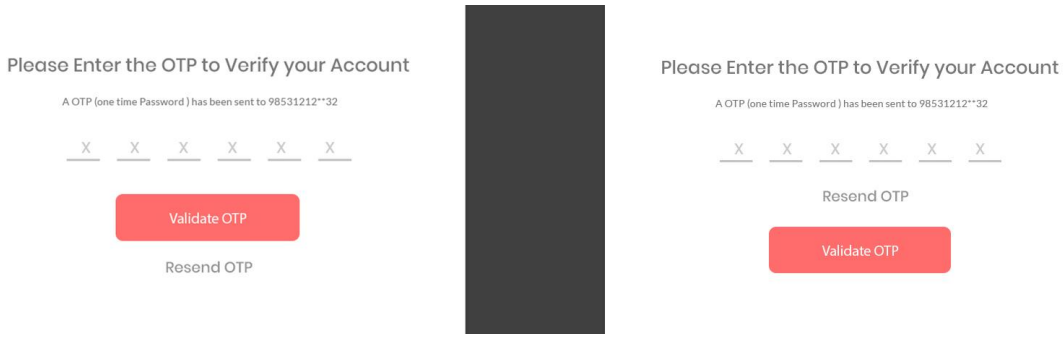
Para aplicar esto, implementaremos un servidor de autentificaciones sobre el cual los usuarios se identifican, y que se encarga de autentificar al usuario sobre los restantes equipos a los que éste pueda acceder. Un ejemplo claro lo tenemos en la gestión de usuarios de **Microsoft Active Directory** (AD) y en **LDAP**.

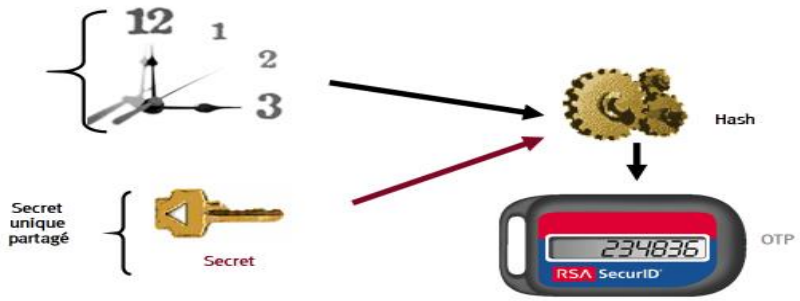
También tenemos la opción del **Single Sign-On (SSO).** Esta opción permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo una cuenta. Por lo tanto, el usuario puede a través de una cuenta, tener múltiples accesos, por ejemplo, ingresando a Gmail accedemos a Google Docs, Google Maps… con la cuenta de correo de Office365 tenemos acceso a Word, Excel, Teams… Otra de las ventajas de SSO es su seguridad, pues la información viaja cifrada por la red.

Como medida de seguridad suplementaria, progresivamente se va implantando la **Autenticación Multifactor (MFA)**. Este sistema de seguridad requiere más de una forma de autenticación para verificar la legitimidad de una transacción. Combina dos o más credenciales independientes, las cuales, si una falla o se rompe en un ataque, dificulta el acceso al objetivo.

Las MFA más utilizadas son:

- Deslizar una tarjeta e introducir un PIN
- Descargar un cliente VPN con un certificado digital válido e iniciar sesión en el VPN antes de que sea concedido el acceso a una red
- Iniciar sesión en un sitio web y que se solicite introducir una contraseña adicional de un solo uso (OTP). Esta clave se envía por teléfono o mail al solicitante
- Deslizar una tarjeta, escanear una huella digital y responder a una pregunta se seguridad





4.3.2. Gestión de Usuarios

Como futuro administrador de sistemas de una empresa, deberás realizar una administración correcta de la identificación, autentificación y autorización de acceso, por lo que deberás tener claro:

- Cómo realizar el proceso de solicitud, creación, manejo, seguimiento y cierre de las cuentas de usuario. Cuando creas un usuario, debe generarse el perfil de seguridad correspondiente
- El nombre del usuario debe asignarse de manera homogénea en toda la empresa
- Hay que revisar periódicamente las cuentas, sus contraseñas y permisos. Se recomienda que se cambien las contraseñas cada seis meses y que los nombres de usuario no lleven a confusión
- Hay que revisar periódicamente el acceso de cada cuenta al sistema, para detectar periodos de inactividad y mejorar la política de seguridad

