

# **Aplicación de Técnicas de Fuerza Bruta con Diccionario de Datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación.**

*Hernán M. Domínguez L.<sup>1</sup>, Edgar A. Maya O.<sup>1</sup>, Diego H. Peluffo O.<sup>1</sup>, Christian M. Crisanto Ñ.<sup>2</sup>*

<sup>1</sup> CIERCOM/FICA, Universidad Técnica del Norte, Av. 17 de Julio 5-21 y Gral. José María Córdova, Ibarra, Ecuador, código postal 199.

<sup>2</sup> DIO, Banco Central del Ecuador, Av. 10 de Agosto y Briseño, Quito, Ecuador.

hmdominguez@utn.edu.ec, eamaya@utn.edu.ec, dhpeluffo@utn.edu.ec

Fecha de recepción: 18 de junio 2016 - Fecha de aceptación: 2016

## **ABSTRACT**

This paper shows the increased security risks in recent years, attacks on authentication controls specifically passwords. Methods and techniques for violating such controls, with emphasis on techniques using brute force attacks with data dictionary; plus a proof of concept outlined using a free distribution of Linux "Kali Linux" and penetration tools "Metaexploits Framework", to finally raise the most commonly used controls to mitigate such attacks with a more detailed use approach and management secure passwords as one of the main controls used in Ecuador in times of crisis.

Keywords: Informatic security, controles, passwords, Brute Force, Data Dictionary, penetration, attacks

## **RESUMEN**

El presente artículo muestra el incremento de riesgos de Seguridad Informática en los cinco últimos años en ataques de control de autenticación específicamente las contraseñas, métodos y técnicas para vulnerar este tipo de controles; con énfasis en las técnicas utilizadas por fuerza bruta con diccionario de datos. Además se presenta una prueba de concepto utilizando una distribución libre de Linux “Kali Linux” y herramientas de penetración “Metaexploits Framework” para finalmente plantear los controles más utilizados que permiten mitigar este tipo de ataques con un enfoque más detallado en el uso y manejo de contraseñas seguras como uno de los controles principales a usarse en Ecuador en época de crisis.

Palabras clave: Seguridad Informática, controles, contraseña, Fuerza Bruta, Diccionario de Datos, autenticación simple, ataque.

## **1. INTRODUCCIÓN**

En los últimos cinco años los incidentes relacionados con la Seguridad Informática han ido incrementando en cifras alarmantes; según la consultora PwC en su reporte Global State of Information Security Survey 2015, indica que 42.8 millones de incidentes de seguridad a nivel mundial equivale a 117,339 ataques por día, con un incremento del 66% respecto al 2009. El promedio de las pérdidas financieras aumentó en un 33% a nivel global. (PwC, 2015).

Así mismo, en el último año existe un 29.27% de empresas en América del Sur, frente a un 31.59% de todas las regiones, que han sufrido cincuenta o más incidentes de seguridad, de acuerdo a la consultora PwC y que se muestra en la Figura 1. (PwC, 2016).

