Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas

Marco Roberto López Vallejo [1]

1Universidad Internacional SEK-Ecuador, marcolopezva@hotmail.com

RESUMEN

Las tecnologías informáticas hoy en día están presentes de forma directa o indirecta en los más diversos aspectos de la sociedad; en el ámbito económico y comercial, las interacciones políticas, e incluso entre los distintos tipos de relaciones interpersonales. Esta presencia de la implementación de la informática, demanda de control y dominio de la información que genera y consume la sociedad contemporánea.

La presente investigación tiene como objetivo mostrar ejemplos prácticos de cómo acceder a ordenadores con diferentes sistemas operativos sin conocer las contraseñas de acceso a los mismos, ósea mediante la ruptura de contraseñas. Para lograrlo este objetivo, se desarrolló un análisis de los principales elementos que intervienen para acceder de forma eficiente a los sistemas operativos más socializados. Como resultado de la investigación se evidencian ejemplos prácticos para los sistemas operativos: Windows 10, Linux (FEDORA) y MAC. Las técnicas presentadas en esta investigación, empleadas con legitimidad y prudencia son una poderosa herramienta. Las cuales asumen la poción de prácticas de hacking ético.

Palabras claves: ruptura de contraseñas, hacking ético, sistemas operativos.

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Ethical hacking. Vulnerability of Operating Systems in access by passwords.

ABSTRACT

Computer technologies today are present directly or indirectly in the most diverse aspects of society; In the economic and commercial field, political interactions, and even between different types of interpersonal relationships. This presence of the implementation of information technology, demand for control and control of the information generated and consumed by contemporary society.

The present research aims to show practical examples of how to access computers with different operating systems without knowing the passwords to access them. To achieve this goal, we developed an analysis of the main elements that intervene to efficiently access the most socialized operating systems. As a result of the research, practical examples are shown for operating systems: Windows 10, Linux (FEDORA) and MAC. The techniques presented in this research, used with legitimacy and prudence are a powerful tool. Which assume the potion of practices of ethical hacking.

Keywords: Breaking of passwords, ethical hacking, operating systems..

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

1. INTRODUCCIÓN

En la actualidad el mundo se mueve en función del uso de las nuevas tecnologías. Las mismas son utilizadas en la educación, la salud, las finanzas y la mayoría de las áreas de la sociedad(Taylor, Fritsch, & Liederbach, 2014). El acceso a los ordenadores es de vital importancia en la seguridad y protección de la información(Mansfield-Devine, 2016). En muchas ocasiones se utilizan las contraseñas con este fin. Violación en varias ocasiones los usuarios olvidan sus contraseñas y luego no tienen acceso a la información que necesitan. En otros casos ocultar las contraseñas se puede utilizar para ocasionar daños a personas y/o empresas(“Hacking Web Intelligence,” 2015).

La informática forense es la disciplina que tiene como objetivo principal la investigación en sistemas informáticos de hechos de relevancia jurídica o simplemente para una investigación privada. (Pagés López, 2013). Debido a esta definición, a partir de esta disciplina, se puede tener acceso a la información de computadoras, de las cuales no se posee la contraseña.

2. METODOS

El aumento del uso de las tecnologías ha provocado problemas de seguridad en los sistemas que se utilizan(Machuca, 2012). Los ordenadores son utilizados en casi todas las áreas de la sociedad. Las propiedades del acceso a las computadoras se han convertido en un aspecto crucial en aras de mantener la seguridad de las mismos(Haughey, Epiphaniou, & Al-Khateeb, 2016).

Uno de los tipos de acceso más usado es el uso de contraseñas. Es necesario poseer claves identificativas para restringir el acceso a los datos. En muchas ocasiones las contraseñas son olvidadas o son cambiadas con fines de hacer daño a una persona o entidad, convirtiéndose esta acción en delito informático(Trejo, Alvarez, & Chimbo, 2016).

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Los ataques informáticos van en ascenso y hace que las empresas o personas pierdan ese activo tan importante que es la información. La informática forense juega un papel crucial en esta situación, debido a que a partir de ella se puede realizar el análisis forense informático necesario para identificar las causas y evidencias de hecho(García & Alexandra, 2014).

