# El uso de contraseñas, un mundo lejos de la extinción: Un Estudio Empírico

Rolando P. Reyes Ch.
Departamento de Seguridad y Defensa
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
Email: rpreyes@armada.mil.ec

Oscar Dieste
Departamento de Ingeniería de Software
Univesidad Politécnica de Madrid
Madrid, España
Email: odiste@fi.upm.es

Efraín R. Fonseca C.
Departamento de Ciencias de la Computación
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador
Email: erfonseca@espe.edu.ec

***Abstract*—*Antecedentes:* En la actualidad los sistemas de información utilizan distintos mecanismos de seguridad para permitir el acceso a sus funcionalidades a usuarios identificados, siendo las contraseñas el modo más común de validación. Existen varias políticas y normas (unas más estrictas que otras) para la creación de contraseñas; sin embargo, éstas aún siguen siendo vulnerables. *Objetivo:* Conocer las vulnerabilidades de diferentes niveles de complejidad de contraseñas propuestos para el presente estudio, así como conocer los tipos de contraseñas usados en los ataques, tipos de atacantes y su procedencia. *Método:* Esta investigación fue llevada a cabo a través de un estudio empírico basado en un experimento controlado. El estudio se fundamentó en la utilización de honeypots para emular un servidor SSH, el cual fue expuesto al internet durante un tiempo aproximado de 30 días. *Resultados:* Se registró un gran número de ataques, los cuales no llegaron a vulnerar ningún nivel de complejidad de contraseñas propuestos. *Conclusión:* A pesar que no fueron vulnerados los niveles de complejidad propuestos, se considera que un incremento en el factor tiempo, podría permitir que dichos niveles sean vulnerados.**

**Keywords:** experimento controlado, vulnerabilidad, contraseña, entropía, ataque, honeypot.

## I. Introducción

Independientemente de la información que desean proteger los usuarios, de la tecnología utilizada para tal efecto y de la potencial consecuencia de una intrusión; las contraseñas se han convertido en el medio de seguridad más habitual de acceso a información digital de toda índole [1, 2]. Las personas y empresas utilizan contraseñas con el afán de proteger todo tipo de recursos (ej. correo electrónico, bancos, portales, citas, sitios de redes sociales, etc.) [3, 2]. Sin embargo, las contraseñas que utilizan los usuarios han demostrado ser vulnerables a potenciales amenazas que atentan contra la privacidad de la información [4].

Existen estudios tales como el de Yan et al. [5] y el de Florencio et al. [3], que han determinado que la memoria humana no gestiona adecuadamente una cantidad considerable de contraseñas. Por ejemplo, para un usuario que maneja 30 cuentas, le resultará muy complejo recordar 30 contraseñas distintas, más aún, si su complejidad es alta. Esto ha obligado a que los usuarios seleccionen un número menor de contraseñas de las que realmente necesitan [6]. En otras palabras, los usuarios se esfuerzan por recordar entre 5 o 6 contraseñas, y las distribuyen entre todas su cuentas, o simplemente usan como contraseña a una combinación entre ellas [3].

Desde esta perspectiva, se podría indicar que la complejidad de las contraseñas es directamente proporcional a su seguridad; es decir, mientras más compleja se torna una contraseña, su seguridad es mayor. La complejidad de las contraseñas es una problemática que se acrecienta cuando los usuarios definen sus contraseñas en base a "supuestos" parámetros básicos de creación, tales como: "fácil de recordar" , "segura" , etc. Por ejemplo, para el caso de las políticas de creación de contraseñas que requieren la inclusión de al menos tres dígitos como parte de la contraseña, el cumplimiento de esta política por parte del usuario se limita en la mayoría de casos a simplemente añadir "123" en uno de los extremo de su contraseña, convirtiéndola en insegura y candidata a ser vulnerada [7].

Existen otros métodos con diferentes factores de autenticación como por ejemplo: biométricos, faciales, etc., como sustitutos o complementos para las contraseñas; justamente para evitar el desfase de la aplicación de las políticas de creación de contraseñas. No obstante, estos métodos tienen problemas de costos elevados y complejidad en su aplicación [2].

En la actualidad, el estudio de la temática de contraseñas ha motivado mucha investigación, dada su incidencia en el día a día de la vida cotidiana de las personas y de las empresas. Como producto de dicha investigación se han obtenido resultados importantes, lo cual motivó el presente estudio. Más específicamente, esta investigación se basa en el experimento de Colombini et al. [4], el cual propone verificar la vulnerabilidad de las contraseñas en función de su complejidad. No obstante, nuestro experimento varía en el hecho de que se elaboraron *tres niveles de complejidad de contraseñas* (*Alto, Medio y Bajo*) con el fin de estudiar la vulnerabilidad de estos. Los niveles de complejidad están basados en distintos estudios empíricos tales como: [1, 8, 9, 10, 4, 7].

Con el propósito de operacionalizar el experimento, las contraseñas fueron definidas dentro de un *servidor SSH* simulado sobre un honeypot, de tal forma que su asignación sea aleatoria. Adicionalmente, el uso del honeypot permitió emular las vulnerabilidades de un sistema operativo con el propósito de atraer, capturar y analizar ataques cibernéticos [4, 11].

El estudio empírico fue llevado a cabo en la Universidad

de las Fuerzas Armadas ESPE de Ecuador, durante un periodo de *treinta días*, sobre la red pública del CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado). Los resultados obtenidos de este estudio muestran que durante el periodo de estudio propuesto se perpetraron *407.029* ataques procedentes de distintos lugares del mundo, de los cuales ningún ataque comprometió los niveles de complejidad de contraseñas propuestos (Alto, Medio, Bajo). Sin embargo, se registró un total de *140.036 sesiones* provenientes de *579 direcciones IP* y *124.387 contraseñas de distintos niveles de complejidad*, que fueron inyectadas utilizando *14 diferentes tipos de clientes SSH* (ej. Putty, Paramiko, etc.).

La estructura del artículo es la siguiente: en la sección II, se analiza la literatura referente a la elaboración y mediciones de contraseñas en distintos estudios empíricos. En la sección III, se hace énfasis en la problemática de la entropía y se proporciona el detalle de los niveles de complejidad de contraseñas establecidos para el experimento. En la sección IV, se presenta el diseño experimental enfocado en las vulnerabilidades de los niveles de complejidad planteados. En la sección V, se detalla la ejecución y resultados del experimento. En la sección VI, se presentan las conclusiones y lecciones aprendidas. Finalmente, en la sección VII, se presenta una discusión de los resultados obtenidos y sus implicaciones.

## II. Antecedentes

La mayoría de sistemas actuales utilizan algún modo de identificación de usuarios para dar acceso a sus funcionalidades. El modo de identificación tradicional se basa en el uso de contraseñas. La administración de las contraseñas generalmente es de responsabilidad de cada usuario al momento de su selección. Sin embargo, para que esta selección sea sustentada bajo un esquema de seguridad, los administradores de los sistemas establecen políticas específicas referentes a la selección de las contraseñas en lo tocante a: su longitud, caracteres menos usados, etc.