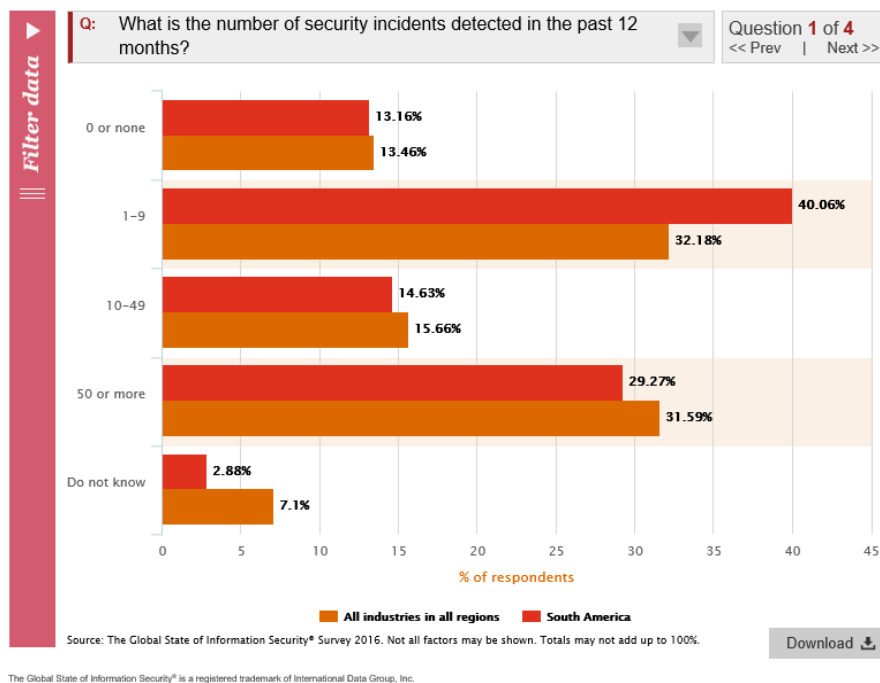


Figura 1. Número de incidentes

Fuente: (PwC, 2016)

Dentro de los incidentes de seguridad más comunes se encuentran los casos de ataques sobre controles de autenticación, en los cuales las contraseñas siguen siendo el talón de Aquiles de este tipo de ataques; como se señala en una encuesta realizada por ESET Latinoamérica (Goujon, 2013), se tiene que:

- El 42.3% de los usuarios aseguran utilizar una palabra o frase real como parte de la contraseña.
- El 36.7% afirma utilizar una o pocas contraseñas para todos los servicios.
- El 33.9% de los encuestados asevera emplear datos personales para conformar sus contraseñas.

De acuerdo al informe “Worst Passwords List” realizado por la empresa SplashData; de las peores contraseñas del 2015 indican que la tendencia de utilizar secuencias numéricas de teclado o nombres cortos se mantiene con respecto a años anteriores, y es así que las contraseñas “123456”, “password”, “12345678”, “qwerty”, “dragon” y “football” siguen manteniéndose en el top ten con respecto al 2011. (SplashData Inc., 2016)

Este tipo de investigación reafirma la grave problemática existente en temas de concientización y capacitación en seguridad informática y sobre todo en la protección de nuestra identidad personal.

Con estos antecedentes, es importante que la sociedad conozca cómo funcionan las técnicas de ataques de Fuerza Bruta con Diccionario de Datos, ya que con el avance de las tecnologías como los GPU (Unidad de Procesamiento de Gráficos) se puede llegar a descifrar contraseñas de 8 caracteres en 5.5 horas, como lo señala (Catoira, 2012) en el boletín WeLiveSecurity de ESET, comprobando de ésta manera que es cuestión de tiempo y de recursos llegar a vulnerar los métodos de autenticación simple “Contraseñas”.

## 2. MATERIALES Y MÉTODOS

### 2.1 Contexto

Existen varias formas de Ataques para vulnerar un método de autenticación simple de tipo contraseña, de entre los cuales se pueden destacar:

- Keyloggers.- es un software que graba todo lo que se tipea en el teclado y envía la información al atacante.

