DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

TEMA: APLICACIÓN DE LA TÉCNICA HACKING – PASSWORD CRACKING EN PLATAFORMAS WINDOWS

AUTOR: VALVERDE VEGA MARCELO FERNANDO
NOBOA CASTILLO ERICK GABRIEL

DIRECTOR: ING. FERNANDO SOLÍS

SANGOLQUÍ
AGOSTO 2015

CERTIFICADO

Ing. Fernando Solís

CERTIFICA

Que el trabajo titulado "APLICACIÓN DE LA TÉCNICA HACKING – PASSWORD CRACKING EN PLATAFORMAS WINDOWS" realizado por los Srs. VALVERDE VEGA FERNANDO MARCELO y NOBOA GABRIEL ERICK, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la Universidad de las Fuerzas Armadas "ESPE".

Sangolquí, Agosto 2015

Ing. Fernando Solis
DIRECTOR

DECLARACIÓN DE RESPONSABILIDAD

VALVERDE VEGA FERNANDO MARCELO
NOBOA CASTILLO ERICK GABRIEL

DECLARO QUE:

El proyecto de grado denominado "APLICACIÓN DE LA TÉCNICA HACKING – PASSWORD CRACKING EN PLATAFORMAS WINDOWS", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Agosto 2015

Valverde Vega Marcelo Fernando

Noboa Castillo Erick Gabriel

AUTORIZACIÓN

Nosotros, VALVERDE VEGA MARCELO FERNANDO
NOBOA CASTILLO ERICK GABRIEL

Autorizamos a la UNIVERSIDAD DE LA FUERZAS ARMANDAS "ESPE", la publicación, en la biblioteca virtual de la Institución del trabajo "APLICACIÓN DE LA TÉCNICA HACKING – PASSWORD CRACKING EN PLATAFORMAS WINDOWS", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Agosto 2015

Valverde Vega Marcelo Fernando

Noboa Castillo Erick Gabriel

DEDICATORIA

A Dios por brindarme todos los recursos necesarios para terminar mis estudios, por fortalecerme y por llenarme de muchas bendiciones, siendo así un apoyo incondicional ya que sin Él no hubiera logrado este sueño tan anhelado de ser ingeniero.

Con mucho cariño, agradezco a mis padres Nelson y Rocío que me dieron la vida y me han apoyado en todo momento, por todos sus consejos y valores que hicieron de mí una gran persona y sobre todo por haberme dado la oportunidad de seguir una carrera para mi futuro y por haber creído en mí, infinitamente gracias papá y mamá. Este proyecto se los dedico a ustedes, este es el resultado de todo el esfuerzo que depositaron en mí, espero lograr hacerles sentir orgullosos y no defraudarlos, así como ustedes no lo hicieron conmigo. A mis hermanos Paola, Nelson Fernando, Erika, gracias por su apoyo incondicional y por estar siempre conmigo, los quiero mucho.

A mi futura esposa Diana Robles quien me apoyó en todo momento sobre todo en los más difíciles y me dio fuerzas para seguir adelante y cumplir este objetivo en mi vida, gracias por todo, te amo mi amor.

Erick Gabriel Noboa Castillo

Gracias a Dios por darme salud y vida para culminar mis estudios, y permitirme vivir este logro tan anhelado de ser ingeniero, con todo mi corazón agradezco a mis padres Marcelo e Isabel que siempre me guiaron por el camino correcto dándome consejos y valores para ser una persona de bien, por su infinito apoyo que me brindaron para alcanzar este sueño, a mi hermana Gabriela que siempre ha sido un ejemplo para mí, dándome fuerza y valor para seguir adelante con mis sueños y lograr mis metas. Gracias por todo les amo.

Marcelo Fernando Valverde Vega

AGRADECIMIENTOS

Agradecemos a todos y cada uno de los maestros que nos supieron guiar por el camino del conocimiento en toda esta etapa de estudio, ya que con su experiencia y profesionalismo han formado en nosotros buenas personas con carácter competitivo y con orientación de vanguardia. Sin su aporte y sus consejos no hubiéramos podido lograr esta objetivo en nuestras vidas; agradecemos de manera especial a nuestro director de tesis, ingeniero Fernando Solís quien nos ayudó durante todo el desarrollo, exigiendo lo mejor de nosotros para poder concluir con los objetivos planteados. Además, no podemos dejar de mencionar y agradecer al Director de Carrera, ingeniero Mauricio Campaña, quien contribuyó con su experiencia a nuestro trabajo y al personal de la empresa López Torres Industrial S.A quienes fueron partícipes de este proyecto.

Gracias por su ayuda, apoyo, orientación y sobre todo comprensión, los cuales nos brindaron durante el desarrollo de este trabajo.

ÍNDICE DE CONTENIDOS

CERTIFICADO i
DECLARACIÓN DE RESPONSABILIDAD ii
AUTORIZACIÓN iii
DEDICATORIA iv
AGRADECIMIENTOS v
ÍNDICE DE FIGURAS x
ÍNDICE DE TABLAS xii
RESUMEN xiii
ABSTRACT xiv
1. CAPÍTULO 1 1
INTRODUCCIÓN 1
1.1 Antecedentes 1
1.2 Planteamiento del problema 2
1.3 Objetivos 3
1.3.1 Objetivo General 3
1.3.2 Objetivos Específicos 3
1.4 Justificación 3
1.5 Alcance 4
1.6 Factibilidad 5
1.6.1 Factibilidad Técnica 5
1.6.2 Factibilidad Operativa 5
2. CAPÍTULO 2 6

MARCO TEÓRICO 6
2.1 Seguridad de la Información.....6
2.1.1 Objetivo de la seguridad informática 7
2.1.2 Importancia de la seguridad informática.....7
2.1.3 Principios de la seguridad informática 8
2.1.4 Características de seguridad informática.....9
2.1.5 Formas de Autenticación.....9
2.1.6 Características para crear contraseñas seguras 10
2.1.7 Norma ISO 27001 del Sistema de Gestión de la Información.....12
2.1.8 Ciberseguridad.....13
2.2 Informática Forense 14
2.2.1 Definición de la Informática Forense 14
2.2.2 Objetivos de la Informática Forense 14
2.2.3 Proceso de la Informática Forense.....15
2.3 Criptografía 15
2.3.1 Objetivo de la Criptografía.....15
2.3.2 Tipos de Criptografías 16
2.3.2.1 Tablas Hash.....16
2.3.2.2 Cifrado simétrico 18
2.3.2.3 Cifrado asimétrico 20
2.3.2.4 Cifrado híbrido 23
2.3.3 Criptoanálisis 24
2.3.4 Objetivo del Criptoanálisis.....24

2.4 Organización y almacenamiento de las contraseñas en el Sistema Operativo Windows....25
2.4.1 Sistema operativo....25
2.4.2 El Sistema Operativo como una Interfaz de Usuario....26
2.4.3 Windows....27
2.4.3.1 Registro de Windows....28
2.4.3.2 Autenticación en Windows....29
Autenticación NTML....31
Protocolo de autenticación NTML....31
Kerberos....32
2.4.3.3 SAM (Administrador de cuentas de seguridad)....33
2.4.3.4 Sistema de encriptación de datos de Windows....36
Cifrado de datos con EFS....36
Cifrado de datos con BitLocker....38
2.5 System Hacking....39
2.5.1 Objetivos de System Hacking....39
2.5.2 Metodología Hacking....40
2.5.3 Password Cracking....41
2.5.4 Herramientas para descifrar contraseñas....43
2.5.4.1 L0phcrack....43
2.5.4.2 Cain & Abel....44
3. CAPÍTULO 3....45
DESARROLLO....45
3.1 Introducción....45

3.2 Técnicas hacking de password cracking 45
3.2.1 Ataque Diccionario 46
3.2.2 Ataque de Fuerza Bruta 46
3.2.3 Ataque Híbrido 46
3.3 Herramienta utilizada para extraer el log de windows 47
3.3.1 Live CD 47
3.3.2 Características de Live CD 48
3.3.3 Para qué se utiliza y aplica Live CD 48
3.3.4 Cómo crear un Live CD en Windows 49
3.4 Recuperación de la contraseña de una cuenta registrada en el Sistema Operativo Windows 53
3.4.1 Obtener del Log de Windows 53
3.4.2 Uso de L0phcrack para obtener la clave del usuario 55
3.4.3 Uso de Cain & Abel para obtener la clave del usuario 62
3.4.3.1 Cargar los usuarios del log 62
3.4.3.2 Ejecutar para obtener la contraseña de los usuarios 65
3.4.4 Análisis de las herramientas utilizadas 68
3.4.5 Uso de LiveCD de Linux Mint para setear contraseñas Windows 69
4. CAPÍTULO 4 72
CONCLUSIONES Y RECOMENDACIONES 72
4.1 Conclusiones 72
4.2 Recomendaciones 73
BIBLIOGRAFÍA Y WEBGRAFÍA 74

ÍNDICE DE FIGURAS

Figura 1 Seguridad de la información 6
Figura 2 Modelo de gobierno y gestión de las TIC con normas ISO 11
Figura 3 Sistema de Gestión de la Seguridad de la Información ISO 27001 12
Figura 4 Cifrado Simétrico 18
Figura 5 Cifrado Asimétrico 20
Figura 6 Niveles y vistas de un sistema informático 26
Figura 7 Logo de Windows 27
Figura 8 Ruta de acceso al registro de Windows 29
Figura 9 Autenticación de seguridad en Windows 33
Figura 10 SID del usuario marcelo 34
Figura 11 Metodología Hacking 40
Figura 12 Password Cracking 41
Figura 13 Herramienta L0phcrack 43
Figura 14 Herramienta Caín & Abel 44
Figura 15 Herramienta USB Installer 50
Figura 16 Herramienta UNetbottin 51
Figura 17 Linux Live USB Creator 53
Figura 18 Menú de Booteo 54
Figura 19 Ubicación del archivo SAM y SYSTEM 54
Figura 20 Herramienta L0phcrack primer paso 55
Figura 21 Herramienta L0phcrack segundo paso 56
Figura 22 Herramienta L0phcrack tercer paso 56
Figura 23 Herramienta L0phcrack cuarto paso 57
Figura 24 Herramienta L0phcrack quinto paso 58
Figura 25 Ubicación del archivo SAM 58
Figura 26 Ubicación del archivo SYSTEM 59
Figura 27 Usuarios cargados desde un log 59
Figura 28 Configuración de L0phcrack 60

Figura 29 Barra de herramientas de L0phcrack 60
Figura 30 Clave recuperada con L0phcrack.....61
Figura 31 Herramienta Cain & Abel 62
Figura 32 Ingreso del archivo SAM.....63
Figura 33 Ingreso del archivo SYSTEM.....63
Figura 34 Archivos SAM y SYSTEM ingresados.....64
Figura 35 Visualización de los usuarios del log ingresado 64
Figura 36 Selección de la técnica Password Cracking.....65
Figura 37 Configuración para iniciar análisis con Cain & Abel 66
Figura 38 Inicio del análisis para recuperar la contraseña 66
Figura 39 Resultado del análisis con Caín & Abel 67
Figura 40 Contraseñas recuperadas de los usuarios con Caín y Abel 68
Figura 41 Menú de booteo del equipo.....69
Figura 42 Ingreso del comando de instalación de chtpw.....69
Figura 43 Instalación de chntpw 70
Figura 44 Ejecución del comando para cambiar la contraseña 70
Figura 45 Selección de la opción que se desea ejecutar 71

ÍNDICE DE TABLAS

Tabla 1 Comparación entre tecnologías de cifrado Windows.....39
Tabla 2 Comparación entre técnicas de Password Cracking 47
Tabla 3 Contraseñas recuperadas de los usuarios con Caín y Abel 67

RESUMEN

Este proyecto describe las técnicas y herramientas utilizadas para recuperar contraseñas mediante el tema “APLICACIÓN DE LA TÉCNICA HACKING – PASSWORD CRACKING EN PLATAFORMAS WINDOWS”. Este tema permitirá conocer las vulnerabilidades del sistema, así como las diferentes herramientas y aplicaciones para encontrar contraseñas perdidas u olvidadas de los usuarios registrados en los Sistemas Operativos Windows, el fin de ese proyecto es para la empresa López Torres Industrial S.A la cual va ayudar a sus empleados a buscar y encontrar las contraseñas en el caso de que no recuerden la misma, esto se logrará aplicando las técnicas hacking mediante la utilización de herramientas especializadas para recuperar claves o contraseñas, además se tomará en cuenta y se analizará el nivel de seguridad de la contraseña sea esta baja, media o alta y también el tamaño de la cual este compuesta para que el proceso sea eficiente y pueda recuperar en el tiempo más rápido. Este tema va apoyar a que los trabajadores se den cuenta si las contraseñas de sus equipos son vulnerables a los ataques de ciberdelicuentes y así tomar diversas precauciones frente a esto, ya sea instalando programas de seguridad, que puedan indicar si las contraseñas que están en sus equipos son las adecuadas para su seguridad, las diferentes aplicaciones indican si sus contraseñas son fuerte o débiles y vulnerables para cualquier tipo de ataque. Además nos va a permitir tener conocimiento para en un futuro proyecto implementar políticas de seguridad y buenas prácticas para llevar de una forma segura la contraseña y también sus sistemas informáticos.

PALABRAS CLAVES:

- **Password**
- **Hacking**
- **Cracking**
- **Técnicas**
- **Ataques**

ABSTRACT

This Project describes the techniques and tools used to recover passwords through the topic “Hacking Technique Application – Password Cracking in Windows Platforms”. This topic will allow knowing the vulnerabilities of the system, as well as the different applications to find lost or forgotten passwords from registered users in Windows Operative Systems; the purpose of that project is for the Lopez Torres Industrial S.A. enterprise; which will help their employees to search and find the passwords in case they don’t know it; this will be accomplished by the application of hacking techniques through the usage of specialized tools to retrieve keys or passwords, also the high or low level of security of the password will be analyzed as well as the size of it so the process will be efficient and could be recovered in fewer time. This topic will help the workers to realize if the passwords of their computers are vulnerable to the attacks of the cyber criminals and take action to prevent this by installing security programs that can tell them if their passwords are the ones needed for their security. The different applications show if their passwords are strong or weak and vulnerable for any attack. In addition, it will allow us to have a knowledge for a future project to implement security policies and best practices to manage in a safe way the passwords and their information systems.

KEYWORDS:

- **PASSWORD**
- **HACKING**
- **CRACKING**
- **TECHNIQUES**
- **ATTACKS**

1. CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

Las contraseñas son uno de los recursos más comunes empleados en la actualidad debido a los avances tecnológicos, principalmente son una forma de autentificación y acceso a los sistemas de un computador o dispositivo móvil e inclusive a documentos o archivos, con una considerable exigencia de seguridad por el mismo motivo que son portadores en mucho de los casos de información valiosa tanto de la empresa como personal.

Es muy importante la seguridad de la información, por este motivo se han creado métodos de cifrado de datos el cual resulta una de las mejoras y medidas al momento de evitar robos de información lo cual permite aumentar dicha seguridad por medio de la codificación de la información mencionada anteriormente, de tal manera que solo pueda leer la persona que disponga de una clave de cifrado adecuada para descodificarlo. El cifrado de la información se remonta hace miles de años atrás mediante la criptografía, como es el caso de los métodos de cifrado que usan papel y lápiz, o quizás ayuda mecánica sencilla.

A comienzos del siglo XX, la creación de máquinas mecánicas y electromecánicas complejas, como por ejemplo la máquina de rotores Enigma, proporcionaron métodos de cifrado más complejos y eficientes. La evolución de la criptografía ha seguido de la mano de la evolución del criptoanálisis que hace referencia al arte de romper los códigos y los cifrados, posteriormente a la

introducción de la electrónica y la computación que ha permitido sistemas elaborados que utilizan el criptoanálisis para descifrar contraseñas complejas.

Así mismo, existen problemas de seguridad por lo cual muchas de las veces existen vulnerabilidades y pueden ser aprovechadas en algunos casos por ciberdelincuentes para cometer delitos informáticos, uno de los problemas ya conocidos es emplear contraseñas con un grado de seguridad muy débil supuestamente para recordar fácilmente, pero así mismo existen sistemas que pueden valorar si las contraseñas son fuertes o muy seguras donde se emplean caracteres alfa numéricos, esto puede llevar al usuario a olvidar dicha contraseña ya sea por su complejidad o dimensión.

Estos son problemas con los cuales nos encontramos diariamente en una empresa por lo tanto es importante buscar soluciones mediante métodos y técnicas que permitan descifrar o recuperar las contraseñas de manera que no se ocasione daños al sistema operativo o a la computadora y que se optimice recursos como tiempo y dinero con la utilización de software especializado.

1.2 Planteamiento del problema

Con el avance de la tecnología existe un aumento simbólico en el uso de ordenadores por lo que esto ha generado importancia en la seguridad de la información lo cual conlleva a la utilización y manejo de contraseñas con más rigurosidad para salvaguardar la información, en estos casos existen organizaciones, instituciones o empresas que no siguen políticas o normas para la creación o manejo de contraseñas en los Sistemas Operativos, tal es el caso de la empresa López Torres Industrial S.A en la cual no existen dichas normas de seguridad por lo que esto causa vulnerabilidad de la información de cada usuario y en mucho de los casos perdida u olvido de las contraseñas por no

llevar de forma ordenada y organizada, estos son temas muy importantes que hay que tratarlos por el mismo hecho que hay que considerar la información valiosa que maneja la empresa y lo cual fue parte de nuestro estudio en esta tesis.

1.3 Objetivos

1.3.1 Objetivo General

Utilizar la Técnica Hacking de Password Cracking mediante el uso de herramientas para encontrar las vulnerabilidades en los sistemas operativos Windows y recuperar la contraseña de una cuenta de usuario de la Empresa López Torres Industrial S.A.

1.3.2 Objetivos Específicos

- Describir la organización y almacenamiento de las contraseñas en el sistema operativo Windows.
- Describir las principales técnicas de Password Cracking.
- Utilizar herramientas Hacking para realizar Password Cracking.