No obstante, los estudios realizados hasta la fecha respecto a esta temática, presentan un panorama bastante sombrío respecto a las vulnerabilidades de las contraseñas, pese a la existencia de políticas específicas y estudios referentes a la creación de contraseñas.

a. Morris y Thompson [12] presentaron un estudio donde idearon varios diseños de esquemas de seguridad de contraseñas con el objetivo de proporcionar una mejor seguridad. Los resultados de este estudio revelaron que aproximadamente el 30% de 3.000 contraseñas fueron vulneradas durante un ataque de diccionario formado de 250.000 palabras conocidas. Asimismo, se utilizó un ataque por fuerza bruta sobre el mismo número de contraseñas de estudio, de las cuales fueron vulneradas el 86% de las contraseñas.

b. Narayanan y Shmatikov [13] experimentaron con la medición de seguridad de contraseñas, con el fin de disminuir la vulnerabilidad de las contraseñas atacadas por fuerza bruta. El estudio utilizó un ataque sistemático basado en fuerza bruta de series de Markov. Los resultados de este estudio determinaron la vulnerabilidad del 67.6% de 142 contraseñas consideradas para el estudio. Estas contraseñas eran pertenecientes a usuarios reales. Los autores enfatizan que mientras las contraseñas sigan siendo formuladas por la memoria humana, serán vulnerables a los ataques de "diccionarios-inteligentes" .

c. Yan et al. [5] realizaron un ensayo controlado con el fin de medir la seguridad de 300 contraseñas creadas a partir de: diccionarios, fichas mnemotécnicas y contraseñas aleatorias. Las contraseñas seleccionadas para el estudio fueron en promedio de entre 6, 7 y 8 caracteres de longitud. El 32% de estas contraseñas fueron vulneradas mediante un ataque basado en diccionario, mientras que las contraseñas basadas en frases mnemotécnicas y aleatorias, fueron difíciles de ser vulneradas. Este estudio es considerado como uno de los primeros experimentos en donde se usaron fichas mnemotécnicas para la formación de contraseñas y el primer paso hacia una mejor comprensión de los aspectos de la psicología aplicada en la seguridad informática.

d. Wu [14] en su estudio, recogió más de 25 mil contraseñas a partir de Kerberos v4, con el fin de intentar vulnerar su seguridad. Durante su experimento logró vulnerar sólo 8.1% de las contraseñas. Con los resultados concluyó que el bajo porcentaje de contraseñas vulneradas se debió a la complejidad computacional de la formulación de contraseñas de Kerberos v4. Discute la naturaleza de la debilidad de Kerberos v4 y el peligro que éste supone.

e. Cazier y Medlin [15] examinaron las contraseñas creadas por los clientes de un sitio web de comercio electrónico, con el fin de investigar la relación entre la longitud y la vulnerabilidad de la contraseña frente a un ataque de fuerza bruta. Concluyeron que el 61.2% de 520 contraseñas tomadas para su estudio, fueron vulneradas en menos de 10 horas con métodos de diccionarios y ataques de fuerza bruta. Este estudio evidenció la necesidad de fortalecer las investigaciones relacionadas a la creación de contraseñas.

Estos estudios ponen de manifiesto que no resulta sencillo determinar un nivel de complejidad de las contraseñas en relación a la seguridad que éstas deben brindar. Por ejemplo, en el caso de la longitud de una contraseña, se ha llegado a concluir que no representa un sinónimo de aumento en la seguridad; es decir que, considerar a la longitud (sea esta demasiado pequeña o demasiado grande) como parte de un nivel de complejidad de una contraseña, podría ser igualmente comprometida [8]. Por el contrario, la longitud de una contraseña se la ha relacionado directamente al tiempo en que esta puede ser vulnerada [2]. Lo mismo sucede con las contraseñas basadas en diccionario, en las que el usuario coloca una falta de ortografía "a propósito" , con el fin de ofrecer "cierta protección" contra ataques de diccionario [10].

## III. Niveles de Complejidad de Contraseñas

Un detalle importante que nos llamó la atención sobre los estudios descritos en la sección II, es que ninguno basó su investigación en el nivel de complejidad de las contraseñas que las políticas actuales podrían ofrecer. Por ejemplo, las políticas de creación de contraseñas de la NIST SP800-63 [7].

La NIST SP 800-63[1] es considerada como el documento más influyente en la elaboración de políticas de creación de contraseñas. Sus recomendaciones han llegado a ser la base para la generación de políticas de contraseña de varios gobiernos e industrias [7]. La base metodológica de la NIST SP800-63, se centra en la puntuación de la "Entropía de Shannon" para la estimación de la resistencia de la contraseña, esto con el fin de emitir políticas de creación y/o generación de contraseñas [7].

El término entropía fue introducido por primera vez por Claude Shannon [7] como una medida de los problemas en el contexto de la comunicación. Sin embargo, de acuerdo a teorías de la información, el término entropía se utiliza como una medida de contenido de información [10]. La entropía es una medida de *incertidumbre* de un fenómeno que es aleatorio [5]. Es por ello que la puntuación de la "entropía de Shannon", considera a los caracteres y números como un valor a nivel de bits. Por ejemplo, el primer carácter de una contraseña se le representa como 4 bits, y los próximos 7 caracteres son 2 bits por carácter, entre otros [5].

No obstante, existen autores como Malone & Maher [10], Weir et al. [7] y Florencio et al. [1]; que afirman que el uso de la *Entropía de Shannon* utilizada en las recomendaciones de la NIST SP800-63 [7], no es una métrica eficaz para medir la seguridad de contraseña (sin arrojar dispersiones sobre el resto del documento NIST SP800-63 [7]). Como consecuencia, los autores afirman que las contraseñas creadas a partir de esta entropía resultan ser fáciles de adivinar, dado que el tipo de entropía base de este documento, no se relaciona directamente con el parámetro de adivinanza de una contraseña [10]. Así mismo, señalaron que no se podría proponer una manera de convertir la noción de la *Entropía de Shannon* en una entropía más realista basada en adivinanzas o probabilidades [7]. En la actualidad existen varias propuestas de entropías que están basadas en adivinanzas, las cuales podrían soportar de manera aceptable un ataque a sus contraseñas [13]. Sin embargo, en algunos estudios a estas propuestas de entropías las consideran como de nivel bajo [10].

La perspectiva anterior, da una idea de que los valores o medidas de entropía usados en las políticas de creación de contraseñas, posiblemente son ingenuos o no reales al momento de estimar o construir contraseñas con un nivel de complejidad aceptable de seguridad durante un ataque (ej. fuerza bruta, ataque de diccionario, etc.) [2, 1]. A esto se agrega, una comprensión equivocada de la eficacia de las entropías (especialmente de la NIST SP 800-63) en relación a las técnicas de ataques actuales y a la omisión del cumplimiento de políticas de creación de contraseñas por parte de los usuarios. Por ejemplo, aplicar la política de incluir al menos tres dígitos en una contraseña, probablemente el resultado del cumplimento por parte del usuario sea simplemente añadir "123" en el extremo final de su contraseña, convirtiéndola en una contraseña insegura y candidata a ser vulnerada [7]. Este caso, incluso se presenta en portales web donde se maneja sistemas de validación automática de contraseñas, los cuales suponen validaciones para que el usuario elija supuestas contraseñas *fuertes*, o no reutilizables [1].

Para el presente estudio empírico, creamos una categorización de niveles de complejidad de contraseñas. Para ello, se consideró como base el resultado de varios estudios empíricos que analizaron distintos parámetros o variables para la elaboración de contraseñas, por ejemplo: longitud, probabilidad de uso de ciertos caracteres y/o números, probabilidad de adivinanza de ciertos caracteres y/o números, frecuencia de uso de distintos tipos de caracteres especiales, probabilidad de posiciones de caracteres o dígitos, entre otros [1, 8, 9, 10, 4]. Creemos que las recomendaciones de estas propuestas pueden aportar positivamente en la construcción de niveles de complejidad de contraseñas que sean al menos difíciles de vulnerar.

