International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 17 No. 3 Aug. 2016, pp. 872-883

http://www.ijias.issr-journals.org/

ANÁLISIS, INCIDENCIA Y MITIGACIÓN DE UN ATAQUE BASADO EN DICCIONARIO

[ANALYSIS, INCIDENCE AND MITIGATION OF A DICTIONARY-BASED ATTACK]

Alfonso Guijarro Rodríguez[1], Lorenzo Cevallos Torres[1], and David Cárdenas Giler[2]

[1]Carrera de Ingeniería en Sistemas Computacionales, Universidad de Guayaquil, Guayaquil, Ecuador

[2]Carrera de Ingeniería en Sistemas Administrativo Computarizado, Universidad de Guayaquil, Guayaquil, Ecuador

ABSTRACT: The negligence of network administrators haves let intruders affect computer systems, generating significant losses in business. The most common security threats to computer crimes are aimed at obtaining privileged access to the system through dictionary-based attacks or brute force. The research analyzes the growth curve that has experienced in the last 5 years this technique and explains why its growth and popularity, detailing its performance, implementation process and to the extent that could compromise an organization if successful. Traditional methodologies considered essential to install multiple software tools to mitigate this threat managing to control, adjust and monitor internal security policies reducing network vulnerabilities. This document is intended to reduce the chances of success and the impact caused by attacks based on dictionary, for this a test scenario was created with virtualization tools, and additionally social engineering is explained as a primary factor in the development of this attack finally necessary security stockings were implemented to mitigate this crime.

KEYWORDS: Unauthorized access; dictionary attack; credentials; brute force; password ; Informatic security; vulnerabilities.

1 INTRODUCCIÓN

La seguridad informática ha evolucionado a tal punto que se ha vuelto una necesidad dentro de las organizaciones, debido al aumento de los delitos informáticos que tienen como finalidad comprometer la continuidad de las empresas. Con el aumento de las tecnologías en la última década, los dispositivos portables se conectan a internet en forma exponencial, lo que supone una mejora en materia de comunicación y movilidad, también incrementan los riesgos a los que están expuestas esas nuevas tecnologías como Smartphone, Smartwatch, tablet, entre otros, de sufrir algún tipo de ataque informático que comprometa la confidencialidad y la autenticidad de los datos [1].

La introducción de la domótica en la automatización de los hogares, ha establecido un nuevo campo de acción para los atacantes, domótica implica que los electrodomésticos y demás aparatos de los hogares cuenten con tecnologías capaces de conectarse a internet [2], lo que evidentemente implica riesgos, y consecuencias de un ataque a sistemas automatizados hogareños que pueden repercutir en daños a nivel de datos, y que también pueden comprometer físicamente a los usuarios [3].

Ningún sistema de seguridad es 100% confiable, a pesar de que las empresas que ofrecen soluciones a nivel de seguridad están investigando y desarrollando nuevas técnicas para la prevención de ataques informáticos, lo cierto es que siempre existirán brechas de seguridad, producto de un mal diseño del software o por falta de mecanismos o conocimientos por parte de los encargado de aplicar la seguridad informática. Paralelamente al desarrollo de los sistemas de seguridad, los hackers o crackers también desarrollan e investigan acerca de los sistemas informáticos pero con el objetivo de vulnerar el sistema, a través del ataque basado en diccionario, el cual busca las credenciales de acceso para comprometer en su totalidad a la

Corresponding Author: Alfonso Guijarro Rodríguez

organización en caso de llegar a efectuarse exitosamente, este ataque tiene una particularidad, su éxito se basa en gran medida a la capacidad de procesamiento de datos que posea el equipo atacante, capacidad que cada día se incrementan debido a las nuevas tecnologías desarrolladas para maximizar el rendimiento de los equipos informáticos, por este motivo necesitamos conocer su funcionamiento y sus variables de ataque, con el objetivo de implementar mecanismos eficaces que puedan reducir la probabilidad la éxito del ataque o minimizar los daños provocados por el mismo.

Existen varios autores que han abordado el tema de seguridad informática y sus distintos métodos de ataques, a manera de introducción [4] explica generalidades y pautas sobre la seguridad informática y sus puntos más relevantes. [5] propone una simulación de varios ataques dirigidos a las redes IP en un ambiente corporativo real, [6] evalúa y analiza varios escenarios de ataques informáticos para proponer medidas para la mitigación de los mismos. Con la información y resultados obtenidos [7] profundiza en el ataque DOS, analizándolo y recreando un escenario de prueba destinado a la ejecución del ataque , con el fin de responder ¿en qué grado puede afectar un ataque DOS a la continuidad de un negocio?, y complementariamente [8] explica como el uso de técnicas y habilidades sociales pueden comprometer gravemente a la seguridad informática.