En las empresas y en las entidades de servicios de la información es necesario el uso de las computadoras. Con el objetivo de conocer las contraseñas de estas unidades, ya sea por olvido o por el daño ocasionado por algún elemento o persona, es necesario conocer algunos conceptos importantes que serán descritos a continuación:

Sistema Operativo

Un sistema operativo es un programa que se encarga de hacer funcionar una computadora, pues gestiona los procesos básicos del sistema. Además, se encarga de gestionar el hardware del ordenador para el usuario. El sistema operativo reconoce todos los dispositivos externos de computadora, como son el teclado o la impresora (Fernández López, 2007)(Di Iorio, 2013).

Los sistemas operativos gestionan de forma lógica las funcionalidades de la computadora, lo que permite la interacción del usuario con el ordenador a través de la solución de tareas específicas(Semprini, 2016).

Existen varios sistemas operativos. Dentro de ellos se encuentran:

Windows (en sus diferentes versiones): Windows XP, Windows Vista, Windows 7, Windows 8, entre otros. Este Sistema operativo es propiedad de Microsoft y es privativo, por lo que es necesario pagar la licencia para poder utilizarlo(“Hacking Web Intelligence,” 2015).

Mac OS: Es un sistema operativo privativo creado por la empresa Apple(Taylor et al., 2014).

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Unix: Es un sistema operativo muy seguro que es utilizado por supercomputadoras y ordenadores de grandes empresas. Es privativo y su propietario es la empresa AT&T(Taylor et al., 2014).

GNU/Linux: Sistema operativo totalmente gratuito. Puede ser modificado según las necesidades del cliente. Es un sistema operativo bastante seguro(Taylor et al., 2014).

Los usuarios utilizan el sistema operativo según las características específicas que necesiten y la disponibilidad de recursos.

Seguridad en los Sistemas Operativos.

Según la ISO ISO/IEC 27001: "La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. "(ISO, 2013)

La seguridad en los sistemas informáticos tiene presente los siguientes elementos:

a) Integridad: La información se modifica de forma autorizada.
b) Confidencialidad: La información es accesible por las personas autorizadas.
c) Control de Acceso: La información es accedida por las personas autorizadas.
d) Autenticidad: Se refiere a la capacidad de comprobar la autenticidad de la persona que accede a los recursos del sistema.
e) Disponibilidad: Los recursos del sistema tienen que estar disponibles para usuarios autorizados en el momento que los necesiten.

Uno de los elementos que poseen los sistemas operativos y que sirven para mantener la seguridad en los mismos es el control de acceso. El control de acceso, se refiere, a los objetos a los que puede acceder cada usuario. Un objeto es una entidad que contiene información, y puede ser físico o abstracto.

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Otro elemento que poseen los sistemas operativos para mantener la seguridad es el sistema de autenticación. La autenticación es el proceso por el cual un usuario se identifica en el sistema obteniendo las credenciales que establecen los permisos de acceso a los objetos.

El sistema operativo crea una cuenta de usuario que está constituida por la siguiente información:

a) Login o nombre de usuario: Término utilizado como identificador único del usuario en el sistema.
b) Identificador de usuario (UID): Número único que se asocia al usuario dentro del sistema y que es utilizado en la autorización.
c) Identificadores de grupo (GID): Son los identificadores de grupos. Un usuario pertenece a un grupo y de ahí se toman los permisos del usuario.
d) Información adicional del usuario: nombre, fecha de nacimiento, teléfono, sexo, entre otros.
e) Información adicional del mecanismo de autenticación: contraseñas, tiempo de validez.

Las claves o contraseñas es una forma de autentificación para controlar el acceso a un objeto. La contraseña debe ser secreta para evitar el acceso de personas que no tienen permiso para entrar al sistema. Los usuarios, en ocasiones, olvidan sus contraseñas. En otras ocasiones la pérdida de claves no es utilizada con buenos fines y pueden ser utilizadas como delitos informáticos.

En noviembre de 2001, la Unión Europea, firma el Convenio de Ciberdelincuencia del Consejo de Europa, siendo el marco de referencia en el campo de las tecnologías y los delitos para esa región. En el mismo, de define delito informático como:

Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de los mismos. (Ministerio de asuntos exteriores. Consejo de Europa, 2001)

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

En (Paéz & Acurio, 2011) se cita a Julio Téllez Valdés que define al delito informático como: “El delito informático son conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.”

Delitos informáticos en Ecuador.