En base a las recomendaciones recopiladas creamos tres niveles de complejidad de contraseñas:

### A. *Contraseñas de Nivel de Complejidad Bajo*

Consideramos contraseñas de nivel de complejidad bajo, a aquellas contraseñas que son "fáciles de recordar", y que comúnmente utilizan los usuarios. Estas contraseñas (en varios estudios) son consideradas como débiles, ya que han sido vulneradas en varios robos; algunos de ellos, bastante publicitados [8, 9]. Son contraseñas reutilizables, predecibles, fáciles de usar, fáciles de adivinar y romper, con baja sofisticación [8] o que se utilizan con gran frecuencia [9]. Las características de esta categoría de contraseñas son:

a. Están basadas en información personal, por ejemplo: nombres, fechas de boda o nacimiento, o cualquier palabra fácil de recordar que tenga relación con la parte emocional / afectiva de los usuarios [2, 10].

b. Están relacionadas con la demografía de los usuarios o con el lugar en que residen [10].

c. Responden a reglas simples de generación de contraseñas, tales como: "Juliet03" para marzo, "Juliet04" para abril, y así sucesivamente [5].

### B. *Contraseñas de Nivel de Complejidad Medio*

Consisten en una evolución de las contraseñas de nivel de complejidad bajo. El usuario incrementa la complejidad de su contraseña, manteniendo la misma contraseña de nivel bajo pero suplantado los caracteres originales por caracteres especiales o similares o simplemente agregando faltas ortográficas [10]. Las características de este tipo de contraseñas son:

a. Contraseñas basadas en diccionario o nombres comunes con transformaciones de uso común. Por ejemplo: sustitución de la letra "s" por "$" , "@" en lugar de la letra "a" , dígitos por letras, entre otros [10].

b. Contraseñas basadas en la unión de palabras de diccionario, donde el usuario agrega cierto nivel de transformación. Por ejemplo, la palabra *full* y la palabra *love* formaría la contraseña: *fu111ove* o *fu11l0ve* [8].

c. Contraseñas en las que intencionalmente son colocadas faltas ortográficas, con el fin de ofrecer cierta protección contra los ataques de diccionario. Por ejemplo: "Amhor" en lugar de "Amor" [10].

Aparentemente a este tipo de estrategias se le ha considerado como una tendencia, por ser supuestamente "segura" . Sin embargo, Malone y Maher [10] detectaron que JohnTheRipper,

[1]NIST "Electronic Authentication Guideline"

Hashcat, y oclHashcat son herramientas que actualmente combinan "diccionarios - inteligentes" que sustituyen caracteres alfabéticos de palabras de diccionarios por caracteres especiales y dígitos.

### C. Contraseñas de Nivel de Complejidad Alto

Son contraseñas que utilizan alguna técnica que permite elevar la seguridad de la contraseña. Las características de esta categoría de clasificación se detallan a continuación:

a. Contraseñas que no están presentes en el diccionario real [1].

b. Contraseñas aleatorias formadas por un hash de letras, caracteres especiales y números [9].

c. Contraseñas consideradas seguras y simples que los usuarios elaboran o eligen a partir de colecciones aleatorias de caracteres [1].

d. Contraseñas que son elaboradas mediante técnicas de memoria, o fichas mnemotécnicas, que ayudan a recordar cómo descodificar su contraseña [10]. Por ejemplo, utilizar las primeras letras de una frase (que no debe ser bien conocida): "An apple a day keeps the doctor away" se obtiene la contraseña: Aaadktda; o de "My dog's first name is Rex", se obtiene la contraseña: MdfniR [5].

Estas técnicas ayudan al usuario con la elaboración de contraseñas que podría ser "más seguras", debido a que podrían tomar más tiempo al atacante para llegar a vulnerarla. Considerando ese intervalo de tiempo como el justo y necesario como para realizar el cambio de contraseña [4].

## IV. Diseño Experimental

El diseño experimental planteado para el experimento siguió las guías para la presentación de reportes experimentales de Ingeniería de Software propuestas por Jedlischka y Pfahl [16].

### A. Objetivo, Preguntas de Investigación e Hipótesis del Experimento

El objetivo de la investigación es analizar la vulnerabilidad de los niveles de complejidad de contraseñas planteados en la sección III, a través de la instanciación de un experimento controlado.

Como guía y orientación para alcanzar el objetivo de esta investigación, fueron planteadas las siguientes preguntas de investigación:

R01: ¿Son más vulnerables las contraseñas de nivel de complejidad Bajo en relación a sus similares?

R02: ¿Qué niveles de complejidad de contraseñas son usadas con más frecuencia durante los ataques en tiempo real?

R03: ¿Qué tipos de atacantes son más frecuentes?

R04: ¿Cuál es la procedencia de los atacantes?

Las hipótesis experimentales planteadas son las siguientes:

$H_0$**:** No existe diferencia en la vulnerabilidad de los distintos niveles de complejidad de contraseñas (Alto, Medio y Bajo).

$H_{1a}$**:** El nivel de complejidad de contraseñas bajo es más vulnerable que el resto de niveles de complejidad de contraseñas (Alto y Medio).

$H_{1b}$**:** El nivel de complejidad de contraseñas medio es más vulnerable que el resto de niveles de complejidad de contraseñas (Alto y Bajo).

$H_{1c}$**:** El nivel de complejidad de contraseñas alto es más vulnerable que el resto de niveles de complejidad de contraseñas (Medio y Bajo).

Cabe recalcar que este experimento es de *carácter confirmatorio* y se podría asumir que las contraseñas de *nivel alto* serían más difíciles de vulnerar que las contraseñas de *nivel medio*, y que estas a su vez estas son más difíciles de vulnerar que las contraseñas de *nivel bajo* [1, 8, 9, 10, 4]. Por lo tanto, para este estudio se prevé utilizar una prueba de hipótesis de *una cola*.

### B. Variable Dependiente

La variable dependiente estudiada es la vulnerabilidad de los niveles de complejidad de las contraseñas indicados en la sección III. No existe una métrica ampliamente aceptada para medir esta variable. En la literatura [1, 8, 9, 10, 4] se utilizan con frecuencia las métricas: Porcentaje (%) de ataques exitosos y el tiempo que se tarda un atacante en obtener un ataque exitoso. En el contexto del presente experimento, nos ha parecido adecuado operacionalizar la vulnerabilidad como el porcentaje (%) de intentos exitosos (se traten de adivinanzas aisladas, ataques de diccionario, ataques de fuerza bruta, etc.) sobre el total de intentos realizados durante el experimento.

### C. Factor

El factor que servirá para comparar la seguridad de las contraseñas es el nivel de seguridad y tiene tres niveles: *Alto, Medio, Bajo*, tal y como se deriva de la sección III.

### D. Selección de Sujetos

Para la selección de sujetos, no se utilizó muestreo sobre una poblacion conocida, sino que utilizaremos como sujetos a cualquier tipo de atacante que acceda a nuestra infraestructura experimental. Esta forma de proceder, evita varios problemas prácticos. Por un lado, no es fácil localizar sujetos con la pericia suficiente para atacar contraseñas, y por otro lado, formar sujetos para este experimento haría que el ataque fuese también construyente sobre la formación impartida, y no sobre el nivel de complejidad de las contraseñas en sí mismas. Es por ello que seleccionar a los atacantes provenientes del internet, asegura la representatividad de los ataques y convierte la validez externa del experimento.