- Phishing.- técnica de robo de identidad virtual más popular en la red, la cual consiste en crear una falsa aplicación y mediante correos o mensajes inducir al usuario que inicie sesión en su cuenta.
- Brute Force Attack.- Es una técnica que permite probar todas las combinaciones posibles hasta encontrar la palabra o texto legible que fue cifrado. De la información obtenida en investigaciones anteriores (RedInfoCol, 2010) que establecen que un Ataque de fuerza bruta consta de siguientes elementos vitales:
  - a. Un Charset o alfabeto utilizado para obtener todas las posibles combinaciones.
  - b. Una longitud de palabra, la cual nos determina todas las posibles combinaciones de la siguiente manera:  $\#Combinaciones = longitud\_palabra \wedge longitud\_charset$ ; esto quiere decir que por una palabra de 2 letras con un alfabeto de 26 letras obtenemos  $26^2 = 676$  combinaciones posibles. Esto es  $26^2 = 676$ . Entre más grande es la palabra ó el charset, mayor es el número de combinaciones y mayor es el tiempo invertido en obtener una posible respuesta.
  - c. Palabra cifrada, la cual va a ser usada para romper el ciclo de iteraciones en caso de encontrar la palabra legible.
  - d. Algoritmo o función de cifrado, ya que sin esta no es posible hacer el bruteforce
- Dictionary Attack.- Un ataque de diccionario es una técnica de violación de contraseñas, en la cual se prueban consecutivamente palabras de un diccionario para validar una clave correcta, para este tipo de ataques se cuenta con listados de claves ó passwords; los cuales son archivos de texto que se pueden descargar de Internet como por ejemplo puede ser el archivo llamado Rockyou o listados de claves de sitios web que sufrieron ataques en sus servidores y los datos de sus usuarios quedaron expuestos. (DragonJAR, 2011)  
Estos diccionarios pueden ser compilados y actualizados con herramientas como Crunch, Theharvester, CeWL, entre otros; las cuales son alimentadas con claves de uso común para una región, una empresa, nombres que se encuentran en un diccionario o listas de las contraseñas más usadas.

Se puede realizar ataques combinados; los de Fuerza Bruta y Diccionario de Datos con lo cual se logra mejorar los tiempos de respuesta en la ejecución de los mismos.

Existen dos herramientas que son parte principal dentro de un proceso de Ataque por Fuerza Bruta con diccionario de datos, las cuales se describen a continuación:

- NMAP. – Herramienta de código abierto para exploración de red y auditoría de seguridad. NMAP utiliza paquetes IP crudos para determinar que equipos se encuentran disponibles en una red, que servicios ofrecen, que sistemas operativos ejecutan, que filtro o cortafuegos se está utilizando entre otras características. (NMAP.ORG, 2016)
- METASPLOIT. - Es un proyecto open source que proporciona información acerca de vulnerabilidades de seguridad, permite realizar tareas de explotación y test de penetración de forma más fácil que los métodos de hacking tradicionales. (Metasploit, 2016)

Estas herramientas descritas anteriormente se encuentran incluidas en una distribución de Linux diseñado y equipado para realizar pruebas de penetración, vulnerabilidad y auditorías de seguridad; esta distribución se la conoce como Kali Linux; la misma que es una re-construcción basada en Debían de la distribución de BackTrack.

Con estos antecedentes descritos anteriormente, un ataque de fuerza bruta con diccionario de datos es sencillo realizarlo sobre ambientes idóneos, por lo cual; en esta investigación se propone realizar un ataque de fuerza bruta por diccionario de datos a un escenario planteado, demostrando lo relativamente fácil que puede ser vulnerar un sistema en el cual requiere el ingreso de una credencial de acceso como único método de autenticación.

## 2.2 Prueba de Concepto

En la Figura 2 se muestra el escenario de red planteado para la realización de esta prueba de concepto, en donde, se tiene de una red LAN con direccionamiento IP de clase C, sobre la cual se encuentran dos servidores; uno de Aplicaciones y otro de Transferencia de Archivos, adicionalmente se cuenta con un router que brinda acceso a la nube Internet.