La técnica que se analizara es un ataque de fuerza bruta basado en diccionario, se escogió este método porque desde el año 2010 ha venido en constante incremento, así lo registra UNAN-CERT [9], siendo el año 2015 cuando el BF (brute force), llego al primer lugar entre varios métodos de ataque como botnets, malware, DOS, entre otros. La investigación iniciará con un análisis del ataque para estudiar sus puntos críticos y conocer sobre los mecanismos que utilizan, con estos datos como base se recreara un escenario virtual sobre el que se ejecutara el ataque posteriormente se implementaran mecanismos de defensas como IPTABLES y UTM para monitorear y controlar los ataques y finalmente se efectuara un análisis de resultados, para llegar a una conclusión que aporte científicamente a la mitigación de los efectos causados por este tipo de ataque o en el mejor de los casos a protegernos en su totalidad.

2 METODOLOGÍA

Se realizó una revisión de la bibliografía referente a diversos escenarios de ataques a sistemas informáticos, para tener una referencia sobre las herramientas que utilizan los distintos autores y los resultados que obtienen, en base a esto se recreó un escenario capaz de simular un ataque de diccionario, con el propósito de estimar el grado de incidencia que tiene en los sistemas informáticos y proponer técnicas y planes de contingencia en el caso de que el ataque se efectivice.

Sistemas operativo: Se utilizó sistemas operativos basados en Linux, para la maquina atacante se utilizó Kali Versión 2016.1 que es una distribución basada en debían desarrollada para efectuar Pentesting y auditorias de seguridad, guarda en sus repositorios centenares de herramientas utilizadas para pruebas de penetración, análisis forense, ingeniería inversa, ataques a redes inalámbricas, entre otras [10]. Para la maquina víctima se implementó un sistema operativo Ubuntu Server en su versión 14.04 [11], que funciona como servidor ftp, web-server, y el acceso remoto se manejó mediante SSH.

Técnicas y herramientas: El servidor web estará trabajando sobre Apache2 versión 2.4.10, complementado por PHP5 versión 5.6.17 y una base de datos MYSQL versión 5.0.67, para trasferir los archivos al servidor web se habilito el servicio VSFTPD versión 3.0.2, y se realizó la configuración de las IPTABLES con las medidas de seguridad adecuadas.

Ataque basado en diccionario: Para realizar las pruebas se utilizó el software TCH-HYDRA versión 8.0, especializado en ataques de fuerza bruta usando diccionario, mientras que para elaborar el diccionario se hizo uso de CRUNCH versión 3.6, un software que mediante el uso de comandos de configuración nos permite personalizar muy detalladamente nuestro diccionario.

Control de tráfico y monitoreo: Se usó un UTM de la marca SOPHOS en su versión 9.4, para controlar el tráfico que genera un ataque de diccionario, el UTM ofrece métodos y herramientas para mitigar y prevenir de futuros ataques a la red. Para medir el uso de recursos internos se utilizó las herramientas propias de los sistemas operativos que permiten tener datos estadísticos sobre el rendimiento y el tráfico a nivel de host, complementado con Wireshark un sniffer de red para monitorear el tráfico que se genera en un segmento especifico de la red.

2.1 CARACTERÍSTICAS Y ANÁLISIS DEL ATAQUE DE DICCIONARIO

Un ataque de diccionario es un método sistemático para intentar descubrir la cuenta de usuario y/o contraseña, en base a directrices previamente establecidas el método de ataque prueba combinaciones de números, símbolos y letras. El hecho de que con un sencillo script, se puedan realizar varios ataques a distintas organizaciones lo convierten en uno de los principales métodos para vulnerar un sistema informático [12]. En la tabla 1 se visualiza una matriz de los factores críticos en este tipo de ataque.

Tabla 1. Factores que influyen en un ataque de diccionario

Factor	Importancia
Procesamiento	Mientras mayor sea la capacidad de procesamiento mayor número de credenciales son comprobadas, es decir, se reduce el tiempo de ejecución
Tiempo de ejecución	El tiempo es crucial porque un ataque de diccionario genera un tráfico detectable pos los IDS, es decir mientras más tiempo este en ejecución el ataque más expuestos estamos frente a las defensas de seguridad
Diccionario	El diccionario es la base para un buen ataque, en él se almacenaran los posibles usuarios y/o contraseñas, un buen diccionario se arma en base al perfil de la víctima o de la organización.
Vulnerabilidades de credenciales	A pesar de que existen muchas fuentes de información que nos explican la necesidad de una contraseña robusta, existen aún personas que prefieren usar credenciales por defecto o credenciales fáciles de recordar, estas credenciales son las más expuestas a un ataque de este tipo.