- Revisar los registros de transacciones para detectar actividades no autorizadas
- Mantener actualizados los permisos de acceso ante cambios temporales o rotación de usuarios
- Determinar cuál es el proceso de desvinculación del personal de la organización, se realice de forma amistosa o no. Como recomendación, en el momento que se conozca la desvinculación, el permiso de acceso al usuario debe anularse informando previamente al interesado

4.3.3. Modalidad de acceso a la información

Tener claro qué permisos se le asigna al usuario sobre cada recurso. Como recordatorio adjunto el listado de permisos de forma general:

- Lectura (**Read**): El usuario puede leer o visualizar la información sin alterarla. Podrá copiarla o imprimirla
- Escritura (**Write**): El usuario podrá agregar datos, modificarlos o borrarlos
- Ejecución (**eXecute**): El usuario tiene el privilegio de ejecutar programas

4.3.4. Listas de Control de Acceso (ACL)

Son registros donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este sistema debe estar habilitado en el sistema de ficheros. Lo podemos comprobar fácilmente en el /etc/fstab de Linux, si al montar el sistema de ficheros, tenemos el parámetro 'acl'. En otro tema trataremos las ACL en más detalle.

4.3.5. Gestión de Contraseñas

Hay muchos criterios y fuentes de información para crear un "método" con el que gestionar las contraseñas. Vamos a seguir el "oficial", que nos proporciona el **Incibe** (Instituto Nacional de Ciberseguridad) que es una fuente de confianza con la que colaboran los mejores especialistas del país.

4.3.5.1. Controles que deben realizarse en cualquier sistema de gestión de contraseñas

Los controles se clasificarán en dos niveles de complejidad:

- **Básico** (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- **Avanzado** (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

Nivel	Alcance	Control	

A	PRO/TEC	Definir un sistema de gestión de contraseñas que contemple todos los aspectos relativos a su ciclo de vida	- Identificar los distintos equipos, servicios y aplicativos para los que es necesario activar credenciales de acceso.
			- Definir la manera con la que se generarán las claves, así como su formato.
			- Distribuir las claves generadas a los usuarios correspondientes, teniendo en cuenta:
			  ○ si esta distribución ha de ser cifrada y con qué método
			  ○ cómo se activarán las claves.
			- Almacenar las claves en repositorios seguros, considerando la necesidad de realizar copias de respaldo.
			- Determinar quién puede acceder a estos repositorios y cómo.
			- Establecer el periodo de validez para cada tipo de clave.
			- Revocar las claves, ya sea por baja de un empleado, por considerar que una clave está comprometida por robo, etc. Además, se determinará la manera con la que las claves serán eliminadas.
			- Registrar:
			  ○ motivo por el que se genera una clave
			  ○ fecha de creación
			  ○ responsable de la custodia
			  ○ periodo de validez
			  ○ posibles observaciones, incidentes, etc.

A	PRO/TEC	Utilización de sistemas de autentificación externa	- Social-login. Se basa en la utilización de identidades ya creadas en redes sociales (como Facebook, LinkedIn, Google o Twitter) para registrarnos automáticamente en otros servicios. - Autenticación federada. Permite disponer de un único punto de autenticación para acceder a servicios de distintas compañías. Puede ser de utilidad para empresas muy integradas con proveedores y Partners. - Single sign-on. Se trata de un mecanismo que permite a un usuario autenticado en un servicio el acceso automático a otras muchas aplicaciones y servicios. - Autenticación condicionada al dispositivo. Nos permiten la autenticación a través de alguna característica del dispositivo previamente registrada en el servidor de autenticación. - CSAB (Cloud Access Security Brokers). Especialmente pensado para empresas que hacen uso de servicios cloud.
A	TEC	Usar herramientas informáticas para garantizar la seguridad de las contraseñas	- LDAP - Active Directory
B	TEC	No utilizar las contraseñas por defecto de aplicaciones y sistemas	
B	TEC	Incorporar sistemas de autentificación Multifactorial	- huella digital - tokens criptográficos hardware - Sistemas OTP (**One Time Password**) - tarjetas de coordenadas.
B	PER	No compartir las contraseñas con nadie	

B	PER	Las contraseñas deben de ser robustas	- deben contener al menos ocho caracteres
			- deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos)
			- no deben contener los siguientes tipos de palabras:
			  ○ palabras sencillas en cualquier idioma (palabras de diccionarios)
			  ○ nombres propios, fechas, lugares o datos de carácter personal
			  ○ palabras que estén formadas por caracteres próximos en el teclado
			  ○ palabras excesivamente cortas.
			- tampoco utilizaremos claves formadas únicamente por elementos o palabras que puedan se públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento)
			- se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas
			- se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo Passphrase (contraseña larga formada por una secuencia de palabras).