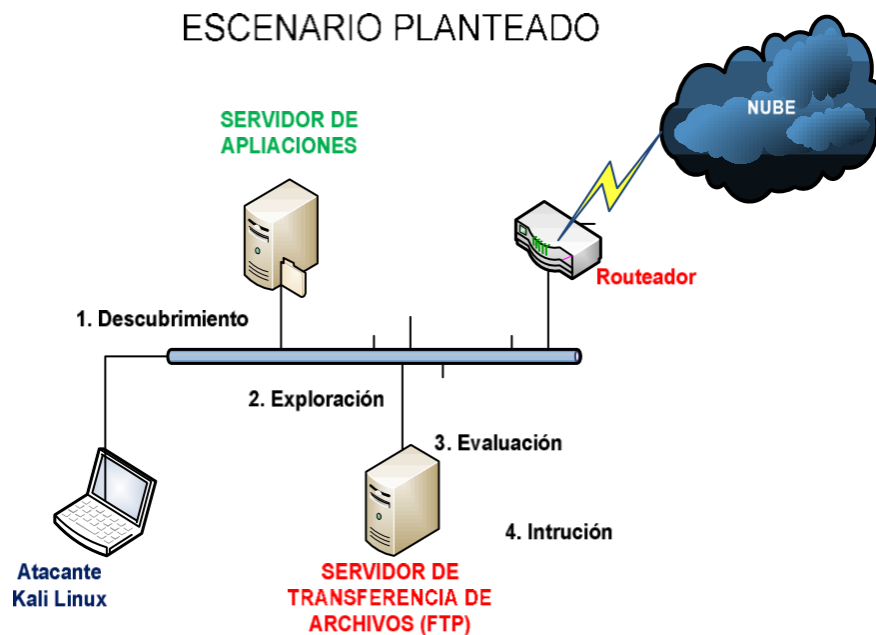


Figura 2. Escenario Planteado.

Esta prueba de concepto se la ha distribuido en cuatro etapas secuenciales, que empieza desde el descubrimiento de la red, para luego realizar una exploración de equipos y servicios, seguido de la evaluación de la vulnerabilidad, y finalmente con la intrusión al sistema vulnerable.

### Etapas de Descubrimiento

En esta etapa se delimita el área de acción, se debe entender los riesgos asociados al negocio y por último se obtiene información como: Segmentos de redes y rangos de direcciones IP's.

Una vez que se tiene conexión a la red, desde la máquina Atacante se envía el comando `#ifconfig -a` que permitirá conocer sobre que segmento de red estamos trabajando; en este caso en la red 192.168.100.x/24.

### Etapas de Exploración

En esta etapa se aplican técnicas no invasivas para identificar todos los blancos potenciales del segmento de red, para ello se utilizan técnicas de scanning; en este caso Nmap con dos variantes:

- a. Desde la máquina Atacante se ejecuta el comando `nmap -v -sn 192.168.100.0/24`. En la Figura 3, se muestra gráficamente la aplicación que permite explorar la red de 254 hosts que estamos trabajando.

```
root@kali:~# nmap -v -sn 192.168.100.0/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016
Initiating ARP Ping Scan at 20:04
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 20:04, 2.02s elapsed (255
Initiating Parallel DNS resolution of 255 hosts. at
Completed Parallel DNS resolution of 255 hosts. at 2
Nmap scan report for 192.168.100.0 [host down]
Nmap scan report for 192.168.100.1
Host is up (0.0017s latency).
MAC Address: 94:04:9C:5A:B7:F1 (Huawei Technologies
Nmap scan report for 192.168.100.2
Host is up (0.00033s latency).
MAC Address: 00:0C:29:9D:DB:83 (VMware)
Nmap scan report for 192.168.100.3 [host down]
Nmap scan report for 192.168.100.4
Host is up (0.00019s latency).
MAC Address: AC:B5:7D:FC:FC:FB (Liteon Technology)
```

Figura 3. Exploración de la red

- b. Desde la máquina Atacante se ejecuta el comando `nmap -O -v 192.168.100.2` ; en donde la dirección IP 192.168.100.2, representa un host activo identificado en el paso anterior. En la Figura 4, se muestra un ejemplo de escaneo del host cuya dirección IP es 192.168.100.2; en donde se conoce los puertos abiertos asociados a un servicio, y con la opción `-O` del comando ejecutado; se obtiene la versión del Sistema Operativo y el release ejecutado en el host.