Nota: *En la tabla 1 se explican los puntos relevantes dentro de un ataque de diccionario, y una breve descripción de la importancia que tienen dentro de un ataque de este tipo.*

El proceso en un inicio parece ser sencillo pero, [13] existen grandes inconvenientes a nivel matemático, porque cada vez que se desea agregar un carácter más a la cadena, o ampliar el diccionario de entrada esta crece exponencialmente. El método matemático consiste en una matriz numérica, estructurada a partir de un abecedario de entrada y el tamaño de la cadena, con estas variables se realiza una operación matemática/logarítmica cuyo resultado es el diccionario, en la tabla 2 se presenta una matriz referencial, en la cual el abecedario estará en la primera columna, el tamaño de la cadena en la segunda columna y en la tercera se presentara el número de posibles usuarios o contraseñas que contendrá nuestro diccionario para posteriormente usarlo en el ataque de diccionario.

Tabla 2. Matriz de una cadena para un ataque de diccionario

Abecedario	Tamaño de la cadena	Número de cadenas
Solo números	6	1 000 000
Números y una letra minúscula	6	3 200 000
Números y dos letras minúsculas	6	10 240 000
Solo letras minúsculas	6	1 073 741 824
Letras mayúsculas y minúsculas	6	68 719 476 736

Nota: *La tabla 2 ejemplifica la creación de un diccionario, exponiendo el número de credenciales totales que se emplearan dependiendo de las variables de entrada en este caso el abecedario y el tamaño de la cadena.*

El resultado es abrumador, se obtienen cantidades exorbítales con una cadena de solo 6 caracteres, ahora, que pasaría si se desea usar un diccionario con una cadena de 7 caracteres, con un abecedario de números, letras y símbolos especiales, y factor adicional, si no conocemos el usuario ni contraseña, las posibilidades de éxito en el ataque disminuyen significativamente por la razón de que se tendría demasiada información, la misma que posiblemente ni si quiera logre vulnerar el sistema, es por esto que en primer lugar se realiza una enumeración pasiva para obtener datos críticos o indicios de posibles usuarios o contraseñas.

2.2 ESTADÍSTICAS DE LOS ATAQUES A REDES EN EL AÑO 2015

UNAN-CERT [9] es un equipo de profesionales que recopilan los datos referente a la seguridad informática de las empresas que deseen formar parte de este proyecto, en la tabla 3 podemos observar las estadísticas de los ataques a las redes informáticas en los últimos años.

Tabla 3. Estadísticas trimestrales de los ataques más comunes en 2015

	Brute Force	Bots	Malware	Worms	DDos	Spam	Defacement	XSS	Redireccionamiento	Pishing	Total
1ºer trimestre	2549	213	13	2	15	5	5	0	3	0	2963
21do Trimestre	93	395	5	19	1	4	3	4	1	0	525
31er Trimestre	2476	70	152	63	4	2	1	1	0	1	2770
41to Trimestre	532	23	8	0	0	2	2	0	0	0	567
Total	**5650**	**859**	**178**	**84**	**20**	**13**	**11**	**5**	4	**1**	**6825**

Fuente: *UNAN-CERT, se observa que en el 2015 el método preferido por los atacantes ha sido el uso de fuerza bruta para vulnerar los sistemas informáticos.*

Las estadísticas mostradas justifican el propósito de esta investigación, [9] es evidente que los ataques de fuerza bruta son los más ejecutados en el año 2015, un dato relevante son los tiempos que se manejan entre ataques, se observa en la tabla que de enero a marzo se reportaron el 45% de los ataques, mientras que los siguientes tres meses tan solo el 5%, esta variante de porcentajes es debido a la necesidad de realizar una enumeración pasiva, que es el método para recopilar información relevante de la víctima antes de lanzar el ataque activo, [13] el uso del ataque de fuerza bruta está tomando mayor relevancia en los últimos años por su capacidad de ejecutar ataques distribuidos a varios servidores sin la necesidad de intervención humana, el proceso es automatizado mediante el uso de un script o de un software previamente configurado. A continuación en la tabla 4 analizamos el ataque de fuerza bruta durante los ultimo 5 años.

Tabla 4. Estadísticas de los ataques desde el 2010 al 2015

Año	Nº de ataques de fuerza bruta	Equivalente en porcentaje
2010	2357	67,52%
2011	297	11,00%
2012	24811	21,25%
2013	8812	55,20%
2014	13712	64,93%
2015	5650	82,78%

Fuente: *UNAN-CERT, la primera columna indica el año, la segunda el número de ataques por año, y la tercera es el porcentaje que representa el ataque de fuerza bruta por año.*

Es evidente que desde el año 2013 el ataque de fuerza bruta ha significado la principal amenaza para los sistemas informáticos, [5] esto en general a la falta de políticas seguridad por parte de los administradores y lo predecible que puede ser el factor humano, este último se vuelve un punto crítico dentro de la aplicación de mecanismos de seguridad, como consecuencia se deben fortalecer las políticas de contraseñas para disminuir el riesgo que puede presentar una organización frente a el ataque de fuerza bruta.