1.4 Justificación

La tecnología de la información es uno de los recursos que juega un papel crecientemente estratégico y es muy importante dentro y fuera de las organizaciones, las cuales establecen cada vez más su competitividad y adaptación a los cambios en el medio de los ordenadores, los mismos que llevan consigo sistemas de información con nuevas características y funciones.

Debido a las mejoras que se han dado en las seguridades de la información y a los problemas que conlleva el manejo de contraseñas, se vió la necesidad de aplicar las técnicas de “Password Cracking” siguiendo varios pasos de la metodología hacking que permita recuperar las contraseñas de los usuarios que se encuentran registrados en el sistema operativo Windows y así también poder identificar las características y vulnerabilidades de dichas contraseñas.

Tomando en cuenta las consideraciones previas, se plantea una solución basada en herramientas tecnológicas para descifrar claves de los usuarios, lo cual permitirá la recuperación de la misma de una manera rápida, si en un caso la clave es débil se la puede recuperar fácilmente, pero por lo general, si esta es creada con estándares y normas de seguridad para que no pueda ser descifrada con facilidad por personas que desean conseguir información, entonces la recuperación de la contraseña lleva más tiempo y se torna más difícil.

La decisión de aplicar técnicas Password Cracking se toma por el gran auge de la actividad electrónica y por tanto aumento significativo de información, y en vista de esto el crecimiento de las seguridades de la información las cuales exigen seguir normas y estándares para la creación de contraseñas por lo cual para los usuarios se torna más complejo el manejo de la misma y tienden a olvidarse.

1.5 Alcance

- Organización y almacenamiento de contraseñas en los sistemas operativos Windows.

- Aplicación de técnicas de Password Cracking:
  - Ataque Diccionario

- Ataque de Fuerza Bruta
- Ataque Híbrido

- Uso de herramientas Hacking.
  - L0phcrack
  - Caín & Abel

Mediante el estudio y análisis de los temas mencionados anteriormente, se obtendrá la contraseña registrada en el log de Windows.

1.6 Factibilidad

1.6.1 Factibilidad Técnica

Utilizar Password Cracking en la empresa nos puede ayudar a recuperar claves olvidadas de los sistemas operativos, así como también para darnos cuenta si las claves que son ingresadas por los usuarios son débiles o fuertes. Poder limitar el acceso al sistema operativo a personal no autorizado y mantener la confidencialidad e integridad de la información.

1.6.2 Factibilidad Operativa

Mediante la aplicación de las técnicas Password Cracking y la utilización de herramientas tecnológicas especializadas en obtener claves se recupera la contraseña de la cuenta de usuario registrado en el sistema operativo Windows con la disponibilidad de los recursos necesarios como computadores que se encuentran operativos y acceso a información de la empresa auspiciante, por lo tanto no existe ninguna limitación real que pueda impedir la normal realización del proyecto encaminado a la solución del problema planteado.

2. CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la Información

La Seguridad de la Información consiste y hace referencia a la protección de cualquier amenaza para salvaguardar los activos fijos y en especial toda información de la cual está basada la continuidad de las operaciones de la empresa sean estas ocasionadas dentro o fuera de la misma, con esto se lograría disminuir los daños y perjuicios que estas amenazas causaría a la organización y a la vez aumentar las oportunidades de servicio hacia otras empresas.

"Seguridad de los Sistemas de Información consiste en la protección de protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso o tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas." (Romero, 2012)

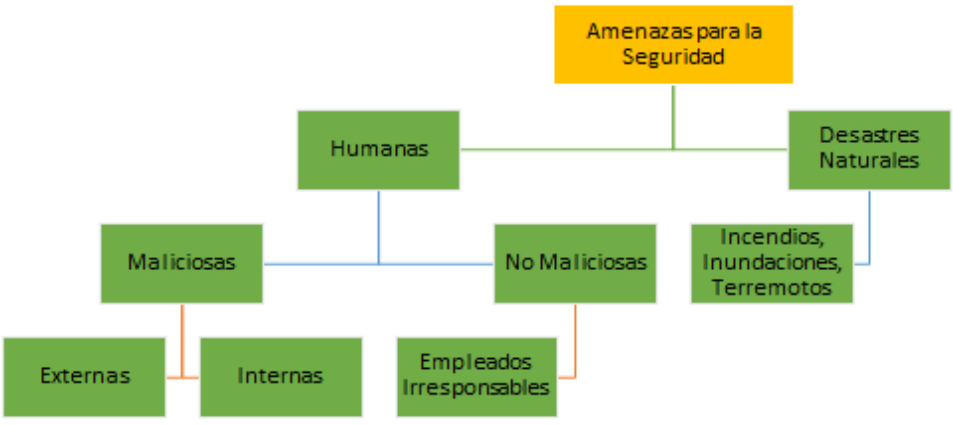

Figura 1 Seguridad de la información

Fuente: (Prandini)

La Seguridad de la información se consigue mediante la implementación de controles efectivos, que pueden ser normas, manual de funciones, buenas prácticas, procedimientos, estructuras organizativas, funciones de software y hardware, planes de contingencia y herramientas que se encargan de proteger la privacidad e integridad de la información que se almacena en un sistema informático. Estos controles necesitan continuamente ser establecidos, monitoreados, revisados y mejorados en donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad en cada área de negocio de la organización.

2.1.1 Objetivo de la seguridad informática

En la seguridad de la información sabiendo que dichos procesos de seguridad permiten proteger el recurso más importante y valioso de una organización, partiendo como principio fundamental los procesos de aseguramiento

El objetivo del proceso de seguridad informática es obtener un nivel aceptable de seguridad, ya que la información es lo más valioso que tiene una institución o empresa, por lo tanto esta debe ser protegida para que no sea vulnerable y utilizada para fines maliciosos.

2.1.2 Importancia de la seguridad informática

En la actualidad, las empresas u organizaciones están ligadas y apoyadas por información y procesos mediante los sistemas y redes que son activos de una gran importancia para las mismas, por lo tanto es necesario limitar,

optimizar, conservar, implementar y ejecutar la seguridad de información los cuales pueden ser fundamentales para certificar competitividad.

Cada vez más, las empresas y sus sistemas de información están expuestas a un sin número de riesgos y vulnerabilidades de seguridad como fraudes establecidos en la informática, ingeniería social, vandalismo, sabotaje, terrorismo y así también de desastres naturales.

Ciertos orígenes de los riesgos como: virus informáticos, negación de servicios y ataques de intrusión cada día se están volviendo más frecuentes y sofisticados los cuales arremeten a los sistemas de información para sacar provecho de las vulnerabilidades que pueden tener y así poder espiar, robar o extraer información de la empresa.

Toda empresa ya sea pública o privada independientemente del tipo del negocio tienen presente la importancia de la seguridad de la información donde pueden contar con una protección adecuada la misma que puede salvaguardar las infraestructuras críticas del negocio.

Desde el afianzamiento del internet como medio de interconexión y de la demanda de tecnología, existen dos elementos que incrementan la importancia de brindar una adecuada seguridad de la información: la importancia del crecimiento de la información y el aumento de los riesgos a la que la misma se ve expuesta.

2.1.3 Principios de la seguridad informática

- **Confidencialidad:** Los datos solo deben ser conocidos y accedidos por quienes estén autorizados durante su almacenamiento, procesamiento o

trasmisión. Verificar y certificar que solo los usuarios con accesos autorizados puedan acceder a la información. (Morales, 2013)

- **Integridad:** Los datos solo pueden ser modificados y eliminados por quienes estén autorizados para ello, es decir los sistemas y aplicaciones solo deben ser operados por personal autorizado. (Morales, 2013)

- **Disponibilidad:** Los sistemas que almacenan datos e información deben garantizar su acceso, cuando así se requiera, por quienes tengan derecho a ello. (Morales, 2013)

2.1.4 Características de seguridad informática

- **Control:** Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

- **Autenticidad:** Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

- **No Repudio:** Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

- **Auditoria:** Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

2.1.5 Formas de Autenticación

- **Contraseña:** Una contraseña es un tipo de seguridad informática, ya que es una serie de caracteres secretos que permiten a un usuario tener

acceso a un archivo, ordenador o programa y negar el acceso a usuarios no autorizados. (Martínez, 2011)

- **Certificado digital:** Es un tipo de seguridad informática que permite la firma digital electrónica que garantiza técnica y legalmente la identidad de una persona en Internet. (Martínez, 2011)

- **Autenticación HTTP:** Tipo de seguridad informática que delega la autenticación de usuarios a un servidor a través de Kerberos. (Martínez, 2011)

2.1.6 Características para crear contraseñas seguras

- Hacer contraseñas difíciles de adivinar mediante el uso de ocho a doce caracteres alfanuméricos, con una combinación de caracteres que pueden ser entre símbolos, números, letras minúsculas y letras mayúsculas. (Inteco, 2011)

- Snowden señala una nueva recomendación la cual dice que la contraseña debe ser una frase que sea familiar y fácil de recordar para el usuario pero difícil para el atacante. Por ejemplo 'maribelguardiaes110%SEXY' (Maribel Guardia es 110% sexy).

- Garantizar que las aplicaciones no almacenen las contraseñas en la memoria ni se escriban en el disco. Si las contraseñas se almacenan en la memoria las contraseñas pueden ser robadas. (Inteco, 2011)

- Nunca utilice información personal como contraseñas, por ejemplo: fecha de nacimiento de tus familiares incluso la tuya, la fecha de matrimonio, los nombres de tus familiares o de tus mascotas. (Inteco, 2011)

Dentro de todo lo que hace referencia la Seguridad de la Información existen estándares o normas que nos ayudan a analizar minuciosamente los riegos y vulnerabilidades de los sistemas de información mediante el sistema de gestión de la seguridad de información en los procesos de negocio y servicios de la Tecnología de Información (TI), dichas normas detallamos a continuación, en la Figura 2.

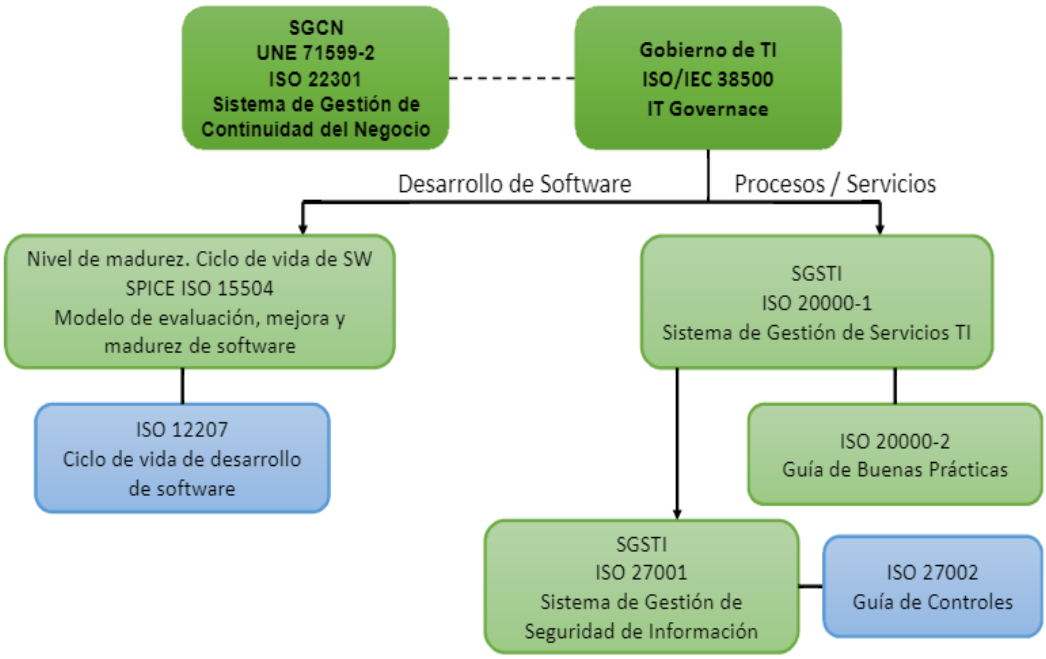

Figura 2 Modelo de gobierno y gestión de las TIC con normas ISO

Fuente: (Fernandéz, 2012)

2.1.7 Norma ISO 27001 del Sistema de Gestión de la Información

La norma/estándar UNE ISO/IEC 27001:2007 del “Sistema de Gestión de la Seguridad de la Información” es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. (Fernandez, 2012). Ver Figura 3.

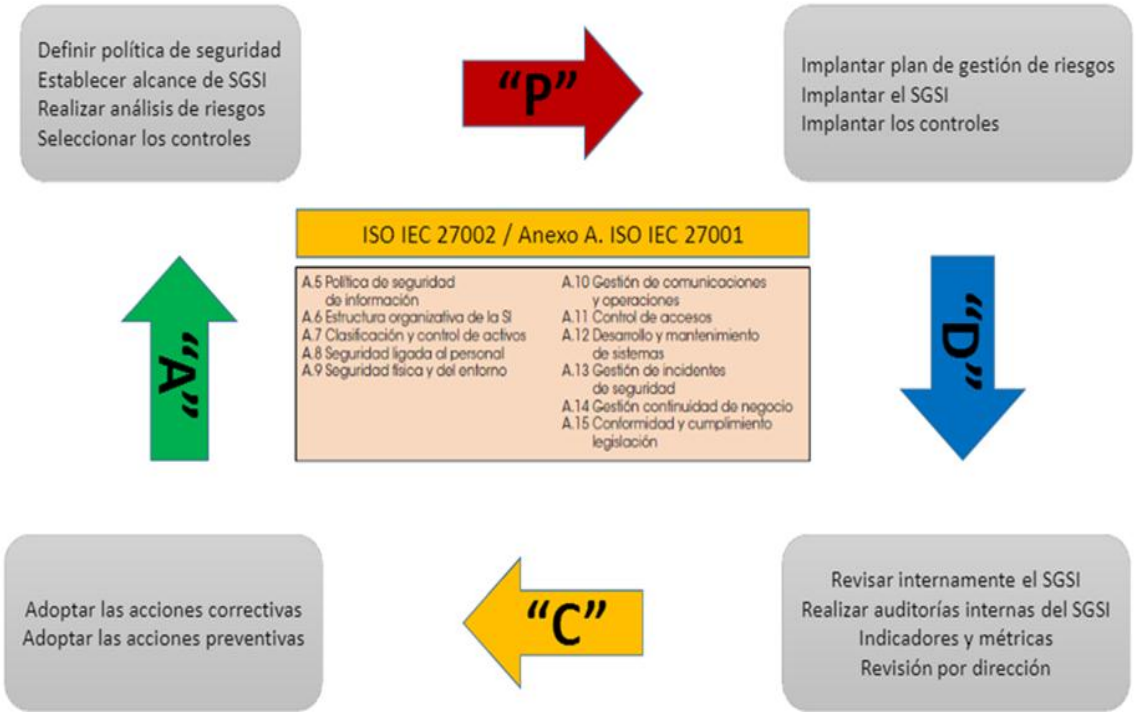

Figura 3 Sistema de Gestión de la Seguridad de la Información ISO 27001
Fuente: (Fernandez, 2012)

El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001:2007, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Panificar- Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés PDCA (Plan- DO-Check-Act) (similar a la más extendida y reconocida norma ISO 9001). (Fernandez, 2012)

La piedra angular de este sistema SGSI-ISO 27001 es el análisis y gestión de los riesgos basados en los procesos de negocio/servicios de TI (por ejemplo, CRM, ERP, Business Intelligence, redes sociales, movilidad, cloud computing, servicios externalizados, etc.). (Fernandez, 2012)

2.1.8 Ciberseguridad

Con los avances tecnológicos y la demanda que ha causado en ello, existe un elevado índice de información personal y empresarial que circula y se mantiene en la red por la utilización del internet, esto permite que toda información quede expuesta a cualquier ataque de ciberdelincuentes los cuales buscan la manera de vulnerar cualquier sistema para espiar, robar información o hacer daño de cualquier tipo por lo que se ha visto la necesidad de tomar medidas de seguridad para salvaguardar la información ya que es muy importante.

Para prevenir estas situaciones que ninguna persona u organización quisiera llegar a tener, se ha desarrollado la ciberseguridad que ha sido utilizado para que de alguna manera ésta ayude a implementar.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de

riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. (UIT, 2010)

2.2 Informática Forense

2.2.1 Definición de la Informática Forense

La Informática Forense es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada. (López, 2012)

2.2.2 Objetivos de la Informática Forense

Según Laidy García la informática forense tiene 3 objetivos, a saber:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

2.2.3 Proceso de la Informática Forense

- Identificar las posibles fuentes disponibles
- Recoger diferentes tipos de evidencias
- Analizar las evidencias encontradas
- Confirmar por pruebas cruzadas

Así se establecen las bases para Probar que se han cometido actos deshonestos o ilegales

2.3 Criptografía

La Criptografía también llamada “escritura oculta”, tradicionalmente en el ámbito de criptografía es donde se ocupan las técnicas de cifrado o codificación que permiten alterar el contenido de cierta información o mensajes con el fin de hacerlos ininteligibles a receptores o personas no autorizas.

En general, la criptografía es el arte de escribir con clave secreta o de un modo enigmático, de modo más específico, es la creación de técnicas para el cifrado de datos. (Sánchez, 2014)

2.3.1 Objetivo de la Criptografía

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. (Barzanallana, 2014)

2.3.2 Tipos de Criptografías

2.3.2.1 Tablas Hash

Los hash o funciones de resumen, también conocidos como tablas hash, son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). (Gutiérrez, 2013)

Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varias funciones, entre ellos está asegurar que no sea modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento. (Gutiérrez, 2013)

Características de los Hash

- Las funciones hash se encargan de representar de forma compacta un archivo o conjunto de datos.