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:9D:DB:83 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

Figura 4. Servicios y Sistema Operativo

Para el caso de estudio el servicio encontrado es FTP por puerto 21 sobre un S.O Linux cuyo kernel es la versión 2.6.

#### Etapa de Evaluación

En esta etapa se analizan los datos encontrados para determinar las posibles vulnerabilidades asociadas a los servicios, existen numerosos sitios en Internet con información y herramientas para hacer más fácil esta etapa.

Para este caso de estudio se usa la herramienta Msfconsole, que es una de las consolas más populares para Metasploit Framework (MSF); la misma que permite entre otras cosas mantener una consola centralizada para todas las opciones disponibles en el Framework y manejar comandos intuitivos.

En la Figura 5, se muestra la consola msf. Para ingresar a la consola de metasploit se ejecuta el comando: #msfconsole



Figura 5. Consola msfconsole.

Una vez ingresado a la consola MSF se envía a buscar con el comando #search ftp, todas las vulnerabilidades asociadas al servicio FTP, para este caso puntual se utiliza el auxiliar: auxiliary/scanner/ftp/ftp\_login (Una vulnerabilidad sobre la autenticación del servicio FTP)

### Etapa de Intrusión

En esta etapa se empieza a vulnerar los servicios encontrados en las etapas anteriores, puede que no se logre el objetivo en el primer intento, con lo cual se debe buscar posibles alternativas o variantes que permitan concluir con la tarea.

Una vez encontrado el auxiliar para intentar vulnerar el servicio FTP, se ingresa el comando:

```
#use auxiliary/scanner/ftp/ftp_login
```

```
#show options
```

Este último comando nos muestra las opciones y parámetros a configurar. Para el caso de estudio se configura los siguientes parámetros:

- USERNAME: en este parámetro se coloca el nombre del usuario de la aplicación, en este caso se conocía el nombre de usuario nsfadmin; si se desconoce el nombre del usuario se debe configurar el parámetro USERPASS\_FILE con un diccionario de posibles nombres.
- PASS\_FILE: En este parámetro se coloca la ruta y el archivo donde se encuentra nuestro diccionario de datos, para este caso práctico se utilizó el diccionario de datos de Rockyou.
- STOP\_ON\_SUCCES: En este parámetro se habilita para que cuando se encuentre la clave de acceso; se detenga el test.
- RHOSTS: En este parámetro se configura la IP del host a vulnerar.
- THREADS: En este parámetro se configura el número de hilos de conexión, para este caso, 205 hilos.

Una vez configurado los parámetros se envía a ejecutar con el comando: #run



Como se aprecia en la Figura 6, al ejecutar el comando #run se empieza a realizar los intentos con las posibles claves, hasta que muestra la clave con la que pudo ingresar, mostrando el mensaje de LOGIN SUCCESSFULL

```
msf auxiliary(ftp_login) > run
[*] 192.168.100.2:21 - Starting FTP login sweep
[!] No active DB -- Credential data will not be saved!
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:123456 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:12345 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:123456789 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:password (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:iloveyou (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:princess (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:1234567 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:rockyou (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:12345678 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:abc123 (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:nicola (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:daniel (Incorrect: )
[-] 192.168.100.2:21 FTP - LOGIN FAILED: nsfadmin:babygirl (Incorrect: )
[+] 192.168.100.2:21 - LOGIN SUCCESSFUL: nsfadmin:nsfadmin
[-] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_login) >
```

Figura 6. Detección de contraseña mediante técnica de Fuerza Bruta.

### 3. RESULTADOS

Como último paso de la prueba de concepto se intenta conectar al servidor FTP (192.168.100.2) utilizando las credenciales entregadas en el paso anterior. El resultado de ingreso satisfactorio se indica en la Figura 7.

```
root@kali:~/hone# ftp 192.168.100.2
Connected to 192.168.100.2.
220 (vsFTPd 2.3.4)
Name (192.168.100.2:root): nsfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  6 1000    1000          4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  3 1000    1000          4096 Apr 28  2010 mysql-ssl
drwxr-xr-x  5 1000    1000          4096 Apr 28  2010 samba
drwxr-xr-x  2 1000    1000          4096 Apr 19  2010 tikiwiki
drwxr-xr-x  3 1000    1000          4096 Apr 16  2010 twiki20030201
226 Directory send OK.
ftp>
```

Figura 7. Intrusión completada.