### E. Asignación de los sujetos a factores

La asignación de sujetos a los factores ha sido realizada mediante una asignación al azar; es decir, por cada vez que un atacante intenta acceder a la infraestructura, se le asigna aleatoriamente un nivel de complejidad de contraseñas. Es por

ello que el tamaño de cada grupo esta dado por el número de atacantes que aparezcan durante el experimento. Al finalizar el experimento se podrá tener una idea clara del tamaño de cada grupo asignado al nivel de complejidad de contraseña correspondiente (Alto, Medio, Bajo).

### F. Objeto Experimental

En la Tabla I, se describen contraseñas elaboradas de acuerdo a los parámetros descritos en cada uno de los niveles complejidad indicados en la sección III. Cabe recalcar que a más de dichos parámetros, para la formación de estas contraseñas, se utilizó los resultados encontrados en la literatura [1, 8, 9, 10, 4]:

| | No. | Alto | Medio | Bajo |
|---|---|---|---|---|
| Inglés | 1 | 13ILPSSG@F | S0c4Cer3 | Soccer1 |
| | 2 | 7TC@S@MBS5 | F!0.w4er | Flower2 |
| | 3 | 5@GIG2MW@D | L0.vE_12 | Love123 |
| | 4 | &DTME*HP13 | Ma!!f0.y | Malfoy2 |
| | 5 | 13G/GF*G/G | Ze4.us12 | Zeus123 |
| | 6 | 5@*BCIS*@5 | MaDr!d.4 | Madrid2 |
| Español | 7 | 13ILPSSG@F | Fut4b0!1 | Futbol1 |
| | 8 | 7TC@S@MBS5 | F!O.r4es | Flores2 |
| | 9 | 5@GIG2MW@D | Am.0r_12 | Amor123 |

TABLE I. CONTRASEÑAS POR NIVELES DE COMPLEJIDAD.

Cada columna de la Tabla I representa un nivel de complejidad detallado en la sección III y cada fila se encuentra relacionada entre sí. Por ejemplo, en la fila 1, encontramos la contraseña de nivel de complejidad *bajo* que se refiere a un deporte comúnmente conocido: *Soccer1*. Esta misma palabra fue elevada a una complejidad de nivel *medio*, donde se incluyeron ciertas transformaciones (ej. la letra "o" sustituida por "0"): *S0c4Cer3*. Finalmente, esta contraseña fue elevada a un nivel de complejidad *alto*, utilizando una frase recordatoria, y extrayendo las letras iniciales de cada palabra (ej. ficha nemotécnica del usuario): *[I] [L]ove [P]laying [S]occer, [S]coring [G]oals [A]nd [F]aults*: *13ILPSSG@F*. Para el uso y posición de dígitos y caracteres especiales nos basamos en las probabilidades del estudio de Weir et al. [7].

Las filas 1 a 6 son contraseñas que se encuentran en el idioma Inglés. Las filas 7 a 9 son sus similares en Español de las filas 1 al 3.

### G. Tarea Experimental

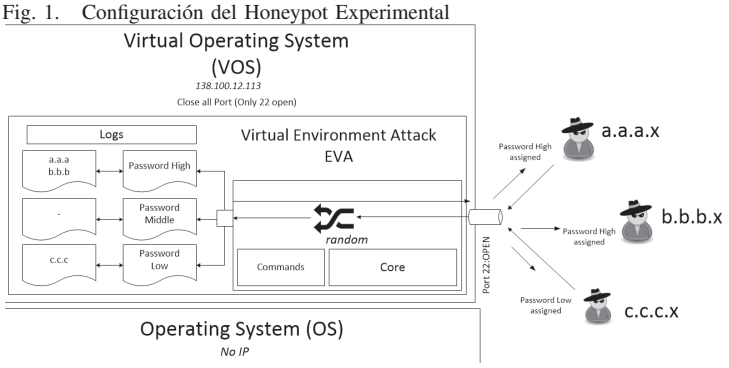
La tarea experimental consiste en la realización de ataques con el propósito de vulnerar el conjunto de contraseñas de distintos niveles de complejidad propuestos. Consideramos que los sujetos experimentales (atacantes) son competentes para llevar a cabo la tarea experimental; es decir, tienen el conocimiento necesario para formular un ataque a las contraseñas propuestas, hasta llegar a vulnerarlas. Cada sesión realizada para perpetrar un ataque queda en manos de los atacantes, sin que haya posibilidad alguna de limitación o control.

### H. Instrumentación

La instrumentación del experimento es relativamente simple. Consiste en la utilización de un único *Honeypot* de mediana interacción. Este *Honeypot* se encuentra conectado a la red del CEDIA en la Universidad de las Fuerzas Armadas ESPE, emulando las vulnerabilidades de un sistema, con el fin de atraer, capturar y analizar los ataques cibernéticos perpetrados hacia las contraseñas [4]. No obstante, para que la instrumentación tenga un nivel experimental, el honeypot fue modificado hasta obtener la capacidad automática de aleatorización de niveles de complejidad de contraseñas (Alto, Medio y Bajo). Esta característica, permite cumplir con los requerimientos necesarios para ejecutar un experimento controlado, y cumplir con las teorías experimentales de Fisher [16].

En la Figura 1 se muestra la configuración interna del honeypot modificado. Básicamente consta de tres logs, donde se almacenan los ataques para cada nivel de complejidad de contraseñas (Ver subsección IV-F). El procedimiento de asignación aleatoria es el siguiente: cuando un atacante trata de vulnerar el honeypot por primera vez, éste le asigna aleatoriamente un nivel de complejidad de contraseña, el cual se mantiene durante toda la vida del ataque, es decir, si el atacante vuelve a intentar ingresar al honeypot en varias instancias, el atacante recibe el mismo nivel de complejidad de contraseña asignado en la primera vez. Adicionalmente, el honeypot permite soportar ataques de herramientas como: diccionarios, ataques de fuerza bruta, entre otros.

Fig. 1. Configuración del Honeypot Experimental




### I. Procedimiento de Medición

Durante cada *sesión de ataques*, el honeyPot almacena la información generada en varios *logs*. El honeypot posee un log por cada nivel de complejidad de contraseña, a fin poder obtener una mejor organización de los resultados. La información obtenida para la medición, está organizada de acuerdo a los siguientes parámetros: Ip de origen, contraseña usada, login utilizado, hora de ataque, tiempo de inicio de sesión, tiempo de finalización de la sesión, duración del ataque, entre otros.

## V. EJECUCIÓN Y RESULTADOS DEL EXPERIMENTO

### A. Ejecución del Experimento

El estudio se inició el día viernes 13 de marzo del 2015 a las 14:30 (GMT-5) hora de Ecuador, utilizando una IP pública perteneciente a la red del CEDIA asignada a la Universidad de las Fuerzas Armadas ESPE. El estudio culminó el día 08 de abril de 2015 a las 14:30 (GMT-5) hora de Ecuador.