B	PER	No utilizar la misma contraseña para servicios diferentes	
B	PER	Cambiar las contraseñas periódicamente	No deben utilizarse contraseñas que hayan sido usadas con anterioridad
B	PER	No hacer uso del recordatorio de contraseñas en navegadores y aplicaciones	
B	PER	Utilizar gestores de contraseñas seguros para poder recordarlas	

Tabla. Política de Gestión de Contraseñas Fuente: Incibe

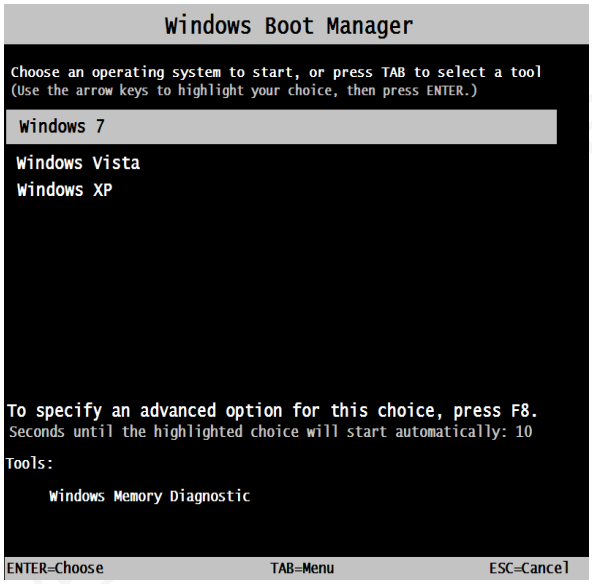
4.3.5.2. Niveles de control de acceso por contraseña

Dentro de un equipo informático nos podemos encontrar control de acceso por contraseña en diversos puntos:

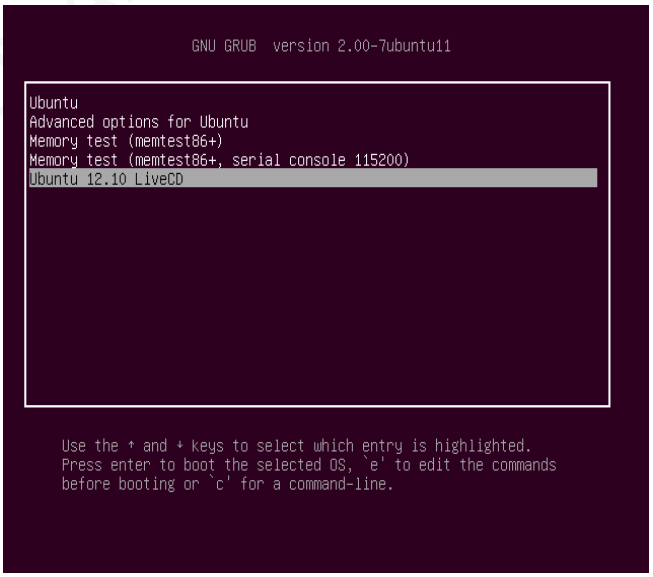
a) **Bios:** Al poner contraseña en la BIOS evitamos, por ejemplo, que se pueda modificar el orden de arranque del ordenador. Esto se utiliza para evitar que el equipo arranque por el DVD y puedan acceder al mismo con un Live-DVD.

b) **Gestor de arranque:** Cuando en los discos tengamos instalados varios sistemas operativos, durante el arranque del equipo ejecuta un programa denominado Boot Manager. Este programa permite elegir entre los diversos sistemas operativos o arranque uno por defecto.

Nos podemos encontrar varios ejemplos: lilo, grub2, Windows Boot Manager. En el grub2 podemos establecer contraseñas para las diferentes opciones.