En (Organización de Estados Americanos (OEA), 2014) se especifica que en el 2013 aumentaron las violaciones de datos en América Latina. Más de 552 millones de identidades quedaron expuestas debido a violaciones de datos. Los delitos cibernéticos y los actos de hacktivismo son el principal origen de esta tendencia. Además, crecen los delitos de ataques dirigidos, adaptando campañas de spear-phishing (robo de identidad con objetivos específicos) para no hacerlas tan evidentes. También aumentaron las estafas en las redes sociales y los robos y troyanos bancarios.

En Ecuador, como en todos los países,existen delitos informáticos. No se encontró evidencia de estadísticas sobre delitos informáticos sobre olvidos o canjes de contraseñas para realizar algún mal a una persona u organización. Sin embargo si se encontró información sobre de delitos de robo de contraseñas en Internet.

En 2013, se registró un aumento en la cantidad de quejas cibernéticas de los ciudadanos en las autoridades nacionales en Ecuador. Los ciudadanos reportaron casos relacionados con ataques de interceptación ilegales sobre la integridad de la información, dispositivos de abuso de sistemas, ciberfalsificación, fraude informático, pornografía infantil y delitos contra la propiedad intelectual. (Organización de Estados Americanos (OEA), 2014)

Desde el 10 de agosto, cuando entró en vigencia el Código Orgánico Integral Penal, hasta el 31 de mayo del 2015, se registraron 626 denuncias por delitos informáticos en la Dirección de Política Criminal de la Fiscalía General.(Fiscalía General del Estado.

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Ecuador, 2015) En el caso de ocurrir algún delito informático es necesario hacer uso de la informática forense.

Análisis forense

La Oficina Federal de Investigación (FBI), por sus siglas en inglés, ha desarrollado soluciones informáticas que permiten realizar análisis forense. Esta institución define la Informática Forense como: "La ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio informático."(FBI, 2001)

La informática forense es una técnica que puede ser utilizada por los peritos o personas naturales en procesos de investigación de delitos informáticos o en cualquier situación que lo amerite.(Azas Manzano, 2015)

Según, Miguel López Delgado, el análisis forense digital es: "El conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que en determinado caso pueden ser aceptadas legalmente en un proceso judicial." (López Delgado, 2007)

Estándares de análisis forense para equipos tecnológicos.

Existen varios estándares a nivel mundial que regulan el análisis forense. A continuación, se especifican algunos.

RCF3227

Los RFC «RequestForComments» son documentos que recogen propuestas de expertos en una materia concreta con el fin de establecer una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento. Puede servir como estándar para la recopilación de información en incidentes de seguridad tecnológica. En el documento se especifica la transparencia que

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

debe tenerse en esta etapa y que debe quedar bien claro la cadena de custodia de la información.

Guía de la ScientificWorkingGroup Digital Evidencie (SWGDE)

La SWGDE es un grupo creado con el objetivo de identificar evidencias latentes en ordenadores. Gestiona una serie de procedimientos administrativos para tener presente en la informática forense. Provee un conjunto de criterios y estándares para la preservación de la evidencia. Muestra las líneas generales para el adiestramiento de los peritos y las buenas prácticas para lograr un buen análisis forense.

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

ISO 27037:2012

Norma que renueva las directrices de la norma RFC 3227 para la recopilación de evidencias. Está dirigida a los nuevos dispositivos y enfocada a la técnica actual. La norma está orientada al procedimiento de los peritos en el proceso de recogida, identificación y secuestro de la evidencia digital, sin embargo, no específica elementos en la fase de Análisis de la evidencia.

Esta Norma Internacional proporciona directrices para las actividades específicas en el manejo de la evidencia digital potencial; estos procesos son: identificación, recolección, consolidación y preservación de evidencia digital potencial. (International Standard (ISO), 2012)

UNE 71505 y UNE 71506.

Normas publicadas por la Asociación Española de Normalización y Certificación (AENOR). Su finalidad es proveer una metodología que permita preservar, adquirir, documentar, analizar y presentar pruebas digitales. Las normas pueden ser utilizadas para dar respuestas a las infracciones legales e incidentes informáticos que puedan ocurrir en las diferentes empresas y/o entidades.

La norma 71506 se conformó para definir el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas. Complementa los procesos que conforman el sistema de gestión de las evidencias electrónicas, según se describe en la Norma UNE 71505. (Áudea, Seguridad de la información, 2013)

Modelo extendido de Séamus Ó Ciardhuain

Es un modelo extendido para investigaciones de ciberdelitos, creado en el 2004 por Séamus Ó Ciardhuáin y publicado por International Journal of Digital Evidence (IJCE).