Durante el tiempo de ejecución del estudio, se registró un total de *407.029 ataques realizados en varias sesiones, de los*

*cuales ninguno fue exitoso*. Se verificó la existencia de un total de *140.036 sesiones* provenientes de *579 Ips de distintos sitios del mundo*. Se utilizaron un total de *124.387 contraseñas distintas* durante los ataques utilizando *14 diferentes clientes SSH* (ej. Putty). En la Tabla II se muestra a detalle el número de IPs, número de sesiones y número de ataques por cada nivel de complejidad de contraseña propuesto (Alto, Medio, Bajo).

| *Nivel* | *Número de Ips* | *Número de Sesiones* | *Número de Intentos* |
|---|---|---|---|
| BAJO | 225 | 69.359 | 204.188 |
| MEDIO | 139 | 13.289 | 35.449 |
| ALTO | 215 | 57.388 | 167.334 |

TABLE II. IPS, SESIONES E INTENTOS POR NIVEL DE SEGURIDAD

## B. Caracterización de la Población

La población de atacantes fue obtenida a partir de los logs del honeypot. Esta población se la pudo desglosar en ataques provenientes de: China (72.7%) y Hong Kong (12,3%); siendo estos dos lugares, los orígenes de donde se produjeron el mayor número de ataques. Adicionalmente, se identificó a un (15%) de ataques pertenecientes a países de Europa y América.

En la Tabla III se muestra a detalle la procedencia de las IPs que generaron el mayor número de ataques al honeyPot. Como se mencionó anteriormente, en su mayoría son IPs de China, con la particularidad que gran cantidad de IPs representan a la empresa *HEETHAI LIMITED* cuyas redes son: 103.41.124/25 y 103.41.125/25. Se investigó acerca de esta empresa y se logró determinar que el punto de origen de los ataques del malware denominado *Massive DDoS Brute-Force Campaign Targets Linux Rootkits* XOR.DDoS. Este malware fue detectado por FireEye en Septiembre del 2014 [17]. En lo que respecta a la existencia de ataques provenientes de Ecuador, determinamos que la IP: 186.68.45.170 es de origen de la ciudad de Guayaquil - Ecuador, desde la cual se realizó 02 ataques al honeyPot.

| *N* | *Ip* | *Ataques* | *Procedencia* | *Empresa registro* |
|---|---|---|---|---|
| 1 | 103.41.124.189 | 5917 | China | HEETHAI LIMITED |
| 2 | 103.41.124.123 | 4635 | China | HEETHAI LIMITED |
| 3 | 103.41.124.153 | 4382 | China | HEETHAI LIMITED |
| 4 | 43.255.190.188 | 4321 | Hong Kong | SEXinSEX (Shimizu Hang Road) |
| 5 | 103.41.125.17 | 3341 | China | HEETHAI LIMITED |

TABLE III. PROCEDENCIA DE IPS CON MAYOR NÚMERO DE ATAQUES

En referencia al promedio de sesiones y ataques, estos fueron distribuidos de acuerdo a los niveles de complejidad de contraseñas propuestos. Los resultados mostrados en la Tabla IV, se evidencia que las contraseñas de *nivel de complejidad de contraseñas bajo* tuvieron un promedio de 907,5 ataques por IP, mientras que los *niveles de complejidad de contraseñas medio y alto* tuvieron un promedio de 255 y 778,3 ataques por IP respectivamente. Por otro lado, se evidenció que las contraseñas de *nivel de complejidad bajo* mantuvieron un promedio de 308,3 sesiones por IP, mientras que los *niveles de complejidad de contraseñas medio y alto* tuvieron un promedio de 95,6 y 266,9 ataques por IP respectivamente. Lo importante de estos resultados, es la evidencia que en cualquier *nivel de complejidad de contraseñas*, siempre existe un promedio entre 2,7 - 2,9 ataques por cada sesión. Lo que ayudó al atacante a enmascarar sus ataques para no ser detectado por el número considerable de intentos continuos durante una única sesión.

| *Nivel* | *Intentos por IP* | *Sesiones por Ip* | *Intentos por Sesión* |
|---|---|---|---|
| BAJO | 907,5 | 308,3 | 2,9 |
| MEDIO | 255,0 | 95,6 | 2,7 |
| ALTO | 778,3 | 266,9 | 2,9 |

TABLE IV. PROMEDIO DE SESIONES Y ATAQUES DURANTE EL ESTUDIO

## C. Caracterización de los ataques

Con referencia a la caracterización de los ataques, se obtuvo que el número de sesiones iniciadas para los ataques en cada nivel de complejidad de las contraseñas; el *nivel de complejidad Bajo* se lleva el mayor numero número de sesiones: 69.359, frente al *nivel de complejidad Medio* con el menor numero número de sesiones: 13.289 sesiones.(Ver Fig. 2).


Fig. 2. Sesiones iniciadas en cada nivel de complejidad de contraseñas

Este fenómeno sucede de manera similar con la cantidad de ataques inyectados en cada nivel de complejidad de contraseñas. Por ejemplo, en la Fig. 3 se muestra que el número de ataques para los distintos niveles de complejidad de las contraseñas, el *nivel de complejidad Bajo* lleva el mayor numero número de ataques: 204.188, frente al *nivel de complejidad Medio* que lleva el menor numero número de ataques: 35.449.

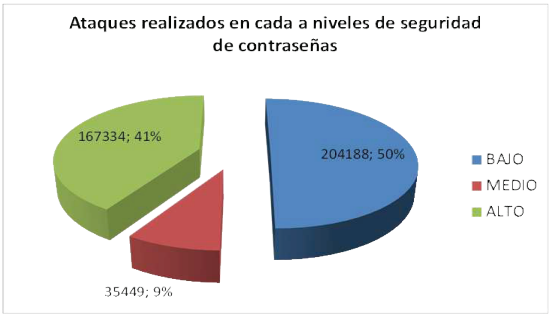



Fig. 3. Ataques realizados en cada nivel de complejidad de contraseñas

Adicionalmente, estos ataques fueron analizados en función del tiempo. En la Fig. 4 se muestra la tendencia de los ataques al HoneyPot durante el tiempo de ejecución del estudio

empírico. Se observó que el 30 de marzo del 2015 (33.405 ataques), 20 de marzo del 2015 (33.141) y 07 de abril del 2015 (29.814 ataques) fueron los días en que el Honeypot recibió el mayor número de ataques. Sin embargo, existe un fenómeno extraño luego de las fechas indicadas. Existe una baja sustancial de ataques, es decir que posterior al pico de ataques, existe un lapso de tiempo donde los ataques disminuyen drásticamente. Por ejemplo, el día posterior al día de mayor número de ataques: 31 de marzo del 2015, se registraron alrededor de 4.002 ataques, es decir 29.403 ataques menos en el lapso de 24 horas.