Esta foto de Autor desconocido está bajo licencia CC BY-SA



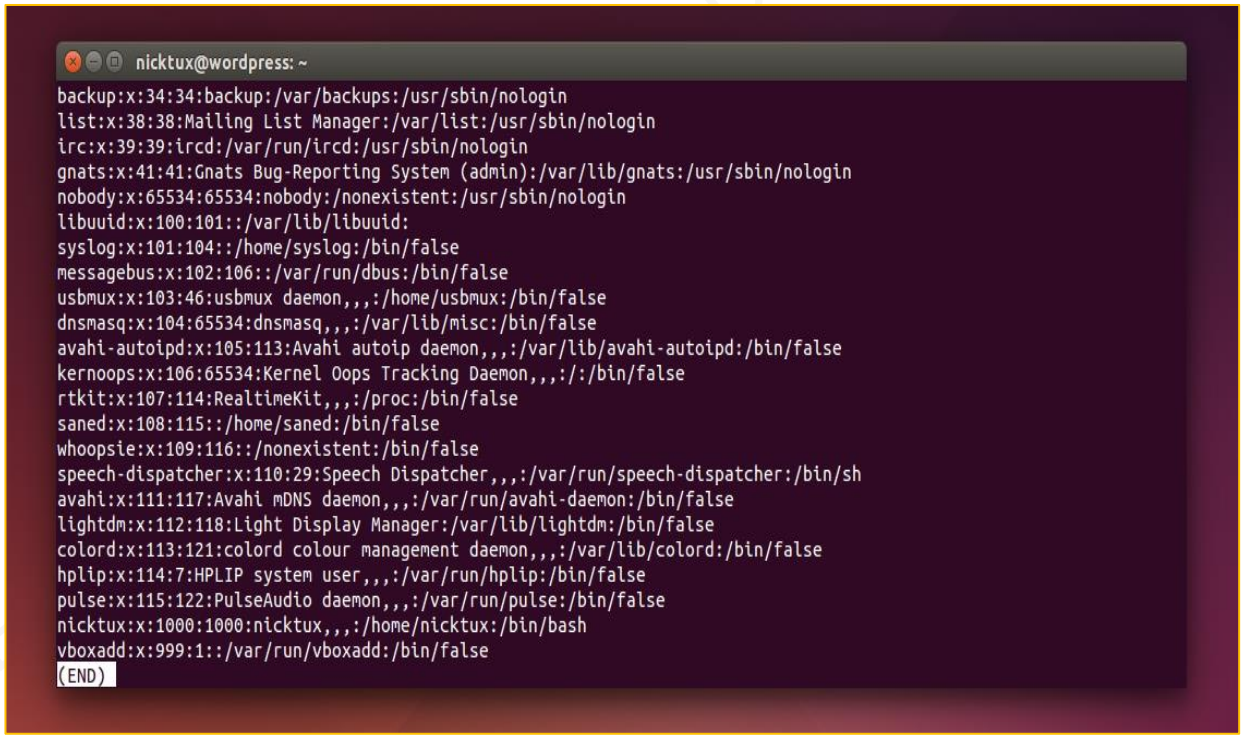
Esta foto de Autor desconocido está bajo licencia CC BY-SA

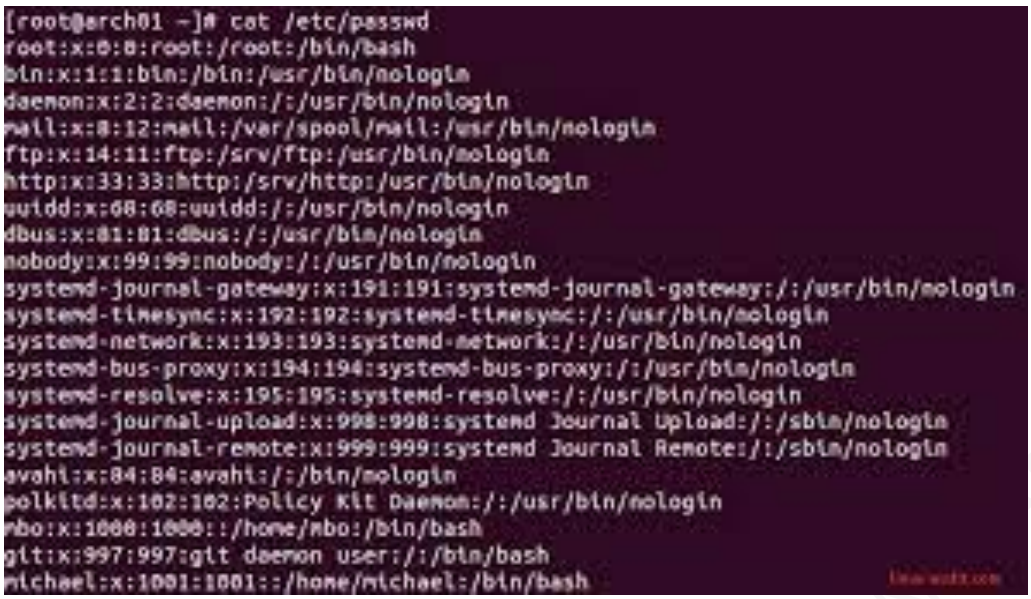
c) **Autenticación en el sistema operativo:** En el arranque del sistema operativo nos requiere identificarnos como usuario de este. Al realizar la verificación, el sistema no asigna el rol que tengamos con los permisos que tengamos asignados por el administrador del equipo.