3 DESARROLLO

El proceso práctico se desarrolló en 3 etapas, la primera etapa es el proceso pasivo en el cual el atacante busca conocer las posibles vulnerabilidades usando herramientas como NMAP o un analizador de vulnerabilidades este tipo de ataques es el más difícil de detectar para los mecanismos de defensa de las empresa porque son ataques que no generan trafico malicioso, solo realizar un escaneo en general a todas las posibles brechas de seguridad, en el proceso pasivo también se dan los ataques de ingeniería social que buscan mediante métodos sociales inducir a algún miembro de la empresa a revelar información que puede servir de base para futuros ataques, por último la generación del diccionario para efectuar el ataque también se incluye aquí puesto que se la realiza sin conocimiento ni relevancia para la víctima. El proceso activo es el ataque propiamente dicho, aquí se realizaron las pruebas con la herramienta HYDRA este proceso si genera un tráfico detectable para los sistemas de defensa, una vez efectuado el ataque se explicaran las medidas adecuadas para minimizar el riesgo de que ocurran este tipo de ataques, aplicando seguridad a nivel de host, luego a nivel de segmento de red, y por ultimo centralizando las medidas de seguridad con un gestor unificado de amenazas, a continuación se observan las tres etapas en detalle en la Figura 1.

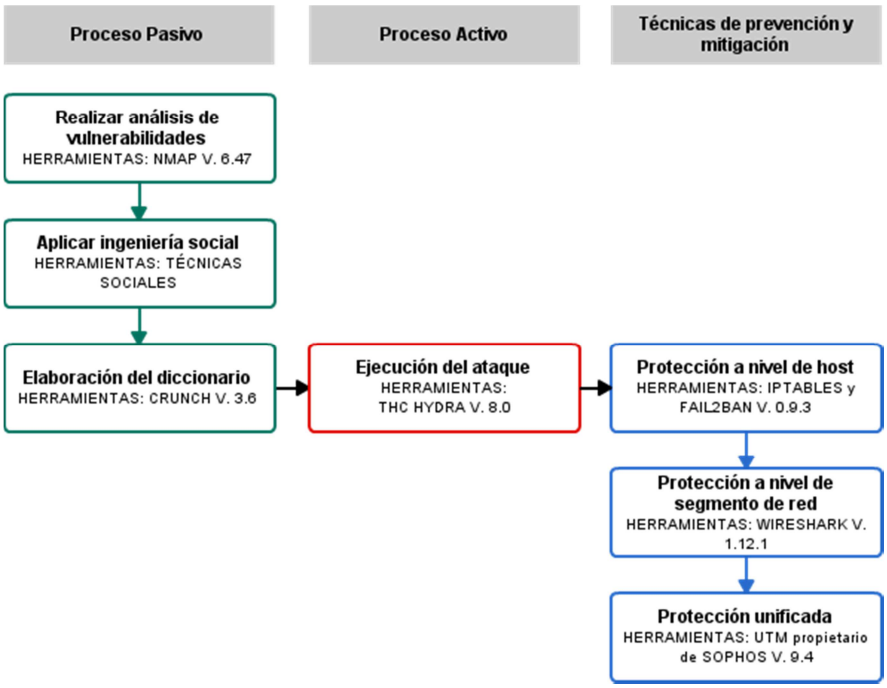


Fig. 1. Proceso para realizar un ataque por diccionario

En la Figura 1 se observa el esquema practico utilizado para realizar el ataque, el proceso pasivo que consta de recopilar información, el proceso activo que es el ataque en concreto y las técnicas de prevención son los mecanismos implementados para contrarrestar el ataque.

3.1 CONFIGURACIÓN Y DISTRIBUCIÓN DE LOS RECURSOS PARA LAS MÁQUINAS VIRTUALES

Para las prácticas de laboratorio usaremos plataformas virtuales, debido a que es más sencillo el manejo y la configuración de las mismas, principalmente por el ahorro de espacio y de recursos físicos, en la tabla 5 podemos verificar la distribución de las máquinas y software que usaremos en la práctica.

Tabla 5. Características de las máquinas

Sistema Operativo	Función	Características Físicas
Debian 8 64 bits	Máquina atacante, desde la cual realizaremos los ataques de diccionario	RAM: 4 Gb Disco Duro: 320 GB Procesador: 4
Ubuntu Server 14.4	Máquina víctima, ubicado en la DMZ, administra los servicios principales	RAM: 1 Gb Disco Duro: 20 GB Procesador: 1
UTM-SHOPOS	Gestor unificado de amenazas, controla y monitorea el tráfico de red.	RAM: 256 Mb Disco Duro: 20 GB Procesador: 1
Windows 8	Cliente de la organización	RAM: 1GB Disco Duro: 20 GB Procesador: 1
Ubuntu 14	Cliente de la organización	RAM: 256 Disco Duro: 20 GB Procesador: 1

Nota: En la tabla 5 se detallan las características de las maquinas usadas para realzar las pruebas técnicas para la ejecución del ataque basado en diccionario.