- Este sistema de criptografía usa algoritmos que aseguran que con la respuesta (o hash) nunca se podrá saber cuáles han sido los datos insertados, lo que indica que es una función unidireccional. Sabiendo que se puede generar cualquier resumen a partir de cualquier dato nos podemos preguntar si se podrían repetir estos resúmenes (hash) y la respuesta es que teóricamente si, podría haber colisiones, ya que no es fácil tener una función hash perfecta (que consiga que no se repita la respuesta), pero esto no es un problema, ya que si se consiguiera con un

buen algoritmo dos hash iguales los contenidos serían totalmente distintos. (Gutiérrez, 2013)

Las funciones Hash criptográficas típicamente producen valores Hash de 128 bits o más. El número de valores Hash diferentes que se obtienen, 2^128, es mucho más amplio que el número de mensajes diferentes que se pueden intercambiar en todo el mundo. (Borghello, 2009)

Tipos de algoritmos Hash

- **SHA-1 (Secure Hash Algorithm - Algoritmo seguro de Hash)**

  Es un algoritmo criptográfico de Hash publicado por el gobierno de los Estados Unidos. Genera un valor Hash de 160 bit a partir de una secuencia de longitud arbitraria.

  SHA-1 es considerado lo suficientemente seguro para aplicaciones prácticas, pero hay disponibles versiones más robustas, SHA-256, SHA-384 y SHA-512 que generan valores Hash de 256, 384 y 512 bits respectivamente, estas versiones reemplazaran a SHA-1 mientras se siga trabajando sobre ellas. (Borghello, 2009)

- **MD5 (Message Digest Algorithm - Algoritmo de resumen de mensaje)**

  El algoritmo MD5 se utiliza como una función de codificación o huella digital de un archivo. A menudo es empleado para codificar contraseñas en bases de datos, el MD5 es igualmente capaz de generar una huella de archivo para asegurar que no haya cambios en el mismo tras una

transferencia, por ejemplo. Un hash MD5 está compuesto por 32 caracteres hexadecimales.

El has que corresponde a la frase “esta es mi tesis” es 9b6477166949a2f5da4f230d17057989. (Borghello, 2009)

- **RIPEMD-160**

  Es una versión mejorada de RIPEMD, que estaba basado sobre los principios del diseño del algoritmo MD4, y es similar en seguridad y funcionamiento al más popular SHA-1, genera un Hash de 20 bytes (160 bits, de ahí su nombre). (Borghello, 2009)

2.3.2.2 Cifrado simétrico

El emisor cifra el mensaje con una clave, y esa misma clave deberá ser la utilizada para descifrarlo, como se puede apreciar en la Figura 4.

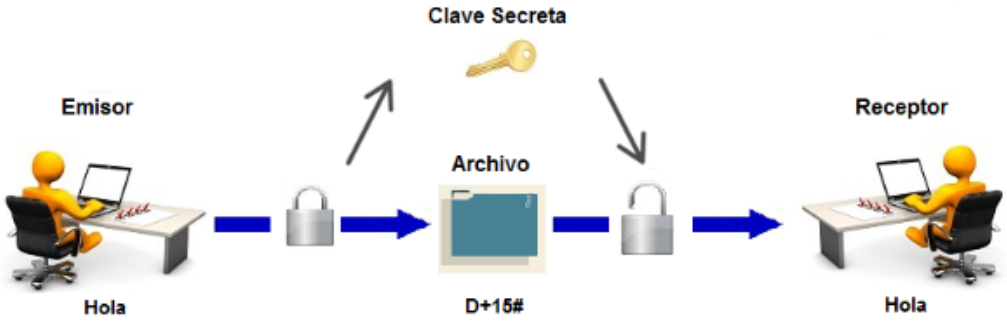

Figura 4 Cifrado Simétrico

Estos algoritmos son rápidos y permiten cifrar y descifrar eficientemente con claves relativamente grandes. (Martinez, 2009)

El problema que tienen es la seguridad de la clave:

- El emisor cifra el mensaje con la clave.
- Manda el mensaje cifrado, de forma que nadie puede descifrarlo sin esa clave.
- El receptor reconoce la clave y puede descifrar el mensaje con la misma clave de envió.

Algunos algoritmos de este tipo son:

- **RC5 (Cifrado de Rivest)**

  Se aplican operaciones XOR sobre los datos, pudiendo ser de 32, 64 o 128 bits. Permite diferentes longitudes de clave, y un número variable de iteraciones (la seguridad del cifrado aumenta exponencialmente cuanto mayor número de iteraciones), también funciona como un generador de número aleatorios, sumándoles a los bloques de texto rotados mediante la XOR. (Luz, 2010)

- **IDEA (International Data Encryption Algorithm)**

  Aplica una clave de 128 bits sin paridad a bloques de datos de 64 bits, y se usa tanto para cifrar como para descifrar.

  Se alteran los datos de entrada en una secuencia de iteraciones parametrizadas, con el objetivo de producir bloques de salida de texto cifrado de 64 bits. (Luz, 2010)
  Según numerosos expertos criptográficos, IDEA es el mejor algoritmo de cifrado de datos existente en la actualidad ya que existen 2 elevado a la 128 claves privadas que probar mediante el ataque de fuerza bruta. (Luz, 2010)

- **DES (Data Encryption Standard)**

  Su arquitectura está basada en un sistema monoalfabético, donde un algoritmo de cifrado aplica sucesivas permutaciones y sustituciones al texto en claro. En un primer momento la información de 64bits se somete a una permutación inicial, y a continuación se somete a una permutación con entrada de 8 bits, y otra de sustitución de entrada de 5 bits, todo ello constituido a través de un proceso con 16 etapas de cifrado. (Luz, 2010)

  El algoritmo DES usa una clave simétrica de 64bits, los 56 primeros bits son empleados para el cifrado, y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, tenemos 2 elevado a la 56 combinaciones posibles, por lo que la fuerza bruta se hace casi imposible. (Luz, 2010)

2.3.2.3 Cifrado asimétrico

Existen dos claves, una pública y una privada, y se puede usar en dos direcciones. (Martinez, 2009), tal como indica la Figura 5.

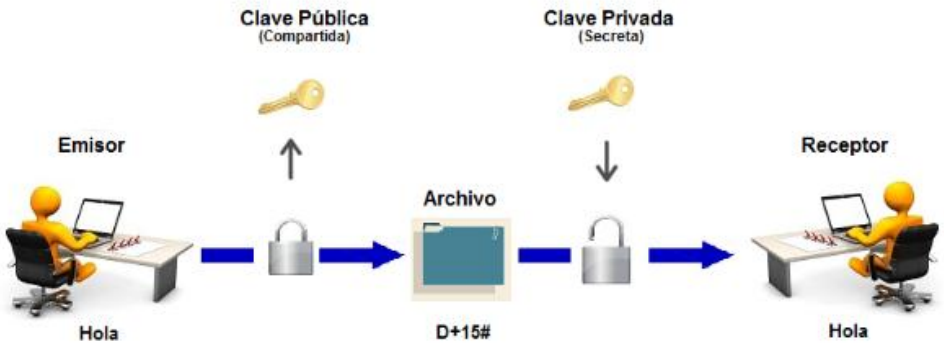

Figura 5 Cifrado Asimétrico

- El emisor cifra el mensaje con la clave pública A, que es la que puede conocer cualquiera. Sin embargo para descifrarlo hace falta la clave B, que sólo tiene el receptor, ya que es privada. Con esto se garantiza confidencialidad, cualquiera podría cifrar, pero sólo quien tenga la clave privada podrá descifrar. (Martinez, 2009)

- El emisor cifra el mensaje con la clave privada B, que sólo él conoce. Ahora cualquiera puede descifrarlo con la clave privada A, pero una vez descifrado con esa clave A, la naturaleza del algoritmo estará garantizando que se ha cifrado con la clave B, por lo que la utilización del algoritmo en este sentido se usa para asegurar la autenticidad, y no para ocultar información. Cualquiera tendrá acceso a la información, pero podrá saber a ciencia cierta de dónde procede. El cifrado asimétrico en esta dirección se usa para certificar la autenticidad de las firmas digitales. (Martinez, 2009)

El funcionamiento de estos algoritmos, basados en factorización de números primos, permite que el cifrado se calcule con relativa sencillez, pero haga falta más procesamiento para descifrarlo. No obstante, aunque este algoritmo garantiza la seguridad de la clave privada, ya que sólo la tiene el receptor, es más lento y hace que los mensajes cifrados tengan un volumen mayor. Ejemplos de este cifrado son:

- **DSA (Digital Signature Algorithm - Algoritmo de Firma digital)**

  Es una parte el estándar de firma digital DSS (Digital Signature Standard).

  Este algoritmo, propuesto por el NIST, data de 1991, es una variante del método asimétrico de ElGamal.

Pasos:

- Por un lado se generará la clave pública compuesta por (p, q, α, y). Y por otro la clave privada a.
- Se genera la firma con la cual podrá operar el emisor.
- El destinatario efectuará las operaciones oportunas, suponiendo que conoce la clave pública (p, q, α , y), para verificar la autenticidad de la firma. (Luz, 2010)

- **RSA**

Este algoritmo se basa en la pareja de claves, pública y privada. La seguridad de este algoritmo radica en el problema de la factorización de números enteros. (Luz, 2010)

Ventajas:

- Resuelve el problema de la distribución de las llaves simétricas (cifrado simétrico).
- Se puede emplear para ser utilizado en firmas digitales.

Desventajas:

- La seguridad depende de la eficiencia de los ordenadores.
- Es más lento que los algoritmos de clave simétrica.
- La clave privada debe ser cifrada por algún algoritmo simétrico.

- **Diffie-Hellman**

No es un algoritmo simétrico propiamente dicho, se usa para generar una clave privada simétrica a ambos extremos de un canal de comunicación inseguro. Se emplea para obtener la clave secreta con la que

posteriormente se cifrará la información, junto con un algoritmo de cifrado simétrico. (Luz, 2010)

Su seguridad radica en la dificultad de calcular los logaritmos discretos de números grandes.

El problema de estos algoritmos es que no proporciona autenticación, no puede validar la identidad de los usuarios, por tanto si un tercer usuario se pone en medio de la “conversación” también se le facilitaría las claves y por tanto podría establecer comunicaciones con el emisor y el receptor suplantando las identidades. (Luz, 2010)

2.3.2.4 Cifrado híbrido

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento. (Gutiérrez, 2013)

El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

2.3.3 Criptoanálisis

Se ocupa de conseguir capturar el significado de mensajes construidos mediante criptografía sin estar legitimado para ello. Podríamos decir que el criptoanálisis tiene un objetivo opuesto al de la criptografía. Su finalidad es buscar el punto débil de las técnicas criptográficas para explotarla y así reducir o eliminar la seguridad que teóricamente aportaba esa técnica criptográfica. A cualquier intento de criptoanálisis se le llama ataque. Un ataque tiene éxito, y se dice que el sistema ha sido roto, cuando el atacante consigue romper la seguridad que la técnica criptográfica aporta al sistema. (Barzanallana, 2014)

El criptoanálisis es el arte y la ciencia de analizar los sistemas de información con el fin de estudiar los aspectos ocultos de los sistemas. Criptoanálisis se utiliza para romper los sistemas de seguridad criptográficos y tener acceso al contenido de los mensajes cifrados, incluso si la clave criptográfica es desconocida. (Tinajero, 2014)

2.3.4 Objetivo del Criptoanálisis

El objetivo del criptoanálisis es encontrar debilidades en los sistemas criptográficos que permitan elaborar ataques (ataques criptoanalíticos) que rompan su seguridad sin el conocimiento de información secreta. Para ello estudia en profundidad el diseño y propiedades de los sistemas criptográficos. (Tinajero, 2014)

Por ejemplo para un sistema criptográfico de cifrado un estudio criptoanalítico puede consistir por ejemplo en conseguir la clave secreta o

simplemente en acceder al texto en claro sin ni siquiera tener dicha clave. (Tinajero, 2014)

2.4 Organización y almacenamiento de las contraseñas en el Sistema Operativo Windows

2.4.1 Sistema operativo

El Sistema operativo es un programa que controla la ejecución de los programas de aplicación, también actúa como una interfaz entre el usuario de un computador y el hardware de la misma. (Tanenbaum, 2010)

El sistema operativo tiene tres objetivos o lleva a cabo tres funciones:

- **Amigable:** El sistema operativo proporciona una interfaz amigable para el usuario, ocultando detalles del hardware para utilizar el sistema, es decir actúa como mediador entre el usuario y los programas de aplicación facilitando el acceso y el uso de todas las características y servicios del sistema.

- **Eficiente:** El sistema operativo permite que los recursos de un sistema informático se aprovechen de una manera más eficiente.

- **Evolutivo:** Un sistema operativo debe construirse de manera que permita el desarrollo, verificación y adaptación de nuevas funcionalidades en el sistema.

2.4.2 El Sistema Operativo como una Interfaz de Usuario

El hardware y el software que se utilizan para facilitar de aplicaciones a los usuarios pueden verse de forma jerárquica, tal como indica la Figura 6.

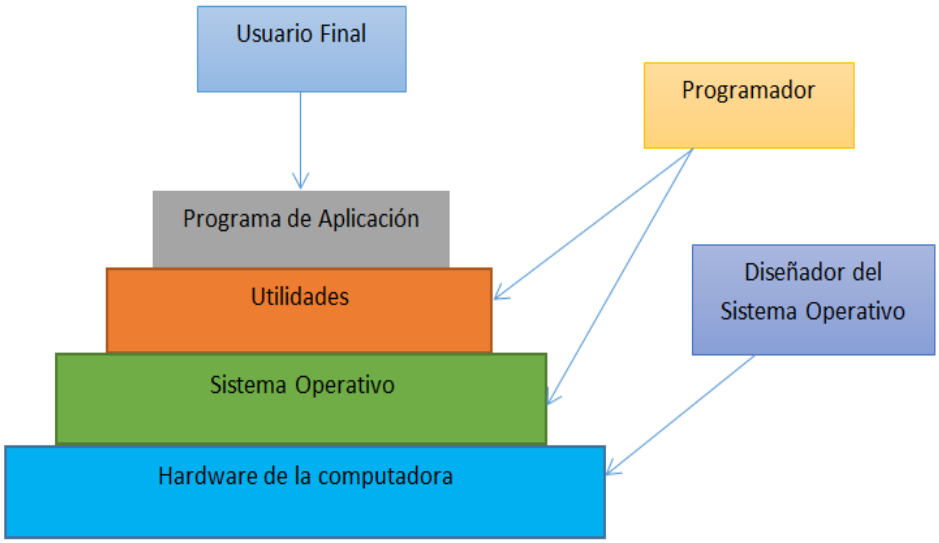

Figura 6 Niveles y vistas de un sistema informático

El usuario que usa estas aplicaciones se los puede llamar usuario final y generalmente, no tiene que ocuparse de la arquitectura del computador.

Se puede decir, que el usuario final ve al sistema informático como una aplicación. Las aplicaciones se pueden construir con un lenguaje de programación y son desarrolladas por programadores de aplicaciones. (WARD, 2011)

2.4.3 Windows

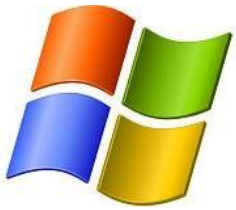

Figura 7 Logo de Windows

Microsoft Windows es un sistema operativo, es decir es un conjunto de programas que permite la administración de los recursos de una computadora. Windows empieza a trabajar cuando se enciende o inicializa el equipo para gestionar el hardware empezando desde los niveles más básicos. (Orozco, 2011)

Es importante conocer que los sistemas operativos funcionan tanto en las computadoras como en diferentes dispositivos electrónicos que usan microprocesadores. En este caso Windows, su versión estándar funciona con computadoras. (Orozco, 2011)

Microsoft domina el mercado de los sistemas operativos debido a su comodidad, se puede decir Windows está instalado en más del 90% de las computadoras con acceso a Internet en todo el mundo. (Orozco, 2011)

Entre sus principales aplicaciones (que estas también pueden ser desinstaladas por los usuarios o actualizadas sin que el sistema operativo se dañe o deje de funcionar), se encuentran, el reproductor multimedia Windows Media, el navegador Internet Explorer el editor de imágenes Paint y el procesador de texto WordPad. (Orozco, 2011)

La principal novedad que aportó Windows desde sus orígenes fue su facilidad para usarlo y el atractivo visual. De hecho, su nombre (“ventanas”) se debe a la forma que sistema presenta los usuarios los recursos de su computadora, lo que facilita las tareas cotidianas. Windows también suele recibir varias críticas por sus problemas de seguridad y por otros fallos. (Orozco, 2011)

2.4.3.1 Registro de Windows

Es una base de datos jerárquica en la que se almacenan las opciones de Windows y las opciones del mismo, este registro es utilizado por:

- Autenticación
- Kernel.
- Controladores de dispositivos.
- Servicios.
- SAM.

El registro tiene dos elementos que son fundamentales: valores y claves.