En el caso de que necesitemos de forma puntual realizar tareas administrativas (instalación de una aplicación) podemos solicitar una elevación de privilegio. Consiste en pedirle al sistema ejecutar un programa determinado con permisos de administración. Una vez finaliza, perdemos el privilegio.

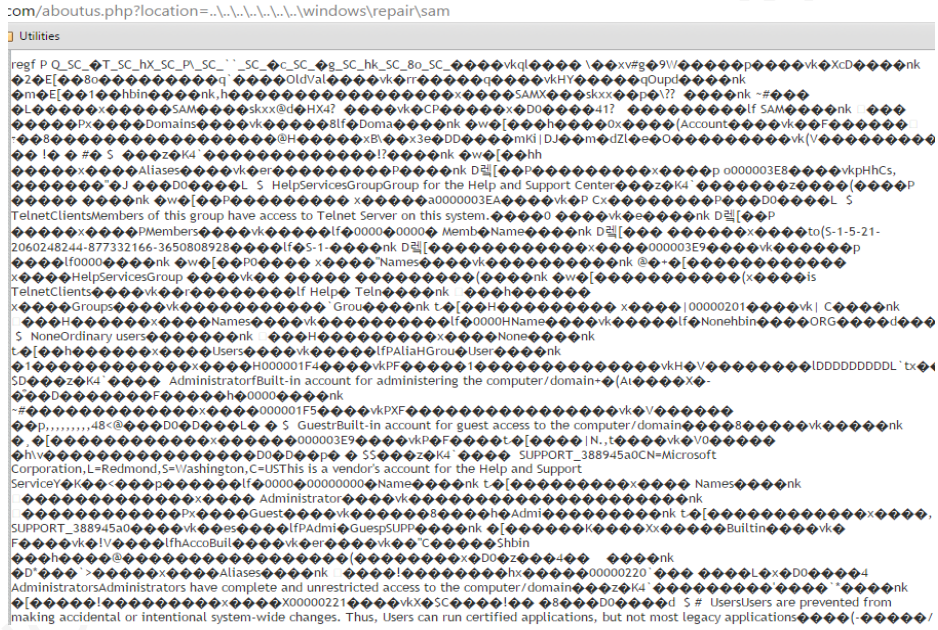
En sistemas Linux, lo realizamos con el comando sudo, pero en sistema Windows tenemos el **UAC** (User Access Control). Este sistema avisa al usuario cuando un programa ejecuta una operación de administración.

Es importante recordar dónde se almacena toda esta información. En los sistemas Linux tenemos dos archivos **/etc/passwd**, el cual almacena los datos de los usuarios, y **/etc/shadow**, donde tenemos las contraseñas encriptadas. En los sistemas Windows tenemos **SAM**, un archivo que encontraremos en **%windir%/system32/config**.





Fuente: Linux Audit



d) **Aplicaciones/página web:** Cogiendo como base el modelo de red de un servidor al que accedemos desde los equipos cliente, desde hace tiempo trabajamos con aplicaciones/páginas que incorporan una identificación que es enviada por Internet a un servidor de autentificación. Esta identificación debe de seguir los mismos criterios que los de un acceso al sistema operativo o a una aplicación cualquiera, pero con un problema añadido, es mucho más sencillo para un atacante acceder a la página web y dedicarle tiempo y recursos para "hackear" la contraseña que a tu ordenador personal o a la aplicación de tu empresa.

4.4. Ataques para obtención de contraseñas

Bueno, ya hemos dedicado un buen tiempo de este tema para conocer las técnicas de defensa, ahora vamos a conocer cómo el atacante puede realizar una identificación en el sistema. Para ello lo más lógico es robarnos nuestras credenciales, sobre todo la contraseña.