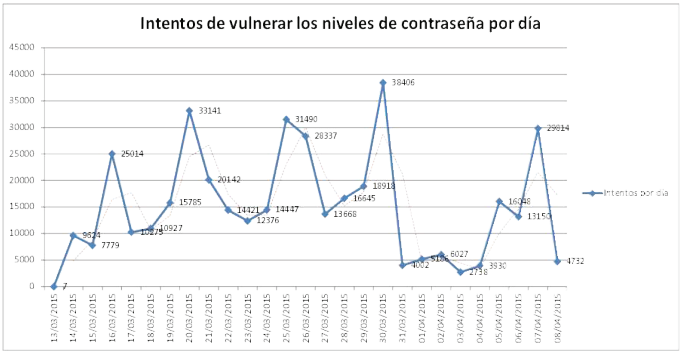



Fig. 4. Intentos de vulnerar los niveles de complejidad de las contraseñas por día


Fig. 5. Diez contraseñas más usadas durante el experimento

| *Tamaño* | *# Contraseñas* | *%* | *Ejemplos* |
|---|---|---|---|
| Menos de 7 caracteres | 39.094 | (31,4%) | wubao (1296), admin (391), 12345 (357), 123456 (348), root (336) |
| 7 caracteres | 15.744 | (12,6%) | jiamima (1251), default (283), root123 (262), 1234567 (175), admin01 (158) |
| 8 caracteres | 31.324 | (25,1%) | password (377), admin123 (260), P@ssW0rd (234), PASSW0RD (213), 12345678 (191) |
| 9 caracteres | 12.948 | (10,4%) | superuser(243), raspberry (193), 123456789 (146), Admin@123 (138), 123qweasd (103) |
| 10 caracteres | 11.168 | (8,7%) | 1234567890 (132), supervisor (127), root!@#!@# (123), 1q2w3e4r5t (97), q1w2e3r4t5 (89) |
| Más de 10 caracteres | 14.116 | (11,3%) | t0talc0ntr0l4! (194), admin-password (178), administrator (139), !!ˆ$%&#$%@ (137), rzx!@!*baizhao (121) |

TABLE V. LONGITUDES DE CONTRASEÑAS

### *D. Caracterización de las contraseñas*

Con referencia a la caracterización de las contraseñas, se pudo determinar que existió contraseñas que fueron mayormente utilizadas. En la Fig. 5 se muestran las 10 contraseñas más utilizadas durante los ataques. Por ejemplo, la palabra *wubao* fue la contraseña mas utilizada durante los ataques, con un total de 1.296 intentos, seguida de la palabra *jiamima* con un total de 1.251 intentos. Las demás palabras utilizadas son contraseñas que típicamente se han encontrado en otros estudios [2, 10]. Por ejemplo, *12345* con 448 intentos, *password* con 334 intentos, *admin* con 317 intentos. Decidimos investigar acerca de la procedencia de las palabras *wubao* y *jiamima*, y logramos determinar que estas palabras son de origen Suajili (Países Africanos) y Malgache (Países de Polinesia) respectivamente.

En la Tabla V, se muestra las diferentes longitudes de contraseñas utilizadas por los atacantes durante la ejecución de nuestro estudio. Se logró determinar que 39.094 contraseñas contienen menos de 7 caracteres (incluyendo letras, números y caracteres especiales), 31.324 contraseñas contienen 8 caracteres (incluyendo letras, números y caracteres especiales). Siendo las contraseñas de longitud de 10 caracteres (incluido letras, números y caracteres especiales) las que fueron encontradas en menor número: 11.168 contraseñas.

La contraseña de mayor longitud encontrada es una contraseña con una longitud de 81 caracteres que incluye números, letras (mayúsculas y minúsculas) y caracteres especiales. Esta contraseña fue utilizada en solo un intento durante un único ataque. La contraseña fue: UqlWX3c1eIaovOLWphShTGXmuUAMq6iu9DrcQqlVUw3 Pirizns4u27w3Ugvb6.:15800:0:99999:7:::. Por otra parte, la contraseña con menor longitud encontrada fue de 0 (cero) caracteres que fue utilizada en 243 intentos.

Con el propósito de tener una mejor perspectiva de las características de las contraseñas utilizadas durante los ataques al honeypod, clasificamos ha estas contraseñas de acuerdo al nivel de complejidad detallado en la sección III. Sin embargo, dada la gran cantidad de contraseñas obtenidas, se decidió obtener una muestra finita para nuestra clasificación. La fórmula utilizada para extraer el tamaño de la población se indica a continuación:

$$n = \frac{Z^2 * p * q * N}{N * e^2 + Z^2 * p * q} \quad (1)$$

El resultado de aplicar esta fórmula, se obtuvo un tamaño de población de 1.000 contraseñas. Consideramos que este tamaño representa una muestra aceptable para nuestro estudio de clasificación de características de contraseñas. En la Tabla VI se muestra la clasificación de la muestra de estudio. Del resultado se clasificaron: 926 contraseñas como de *nivel de complejidad Bajo*, mientras que 76 contraseñas fueron clasificadas como contraseñas de *nivel de complejidad Medio*.

| NIVEL DE COMPLEJIDAD | TITULO | EJEMPLO |
|---|---|---|
| NIVEL BAJO (926) | Diccionario | default (283), test (273), power (227) |
| | Nombres | calvin (206), alex (116), david (82) |
| | Personajes | superman 108, batman 73, gandalf 60, cooper 59, merlin 52, barney 51 |
| | Marcas | raspberry 193, dreambox 135, samsung 112, redhat 92, oracle 91 |
| | Comb. Teclas | 123456789 146 , !qaz2wsx 86, asdfgh 84, qwert 84, qwer1234 83, 1a2b3c4d 81, qazwsx123 79 |
| | Comb. Palabras y Números | root123 262, admin123 260, abc123 172, password123 81, abc@123 81, 123456abc 78, root!! 159, |
| | Comb. palabras de diccionario | superuser 243, rootme 234, adminpassword 178, changeme 108, rootroot 92, sysadmin 92 |
| | Palabras Simples | admin 391, password 377, root 336, toor 195, wsad 184, manager1 14 |
| | Letras, números y caracteres especiales | !! 178, 0 244, ! 215, 111111 168, 666666 160, !#%& 156, !@#$% 148, aaaaaa 141, ) 137 |
| | Fechas | 1986-04-12 1, 19-11-1995 1, 1986-04-12 1, 23-06-1987 1 |
| | Palabras extranjeras | wubao 1296, jiamima 1251, blahblah 99, PlcmSpIp 57, wvhlyf 49, abgrtyu 44 |
| NIVEL MEDIO (76) | Transformaciones simples | P@ssW0rd 234, t0talc0ntr0l4! 194, root!@#!@# 123, p@$$w0rd 114, p@ssword 63, p@ssw0rd123 57, p4ssw0rd 53, p@ssw0rd1 51, p@55w0rd 50, pa$$w0rd 48, pa55w0rd 48, P2ssw*rdD147 1, p@sswd 9, r00tr00t 40, @dm1n 45, pru3ba 1, u$3r 1 |
| ALTO (0) | - | - |

TABLE VI. CARACTERÍSTICAS CONTRASEÑAS DE ACUERDO A NIVEL DE COMPLEJIDAD DE CONTRASEÑAS

De la clasificación de contraseñas de *nivel de complejidad Bajo*, se determinó que la mayoría estaban relacionadas con palabras de diccionario (ej: "default" con 283 intentos), nombres de personas (ej. "calvin" con 206 intentos), personajes de libros/ historietas / tv (ej. "superman" con 108 intentos), combinaciones de palabras y números simples, palabras de administrador (ej. s "uperuser" con 243 intentos), fechas o combinaciones de teclado (ej. "!qaz2wsx " con 86 intentos).

Por otra parte, de la clasificación de contraseñas de *nivel de complejidad Medio*, se determinó que existió un ataque de *diccionario-inteligente* a las contraseñas que comúnmente son utilizadas por los usuarios. Por ejemplo: p@$$w0rd con 114 intentos, p@ssword con 63 intentos, p@ssw0rd123 con 57 intentos, entre otros.

Con respecto al uso de dígitos, se determinó que 68.210 contraseñas contenían al menos un dígito. En la Tabla VII se muestran los dígitos que son mayormente utilizados en las contraseñas durante los ataques. A breves rasgos, se puede observar que el dígito 1 fue encontrado en 46.310 contraseñas y el dígito 2 fue encontrado en 34.636 contraseñas. Siendo estos dígitos los que son mayormente utilizados en las contraseñas de ataques. Para el dígitos 7, encontrado en 14.410 contraseñas y dígito 6, encontrado en 14.611 contraseñas, son los dígitos que menos utilizados en las contraseñas de ataques.