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

El modelo permite comprender el proceso completo de un análisis forense de computadoras. Propone las siguientes actividades: Conciencia, Autorización, Planificación, Notificación, Búsqueda e identificación de pruebas, recolección de pruebas, Transporte de las pruebas, almacenamiento de pruebas, examen de prueba, hipótesis, presentación de hipótesis, prueba /defensa de hipótesis y diseminación de información. El modelo tiene forma de cascada y cada actividad es la entrada de la próxima (International Journal of Digital Evidence Summer (IJCE), 2004).

Los estándares reflejados anteriormente pueden ser adecuados por la empresa o persona que vaya a utilizarlos.

Herramientas para acceder a las contraseñas de un ordenador

Existen diferentes herramientas para la recuperación de contraseñas. Por ejemplo, en el sistema operativo Windows, existen herramientas para recuperar claves de diferentes programas. A continuación, se muestran algunas:

a) PasswordFox y ChromePass: recupera los usuarios y contraseñas del navegador Firefox y Chrome respectivamente.
b) IE PassView: recupera elementos de Internet Explorer.
c) MessenPass: recupera claves de servicios de mensajería instantánea, como: Google Talk, MSN Messenger, Pidgin,ICQ, AOL Instant Messenger, Windows Live Messenger o Yahoo! Messenger.
d) Mail PassView: recupera las contraseñas de correo electrónico como: Hotmail,Gmail, Outlook, Mozilla Thunderbird, Netscape, Yahoo! Mail.
e) Free Word/Excel Password: recupera claves de Word y Excel que no superen los 8 caracteres. Es necesario tener instalado el Microsoft .NET Framework.

La herramienta Windows PasswordRecoveryLasticse utiliza para borrar la contraseña de una cuenta de Windows y poder acceder al ordenador sin esta restricción. Además, puede recuperar el hash de una clave y restaurar la contraseña original. Para ejecutar la herramienta se deben seguir los siguientes pasos:

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

a) Ejecutarla herramienta y crear un disco o USB de arranque.
b) Reiniciar el ordenador y arrancarlo desde el dispositivo.
c) Restablecer los hash o eliminar las contraseñas de las cuentas de usuario.

La desventaja de esta herramienta es que es privativa y es necesario pagar por su uso.

La herramienta Windows PasswordUnlocker elimina la contraseña del usuario de Windows para poder acceder al sistema. Para su utilización es necesario crear una imagen ISO en un CD o en un USBy reiniciar el ordenador. La aplicación muestra los usuarios y permite eliminar las contraseñas. Cuenta con una versión gratuita limitada y solo puede ser utilizada para sistema operativo Windows.

Las herramientas primeras herramientas analizadas no pueden ser utilizadas para obtener la clave de un usuario para un sistema operativo. Windows PasswordRecoveryLastic es privativa y sería necesario obtener la licencia para poder utilizarla. Windows PasswordUnlocker posee una versión gratuita, pero es limitada y solo sirve para eliminar las contraseñas.

Informática forense en Ecuador

Ecuador, no está exento de los delitos informáticos, por lo que sus leyes rigen el proceso de auditoría informática o de análisis forenses.

La Constitución de la República del Ecuador, en su artículo 178 establece que: “El Consejo de la Judicatura es el órgano de gobierno, administración, vigilancia y disciplina de la Función Judicial”.(Asamblea Constituyente, 2008)

El Reglamento del Sistema Pericial Integral de la Función Judicial, Resolución 040-2014, regula el funcionamiento y administración del sistema pericial integral de Ecuador. En dicho documento se regula la calificación, designación, obligación, honorarios, evaluación, capacitación y régimen disciplinario de los peritos, además del informe pericial. (Consejo de la Judicatura, 2014)

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos plante que: “Artículo 1. Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.” (Congreso Nacional, 2002)

El Código del Sistema Pericial Integral de la Función Judicial establece las reglas del sistema penal. A continuación se especifican 2 artículos que regulan a los peritos y el informe pericial.

Artículo 3: “Todo perito que sea designado como tal en cualquier tipo de proceso judicial o pre procesal, debe estar previamente calificado por el Consejo de la judicatura, y debe cumplir con las regulaciones y la normativa de la resolución”.