3.2 ESQUEMA DE LA RED

Para el diseño del escenario se usó una herramienta disponible en Internet llamada “Cacoo” la misma que puede ser encontrada en la siguiente URL “https://cacoo.com/lang/es/”, muy completa y sencilla de usar, el escenario planteado es el común denominador en las redes de datos de la mayoría de las empresas, en la Figura 2 planteamos la topología y la distribución de los elementos de nuestra red experimental.

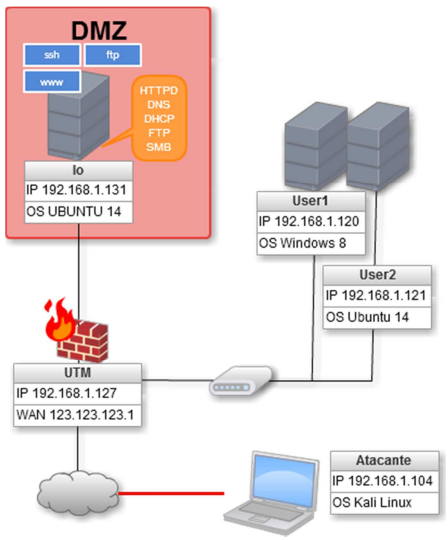


Fig. 2. Esquema de la red de pruebas

Esquema virtual sobre el que se realizaran ataques de diccionario con la finalidad implementar métodos efectivos para neutralizar o mitigar un ataque de este tipo.

3.3 ESCANEO DE VULNERABILIDADES

La fase inicial del ataque por diccionario consiste en recopilar información relevante acerca de la organización y de los usuarios [14], en primera instancia se analizó los puertos con nmap una herramienta que nos permite mapear la red [15], es decir, analiza el estado actual de la red o un host en específico, en la Figura 3 podemos ver el resultado del nmap realizado a la máquina ubuntu server.

```
root@85626:/home/javi# nmap -sS 192.168.1.131

Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-15 10:42 ECT
Nmap scan report for 192.168.1.131
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:ED:B9:84:6C:AF (Hon Hai Precision Ind. Co.)

Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
root@85626:/home/javi#
```

Fig. 3. Resultados del NMAP a la maquina victima

En la Figura 3 se presenta el resultado el análisis de puertos con la herramienta nmap.

El comando puede ser ejecutado como usuario normal o como súper-usuario dependiendo de la configuración del administrador, existen varios comando para personalizar el análisis de puertos, dependiendo de las necesidades, en este caso usaremos el más básico, nmap que es el inicial e imprescindible, el parámetro que lo precede es –sS el cual abre parcialmente una conexión tcp, enviando un SYN y en base a la respuesta de este se genera el estado del puerto, por último la ip del a máquina víctima, en este parámetro puede darse el caso de poner un segmento de red, o especificar un puerto, para obtener un mayor detalle en la respuesta.

3.4 USO DE INGENIERÍA SOCIAL

Con los resultados del escaneo se obtiene una idea, de las cuáles son los posibles servicios que maneja la organización, a continuación se aplica ingeniería social con el fin de obtener posibles usuarios e indicios de contraseñas,[8] la ingeniería social consiste en la aplicación de técnicas sociales para obtener información o privilegios, es decir, sin el uso de herramientas informáticas, convencer a las personas de hacer o divulgar información sensible. [8] En reiteradas ocasiones se excluye al ser humano como un factor relevante al momento de aplicar seguridad informática, este al ser un ente racional y no uno cibernético, es muy impredecible y por lo tanto vulnerable a las técnicas aplicadas por los profesionales al momento de recabar información sobre credenciales de acceso o algún indicio de las mismas.

3.5 ELABORACIÓN DEL DICCIONARIO

El diccionario es el motor de búsqueda del ataque por fuerza bruta, es de donde se van a probar una a una las posibles credenciales, por lo tanto es un factor fundamental durante el ataque, un buen diccionario se realiza en base a los datos que hemos recabado durante el escaneo de vulnerabilidades y durante la fase de ingeniería social, para el caso experimental se construyó un diccionario con 10 000 posibles contraseñas, para el cual usamos una herramienta open source denominada CRUNCH es un software especializado en la creación de diccionarios informáticos, a continuación en la Figura 4 se muestra el comando utilizado al momento de crear el diccionario de datos.

```
root@85626:/home/javi# crunch 16 16 -t ecua1220-%%%%%%% > dicc
_ssh.txt
Crunch will now generate the following amount of data: 1700000
00 bytes
162 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000
00
root@85626:/home/javi#
```

Fig. 4. Creación del diccionario de contraseñas

Nota: En la Figura 4 se observa el resultado de ejecutar la herramienta CRUNCH, se muestra el número de bits que contiene el fichero y el número de líneas del mismo.

La herramienta CRUNCH posee una gran variedad de comandos para personalizar y crear el diccionario de acuerdo a las diferentes necesidades que se presenten, la sintaxis del comando se describe a continuación; Crunch, comando identificador del software a utilizar, longitud de la cadena expresada en números enteros indica la longitud inicial y la final de la cadena, parámetros adicionales usados para personalizar el diccionario de acuerdo a las exigencias de cada usuario, el abecedario de entrada, es decir, los posibles caracteres a usar para crear el diccionario y por último se re direccionan los datos del resultado a un archivo de texto.