Vamos a revisar los diferentes métodos para ello:

4.4.1. Ataque de Fuerza Bruta

Consiste en descifrar la contraseña mediante la repetición, es decir, a base de ensayo y error. Se prueban diferentes combinaciones al azar, mezclando nombres, letras y números, hasta que dan con la contraseña. Utilizan números comunes, fechas de nacimiento, nombres de mascotas, actores, actrices…

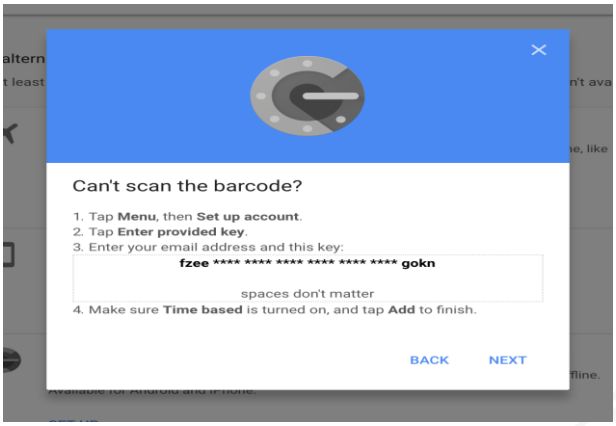
Esta foto de Autor desconocido está bajo licencia CC BY-NC

La herramienta más conocida para realizar este tipo de ataques es **HYDRA**.

Esta foto de Autor desconocido está bajo licencia CC BY-SA-NC

Para defendernos de estos ataques podemos tomas las siguientes medidas:

- Disponer de herramientas que monitoreen el número de inicios de sesión
- Restringir el acceso a IP autorizadas
- Bloquear la IP del atacante para evitarlo en el futuro
- Bloquear cuentas con demasiados intentos fallidos
- Utilizar **CAPTCHA** (son su Talón de Aquiles)
- Introducir un tiempo de inicio de sesión importante, por ejemplo 10 segundos
- Autentificación de dos factores (**2FA**)

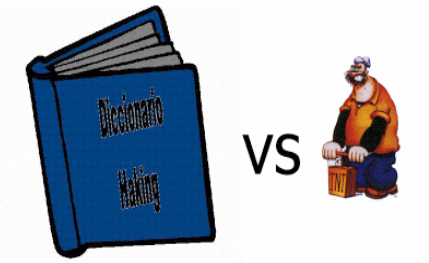


4.4.2. Ataque de Diccionario

Este ataque es una mejora del ataque por fuerza bruta. Tenemos un software que se encarga de descifrar la contraseña. Para ello tiene un archivo, que denominamos Diccionario, con un listado extenso de combinaciones alfanuméricas, palabras conocidas, números, fechas… El software realiza la identificación hasta que en el sistema responde.

Para realizar este tipo de ataques se utilizan programas como:

- Crack
- John the Ripper
- L0phtCrack
- Cain
- Aircrack-Ng



También tienes programas para generar tus Diccionarios personalizados:

- Crunch
- Cewl
- Cupp
- Pydictor
- Dymerge

4.4.3. Suplantación de identidad o phishing

Consiste en engañar a la víctima para que rellene un formulario falso con sus credenciales de inicio de sesión. Esta muy de moda porque ¡¡¡FUNCIONA!!! Cada vez los clones son más y más realistas y desde que se implantó en el mundo de la banca electrónica, la cantidad de dinero que se obtiene es muy considerable.

4.4.4. Spidering o Araña Web

Es una de las herramientas más potentes que hay en Internet actualmente. Una **Spider** funciona inspeccionando las páginas de un site automáticamente una por una, link por link, almacenando toda la información relevante para crear un registro de páginas, direcciones e-mail, metatags, datos de formularios, información sobre las direcciones URL, enlaces, … Así página a página. Toda esta información la manda al **Crawler** que es el programa que almacena la información y la analiza.

Después esta base de datos va actualizando su información con el Spyder y el uso que le demos…. SI SI, ES EL MÉTODO DE GOOGLE

Un ejemplo de esto lo tenemos en:

- WebScarab
- FOCA
- Wget

4.4.5. KeyLogger

Es una técnica que consiste en almacenar las pulsaciones de teclado y enviar esta información al pirata. Puede residir en el sistema operativo del equipo, en el nivel de API de teclado, en la memoria o en el propio nivel del kernel. Pueden ser difíciles de detectar, ya que no provocan problemas en el equipo, ni los ralentizan.