Artículo 511, inciso 6 plantea que: “El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.” (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

Todas las disposiciones dictadas por estas leyes deben ser cumplidas por las personas que estén involucradas en algún delito informático.

En Ecuador las investigaciones de delitos informáticos se realizan de forma técnica y requiere bastante tiempo para establecer la responsabilidad de aquellos que violan la ley a través de una computadora. En el país es difícil se dificultan las investigaciones propiciadas por delitos informáticos pues la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país.

3. RESULTADOS

En varias ocasiones los peritos o personas se encuentran ante la dificultad de que no pueden acceder a los ordenadores pues no cuentan con las claves. Como resultados de

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

esta investigación, se evidencia cómo obtener las contraseñas en los sistemas operativos: Windows 10, Linux (FEDORA 23) y MAC.

Windows 10

1. En la figura 1 se muestra el arranque del sistema operativo por medio del disco de instalación de Windows 10.

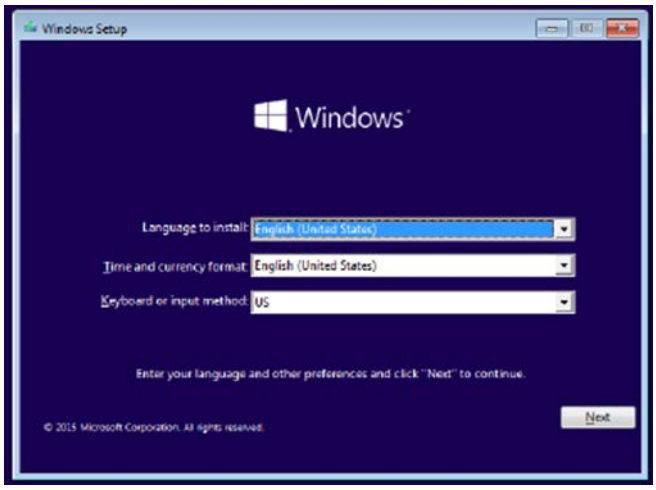
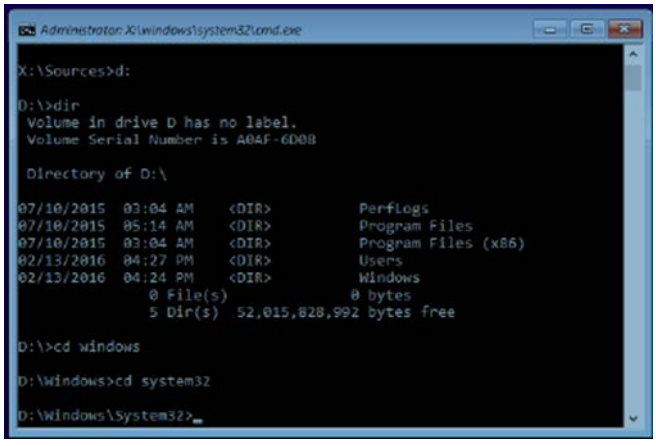


Figura 1: Disco de instalación Windows 10

2. PresionarSHIFT+F10. Se abre una consola de comandos del sistema donde el usuario ubicará la partición donde está instalado el sistema operativo y accederá a la carpeta system32. Como se puede observar en la figura 2.



Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Figura 2: Acceso a la carpeta System32

3. Como se muestra en la figura 3, especificar los siguientes comandos:

a) ren utilman.exe utilman0.exe.
b) ren cmd.exe utilman.exe.
c) Cerrar y reiniciar.

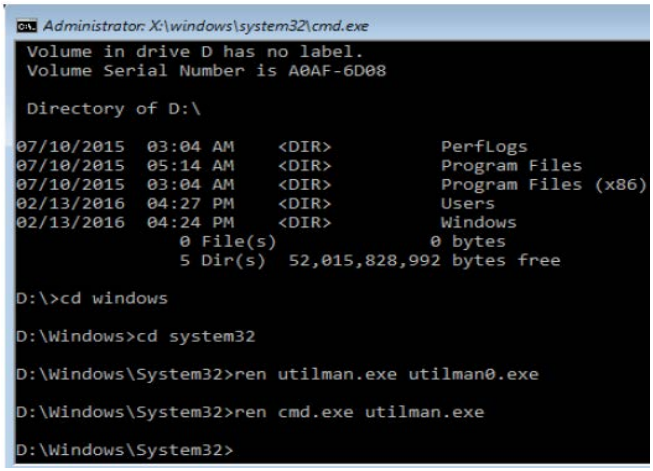


Figura 3: Comandos en System32

4. Presionar Windows+U en la pantalla de inicio del sistema para abrir la consola. En la figura 4 se muestra la consola referida.