### **3.1 Consideraciones Legales**

Antes de realizar un ataque de fuerza bruta u otros ataques que atenten contra la integridad de los sistemas o accesos no autorizados, se debe considerar la tipificación de los delitos informáticos en el Ecuador.

En la Sección 3ra. “Delitos contra la seguridad de los activos de los sistemas de información y comunicación” del Código Orgánico Integral Penal (COIP) publicado en el Registro Oficial de 10 de febrero de 2014 (Asamblea Nacional del Ecuador, 2014), se tipifican entre otros los siguientes delitos:

- Artículo 232.- Ataque a la integridad de sistemas informáticos, penas de tres a cinco años de privación de libertad, y si la infracción se comente a un servicio.
- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, con penas de tres a cinco años de privación de libertad.

### **3.2 Remediaciones**

Partamos que el mejor control es la prevención y la capacitación sin mucha inversión en hardware o software especializado, se puede llegar a implementar controles los cuales disminuyan el riesgo asociado, teniendo en cuenta que para el 2016 en Ecuador el presupuesto Nacional será reducido en unos 4.000 millones de dólares con respecto a 2015, recortando el monto destinado a la inversión en sectores estratégicos, como lo señala diario (El Tiempo, 2015).

Con estos antecedentes se debe optimizar todo tipo de recursos, por tal razón se debe apuntar a los siguientes controles:

- Contraseñas fuertes. Es importante que los accesos estén protegidos con contraseñas fuertes para no recibir ataques de fuerza bruta que puedan lograr acceso fácilmente a información sensible y confidencial, Paus (2016) recomienda principalmente:
  - No usar palabras o expresiones que se encuentren en un diccionario.
  - Elegir un sistema en el cual desde una frase se obtenga una contraseña, tomando las primeras o últimas letras de cada palabra, alternando entre mayúsculas y minúsculas, mezclándolas con números y caracteres especiales, como resultado tendríamos una contraseña más segura y difícil de adivinar. Ejem. Mi contraseña debe tener mínimo 8 caracteres = McDtM8c\*
  - Se debe cambiar periódicamente las contraseñas y no tener una única contraseña para varios servicios.
- Concientización del usuario. Cuando se trata de garantizar la Seguridad de la Información el factor humano cuenta con un lugar más que relevante y los programas de concientización son el principal y más efectivo control que se pueda implementar (ESET welivesecurity, 2015), además dichos controles pueden hacer la diferencia si se los realiza constantemente y se los maneja como una política institucional.

## **4. CONCLUSIONES**

De la presente investigación se puede concluir que la tendencia de los incidentes en Seguridad Informática en Latinoamérica se ha mantenido en los últimos 5 años.

Con respecto al manejo de contraseñas se ha podido observar que se siguen utilizando las mismas tendencias desde hace varios años atrás, confirmando de esta manera, que no existe o es muy poca la concientización del uso y manejo de las mismas, teniendo en cuenta que resultaría sumamente más económico aplicar este tipo de controles que invertir en equipamiento costoso de seguridad.

Mediante el caso de estudio se pudo concluir que, con un poco de tiempo dedicado a la investigación de Ataques por Fuerza Bruta con Diccionario de Datos, se puede vulnerar sistemas y servicios que utilicen contraseñas débiles como su único método de autenticación.



Las actividades de concientización y capacitación a los empleados y/o funcionarios de las instituciones, son factores claves para mitigar los riesgos asociados a la seguridad; un empleado capacitado que sabe cómo crear contraseñas robustas y cambiarlas periódicamente, por lo tanto, es menos propenso a que sufra ataques de fuerza bruta y por ende colaborará con la seguridad de la empresa y de su hogar.