3.6 EJECUCIÓN DEL ATAQUE

El software THC-HYDRA [16] se ha escogido por su amplia gama de protocolos soportados, y su método de ataque sencillo pero muy eficiente, trabaja con un diccionario el cual previamente se debe tener en un documento de texto, en la Figura 5 se observa la ejecución del comando HYDRA.

```
root@85626:/home/javi# hydra -l root -P dicc_ssh.txt -vV 192.168.1.131 ssh

Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use
 in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-03-15 10:48:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it i
s recommended to reduce the tasks: use -t 4
```

Fig. 5. Ej ecución del comando HYDRA

Nota: En la Figura 5 se observa la ejecución del comando hydra para realizar un ataque via SSH hacia la maquina Ubuntu server.

HYDRA posee multitud de variantes en sus comandos, existen ataques directos a un host en específico, pero también existe la posibilidad de realizar ataques a varios servidores, a continuación describiremos cada parámetro usado en el comando.

-l: se usa para definir un usuario, se puede usar –L para usar un diccionario.

-P: lo usamos para definir un diccionario de posibles contraseñas acompañado del diccionario en TXT.

-vV: Muestra la descripción de las acciones realizadas en tiempo real.

IP: define la IP de la maquina víctima.

Protocolo: se ubica el protocolo por el que vamos a realizar el ataque, en caso de que el puerto sea uno diferente al que se usa por defecto, tenemos que adicionarlo con el comando –s.

EL tiempo que se tome el ataque dependerá principalmente de la capacidad de procesamiento de la máquina, para el ejemplo se usó una máquina con 4 GB de RAM, y un procesado I3 de 1.8 GHz, con 4 núcleos internos, en la figura 6 se observa el uso de los distintos procesadores de la maquina kali Linux

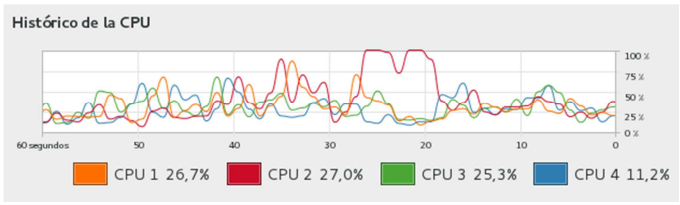


Fig. 6. Grafico del uso del procesador en la máquina atacante

Se observa en la Figura 6 el uso del procesador, especificado con un color distinto de cada núcleo interno del mismo.

En las pruebas realizadas, el tiempo que se demoró en probar las 10 000 contraseñas fue de 4 horas, evidentemente las máquinas superan con creces el rendimiento usados para ejecutar el ataque, el proceso que se realizo fue exitoso, puesto a que la máquina víctima no disponía de las medidas de seguridad adecuadas para mitigar un ataque de este tipo, a continuación se recomiendan herramientas y métodos para aumentar significativamente los parámetros de seguridad.

3.7 TÉCNICAS DE PREVENCIÓN Y MITIGACIÓN

El análisis de riesgos es un factor sustancial en materia de seguridad informática, se lo realiza para obtener un registro de todos los posibles ataques y sus potenciales consecuencias [17], adicional a esto también se emplea métodos estadísticos para obtener la probabilidad de que dicho riesgo se concrete [18]. Uno de los riesgos en este análisis evidentemente es la protección de los datos, y las medidas que se implementaran frente a un ataque de diccionario, inicialmente usaremos el firewall por defecto de Linux, que son las IPTABLES, lo configuraremos de tal manera que solo admita hasta 4 intentos de acceder al servicio, si se ejecutan más de 4 inmediatamente se bloquea a la IP que posiblemente está intentado vulnerar la red. Como un dato adicional existen los denominados firewall de aplicación cuya función principal es proteger únicamente algún protocolo o aplicación específica, estableciendo reglas destinadas a proteger una única vía o un único servicio [19]. En

la Figura 7 se observa las políticas para el tráfico de entrada, es aquí donde se implementó la medida de seguridad contra el ataque de diccionario.

```
root@Web-Server:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere            multi
           tcp  --  anywhere             anywhere            tcp dpt:
: ftpattack side: source mask: 255.255.255.255
LOG        all  --  anywhere             anywhere            recent:
4 name: ftpattack side: source mask: 255.255.255.255 limit: avg 4/min
ix "Ataque ftp"
DROP       all  --  anywhere             anywhere            recent:
4 name: ftpattack side: source mask: 255.255.255.255
```

Fig. 7. IPTABLES configurado contra ataque de diccionario

En la Figura 7 se muestran las políticas configuradas para el servidor Ubuntu.