Las claves del Registro de Windows son muy similares a las carpetas, además de los valores cada clave puede contener sub claves que pueden contener otras sub claves, en si dentro de estas claves y valores encontraremos configuraciones y opciones del sistema operativo y que el usuario ha realizado sobre el mismo. (Férez, 2010)

Dependiendo de la versión de sistema operativo que utilicemos las carpetas del sistema se almacenaran en distintas rutas de acceso sin embargo para Windows, cuatro de los cinco ficheros que más nos interesan se encuentran en

la siguiente ubicación %SystemRoot%\System32\Config\ en las siguientes sub llaves: (Férez, 2010). Ver Figura 8

- SAM - HKEY LOCAL MACHINE\SAM
- SECURITY - HKEY LOCAL MACHINE\SECURITY
- SOFTWARE- HKEY LOCAL MACHINE\SOFTWARE
- SYSTEM- HKEY LOCAL MACHINE\SYSTEM

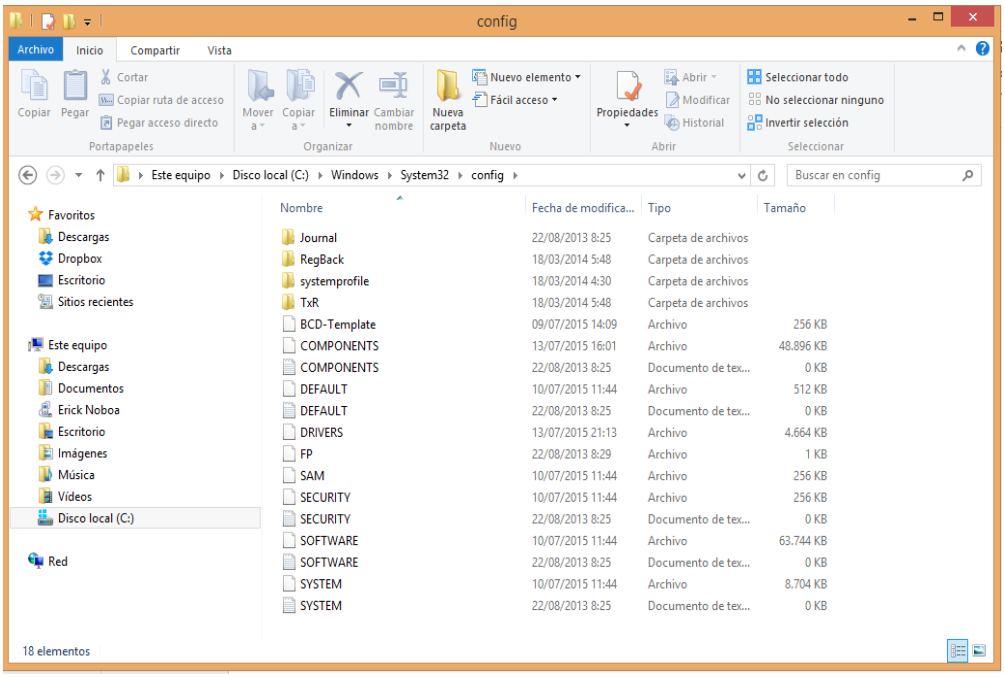

Figura 8 Ruta de acceso al registro de Windows

2.4.3.2 Autenticación en Windows

SAM es una base de datos en donde se encuentran las cuentas de seguridad. Esto es utilizado por Windows para administrar las cuentas de usuario y contraseñas en el formato de hash (hash unidireccional).

Las contraseñas nunca se almacenan en formato de texto claro. Se almacenan en el formato de hash para protegerlos de los ataques. La base de datos SAM se implementa como un archivo de registro y las obtiene del kernel de Windows y mantiene un bloqueo exclusivo al archivo SAM, esto quiere decir que el archivo tiene cierta medida de seguridad para el almacenamiento de las contraseñas. (Férez, 2010)

No es posible copiar el archivo SAM a otra ubicación en el caso de los ataques en línea. Dado que el archivo SAM está bloqueado con un bloqueo exclusivo al sistema de archivos, no puede ser copiado o movido mientras se ejecuta Windows. El bloqueo no iniciará hasta que la excepción de la pantalla azul haya sido inicializada o el sistema operativo haya sido apagado. Sin embargo, los hashes de contraseñas fuera de línea están disponibles para los ataques de fuerza bruta, el contenido del archivo SAM puede ser la copiado o descargado utilizando diversas técnicas. (Férez, 2010)

Microsoft introdujo la función SYSKEY en Windows NT 4.0 en un intento de mejorar la seguridad de la base de datos SAM contra software de craqueo fuera de línea. La copia en disco del archivo SAM está cifrada parcialmente cuando la SYSKEY está habilitada. De esta manera, la contraseña para todas las cuentas locales almacenados en el SAM se cifran con una clave. Incluso si su contenido es descubierto por algún medio, las claves están codificadas con un hash de un solo sentido, por lo que es difícil de romper. Además, algunas versiones tienen una clave secundaria, haciendo que la copia del sistema operativo tenga una encriptación específica. (Férez, 2010)

Autenticación NTML

NTLM (NT LAN Manager) es un protocolo empleado por muchos productos de Microsoft para realizar la autenticación desafío / respuesta, por lo tanto es el esquema de autenticación que por defecto usa Firewall de Microsoft y también los productos del servidor de proxy. (Ec-Council, 2011)

Este software fue desarrollado para afrontar el problema del trabajo con Tecnologías Java en un entorno orientado a Microsoft. Puesto que no se basa en ninguna especificación oficial de protocolo, por lo tanto no hay garantía de que funciona correctamente en todos los casos. También ha estado en algunas instalaciones de Windows, donde funcionó con éxito. (Ec-Council, 2011)

La Autenticación NTLM se compone de dos protocolos: protocolo de autenticación NTLM y protocolo de autenticación LM. Estos protocolos utilizan una metodología de hash diferente para almacenar contraseñas de los usuarios en la base de datos SAM. (Ec-Council, 2011)

Protocolo de autenticación NTML

Los productos que son compatibles con el protocolo NTLM se publican sólo por Microsoft debido a la falta de disponibilidad de las especificaciones oficiales de protocolo. (Ec-Council, 2011)

Como consecuencia de ello, en un entorno de red orientada a Microsoft, casi todos los productos no-MS tienen problemas para realizar sus tareas correctamente. Los entornos de desarrollo de software sufren el problema antes mencionado, no hay bibliotecas para implementar este esquema de autenticación, salvo los paquetes en el sistema operativo Windows. En la

comunidad de código abierto, hay muchos proyectos centrados en la aplicación de este protocolo, pero la mayoría de ellos tienen Java como el entorno de destino. (Ec-Council, 2011)

La falta de la disponibilidad de este esquema de autenticación en la plataforma Java podría significar un serio problema en el desarrollo y despliegue de aplicaciones de cooperación basados en tecnologías como los servicios web SOAP que se basan en el protocolo HTTP (Ec-Council)

Kerberos

El Kerberos es un protocolo de autenticación de red que está perfilado para la autenticación fuerte de las aplicaciones cliente/servidor mediante el uso de criptografía de clave secreta. Este proporciona la autenticación mutua. Tanto el servidor y el usuario verificar se verifican mutuamente la identidad. Cuando se envían mensajes a través del protocolo Kerberos están protegidos contra ataques de repetición y espionaje. (Ec-Council, 2011)

Kerberos hace uso de Centro de distribución de claves (KDC), este consta de dos partes distintas:

- Servidor de autenticación (AS) (Authentication Server).
- Servidor emisor de tickets (TGS) (Ticket Granting Server).

Kerberos trabaja en base a "tickets", estos permiten demostrar la identidad de los usuarios. (Ec-Council, 2011)

Figura 9 Autenticación de seguridad en Windows

2.4.3.3 SAM (Administrador de cuentas de seguridad)

El Administrador de cuentas de seguridad (SAM) es una base de datos en el sistema operativo Windows que contiene los nombres de usuario y contraseñas. SAM es parte del registro y se puede encontrar en el disco duro. (Hernandez, 2013)

En el archivo SAM se encuentra el principal componente que es el SID de los usuarios de la máquina, el SID o Security Identifier es un numero único e irrepetible que identifica a un usuario dentro de un sistema de Windows, esto ancla una cuenta de por vida con un SID y todas las propiedades de esa cuenta incluido el nombre de la cuenta, esto es importante conocerlo porque Windows da o niega acceso y privilegios dentro de un sistema basado en ACL's o listas

de control de acceso, estos ACL's utilizan los SID's para identificar de manera única a un usuario y los privilegios asociados con esta cuenta y grupo. (Hernandez, 2013)

Cuando cualquier usuario ingresa al sistema se genera una llave de acceso o un token de acceso, esa llave contiene el SID y junto con ello el nivel de privilegios que con los que el usuario cuenta, cuando un usuario solicita acceso a algún recurso del sistema, la llave de acceso o token es comparada con el ACL para permitir o negar una la petición. (Hernandez, 2013)

Para entender de mejor manera la estructura del SID se utilizará como ejemplo el siguiente valor: Ver Figura 10

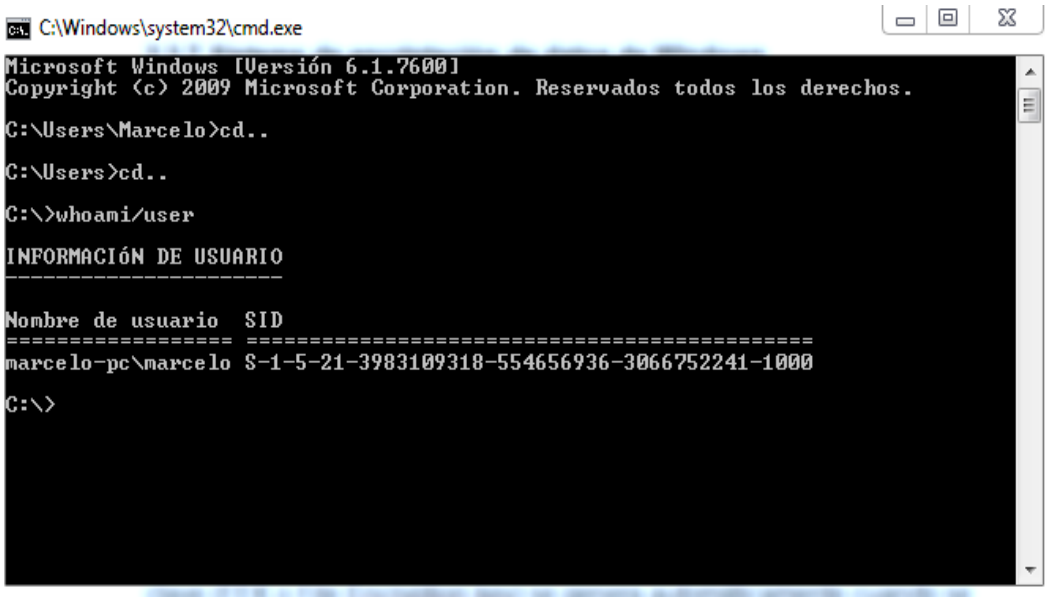

Figura 10 SID del usuario Marcelo

SID S-1-5-21-3983109318-554656936-3066752241-1000

S- indica que es un string de SID
1- el nivel de revisión
5- el identificador de valor de autoridad o authority value no siempre será 5 entre otros valores que se pueden encontrar están los siguientes:

- 0 - sin autoridad
- 1 - autoridad global
- 2 - autoridad local
- 3 - autoridad de creador
- 4 - autoridad no única
- 5 - autoridad NT
- 9 - autoridad de administrador de recursos

21-3983109318-554656936-3066752241 - es el dominio en el que se encuentra el sistema o el identificador local de la computadora.

1000- un ID único para cada cuenta, aquí se puede encontrar lo que se conoce como RID o relative identifier el cual es un número que varía en su longitud, cualquier grupo o usuario que no se cree de manera predeterminada recibirá un RID de 1000 o mayor, en este caso es 500 esto se debe a que este SID representa la cuenta de un administrador, este valor de 500 será SIEMPRE el mismo en cualquier cuenta de administrador así como también el valor 501 representa el SID de una cuenta Guest estos valores se encuentran en cada uno de nuestros sistemas y al momento de efectuar un análisis forense es de vital importancia conocer sobre que cuenta se enfocará y a quien pertenece esa cuenta. (Hernandez, 2013)

2.4.3.4 Sistema de encriptación de datos de Windows

Cifrado de datos con EFS

Windows ofrece un método de cifrado integrado, que se llama EFS (Encrypted File System) y solo está presente si el disco duro está formateado con NTFS. (INTECO, 2010)

EFS es un sistema que utiliza tecnología estándar y, por tanto, es seguro. EFS se basa en una mezcla de criptografía pública y privada. En realidad EFS utiliza una clave única por fichero para cifrarlo y descifrarlo. Esta clave (FEK o File Encryption key) se genera automáticamente cuando se cifra un fichero y se almacena con él. Aunque esto parezca inseguro (sería como almacenar la llave junto al candado que protege una puerta) esta FEK es a su vez cifrada con la clave pública del usuario, con lo que queda protegida. (INTECO, 2010)

Tanto las FEK como las claves públicas y privadas del usuario se generan de forma transparente para él la primera vez que cifra un archivo o carpeta y de forma automática. Se almacenan en forma de certificado en el repositorio de certificados del sistema operativo. El usuario no tiene por qué conocer estos datos. (INTECO, 2010)

La ventaja de este método es que no tiene que utilizar contraseñas adicionales cada vez que quiera acceder a los datos: todo es gestionado por el sistema operativo.

Es imprescindible destacar que sólo el usuario con el que se ha cifrado la información (y sólo ese mismo usuario) puede acceder a los datos. Esto significa que en el caso de que el usuario del sistema operativo se pierda, los datos quedan inaccesibles irremediablemente, incluso si se crea un nuevo usuario con el mismo nombre y características. (INTECO, 2010)

Ventajas y Desventajas de EFS

Su mayor ventaja es la facilidad de uso. Cada vez que el usuario inicie sesión, los datos están ahí para poder ser manipulados, pero una vez cerrada la sesión, o si otro usuario utiliza el sistema, los datos aparecen inaccesibles. (INTECO, 2010)

Sin embargo, una de las desventajas que tiene EFS es que está totalmente ligado a Windows y NTFS. Esto quiere decir que si el archivo es copiado a una unidad en red que no sea NTFS (muchas unidades USB no están formateadas así, y muchos sistemas operativos tampoco soportan NTFS), el archivo se copia sin contenido (un archivo de 0 bytes de tamaño). Por el contrario, si se copia de una unidad NTFS a otra unidad NTFS, permanece perfectamente cifrado y con todo su contenido. (INTECO, 2010)

Esto hace que cifrar con NTFS no sea muy adecuado para transportar estos ficheros. Sin embargo, lo hace útil para utilizar en portátiles, por ejemplo, puesto que pueden llegar a ser sustraídos o extraviados con mayor facilidad. En estos casos, la información en el disco duro cifrada no puede ser obtenida por alguien que tenga acceso al mismo. También es útil en sistemas compartidos (un mismo ordenador con varios usuarios diferentes) para mantener ciertos datos accesibles por un solo usuario. (INTECO, 2010)

Otro inconveniente a tener en cuenta es que toda la seguridad se concentra en su eslabón más débil, y en este caso es la contraseña de usuario de Windows. La contraseña es la que permite descifrar el certificado que es utilizado a su vez para descifrar la contraseña con la que se cifra cada archivo. Por tanto, es imprescindible proteger la cuenta de usuario con una contraseña mayor de catorce caracteres, que mezcle letras, números y símbolos. Para asignar una clave al usuario, se debe ir al panel de control, "cuentas de usuario" y "crear una contraseña" en el usuario elegido. (INTECO, 2010)

Cifrado de datos con BitLocker

BitLocker es una tecnología introducida por Microsoft exclusivamente en las versiones más avanzadas de Windows Vista y 7. Permite aprovechar una característica de cierto hardware, llamada TPM (Trusted Platform Module) que lo hace muy robusto. El TPM interactúa con BitLocker para proporcionar una protección mejorada incluso durante el inicio de sistema. (INTECO, 2010)

BitLocker es mucho más potente que EFS y ha sido introducido para complementarlo. Permite cifrar todo un disco duro, incluido el sistema operativo. Esto evita una debilidad en EFS ya mencionada: toda la seguridad recae sobre la contraseña del usuario de Windows y el problema es que ésta se mantiene almacenada en el disco duro (lógicamente cifrada por Windows independientemente del EFS). Aunque, si es suficientemente compleja, no supone mayor problema. (INTECO, 2010)

BitLocker también permite el cifrado de unidades del sistema que se pueden dedicar exclusivamente a datos e incluso unidades extraíbles gracias a su función "BitLocker To Go". (INTECO, 2010)

Al igual que EFS, está pensado para la comodidad del usuario, sin embargo, el hecho de que esté disponible exclusivamente para versiones más caras de Windows, lo ha hecho menos popular. (INTECO, 2010)

BitLocker no sustituye a EFS, sino que lo complementa. Por ejemplo, con BitLocker no es posible en un sistema multiusuario, que cada usuario proteja sus propios archivos, aunque es posible combinar ambas tecnologías y obtener mejores resultados (EFS sigue presente en todas las versiones de Windows y ambos métodos son compatibles). (INTECO, 2010). Ver Tabla 1

Tabla 1 Comparación entre tecnologías de cifrado Windows

BitLocker	EFS
Permite cifrar todo: datos, unidades de disco extraíbles, unidad de sistema.	Solo permite cifrar archivos o carpetas, excluyendo las de sistema.
No depende de los usuarios. Está activo o inactivo.	Permite que múltiples usuarios cifren independientemente sus datos en un sistema multiusuario.
Se debe ser administrador de sistema para usarlo.	Cualquier usuario de sistema, independientemente de sus permisos, puede utilizarlo.
Sólo disponible en las versionas más completas de Windows 7, Vista y 2008.	Disponible desde Windows 2000, en todas las versiones.
Utiliza TPM (Trusted Platform Module).	Es independiente del hardware.