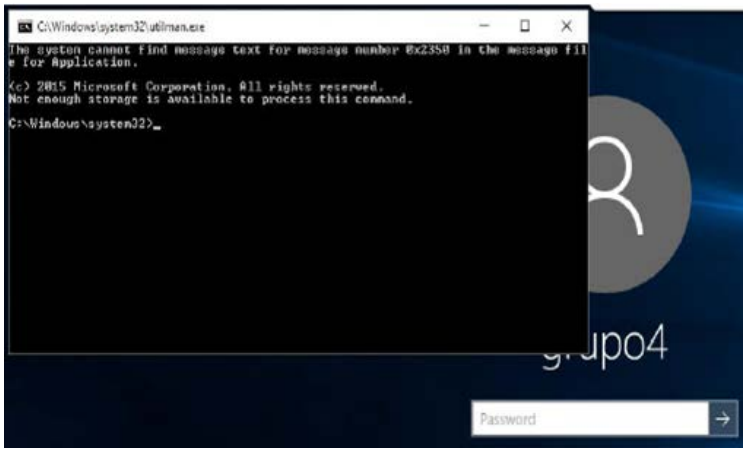


Figura 4: Consola en la pantalla de inicio

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

5. En la consola que se muestra en la figura 4 se especificar los comandos presentados a continuación:

a) net user.
b) net user (nombre del usuario) *.
c) Nueva contraseña y la confirman.

Obteniéndose el panel mostrado en la figura 5.

6. Ingresar al sistema con la nueva contraseña. En el panel mostrado en la figura 5 ya puede introducir la nueva contraseña de acceso al sistema.

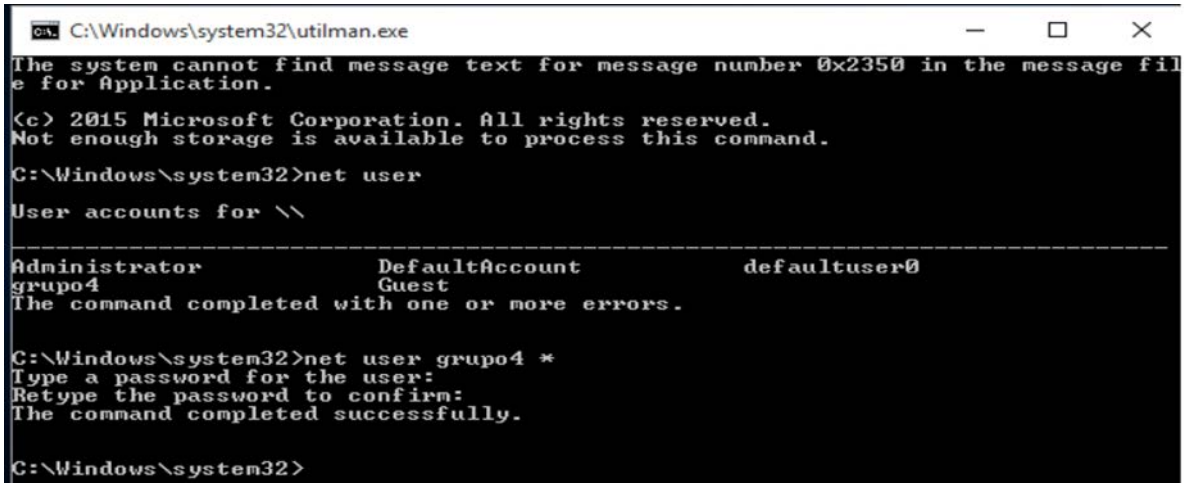


Figura 5: Panel que permite la introducción de la nueva contraseña de acceso.

Linux (FEDORA 23)

1. Pulsar la tecla “e” en la pantalla de arranque del SO para poder editar el GRUB.Como se muestra en la figura 6.

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

Figura 6: Línea de arranque de Linux

2. Buscar la línea del KERNEL, digitar la instrucción (init=/bin/sh) y pulsarCrtl+X. Como puede observarse en la figura 7.