## 5. REFERENCIAS

- Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Quito, Pichincha, Ecuador: Registro Oficial. Recuperado el 12 de Marzo de 2016, de <https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/2215-suplemento-al-registro-oficial-no-180.html>
- Catoira , F. (11 de Diciembre de 2012). *Cluster de 25 GPU*. (ESET, Productor) Recuperado el 08 de Mayo de 2016, de WeLiveSecurity : <http://www.welivesecurity.com/la-es/2012/12/11/cluster-25-gpu-descifra-contrasenas-8-caracteres-5-5-horas/>
- DragonJAR. (16 de Febrero de 2011). *DragonJAR*. Recuperado el 8 de Mayo de 2016, de <http://www.dragonjar.org/diccionarios-con-passwords-de-sitios-expuestos.xhtml>
- El Tiempo. (11 de Noviembre de 2015). Presupuesto 2016 tendrá USD 4.000 millones menos. *Diario El Tiempo*. Recuperado el 12 de Febrero de 2016, de <http://www.eltiempo.com.ec/noticias-cuenca/171158-presupuesto-2016-tendra-usd-4-000-millones-menos/>
- ESET welivesecurity. (15 de Marzo de 2015). *ESET Security Report Latinoamérica 2015*. Recuperado el 20 de Febrero de 2016, de <http://www.welivesecurity.com/la-es/articulos/reportes/>
- Goujon, A. (21 de Marzo de 2013). *¿El fin de las contraseñas? La autenticación simple cada vez más amenazada*. Recuperado el 28 de Abril de 2016, de WeLiveSecurity: <http://www.welivesecurity.com/la-es/2013/03/21/articulo-el-fin-de-las-contrasenas-la-autenticacion-simple-cada-vez-mas-amenazada/>
- Metasploit. (2016). *metasploit.com*. (O. Source, Ed.) Recuperado el 8 de Mayo de 2016, de <https://www.metasploit.com/>
- NMAP.ORG. (8 de Mayo de 2016). *nmap.org*. (OpenSource, Ed.) Recuperado el 8 de Mayo de 2016, de <http://nmap.org/book/>
- Paus, L. (6 de Mayo de 2016). *Cómo crear una contraseña fuerte en un minuto y proteger tu identidad digital*. (ESET Latinoamérica) Recuperado el 8 de Mayo de 2016, de WeLiveSecurity : <http://www.welivesecurity.com/la-es/2016/05/06/crear-contrasena-fuerte-un-minuto/>
- PwC. (2015). *The Global State of Information Security® Survey 2015*. Recuperado el 21 de Febrero de 2016, de [http://www.pwccn.com/home/eng/rcs\\_info\\_security\\_2015.html](http://www.pwccn.com/home/eng/rcs_info_security_2015.html)
- PwC. (2016). *The Global State of Information Security® Survey 2016*. Recuperado el 8 de Mayo de 2016, de <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html>

RedInfoCol. (21 de Diciembre de 2010). *¿Qué es y cómo funciona un ataque por fuerza bruta?*  
Recuperado el 8 de Mayo de 2016, de <http://www.redinfocol.org/atacando-por-fuerza-bruta-bruteforce-1/>

SplashData Inc. (19 de January de 2016). *Worst Passwords List of 2015*. (M. Slain, Editor)  
Recuperado el 08 de Mayo de 2016, de <http://splashdata.com/blog/> :  
<https://www.teamsid.com/worst-passwords-2015/>

## **AGRADECIMIENTOS**

Los autores hacen extensivo el agradecimiento a la Coordinación de Ingeniería en Electrónica y Redes de Comunicaciones de la Universidad Técnica del Norte, así como a la Dirección de Infraestructura y Operaciones de TI del Banco Central del Ecuador, por el apoyo técnico brindado.