2.5 System Hacking

Así como un delincuente comete un crimen para lograr un determinado objetivo, del mismo modo, un atacante también tiene ciertos objetivos por los cuales ataca a un sistema. (Ec-Council, 2011)

2.5.1 Objetivos de System Hacking

- Obtener acceso
    - Recolectar suficiente información para obtener acceso
    - Passwords, espionaje, fuerza bruta

- Escalar privilegios
    - Crear una cuenta de usuario privilegiado si se obtiene nivel de usuario
    - Password cracking, exploits conocidos

- Ejecutar aplicaciones
    - Crear y mantener acceso a puertas traseras
    - Troyanos
- Ocultar ficheros
    - Ocultar ficheros maliciosos
    - Rootkits
- Encubrir pistas
    - Ocultar la presencia de compromiso
    - Limpieza de logs

2.5.2 Metodología Hacking

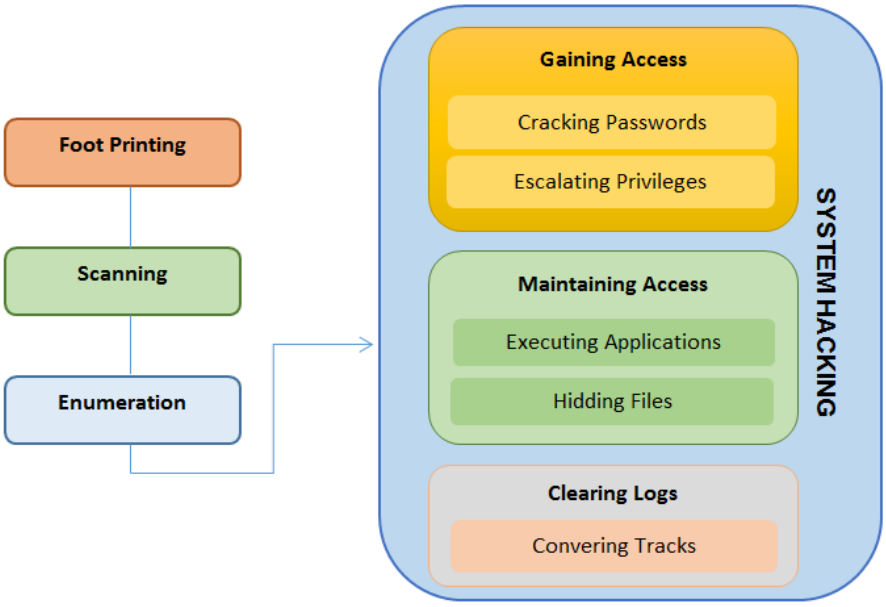

Figura 11 Metodología Hacking

Fuente: (Ec-Council, 2011)

Antes de hackear un sistema, un atacante utiliza las siguientes técnicas, footprinting (huellas), scanning (exploración) y enumeration (enumeración) para detectar el objetivo al que se le realizará el ataque así como las vulnerabilidades que son doorways (puertas de entrada) para el atacante. (Ec-Council, 2011). Ver Figura 11

Un hacker también sigue los mismos pasos que un atacante para probar un sistema, con el fin de garantizar la eficacia de la prueba, el hacker sigue la metodología de hacking. (Ec-Council, 2011)

La Figura 12 describe la metodología de hacking seguido por los hackers. (Ec-Council, 2011)

2.5.3 Password Cracking

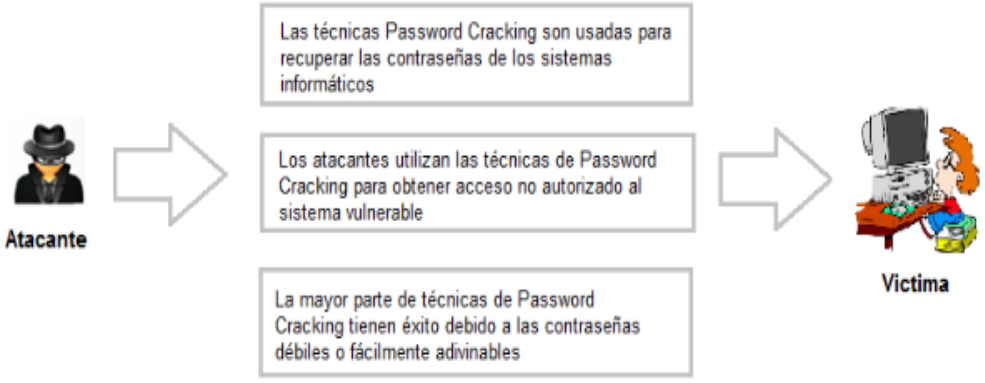

Figura 12 Password Cracking

Fuente: (Ec-Council, 2011)

Password cracking es el proceso de recuperación de contraseñas a partir de los datos que han sido transmitidos por un sistema informático o almacenada en él. El propósito de password cracking es ayudar a un usuario recuperar una contraseña olvidada o perdida, también como medida preventiva por los administradores del sistema para comprobar si hay contraseñas fácilmente manipulables o también se puede utilizar para obtener acceso no autorizado a un sistema. (Ec-Council, 2011)

Muchos intentos de hacking comienzan con intentos de craqueo de contraseñas. Las contraseñas son la pieza clave de la información necesaria para acceder a un sistema. En consecuencia, la mayoría de los atacantes utilizan técnicas de descifrado de contraseñas para obtener acceso no autorizado al sistema vulnerable. Las contraseñas pueden ser descifradas manualmente o con herramientas automatizadas, como un método de diccionario o de fuerza bruta. (Ec-Council, 2011)

Los programas de computadora que están diseñados para el craqueo de contraseñas tienen funciones de las series de posibles contraseñas por segundo que se pueden comprobar. A menudo los usuarios, mientras crean las contraseñas, seleccionan contraseñas que están predispuestas a ser craqueadas porque usan como contraseñas el nombre de una mascota o eligen uno que sea sencillo para que puedan recordarlo. (Ec-Council, 2011)

La mayoría de técnicas de Password Cracking tienen éxito debido a que las contraseñas son débiles o fáciles de adivinar. (Ec-Council, 2011)

2.5.4 Herramientas para descifrar contraseñas

2.5.4.1 L0phcrack

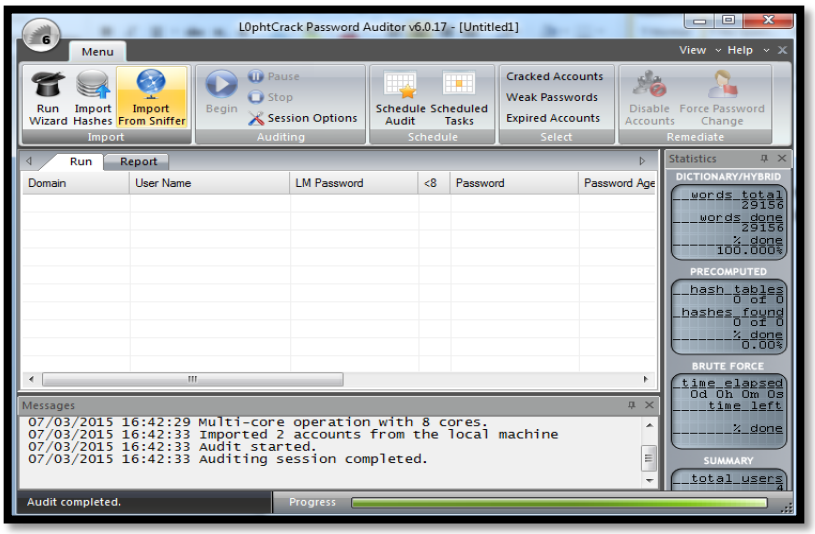

Figura 13 Herramienta L0phcrack

Es una herramienta de recuperación y auditoría de claves que es usada para verificar:

- La debilidad de las contraseñas
- Recuperar las contraseñas que se han perdido u olvidado en sistemas Microsoft Windows.

L0phcrack realiza ataques por diccionario, ataques por fuerza bruta o una combinación de los dos anteriores (ataques híbridos).

L0phcrack usa una copia del archivo SAM que Windows guarda en el fichero regback, este archivo es usado por Lophtcrack, que nos sacara una copia de este fichero para intentar desencriptarlo.

Esta herramienta fue originada por @stake después de que L0pht se uniera con @stake en el 2000. @stake fue obtenida porSymantec en 2004. (L0phcrack)

2.5.4.2 Cain & Abel

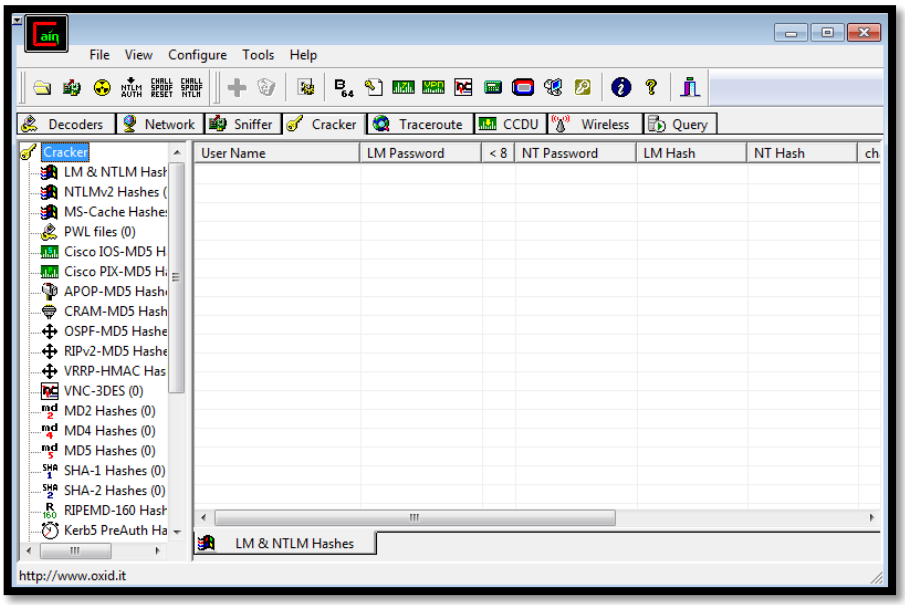

Figura 14 Herramienta Caín & Abel

Es una herramienta de recuperación de contraseñas para Microsoft Windows. Puede recuperar muchos tipos de contraseñas utilizando métodos como el sniffing de paquetes de red, también puede crackerar varios hashes de contraseñas utilizando métodos como ataques de diccionario, de fuerza bruta y ataques basados en criptoanálisis. (Montoro, 2009). Ver Figura 14

3. CAPÍTULO 3

DESARROLLO

3.1 Introducción

En la actualidad, los avances tecnológicos han roto muchas barreras las cuales permiten establecer nuevos paradigmas con el único propósito de proteger la información valiosa siendo base importante las operaciones administrativas y financieras de las empresas de hoy por el mismo hecho que existen cyberdelincuentes que lo único que buscan es espiar, robar información o ver la manera de hacer daño sin dejar rastro alguno, pero por otro lado también existe personal que se dedica a realizar hacking ético lo cual hace referencia a la aplicación de procesos o técnicas hacking pero con la finalidad de mejoramiento de la seguridad informática o la recuperación de información de dichas empresas, la cual consiste en buscar, encontrar y demostrar vulnerabilidades de los sistemas para de una u otra manera resolver los problemas de seguridad u obtener información necesaria, tal es nuestro caso de estudio el cual se enfocará en el problema planteado en donde se analizará el funcionamiento de las diferentes técnicas hacking para ponerlos en práctica de forma ética mediante una herramienta especializada llamada L0phcrack que permitirá vulnerar y recuperar las contraseñas de los usuarios registrados en el sistema operativo Windows.

3.2 Técnicas hacking de password cracking

La diferentes técnicas que existen en el mercado son muchas por la cuales se han tomado las siguientes para ser analizadas y puestas en ejecución, dependiendo de sus diferentes procesos a realizar.

3.2.1 Ataque Diccionario

El ataque por diccionario es un tipo de ataque informático relacionado al hacking que utiliza un diccionario de palabras para llevar a cabo su cometido.

El ataque diccionario suele ser más eficiente que un ataque de fuerza bruta, debido a que varios usuarios casi siempre suelen utilizar contraseñas con una o varias palabras existentes en su lengua, para que la contraseña no sea olvidada y sea fácil de recordar, esto no es una práctica recomendable. (Alegsa, 2010)

3.2.2 Ataque de Fuerza Bruta

Ataque por fuerza bruta es el método para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Los ataques por fuerza bruta son una de las técnicas más habituales de robo de contraseñas en Internet dado que no es necesario tener grandes conocimientos en seguridad informática para realizar un ataque, existen programas que realizan de forma automática todo el trabajo. (García, 2013)

3.2.3 Ataque Híbrido

Apunta específicamente a contraseñas compuestas la cual puede ser una palabra tradicional seguida de una letra o de un número (como por ejemplo "pedro8").

Este ataque es una mezcla entre el ataque de diccionario y el de fuerza bruta.

Tabla 2 Comparación entre técnicas de Password Cracking

Características	Ataque diccionario	Ataque de fuerza bruta
Encuentra la contraseña	X	X
Es más rápido	X	
Encuentra la contraseña sin diccionario		X
Es más lento pero encuentra la contraseña		X
Utiliza diccionario	X	
Realiza las todas las combinaciones posibles de un alfabeto		X

Se utilizó el ataque de fuerza bruta a pesar de que se demora un tiempo estimado en encontrar la contraseña dependiendo de la longitud de la misma, pero a la final es descubierta, en cambio es difícil encontrar un diccionario con todas las palabras posibles del usuario que va a ser atacado.

3.3 Herramienta utilizada para extraer el log de windows

Para extraer el log de Windows que consta de los archivos SAM y SYSTEM se puede utilizar cualquier dispositivo de que pueda se booteado, el cual contenga un sistema operativo recortado, para esta práctica se utilizó un Live CD con sistema operativo Linux.

3.3.1 Live CD

Es una forma en que se les conoce a los Sistemas Operativos que son utilizados sin necesidad de ser instalados, los mismos son distribuciones que pueden ser almacenados y ejecutados directamente desde un CD, DVD, USB o cualquier dispositivo estático.

3.3.2 Características de Live CD

- La gran mayoría de Live CD's usa sistema operativo basado en el núcleo Linux, también existen Live CD's que utilizan sistema operativo Windows pero estos no son muy comunes.
- Un Live CD no requiere instalación, por lo que no es necesario utilizar el disco duro del computador.
- El uso de Live CD no provoca pérdida de datos, particiones o el daño de disco duro, por lo general no se efectúan cambios en el computador utilizado.

3.3.3 Para qué se utiliza y aplica Live CD

- Clonar el disco duro a una imagen
- Clonar el disco duro a un disco
- Usar con seguridad un pc infectado
- Scanear con antivirus un PC infectado
- Recuperar datos
- Ver datos en un mapa del contenido en el disco
- Buscar archivos/carpetas
- Buscar archivos/carpetas ocultos
- Borrar archivos en exceso y/o innecesarios
- Editar/Trabajar con archivos
- Recuperación de un disco ntfs corrupto
- Obligar a Windows a escanear particiones
- Sobrepasar permisos de Windows
- Hackear contraseñas de sistemas operativos Windows
- Usar un pc sin contraseña
- Hackear contraseñas de wifi
- Bypass un master boot record (mbr) corrupto

- Reparar un master boot record corrupto
- Navegar por internet de forma segura
- Usar de forma segura un pc público
- Evitar el “espionaje” por padres o empleadores
- Sobrepasando filtros de conexión
- Jugar, o usar software inadecuado en el trabajo
- Recuperar el Grub
- Comprobar las particiones del sistema linux instalado en el disco duro
- Probar software
- Hacer que un invitado pueda usar un sistema operativo
- Manejar particiones
- Comprobar la memoria
- Comprobar el disco duro
- Comprobar otro hardware
- Comprobar si un problema es hardware o software
- Instalar una distro Linux
- Conectar a un servidor en red

3.3.4 Cómo crear un Live CD en Windows

Para crear un Live Cd en Windows la forma más recomendada es utilizar un programa externo, para mayor facilidad para el usuario promedio que prefiere no utilizar la consola. Con el tiempo se ha probado diversas maneras para crear Live Cd’s, ya sea mediante comandos o programas, por lo cual lo más conveniente para un usuario que no tenga el suficiente conocimiento sobre el tema es utilizar programas para crear el mismo.

Tres de los programas que más se recomienda son los siguientes:

Nota: Sí se utiliza, se debe formatear en FAT32. (Guerra, 2013)

- **Universall USB Installer**

Este programa incluso es el recomendado por Ubuntu para crear el Live Cd, es fácil de usar, no necesita instalación y en sólo 4 pasos puedes crear el Live Cd:

- Selecciona tu distribución entre la lista
- Selecciona el archivo .iso
- Selecciona el dispositivo donde será creado el Live Cd (C:, D:, F:, etc.)
- Haz click en Crear.

Para poder crear el Live Cd con Universal USB Installer es necesario un descompresor, recomiendo 7zip y PeaZip.
(Guerra, 2013). Ver Figura 15.

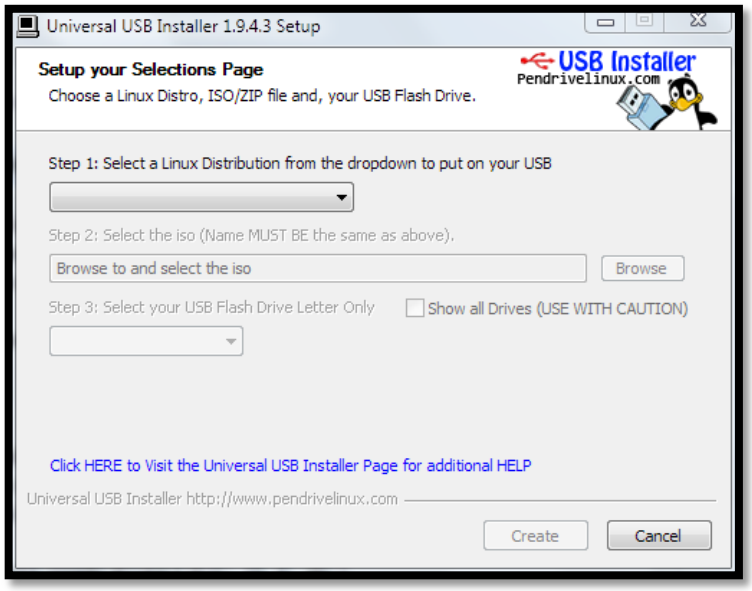

Figura 15 Herramienta USB Installer

- **UNetbottin**

  Su funcionamiento es similar a Universal USB Installer, pero lo supera en algunos aspectos, como por ejemplo, está disponible también en las distribuciones Linux y no sólo en Windows. También permite instalar el Live Cd en el disco duro, así podrás usarlo sin USB, pero no será posible instalar la distribución seleccionada. (Guerra, 2013). Ver Figura 16.