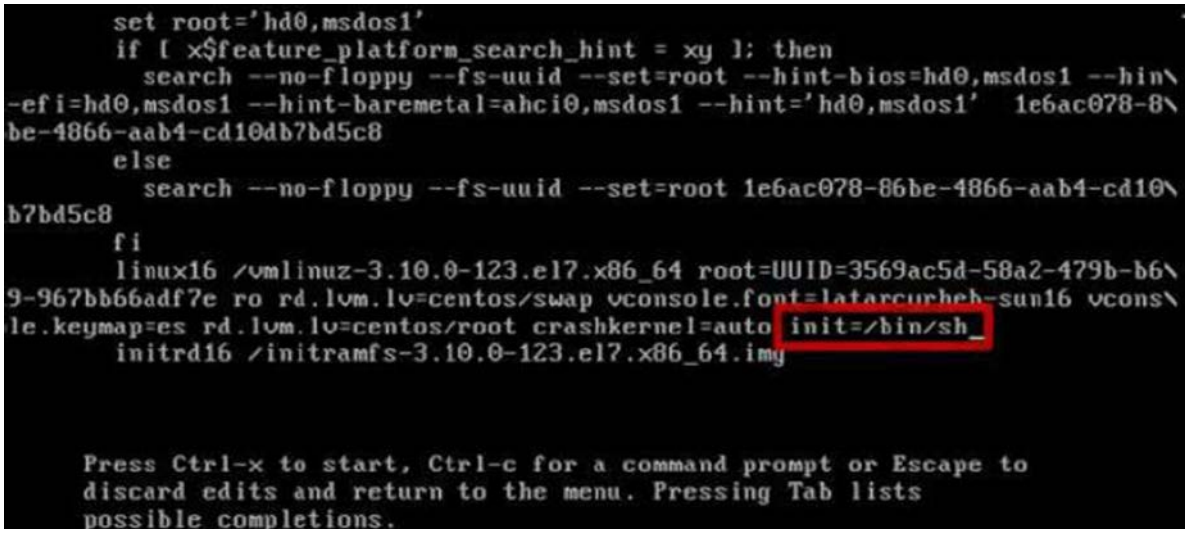


Figura 7: Acceso y comando dentro del Kernel

3. Ingresar al sell donde se podrá acceder como Súper Usuario sin tener la contraseña. Luego se ingresan los siguientes comandos:

a) Sh-4.2# su - para ingresar como administrador
b) [root@localhost] # mount –o remount,rw / (para dar permisos de lectura y escritura a la raíz)
c) Una vez con los respectivos permisos procedemos a cambiar la contraseña
d) [root@localhost] # passwdmchuquitarco

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

e) New passwdord : ********
f) Confirmpassword :********
g) [root@localhost] # touch /.autoreload (para forzar los cambios)
h) [root@localhost] # reboot –f (para reiniciar el sistema)

MAC

En el sistema operativo MAC el usuario debe disco de instalación de software de Mac OS, reiniciar el ordenador y mantener presionada la tecla C con el objetivo de iniciar desde el disco.

En el momento que aparezca el menú del Instalador, el usuario debe seleccionar la opción Cambiar contraseña y continuar con las instrucciones para poder cambiar la clave.

Cuando aparezca el Instalador, elige Cambiar contraseña del menú Instalador y sigue las instrucciones que aparecen en pantalla para cambiar la contraseña.

Otra forma de realizar el cambio de clave en MAC se especifica a continuación. El usuario debe entrar en modo recuperación reiniciando el ordenador y mantener presionad Comando+R. En el menú Herramientas, seleccionar el terminal y teclear resetpassword. Luego pulsar Enter y modificar la clave para acceder a la computadora.

4. CONCLUSIONES

Como resultado del presente trabajo se concluye que:

Evidentemente uno de los elementos necesarios para mantener la seguridad de los sistemas operativos es el uso de contraseñas. Dada que cada vez más los usuario e instituciones almacenas y/o procesan información su información en plataformas informáticas.

Existe una tendencia a nivel global al aumento de los delitos informáticos que se centran en el robo o rupturas de claves de acceso a sistemas. El análisis forense y los estándares

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

internacionales descritos en este trabajo son los más comúnmente utilizado por personas naturales e instituciones. En Ecuador existen las regulaciones legislativas pertinentes para afrontar irregularidades de esta índole.