Finalmente con los caracteres especiales, se estableció que en 7.083 contraseñas fueron encontrados al menos un caracter especial. En la Tabla VIII se muestran los caracteres especiales que mayormente son utilizados en las contraseñas de ataques. A breves rasgos, se puede observar que el caracter especial "@" fue encontrado en 3.372 contraseñas y el caracter especial "!" fue encontrado en 2.577 contraseñas. Siendo estos caracteres especiales los utilizados en las contraseñas de ataques. En tanto, los caracteres especiales "(espacio)" , encontrado en 185 contraseñas y el caracter especial "&" , encontrado en 334 contraseñas, son los caracteres especiales menos utilizados en contraseñas de ataques.

| *Número* | *# Contraseñas* | *%* | *Ejemplos* |
|---|---|---|---|
| Con el (1) | 46310 | (37,2%) | 1 (140), g1t (2), $1$ (3), a1b2 (14), 1q@WS (1), 123!@ (43) |
| Con el (2) | 34636 | (27,8%) | 2 (38), 3230 (1), k23.n (1), post12 (1), lovely02 (1),qwer4321 (14) |
| Con el (3) | 26063 | (21,0%) | 3(7), 3edc (8), mui3 (1), my123 (2), vhs123 (2) |
| Con el (4) | 16148 | (13,0%) | 94 (2), off4 (3), h2so4 (1), qwn456 (1) |
| Con el (5) | 15785 | (12,7%) | 35com 6, 23456 2, tony15 1, ps1205 1, ecco15 1 |
| Con el (6) | 14611 | (11,7%) | 6 (20), .369* (1), 61e2b (1), 4+5+6 (1), 6gy7cg (2) |
| Con el (7) | 14410 | (11,6%) | 7 (1), 7mp3 (6), 789!@ (1), gch587 (6), eee789 (1) |
| Con el (8) | 15686 | (12,6%) | 8 (7), t2518 (2), baby81 (1), q7w8e9 (1), 1748hi (1) |
| Con el (9) | 18611 | (15,0%) | 9 (12), love9 (1), Viper9 (1), dr149a (1), emil09 (1) |
| Con el (0) | 24817 | (20,0%) | |

TABLE VII. DIFERENTES DÍGITOS ENCONTRADOS EN CONTRASEÑAS DE ATAQUE

| *Número* | *# Contraseñas* | *%* | *Ejemplos* |
|---|---|---|---|
| Con el (@) | 3372 | (2,7%) | @ (37), st!@ (3), !A@B (12), qwe!@ (14), ap@ch3 (4) |
| Con el (!) | 2577 | (2,1%) | ! (215), !!2004 (1), !@123455 (3), password1! (41), k!956?bkf10 (1) |
| Con el (#) | 1626 | (1,3%) | # (12), !@# (48), !#%&( (55), !@#POI (1), hct!@# (1), c#mming (28) |
| Con el (.) | 1527 | (1,2%) | . (43), 123. (7), v01.cn (5), w.s.x.e (2), 123qqq... (2) |
| Con el (%) | 716 | (0,6%) | !#%& (154), !@#$% (148), 1234% (30), Abc1234% (3) |
| Con el (*) | 551 | (0,4%) | !!!** (14), *-*haha (1), *1*1, (5), :* (10), *root* (1) |
| Con el (-) | 546 | (0,4%) | - (72), password-123 (1), ———— - (3), dchilds-good (3), debian-xfs (1) |
| Con el (_) | 363 | (0,3%) | _ (14), ! @_ (7), htxg_WX (2), 3W0k_3Nd0r (3), 12345&*(6)_+ (2) |
| Con el (&) | 334 | (0,3%) | & (6), !@#$%& (26), &&&&&&&& (2) |
| Con el ( ) | 185 | (0,1%) | -* (3), abc 123 (3), c major (2), nne sanne (1) |

TABLE VIII. DIFERENTES CARACTERES ESPECIALES ENCONTRADAS EN CONTRASEÑAS DE ATAQUE

### *E. Resultados*

En referencia a la asignación aleatoria de los niveles de complejidad de las contraseñas entregada por el honeypot a cada atacante, consideramos que fue el adecuado. En la Fig. 6 se muestra que el honeypot realizó una distribución aparentemente balanceada entre todos los niveles de complejidad de las contraseñas. Por ejemplo, a 215 IPs que intentaron atacar al honeypot, se les asignó el *nivel de complejidad de contraseña Alto*, a 139 IPs se les asignó el *nivel de complejidad de contraseña Medio*y a 225 IPs se les asignó el *nivel de complejidad Bajo*.


Fig. 6. Resultado de la asignación aleatoria de niveles de complejidad de contraseñas a sujetos experimentales

Finalmente, en la Tabla IX se muestra el resultado de la vulnerabilidad de las contraseñas creadas en la subsección IV-F para cada nivel de complejidad de contraseña. El resultado fue sorpresivo, puesto que a pesar de la cantidad considerable de IPs (579) y número considerable de ataques (407.029), no existieron ataques exitosos; es decir, ningún ataque llegó a vulnerar las contraseñas propuestas para cada nivel de complejidad.

TABLE IX. ATAQUES EXITOSOS Y NO EXITOSOS

| | Ataques Exitosos | Ataques No exitosos |
|---|---|---|
| Bajo | 0 | 204.188 |
| Medio | 0 | 35.449 |
| Alto | 0 | 167.334 |

## VI. CONCLUSIONES Y LECCIONES APRENDIDAS

### A. Conclusiones

Consideramos inicialmente que la vulnerabilidad de las contraseñas de *nivel de complejidad Bajo* propuestas para este estudio, serían las primeras contraseñas en ser vulneradas. Sin embargo, para nuestra sorpresa, ninguna de las contraseñas propuestas para todos los niveles de complejidad fueron vulneradas. Consideramos que probablemente el tiempo de ejecución del estudio fue muy corto como para que, alguna de las contraseñas construidas para este estudio fuera vulnerada. Creemos que, al considerarse una mayor cantidad de tiempo, podría llegarse a vulnerar alguna contraseña de los niveles de complejidad. En otras palabras, considerar a un tiempo prolongado en una próxima replicación de este estudio, permitirá que las contraseñas propuestas puedan ser vulneradas.

Por otro lado, el estudio permitió demostrar que durante los intentos de ataque hacia nuestras contraseñas propuestas, los atacantes probablement utilizaron herramientas sofisticadas. La razón esta atribuida a las palabras de diccionario con trasformaciones especiales utilizadas por *diccionarios-inteligentes*, tal como fue indicado por Narayanan y Shmatikov [13] y Morris & Thompson [12] en sus estudios.

Un hecho que nos llamo la atención, es el gran número de ataques basados en *Bots* provenientes de China. Nos referimos específicamente al ataque del Malware denominado *Massive DDoS Brute-Force Campaign Targets Linux Rootkits* XOR.DDoS. Consideramos que la Universidad de las Fuerzas Armadas ESPE, así como otras universidades ecuatorianas conectadas en la misma red (CEDIA), deberían incrementar su seguridad a nivel de complejidad de contraseñas. Nuestra preocupación de fundamenta en el reporte de Paganini [17], en el cual manifiesta que la *Universidad Estatal de Pennsivania (Penn State) - EEUU* fue blanco de dos ataques sofisticados a sus contraseñas desde China, en donde se vulneraron alrededor de 18.000 contraseñas de estudiantes.