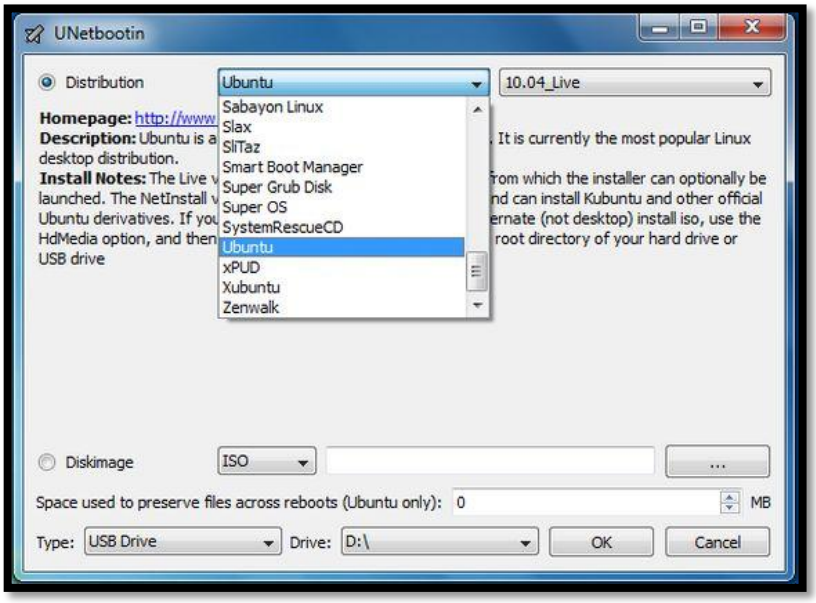

Figura 16 Herramienta UNetbottin

- **Linux Live USB Creator**

  También conocido como LiLi USB Creator, es una aplicación que está disponible únicamente para Windows. A diferencia de las otras dos opciones es necesario instalarlo, aunque también existe una versión portable. (Guerra, 2013)

LiLi USB Creator muestra una interfaz bastante amigable, ya que el programa está orientado a todo tipo de usuario, no sólo experimentados.

Esta interfaz se divide en 5 pequeñas “ventanas” que enumeran cada uno de los pasos:

- Elegir unidad donde se instalara el Live Cd.

- Elegir fuente del Live Cd (Archivo .iso, Cd/Dvd con la distribución instalada o Descargar distribución)

- Elegir tamaño de persistencia (Tamaño de persistencia es el espacio que hagas durante la sesión en el Live Cd, es decir, que cada archivo que guardes o programa que instales se guardara en ese espacio, si no sabes que poner, se recomienda entre 300 y 500 MB)

- Opciones (Formatear en FAT32, Ocultar archivos, Iniciar Linux Live)

- Crear Live Cd

Cada paso viene junto a un botón de ayuda que se mostrará la ayuda web de LiLi USB Creator, pero sólo está disponible en Inglés. (Guerra, 2013). Ver Figura 17.

Figura 17 Linux Live USB Creator

Estos son los programas que pueden ayudar a crear un Live Cd sin la necesidad de utilizar comandos, lo cual se hace para el usuario más amigable y fácil de usarlo.

3.4 Recuperación de la contraseña de una cuenta registrada en el Sistema Operativo Windows

3.4.1 Obtener del Log de Windows

Para obtener el log de Windows (SAM, SYSTEM) se ha utilizado el live CD de Linux Mint

- Reiniciar el equipo del cual vamos a obtener el log de Windows.

- Bootear desde el cd que contiene el sistema operativo de Linux Mint. Ver Figura 18.

Figura 18 Menú de Booteo

- Entrar a la carpeta que contiene el archivo SAM y SYSTEM, ubicado en la dirección Disco/Windows/System32/Config copiamos estos archivos ya que son los que se usarán para obtener la clave del usuario del sistema operativo. Ver Figura 19.

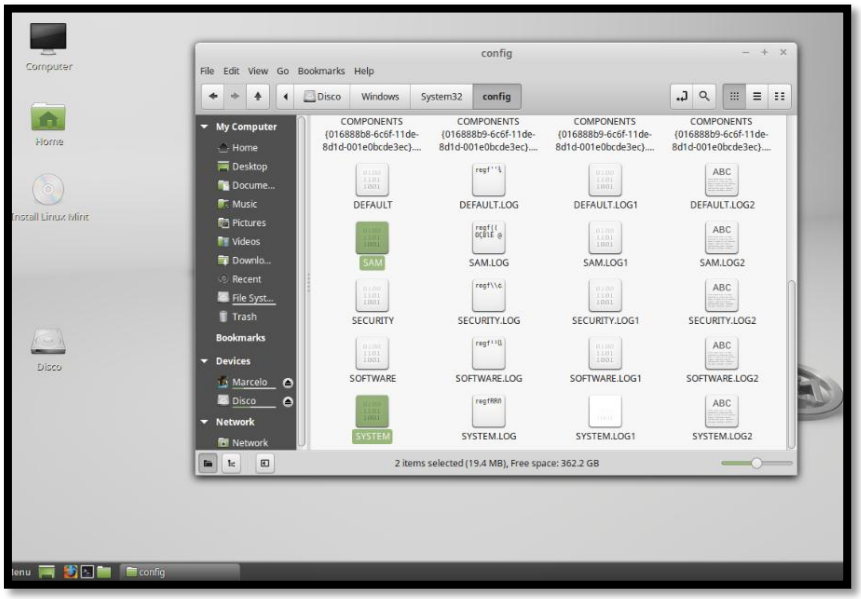

Figura 19 Ubicación del archivo SAM y SYSTEM

Una vez que se ha obtenido los archivos SAM y SYSTEM (log de windows), se procede a realizar los diferentes procesos en el laboratorio especializado

para forense, donde dichos archivos fueron utilizados para el análisis del usuario y contraseña de Windows con la herramienta L0phcrack la cual nos permite hacer los ataques mencionados.

3.4.2 Uso de L0phcrack para obtener la clave del usuario

- Abrir el programa y presionar siguiente (Next). Ver Figura 20.

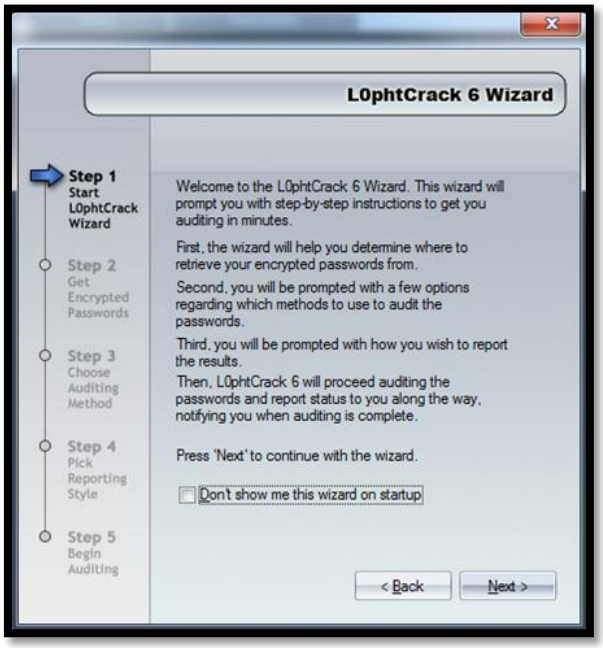

Figura 20 Herramienta L0phcrack primer paso

- Se verán varias opciones, seleccionar la opción “Retrieve from SAM/SYSTEM backup”. Esta opción nos permite ingresar el archivo SAM y SYSTEM que se copió en la obtención del log cuando finalicemos la configuración. Ver Figura 21.

Figura 21 Herramienta L0phcrack segundo paso

- Marcar la opción “Strong password audit” esta opción comprueba las contraseñas simples que pueden ser encontradas en un diccionario y también realiza un ataque de fuerza bruta que intenta todas las combinaciones de letras y números posibles. Ver Figura 22.

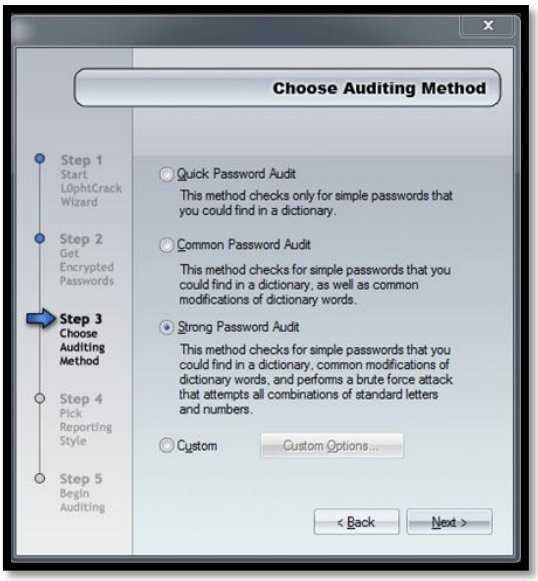

Figura 22 Herramienta L0phcrack tercer paso

- Permitirá elegir las opciones que se desea ver en la pantalla tales como:
  - Mostrar las contraseñas después de haber encontrado
  - Mostrar el hash de la clave
  - Mostrar el método que se usó para encontrar la clave
  - Mostrar el tiempo que se demoró en encontrar la clave
  - Mostrar notificación cuando se termine de auditar

  Ver Figura 23.

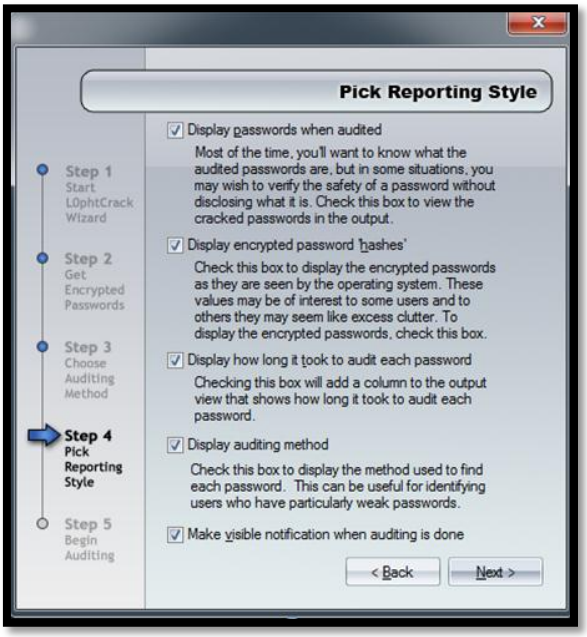

Figura 23 Herramienta L0phcrack cuarto paso

- Para finalizar se puede apreciar un resumen de todas las opciones que han sido elegidas.

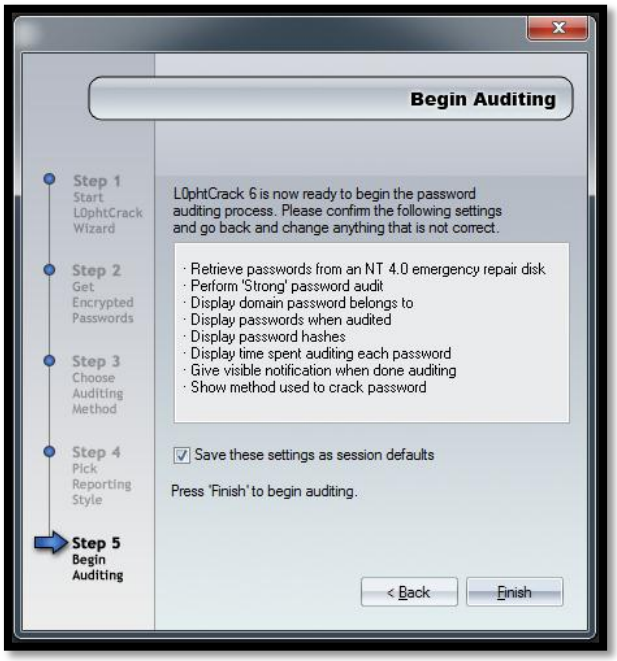

Figura 24 Herramienta L0phcrack quinto paso

- Una vez finalizada la configuración inicial, pedirá ingresar la ubicación del archivo SAM y SYSTEM que fue copiado anteriormente. Ver Figuras 25 y 26

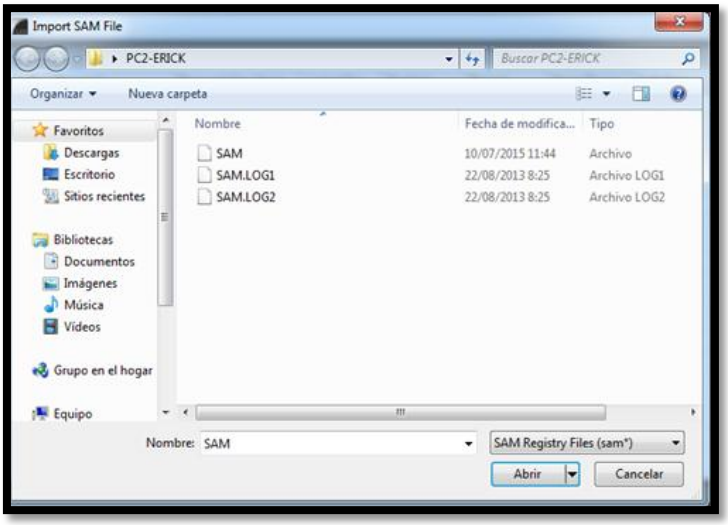

Figura 25 Ubicación del archivo SAM

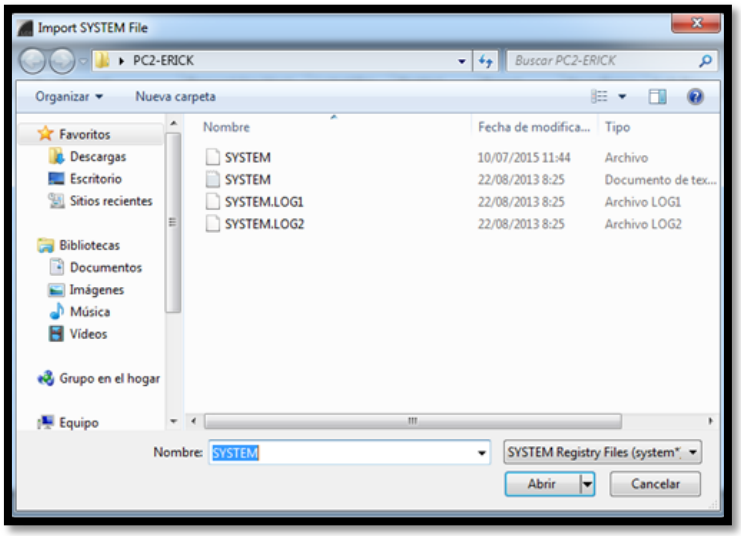

Figura 26 Ubicación del archivo SYSTEM

- Con los archivos ingresados se puede apreciar todos los usuarios que registrados en el log cargado

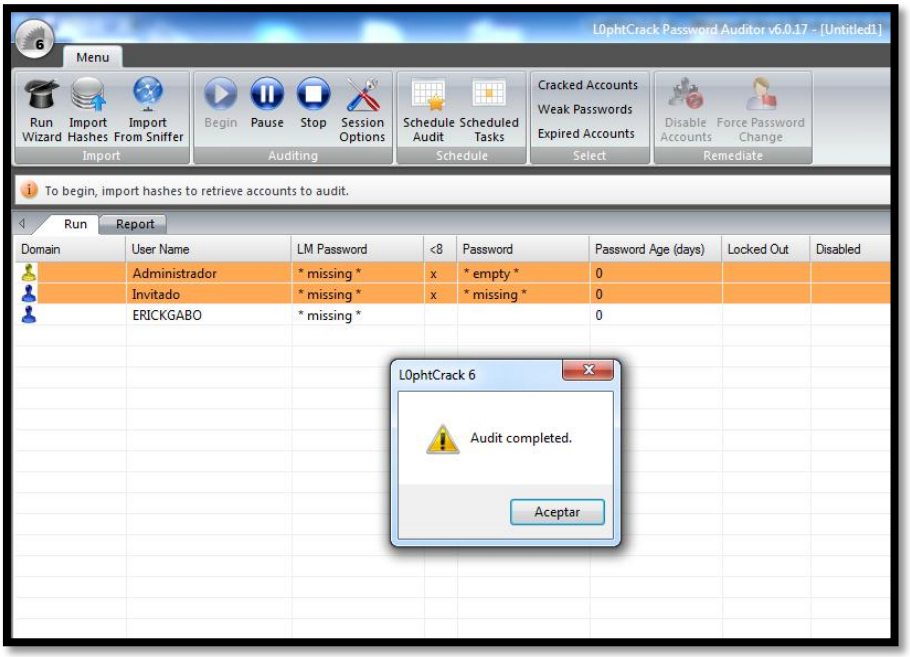

Figura 27 Usuarios cargados desde un log

- Presionar en “Sesion Options” que está ubicada en la barra de tareas del programa y se podrá apreciar de forma gráfica las opciones que han sido elegidas en la configuración inicial. Ver Figura 28.