Los ejemplos desarrollados en esta investigación para el restablecimiento de contraseñas pueden ser utilizados para sistemas operativos Windows 10, Linux (FEDORA 23) y MAC, con efectividad y facilidad. Estas técnicas deben ser empleadas prudentemente y con finalidades benéficas; considerándose dentro de estos parámetros hacking ético.

5. REFERENCIAS BIBLIOGRÁFICAS

AENOR publica nueva norma UNE 71506:2013. (2013, September 13). Retrieved February 12, 2017, from http://www.audea.com/aenor-publica-nueva-norma-une-715062013/

Asamblea Constituyente. (2008). Constitución de la República de Ecuador. Ecuador.

Áudea, Seguridad de la información. (2013). AENOR publica nueva norma UNE 71506:2013. Obtenido de http://www.audea.com/aenor-publica-nueva-norma-une-715062013/

Azas Manzano, M. F. (2015). DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR. Universidad Internacional SEK. Recuperado de http://repositorio.uisek.edu.ec/handle/123456789/1417

Congreso Nacional. (2002). Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Registro Oficial Suplemento 557. Ecuador.

Consejo de la Judicatura. (2014). Resolución 040-2014. Ecuador.

Di Iorio, A. H. (2013). La Informática Forense y el proceso de recuperación de información digital. Revista Democracia Digital E Governo Eletrônico, 1(8). Recuperado de http://www.buscalegis.ccj.ufsc.br/revistas/index.php/observatoriodoegov/article/view/34270

Revista Publicando, 4 No 10. (1). 2017, 31-51. ISSN 1390-9304

FBI. (2001). Computer Evidence Examininations at the FBI.Estados Unidos.

Fernández López, G. (2007). Seguridad en sistemas operativos. España.

Fiscalía General del Estado. Ecuador. (13 de 6 de 2015). Fiscalía General del Estado. Recuperado el 2 de 3 de 2016, de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

García, U., & Alexandra, M. (2014). Artículo Científico-Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. Recuperado de http://repositorio.espe.edu.ec:8080/handle/21000/8123

Hacking Web Intelligence. (2015). Network Security, 2015(8), 4. https://doi.org/10.1016/S1353-4858(15)30066-0

Haughey, H., Epiphaniou, G., & Al-Khateeb, H. M. (2016). Anonymity networks and the fragile cyber ecosystem. Network Security, 2016(3), 10–18. https://doi.org/10.1016/S1353-4858(16)30028-9

International Journal of Digital Evidence Summer (IJCE). (2004). An extended model of cybercrime investigations. Estados Unidos.

International Standard (ISO). (2012). Information technology-Security techniques-Guidelines for identification, collection, acquisition, and preservation of digital evidence. ISO 27037:2012. Suiza.

ISO. (2013). Sistema de gestión de seguridad de la información. ISO/IEC 27001.

López Delgado, M. (2007). Análisis forense digital. España: Red Iris.

Machuca, L. (2012). Los delitos informáticos en la ley de comercio electrónico, firmas electrónicas y mensajes de datos y el principio de seguridad jurídica y legalidad. Recuperado de http://dspace.uniandes.edu.ec/bitstream/123456789/4814/1/TUAMDP006-2012.pdf

Mansfield-Devine, S. (2016). The battle for privacy. Network Security, 2016(6), 11–15. https://doi.org/10.1016/S1353-4858(16)30058-7

Ministerio de asuntos exteriores. Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Budapest.

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). Código Orgánico Integral Penal. Ecuador.

Organización de Estados Americanos (OEA). (2014). Tendencias de seguridad cibernética en América Latina y le Caribe.

Paéz, J., & Acurio, S. (2011). Derecho y Nuevas Tecnologías.

Pagés López, J. (2013). Temas avanzados en seguridad y sociedad de la información. España.

Semprini, G. (2016). Lineamientos para la creación de laboratorios informáticos forenses. In XVI Simposio Argentino de Informática y Derecho (SID 2016)-JAIIO 45 (Tres de Febrero, 2016). Recuperado de http://sedici.unlp.edu.ar/handle/10915/58306

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital Crime and Digital Terrorism (3rd ed.). Upper Saddle River, NJ, USA: Prentice Hall Press.

Trejo, C. A., Álvarez, G. A. D., & Chimbo, K. M. O. (2016). LA SEGURIDAD JURÍDICA FRENTE A LOS DELITOS INFORMÁTICOS. AVANCES, 10(12), 41.