Lo mejor es tener actualizado el sistema operativo, el software y navegadores con los últimos parches y un buen programa antispyware. Os recomiendo soluciones como **Spybot** y **Malwarebytes**.

4.4.5. Password Spray

Este ataque consiste en probar de forma desatendida, mediante software, la misma contraseña en un gran número de nombres de usuario. Se utilizan contraseñas simples de teclear y recordar.

4.5. El análisis forense

El **Análisis Forense Informático** abarca todas las técnicas pensadas para extraer la información de cualquier soporte sin alterar su estado, lo que nos permite buscar datos ocultos, dañados o eliminados. Este es un campo muy en boga, pues cada vez más esta información puede ser una prueba determinante en un proceso judicial.

Las fases de este análisis son:

1. Identificar el crimen cibernético
2. Recolectar evidencia preliminar.
3. Obtener una orden judicial para un allanamiento (Si es requerido).
4. Incautar las pruebas de la escena del crimen. Es importante realizar el reconocimiento técnico a cada evidencia, digital y/o física, el cual permite hacer una descripción detallada del material recibido, individualizando sus características físicas particulares, como marca, modelo, serial y otras que permitan particularizar la pieza en estudio.

5. Trasladar la evidencia a un laboratorio forense.
6. Crear copias bit a bit de la evidencia
7. Generar un valor de comprobación de la imagen, ejemplo un Hash MD5
8. Almacenar la información o evidencia original en una locación segura.
9. Analizar la copia de la imagen en búsqueda de evidencia.
10. Preparar un reporte forense.
11. Enviar el reporte al cliente.
12. Si es requerido, acudir a una corte como testigo experto.

Vamos a suponer un caso real. Estamos en la escena del crimen con un caso de pornografía infantil. Lo primero que haremos será desconectar el disco duro del PC y conectar a un dispositivo de bloque de escritura de hardware. El objetivo es que sea imposible alterar el contenido de este al mismo tiempo. Así podemos capturar y previsualizar el contenido del disco.

Lo segundo es realizar una copia exacta del disco, para asi poder trabajar con ella sin modificar la evidencia. La copia se puede realizar con herramientas como *FTK Imager*, *Live RAM Capturer* y *Disk2vhd* de Microsoft. Para los correos electrónicos podemos utilizar *EDB Viewer, Mail Viewer o MBOX Viewer*.

Los usuarios y claves los podemos obtener con *Disk Arbitratos, Volafox y ChainBreaker*.

Para el análisis de Internet tenemos *Dumpzilla*, *Chrome Session Parser*, *IEPassView*, *OperaPassView* y *Web Page Saber*.Todas estas herramientas son para tener nuestra propia "caja de herramientas forense".

Tenemos grandes empresas que comercializan potentes herramientas forenses:

- BlackLight
- MacQuisition
- E-Discovery
- EnCase Forensic Software
- Magnet Forensics
- X-Ways
- CERT Triage Tools
- Disk Drill

Pero esto solo es el principio. A continuación, os adjunto una tabla con más herramientas que se utilizan en este mundo clasificadas según su campo de uso.

Campo de uso	Herramientas
Red	• TCPDump • NetworkMiner • Network Appliance Forensic Toolkit • WireShark • Xplico • Splunk • Snort
Cifrado	• PGP • GNG4Win
Editores	• WinHEX • GHEX
Recuperación de archivos	• Raid Reconstructor • Raid Recovery • NTFS Recovery • FAT Recovery • Linux Recovery • Recuva • CNW Recovery • Rstudio • FreeRecover • Internet Evidence Finder • Bulk_extractor
Borrado de Archivos	• Wipe • HardWipe
Recuperación de contraseñas	• Ntpwedit • John The Ripper • Ntpasswd • Cain & Abel
Suites de herramientas estándar	• Sleuth Kit • Encare Forensic • OSForensics • Forensic Toolkit • Digital Forensic Framework

Análisis de discos	• Smart • ILook • ImDisk • Daemon Tools • PassMark OSFMount • LiveView • MountImagePro • PhotoRec
Clonación	• Ghosts • Acronis • Dc3dd
Análisis de Memoria RAM	• RedLine • FTK Imager • Proccess Dumper • Dumplt • Volatility
Sistema de Archivos	• AnalyzeMFT • MFT Extractor • MFT Tools • MFT_Parser
Análisis del Registro de Windows	• RegRipper • WRR • Shellbag Forensics
Distribuciones LiveDVD	• Backtrack • Kali • CAINE • DEFT • MATRIUX • BUGTRAQ

Tabla: Herramientas de Análisis Forense

Recursos y enlaces

Integridad Linux y Windows. MD5SUM

Objetivo: En esta práctica vamos a aprender a comprobar la integridad de un archivo iso descargado mediante el uso de MD5SUM.