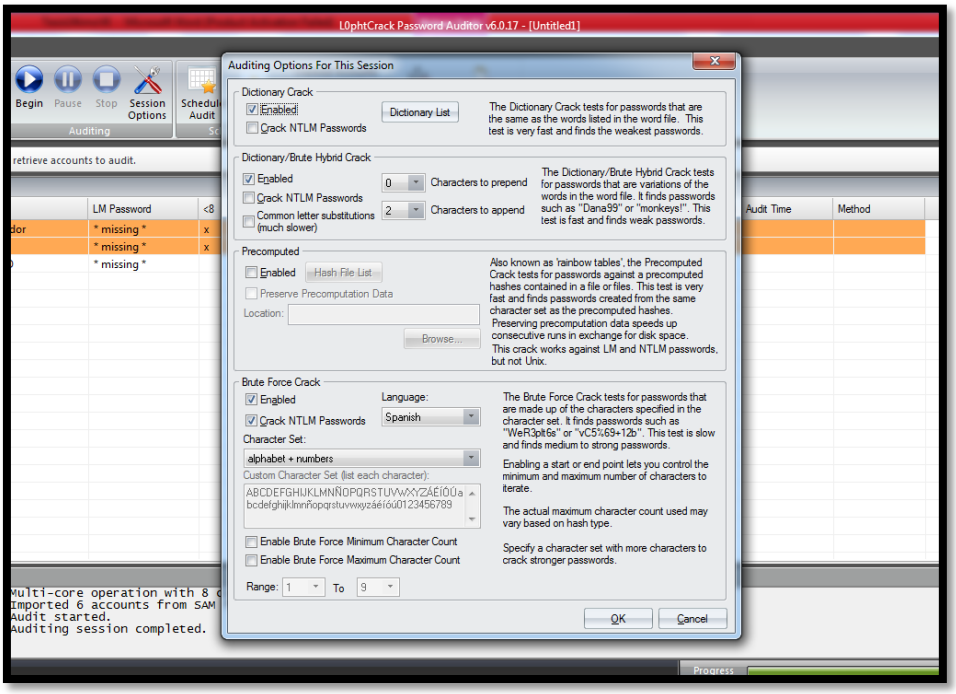

Figura 28 Configuración de L0phcrack

- Presionar “Begin” para empezar con el análisis y la recuperación de la contraseña. Ver Figura 29.

Figura 29 Barra de herramientas de L0phcrack

- Se puede apreciar en la Figura 30 que la clave fue recuperada. Ver Figura 30

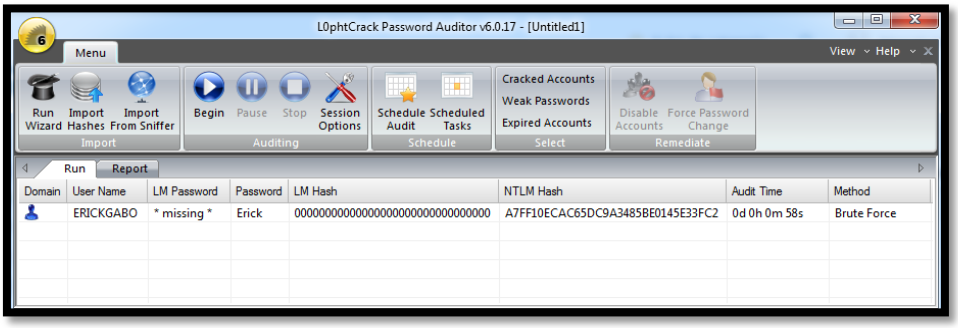

Figura 30 Clave recuperada con L0phcrack

Como se puede ver en la Figura 30 la contraseña del usuario ERICKGABO es Erick, se demoró 58 segundos en analizar y encontrar la contraseña del usuario indicado y el método por el cual se encontró la clave es Ataque de Fuerza Bruta.

Esta herramienta es muy útil ya que permite darse cuenta si una clave es débil o fuerte, en este caso la clave que utilizó para el Sistema Operativo Windows el usuario ErickGabo es una clave débil, ya que la herramienta solamente se demoró 58 segundos en recuperarla y además como se puede apreciar la clave solo contiene letras mayúsculas y minúsculas.

Cuando una clave es fuerte la herramienta puede tardar horas e inclusive días en recuperarla, esto sucede cuando la contraseña contiene una combinación de letras, números y caracteres especiales.

3.4.3 Uso de Cain & Abel para obtener la clave del usuario

3.4.3.1 Cargar los usuarios del log

- Abrir el programa y presionar en “Craker” y click derecho en “Add to list”. Ver Figura 31.

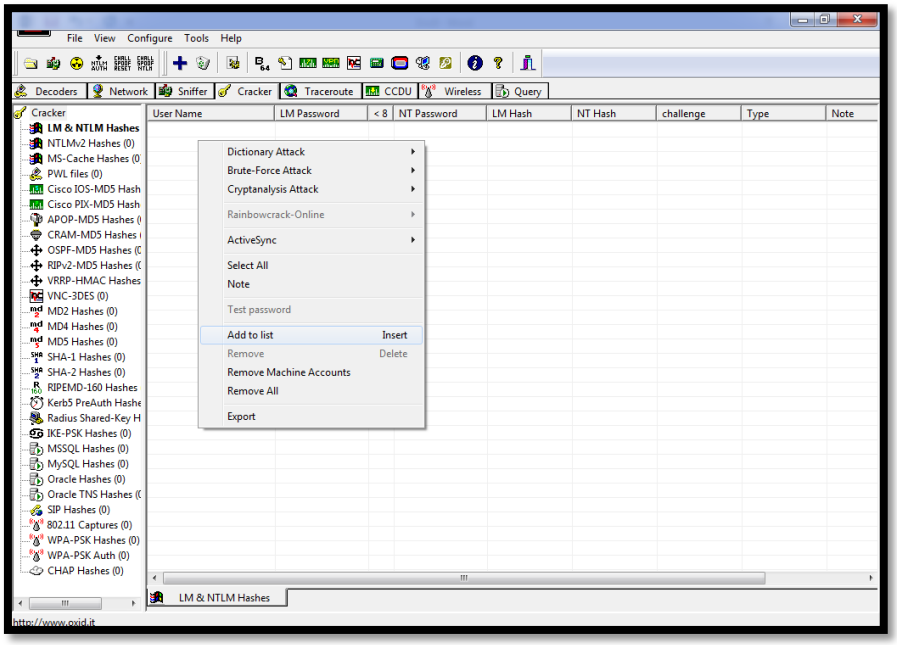

Figura 31 Herramienta Cain & Abel

- Seleccionar la opción “Import hashes from a SAM database”, y añadir el archivo SAM y SYSTEM recuperados. Ver Figura 32, 33 y 34

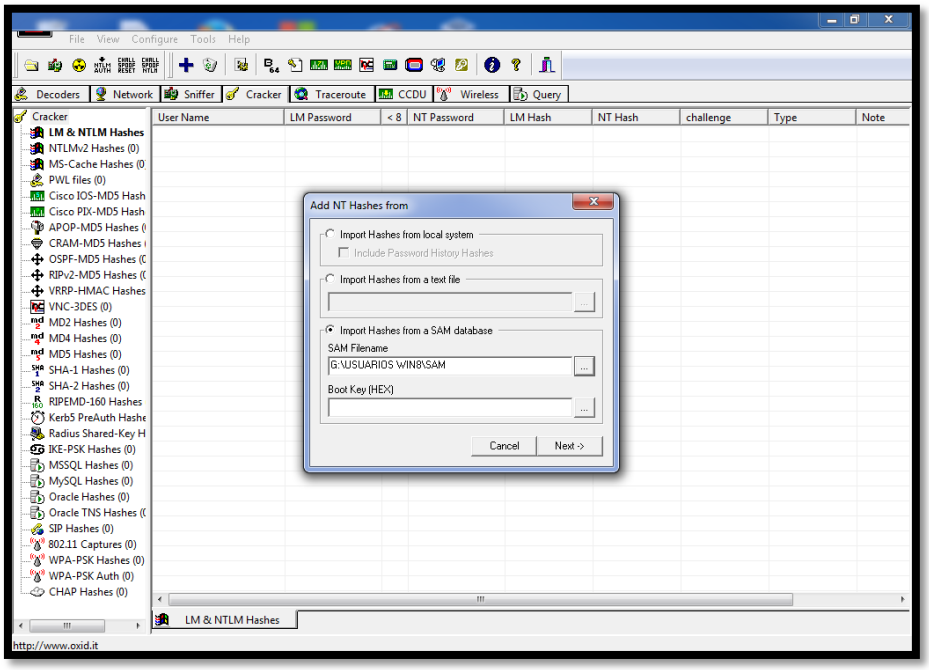

Figura 32 Ingreso del archivo SAM

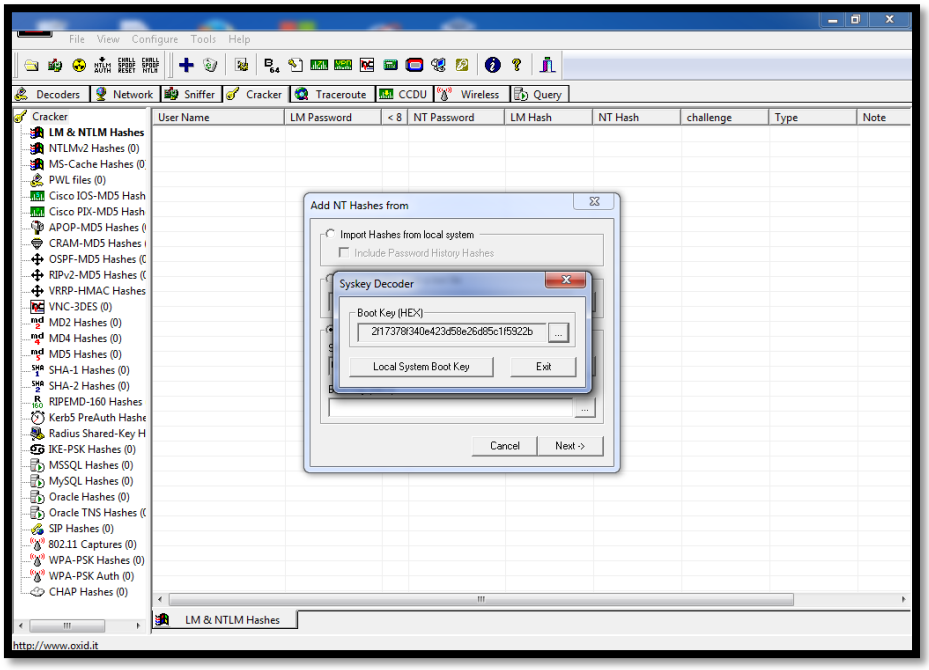

Figura 33 Ingreso del archivo SYSTEM

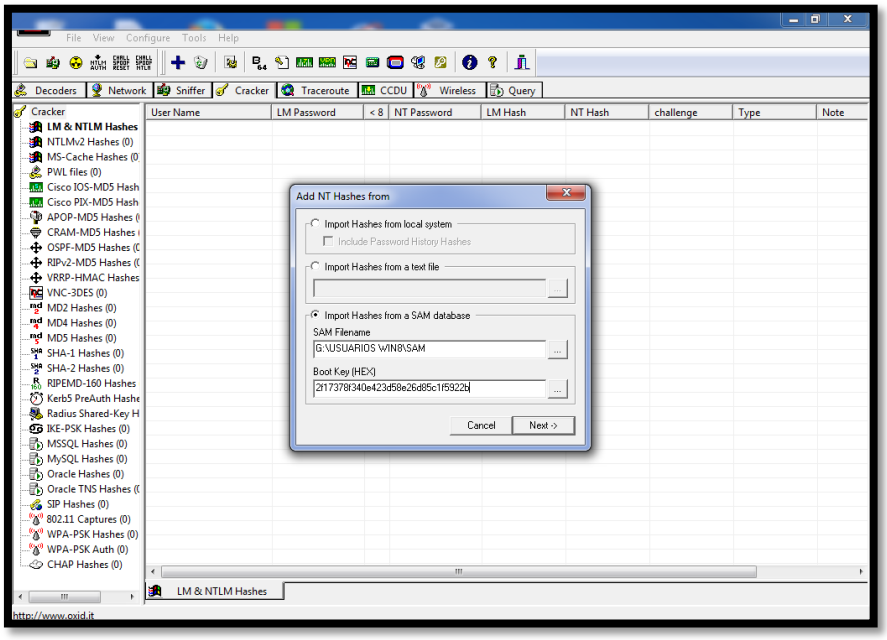

Figura 34 Archivos SAM y SYSTEM ingresados

- Presionar siguiente “Next” y se verán los usuarios del log ingresado. Ver Figura 35.

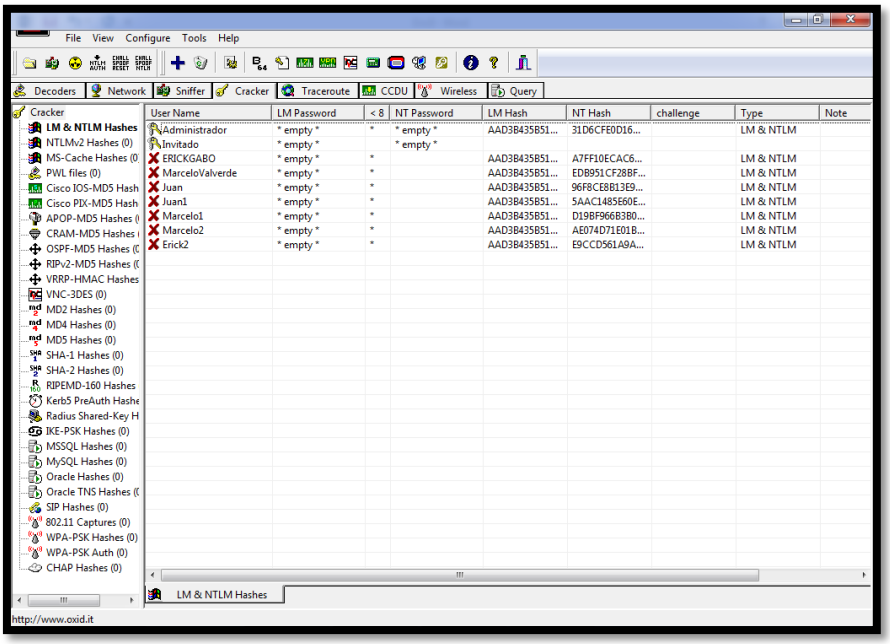

Figura 35 Visualización de los usuarios del log ingresado

3.4.3.2 Ejecutar para obtener la contraseña de los usuarios

- Para iniciar el análisis de un usuario, hacer click derecho > Brute-Force Attack > NTLM Hashes. Ver Figura 36

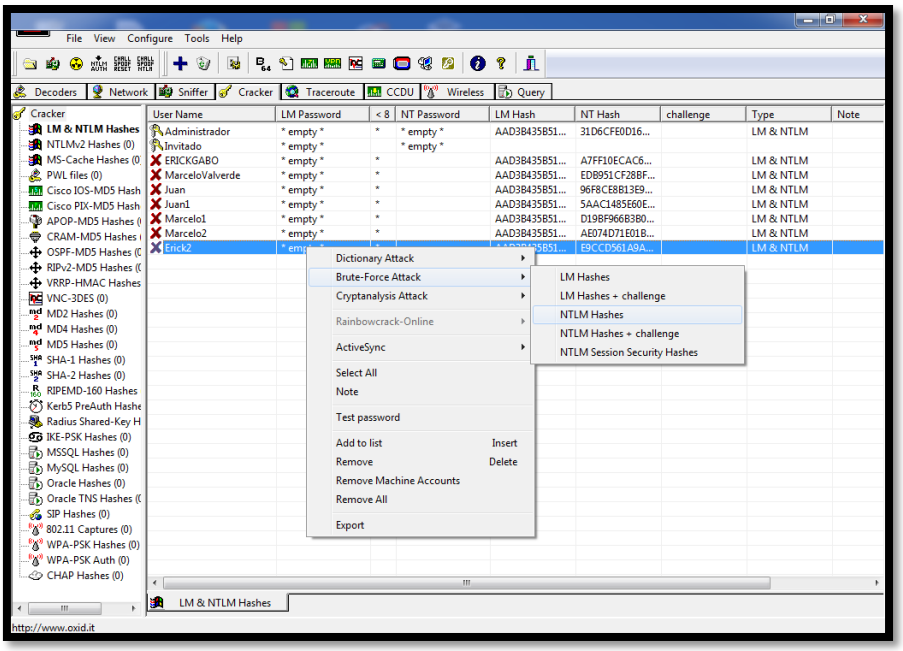

Figura 36 Selección de la técnica Password Cracking

- En esta ventana se puede seleccionar el tamaño o número de letras que contiene la clave, el patrón con el que se desea buscar la contraseña y precionar “Start”. Ver Figura 37.

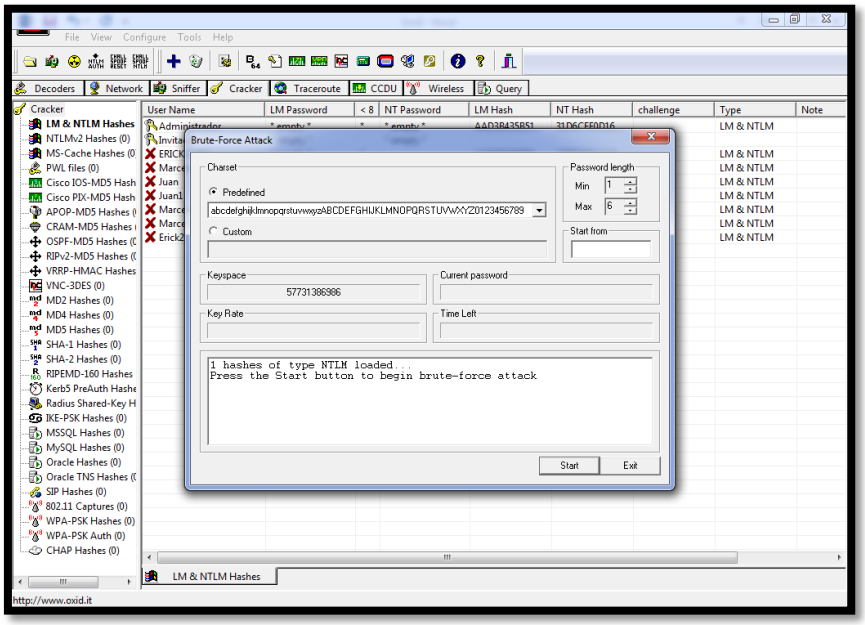

Figura 37 Configuración para iniciar análisis con Cain & Abel

- Cuando inicia el análisis la herramienta indica en tiempo máximo que se demorará en encontrar la contraseña del usuario indicado. Ver Figura 38.