## VII. DISCUSIÓN

### A. ¿Son más vulnerables las contraseñas de nivel de complejidad Bajo en relación a sus similares?

Considerandoa los resultados obtenidos en el presente estudio empírico, aparentemente no serían vulnerables las contraseñas de nivel de complejidad bajo o contraseñas simples. Sin embargo, consideramos que el tiempo utilizado para nuestro estudio empírico posiblemente fue muy corto como para que un atacante pueda quebrantar o descifrar alguna de las contraseñas. Creemos que es necesario realizar nuevos estudios empíricos, de hecho, realizaremos un experimento posterior para responder a esta pregunta de investigación, en base a una mayor evidencia.

Coincidimos con Ma et al. [18] en que la calidad de las contraseñas depende del tiempo que le toma a un atacante en vulnerarla/descifrarla. Es decir, que cuanto más tarde en ser vulnerada una contraseña, mejor es su calidad.

### B. ¿Qué niveles de complejidad de contraseñas son usadas con más frecuencia durante los ataques en tiempo real?

De acuerdo a los resultados de nuestro estudio empírico, las contraseñas de *nivel de complejidad Bajo* y *nivel de complejidad Medio* serían las más usadas. Siendo las contraseñas de *nivel de complejidad Bajo* el tipo de contraseñas que existe en un gran número dentro de nuestros resultados. De la muestra de contraseñas establecida, se logró clasificar que las contraseñas *nivel de complejidad Bajo* utilizadas para los ataques eran palabras de: diccionario, nombres de personas, personajes libros/ historietas/tv, combinaciones entre palabras de diccionario y números simples, palabras de administrador de sistemas, fechas o combinaciones de teclado, etc.

Tomando como referencia al cuasi-experimento realizado por Colombini et al. [4], con el propósito de verificar la vulnerabilidad de sus contraseñas, y en el cual manifiestan que durante su estudio de 30 días y con la ayuda de dos Honeypots (uno que contiene contraseñas fáciles y otro que contiene contraseñas complejas), podemos asegurar que vulnerar al Honeypot que contenía las contraseñas difíciles, en el tiempo de estudio propuesto, sería prácticamente casi imposible. Sin embargo, coincidimos con el estudio de Colombini et al. [4] en sus contraseñas fáciles, que la mayoría de este tipo de contraseñas también fueron encontradas en los resultados de nuestro estudio.

### C. ¿Qué tipos de atacantes son más frecuentes?

Consideramos que existieron dos tipos de atacantes: Bots y Humanos. Sin embargo, el mayor número de ataques fueron

provenientes de Bots. Este es el caso del Malware denominado *Massive DDoS Brute-Force Campaign Targets Linux Rootkits* XOR.DDoS.

Tal como indican Pinkas y Sander [19], pudimos establecer que los atacantes (especialmente los Bots) realizan ataques con varios intentos de conexión de forma paralela, debido a que los servidores permiten varios inicios de sesión de usuario lo que permite esta maniobra de ataque. Es la razón por la que detectamos ataques a todos los niveles de complejidad en un promedio de 2,9 ataques por sesión. Esto ayuda al atacante a eludir la medida del tiempo.

### *D. ¿Cuál es la procedencia de los atacantes?*

La mayoría de ataques son provenientes de China (72.7 %) y Hong Kong (12,3 %). El (15%) de ataques restantes se distribuyen entre países de Europa y América. Con respecto a la existencia de ataques provenientes de Ecuador, determinamos que la 186.68.45.170 de la ciudad de Guayaquil, efectuó 2 ataques nuestro Honeypod.

Finalmente, coincidimos con lo señalado por Ma et al. [18] durante la mesa redonda en la conferencia RSA 2005, en que el uso de las *contraseñas estará con nosotros para siempre*, y por que ello *tenemos que continuar con estudios e investigaciones para hacer de la seguridad de contraseñas más sencilla de usar y a la vez eficaz.*

## AGRADECIMIENTOS

Nuestro agradecimiento al Grupo de Investigación de Modelos de Producción de Software (GRIMPSOFT) de la Universidad de las Fuerzas Armadas ESPE, quienes colaboraron con su infraestructura experimental para la realización del presente experimento. Al Grupo de Investigación en Ingeniería de Software Empírica (GRISE) de la Universidad Politécnica de Madrid por brindarnos el asesoramiento en la contrucción del honeypot experimental. A la SENESCYT y Armada del Ecuador por los recursos destinados en la elaboración del presente artículo.

## REFERENCES

[1] D. Florêncio, C. Herley, and P. C. van Oorschot, "An administrators guide to internet password research," in *Proceedings of the 28th Large Installation System Administration Conference (LISA14).*, 2014.

[2] J. Weber, D. Guster, P. Safonov, and M. Schmidt, "Weak password security: An empirical study," *Information Security Journal: A Global Perspective*, vol. 17, pp. 45–54, 2008.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[4] C. M. Colombini, A. Colella, M. Mattiucci, and A. Castiglione, "Cyber threats monitoring: Experimental analysis of malware behavior in cyberspace," in *Security Engineering and Intelligence Informatics*, Springer, Ed., no. 8128, CD-ARES 2013 Workshops: MoCrySEn and SeCIHD Regensburg. Springer, 2013, pp. 236–252.

[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: empirical results," *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 25 – 31, October 2004.

[6] M. DellAmico, P. Michiardi, and Y. Roudier, "Password strength: An empirical analysis," *INFOCOM, 2010 Proceedings IEEE*, pp. 1 – 9, March 2010.

[7] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 162–175. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866327

[8] E. Spafford, "Preventing weak password choices," Purdue University, Tech. Rep. 91-028, 1991. [Online]. Available: http://docs.lib.purdue.edu/cstech/875

[9] E. H. Spafford, "Observing reusable password choices," Purdue University, Tech. Rep. 92-049, 1992. [Online]. Available: http://docs.lib.purdue.edu/cstech/970

[10] D. Malone and K. Maher, "Investigating the distribution of password choices," *CoRR*, vol. abs/1104.3722, 2011. [Online]. Available: http://arxiv.org/abs/1104.3722

[11] Infosec, "Honeypots resources," October 2012. [Online]. Available: http://resources.infosecinstitute.com/honeypots/

[12] R. Morris and K. Thompson, "Password security: A case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, Nov. 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359172

[13] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 364–372. [Online]. Available: http://doi.acm.org/10.1145/1102120.1102168

[14] T. Wu, "A real-world analysis of kerberos password security," 1989.

[15] J. A. Cazier and B. D. Medlin, "Password security: An empirical investigation into e-commerce passwords and their crack times," *Information Systems Security*, vol. 15, no. 6, pp. 45–55, 2006.

[16] A. Jedlitschka and D. Pfahl, "Reporting guidelines for controlled experiments in software engineering," in *Empirical Software Engineering, 2005. International Symposium*, Nov 2005, pp. 10 pp.–.

[17] P. Paganini, "Chinese hackers hit penn state university, 18k people impacted," www.cyberdefensemagazine.com, Mayo 2015. [Online]. Available: http://www.cyberdefensemagazine.com/chinese-hackers-hit-penn-state-university-18k-people-impacted/

[18] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in *Network and System Security (NSS), 2010 4th International Conference on*, Sept 2010, pp. 583–587.

[19] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 161–170.