- https://youtu.be/T2H7pOcLkx4

Contraseñas Linux. Ataque Contraseña John The Ripper

Objetivo: En esta práctica vamos a repasar dónde se encuentran los usuarios y las contraseñas de Linux. También veremos cómo realizar un ataque de diccionario.

- https://youtu.be/1BcHHJo0jvA

Directivas Contraseñas Windows 10

Objetivo: En esta práctica vamos a configurar la directiva de contraseñas en un sistema operativo Windows 10.

- https://youtu.be/6eA16KkOmMw

Seguridad BIOS

Objetivo: En esta práctica vas a ver cómo podemos configurar una BIOS estándar para asignarle una contraseña.

- https://youtu.be/XwYEvswMo4g

Contraseña en Arranque. Grub2

Objetivo: Aprenderás a instalar el gestor de arranque Grub2 y a configurar una contraseña segura para iniciar el sistema operativo Kali.

- https://youtu.be/xPkLpY-KHNY

Recuperar Ficheros en Linux. Software Foremost

Objetivo: Aprenderás a recuperar ficheros que has borrado accidentalmente en entornos Linux.

- https://youtu.be/j9aT3glMX6o

Recuperar ficheros en Windows. Recuva

Objetivo: En la siguiente práctica vamos a recuperar información perdida en entorno Windows y en el OneDrive de Linkia FP.

- https://youtu.be/ThU1uTQD2hM

Keylogger y Antimalware. MalwareBytes

Objetivo: Instalaremos un software de detección de pulsaciones, Keylogger, y lo detectaremos con un Antimalware.

- https://youtu.be/fXAZk7ff06Q
- https://youtu.be/GRY60gFV8Pw

- Incibe https://www.incibe.es/

- Análisis Forense https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_guia_analisis_forense_sci.pdf

- Análisis Forense http://www.elladodelmal.com/2018/01/tecnicas-de-analisis-forense.html

- Hydra https://github.com/vanhauser-thc/thc-hydra

- El Robot de Google https://support.google.com/webmasters/answer/182072?hl=es

Test de autoevaluación

1. Si quiero buscar en internet un programa para saber qué pulsa en el teclado mi compañero de trabajo, estoy buscando:
   a) Ataque Fuerza Bruta
   b) KeyLogger
   c) SNORT
   d) Spyder

2. Si estoy en Ubuntu y quiero saber el listado de usuarios de un ordenador, editaré el archivo:
   a) /etc/passwd
   b) /etc/shadow
   c) /etc/fstab
   d) /etc/mtab

3. No quiero que puedan arrancar el servidor con un Live-DVD, donde debo impedir que entren mediante contraseña:
   a) Boot Manager
   b) SAM
   c) BIOS
   d) UAC

4. Cuál de las siguientes distribuciones de Linux está orientada para la Seguridad Informática:
   a) SUSE
   b) Gnome
   c) Ubuntu
   d) Kali

Solucionarios

Test de autoevaluación tema 4

1. Si quiero buscar en internet un programa para saber qué pulsa en el teclado mi compañero de trabajo, estoy buscando:
   a) Ataque Fuerza Bruta
   b) KeyLogger
   c) SNORT
   d) Spyder

2. Si estoy en Ubuntu y quiero saber el listado de usuarios de un ordenador, editaré el archivo:
   a) /etc/passwd
   b) /etc/shadow
   c) /etc/fstab
   d) /etc/mtab

3. No quiero que puedan arrancar el servidor con un Live-DVD, donde debo impedir que entren mediante contraseña:
   a) Boot Manager
   b) SAM
   c) **BIOS**
   d) UAC

4. Cuál de las siguientes distribuciones de Linux está orientada para la Seguridad Informática:
   a) SUSE
   b) Gnome
   c) Ubuntu
   d) **Kali**