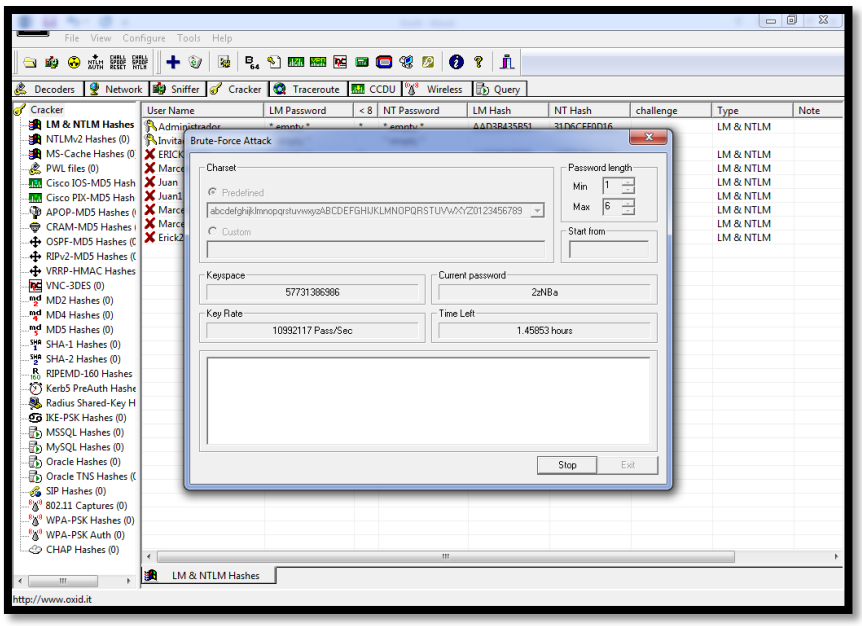

Figura 38 Inicio del análisis para recuperar la contraseña

- Al final del análisis se puede visualizar la contraseña del usuario. Ver Figura 39.

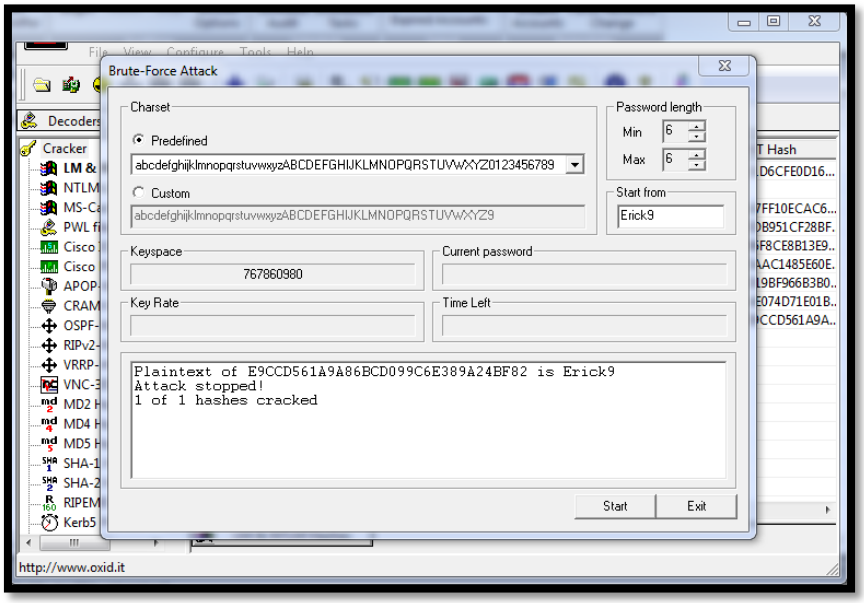

Figura 39 Resultado del análisis con Caín & Abel

- En esta práctica se han realizado varios análisis de los diferentes usuarios con esta herramienta como se puede ver en la Figura 40.
  Se han recuperado las siguientes claves: Ver Tabla 3

Tabla 3 Contraseñas recuperadas de los usuarios con Caín y Abel

Usuario	Clave
ERICKGABO	Erick
MarceloValverde	Marcelo89
Juan	Ju@n.1989
Juan1	Juan89
Marcelo1	7u@n1
Marcelo2	Marcelo
Erick2	Erick9

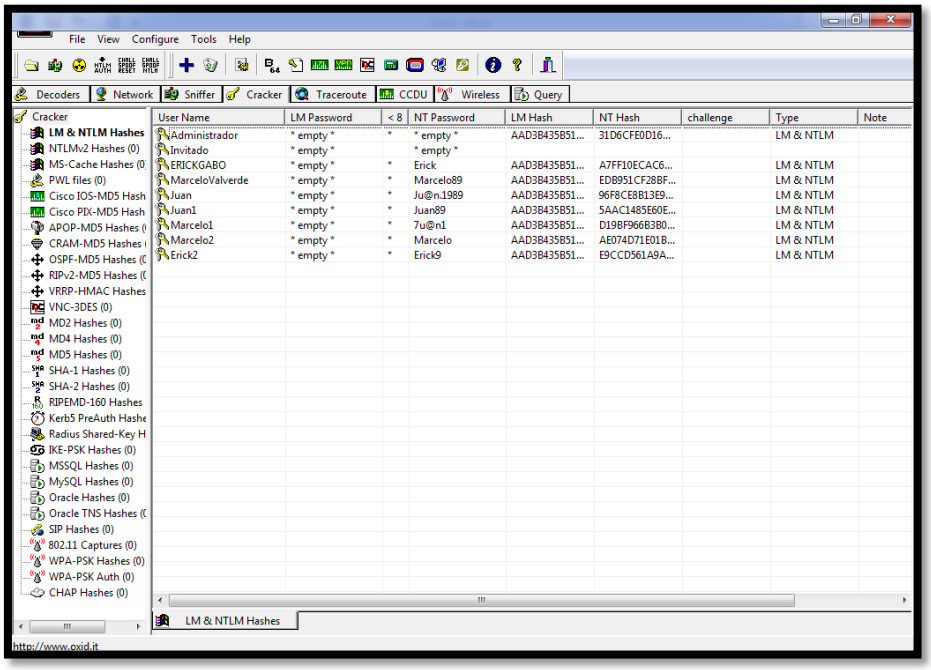

Figura 40 Contraseñas recuperadas de los usuarios con Caín y Abel

3.4.4 Análisis de las herramientas utilizadas

Las herramientas que han sido utilizadas para esta práctica (L0phcrack y Cain & Abel) son de una versión de prueba, por ese motivo no tienen habilitadas el 100% de su capacidad y velocidad para recuperar claves fuertes es decir que la misma contenga letras mayúsculas, letras minúsculas, números, caracteres especiales y sean mayores a 6 caracteres.

Se ha tratado de resolver el problema planteado sin utilizar recursos económicos de la empresa auspiciante de este proyecto, por este motivo se ha podido dar una solución adicional para el seteo de las contraseñas de los usuarios, la cual se pueden ver a continuación.

3.4.5 Uso de LiveCD de Linux Mint para setear contraseñas Windows

- Reiniciar el equipo el cual se va a setear la contraseña

- Bootear desde el cd que contiene el sistema operativo de Linux Mint. Ver Figura 41.

Figura 41 Menú de booteo del equipo

- Abrir el terminal e instalar el chntpw (Change NT Password) "$ sudo aptitude install chntpw". Ver Figura 42 y 43

Figura 42 Ingreso del comando de instalación de chtpw

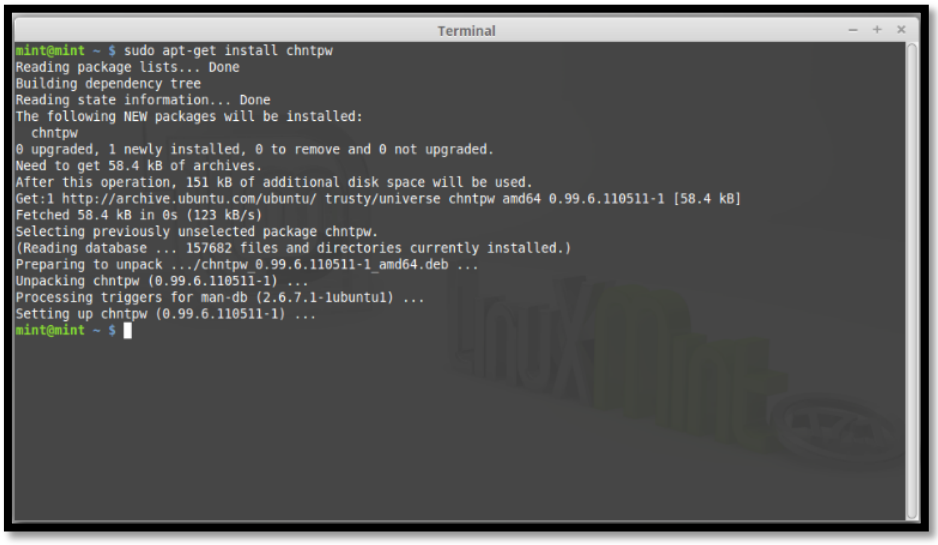

Figura 43 Instalación de chntpw

- Ingresar en el directorio donde está el archivo SAM " cd /media/Mint/Disco/Windows/System32/config" y ejecutar "chntpw –u Usuario SAM". Ver Figura 44 y 45

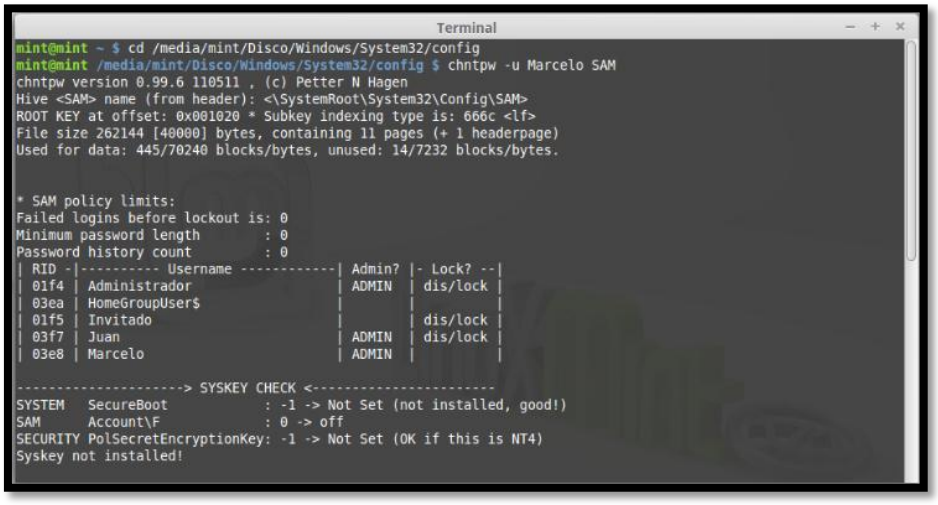

Figura 44 Ejecución del comando para cambiar la contraseña

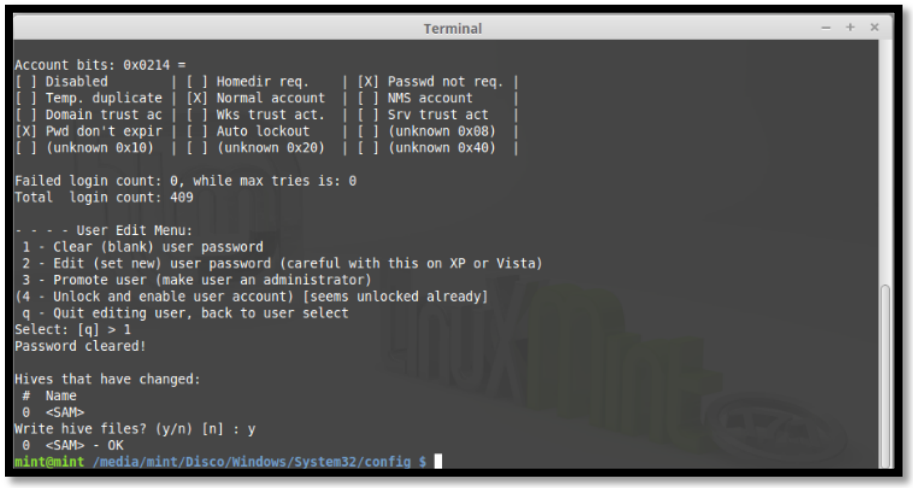

Figura 45 Selección de la opción que se desea ejecutar

Puede elegir una de las siguientes opciones a realizar sobre la contraseña.

- Dejar la cuenta sin contraseña (1).
- Especificar una nueva contraseña para la cuenta (2).
- Promover al usuario a Administrador (3).
- Desbloquear y activar la cuenta (4).

4. CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Todas las empresas deben tener asignado a sus empleados un usuario y contraseña para mantener de una forma organizada la información y sobre todo por seguridad, las mismas que son registradas en el log del sistema la cual consta de dos archivos encriptados SAM y SYSTEM, y se encuentran ubicados en el siguiente path “C:\Windows\System32\config”, estos archivos no se pueden ser copiados ni alterados mientras el sistema operativo se está ejecutando.

- Las principales técnicas hacking para realizar Password Cracking son Ataque Diccionario, Ataque de Fuerza Bruta y Ataque Híbrido, por lo que concluimos que para nuestra práctica se utilizó la técnica de Fuerza Bruta dando los resultados esperados.

- Las diferentes herramientas para la desencriptar contraseñas o vulnerar cualquier sistema se ofrecen en la web sin restricción alguna por lo que nos permite realizar cualquier tipo de espionaje u obtención de información, en este caso la contraseña de un usuario de Windows.

- Se realizó un estudio y comparación entre varias herramientas que sirven para recuperar contraseñas y se han escogido L0phcrack y Caín ya que estas herramientas no afectan al log de Windows directamente, sino que utilizan una copia del mismo.

4.2 Recomendaciones

- Para que las contraseñas sean seguras se recomienda que cumplan con estándares o políticas de seguridad tales como tener números, letras, caracteres especiales y que tengan un tiempo de caducidad es decir cambiar de contraseña cada cierto tiempo, cada mes es lo recomendable.

- Para realizar la recuperación de contraseñas de un usuario de Windows se recomienda utilizar el Ataque de Fuerza bruta siempre y cuando se lleve a cabo el proceso de autorización por parte de la empresa. Esto puede ser utilizado en el caso de que exista personal que haya sido liquidado o que se haya olvidado su contraseña.

- Es recomendable utilizar las herramientas llamadas L0phcrack y Caín & Abel ya que estas tienen características y funciones adecuadas para la recuperación de ciertas contraseñas dependiendo del nivel de seguridad y la longitud de la misma, utilizando el log de Windows, así como también es posible utilizar un LiveCD del Linux para setear la contraseña del usuario.

BIBLIOGRAFÍA Y WEBGRAFÍA

Alegsa, L. (2010). Obtenido de http://www.alegsa.com.ar/Dic/ataque%20por%20diccionario.php

Barzanallana, R. (2014). Criptografía. Obtenido de http://www.um.es/docencia/barzana/IACCSS/Criptografia.html

Borghello, C. (2009). Segu.Info. Obtenido de http://www.segu-info.com.ar/proyectos/p1_hash.htm

Ec-Council. (2011). System Hacking.

Férez, P. G. (2010). El registro de Windows.

Fernandez, C. M. (2012). Norma ISO 27001:2007 del Sistema de Gestión de la Seguridad de Información. Seguridad y Salud, 5.

Fernandéz, C. M. (2012). Normar ISO Relativas a TICS. Madrid.

García, J. (07 de 05 de 2013). faqoff. Obtenido de http://faqoff.es/que-es-un-ataque-por-fuerza-bruta/

García, L. (2013). Informatica Forense. Obtenido de http://es.slideshare.net/leidyjohanagarciaortiz/informatica-forense-17491793

Guerra, N. R. (2013). Technodyan. Obtenido de http://www.technodyan.com/3-programas-para-crear-live-cds-de/

Gutiérrez, P. (2013). Obtenido de http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Gutiérrez, P. (2013). Obtenido de http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Hernandez, M. (2013). Obtenido de http://forensicsmexico.blogspot.com/2013/09/la-importancia-del-registro-de-windows.html

Hernandez, M. (2013). Obtenido de http://forensicsmexico.blogspot.com/2013/09/la-importancia-del-registro-de-windows.html

INTECO. (2010). Instituto Nacional de Tecnologías de la Computación.

Inteco. (2011). Recomendaciones para la creación y uso de contraseñas seguras.

L0phcrack, W. (s.f.). Obtenido de http://es.wikipedia.org/wiki/L0phtCrack

Linux.org. (s.f.). Taringa. Obtenido de http://www.taringa.net/posts/linux/17611310/Live-CD-de-linux-que-es-y-para-que-sirve.html

López, J. P. (2012). Temas Avanzados en Seguridad y Sociedad de la Información.

Luz, S. D. (2010). Obtenido de http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Luz, S. D. (16 de 11 de 2010). Obtenido de http://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

Martínez, A. (2011). Identificación, autenticación y control de accesos.

Martinez, G. O. (2009). Introducción a la criptografia.

Montoro, M. (2009). Obtenido de http://www.net-security.org/article.php?id=1266

Morales, R. (2013). Retico. Obtenido de http://retico.gt/2013/10/09/principios-de-la-seguridad-informatica-2/

Orozco, D. (2011). Windows.

Prandini, P. (s.f.). magazcitum. Obtenido de http://www.magazcitum.com.mx/?p=2193#.VctC0_l_Oko

Romero, I. V. (2012). Auditorias de Sistemas. En Auditorias de Sistemas.

Sánchez, H. C. (2014). Criptografía y metodos de cifrado.

Tanenbaum, A. S. (2010). Obtenido de http://wcruzy.pe/so/01introduccion.pdf

Tinajero, M. (2014). Obtenido de http://es.slideshare.net/marcotinajero/criptonalisis-41603195?from_action=save

UIT. (2010). Unión Internacional de Telecomunicaciones. Obtenido de Ciberseguridad: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

WARD, J. (2011). Obtenido de http://informetecnicodesistemaoperativo.blogspot.com/