Las políticas se aplicaron en función a mitigar un ataque por diccionario por el puerto ftp, se limitan las posibles conexiones a 4, es decir, si se detectan más de 4 conexiones por minuto, automáticamente se bloquean todos los paquetes que tengan como origen la ip atacante, la información de los puertos y configuración de la sintaxis es obligación del administrador de red, que debe implementar políticas de seguridad para cada servicio que maneje la empresa, orientado a ataques provenientes del internet así como posibles ataques internos.

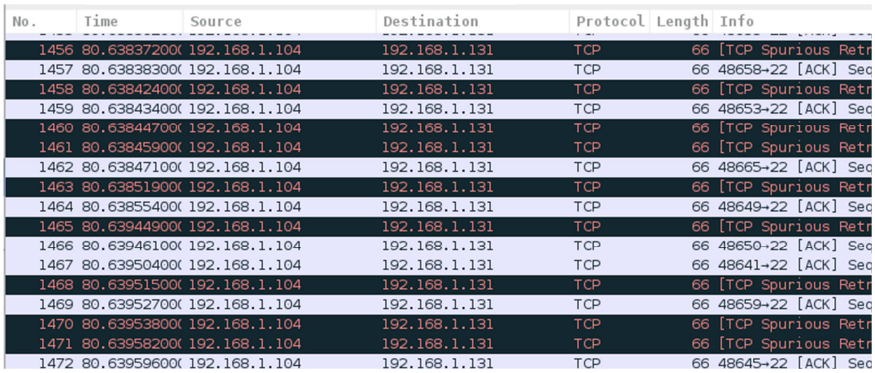
El configurar IPTABLES es una medida factible pero tiene sus limitantes, al momento de cambiar los servicios o los puertos, o cuando se necesiten incluir nuevos servicios, se deben actualizar todas las IPTABLES, como segundo método de protección a nivel de host se implementó un software llamado FAIL2BAN [20], es un software desarrollado para mitigar ataques de diccionario, el cual soporta gran variedad de protocolos, su función es sencilla, mediante un archivo de configuración, especificamos los servicios, y el número de intento de autenticación, si supera el límite establecido inmediatamente se modifican las tablas ip para denegar temporalmente o definitivamente la IP que está generando el posible ataque. En la Figura 8 observamos el fichero de configuración de FAIL2BAN.

```
[ssh]

enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 6

[dropbear]

enabled  = false
port     = ssh
filter   = dropbear
logpath  = /var/log/auth.log
maxretry = 6
```

Fig. 8. Configuración de FAIL2BAN para el servicio SSH

En la Figura 8 se especifican los parámetros de configuración para el servicio SSH.

Para proteger los segmentos de red, se utilizó un sniffer de red, usaremos una herramienta disponible en los repositorios del S.O. kali Linux llamada wireshark, la principal función del wireshark es escanear los paquetes que se envían en un segmento de red, especificando el protocolo, la ip de origen y destino, la longitud, el tiempo, un identificación y el contenido del paquete, el cual puede o no estar encriptado, en la Figura 9 se observa el resultado del wireshark al momento de realizar el ataque de diccionario.



No.	Time	Source	Destination	Protocol	Length	Info
1456	80.63837200(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1457	80.63838300(	192.168.1.104	192.168.1.131	TCP	66	48658→22 [ACK] Seq
1458	80.63842400(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1459	80.63843400(	192.168.1.104	192.168.1.131	TCP	66	48653→22 [ACK] Seq
1460	80.63844700(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1461	80.63845900(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1462	80.63847100(	192.168.1.104	192.168.1.131	TCP	66	48665→22 [ACK] Seq
1463	80.63851900(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1464	80.63855400(	192.168.1.104	192.168.1.131	TCP	66	48649→22 [ACK] Seq
1465	80.63944900(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1466	80.63946100(	192.168.1.104	192.168.1.131	TCP	66	48650→22 [ACK] Seq
1467	80.63950400(	192.168.1.104	192.168.1.131	TCP	66	48641→22 [ACK] Seq
1468	80.63951500(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1469	80.63952700(	192.168.1.104	192.168.1.131	TCP	66	48659→22 [ACK] Seq
1470	80.63953800(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1471	80.63958200(	192.168.1.104	192.168.1.131	TCP	66	[TCP Spurious Retr
1472	80.63959600(	192.168.1.104	192.168.1.131	TCP	66	48645→22 [ACK] Seq

Fig. 9. Paquetes filtrados por el Wireshark

En la Figura 9 los paquetes con color oscuro representa el tráfico generado por un ataque de diccionario.

Durante la ejecución del wireshark se analiza en tiempo real el tráfico generado durante el ataque por diccionario, la figura 9 revela que se está ejecutando trafico adicional desde la maquina kali Linux, hacia la maquina con el S.O. Ubuntu server, el tráfico generado es de tipo tcp, con la característica de ser un mensaje ACK, lo que evidentemente hace referencia a un posible intento de conexión con alguno de los servicios disponibles que se ejecutan en el servidor Ubuntu, estos datos deben ser revisados y monitoreados constantemente en busca de posibles amenazas que puedan comprometer a la empresa y complementado con mecanismos de detección de intrusos para que se ejecuten acciones inmediatas en caso de detectar un tráfico similar al generado durante el ataque por diccionario.

A nivel de protección de red, se implementó un gestor unificado de amenazas por sus siglas en ingles UTM, el cual posee varias funcionalidades embebidas en una sola solución de seguridad. Las características de los UTM pueden variar dependiendo de la empresa que lo desarrolla pero las principales funcionalidades que incluyen son: antivirus, firewall, ids, ips, filtro de paquetes web, filtro de paquetes locales, entre otras funcionalidades, puede ser un dispositivo hardware o un software [21], las principales desventajas de un UTM radica en el menor grado de configuración que pueden tener las aplicaciones, y la implementación de este debe darse en un punto de convergencia de toda la red interna, obligando a que los paquetes del exterior y del interior tengan que pasar por el UTM, con esto se garantiza el correcto funcionamiento del mismo. En la Figura 10 se presentan las principales características y herramientas disponibles en el UTM de la marca SOPHOS.

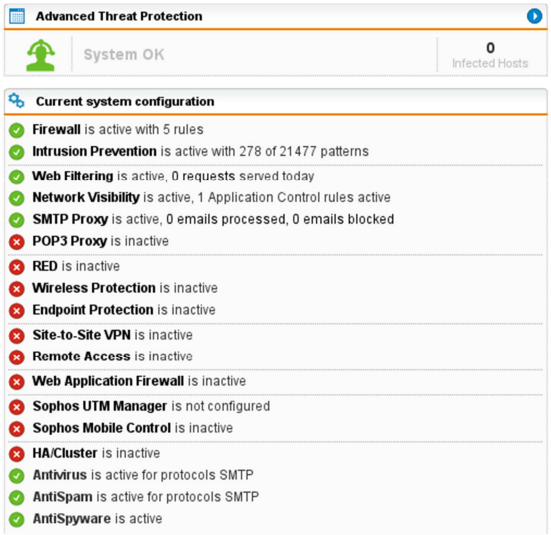


Fig. 10. Características del UTM de SHOPOS

En la Figura 10 se presentan las herramientas y métodos de seguridad que incluye el UTM de la marca SHOPOS.

Las medidas de seguridad implementadas se basan en reducir las probabilidades de que se efectivice el ataque, mediante el aprovechamiento de hardware y software creados específicamente para los ataques de diccionario, pero la vulnerabilidad en el factor humano siempre estará latente, y es un factor muy difícil de asegurar mediante mecanismos, los métodos adoptados por la mayoría de las empresas pasan por conferencias sobre la seguridad informática, que muchas veces no llegan a significar nada de valor o importancia para los usuarios, el riesgo humano es un factor que muy difícilmente se puede asegurar.

4 CONCLUSIONES

Los ataques de fuerza bruta basados en diccionario, son un método que puede llegar a comprometer parcial o completamente a una organización, es uno de los ataques más básicos pero también muy efectivo debido a la naturaleza matemática con la que se ejecuta. Durante el desarrollo de las pruebas de penetración, los niveles de procesamiento y el uso de recursos de la máquina atacante se incrementaron a la par de el de la maquina víctima, es decir, se puede dar el caso de que colateralmente un ataque de diccionario pueda generar una denegación de servicios, lo que evidentemente compromete en mayor grado a el desarrollo normal de las actividades de la empresa.

A pesar de los métodos implementados para aumentar los parámetros de seguridad, estos serán efectivos siempre y cuando se mantengan actualizadas las tecnologías y las defensas de la organización, se debe eliminar el paradigma de que la seguridad informática solo la deben aplicar los administradores o los departamentos pertinentes, se necesita una cooperación de todas aquellas personas que conforman una organización, ampliar el estereotipo de seguridad informática, pasar de verla como hardware y software, y empezar a centrarse más en el factor humano, capacitarlo de manera adecuada, prevenirlo y brindarle las herramientas necesarias para que pueda implementar protección a nivel de aplicaciones, concientizándolo de los riesgos potenciales que suponen los ataques informáticos y las metodologías aplicadas para mitigar el mismo, convirtiendo al factor humano en un representante más de la seguridad informática.

Una investigación a futuro se puede centrar en las vulnerabilidades de los dispositivos móviles, cuan propensos estamos a ser afectado por un ataque y cuáles son los mejores mecanismos y metodologías para proteger nuestros datos ante una amenaza cada día más latente.

Se debe implementar mecanismos de protección y mitigación a nivel de host, a nivel de segmento de red, y a nivel de red, es decir, implementar un modelo de seguridad con un diseño de cascadas, maximizando con esto la eficacia de la seguridad.

Se recomienda la utilización de un Honeypot para reconocer el tráfico que genera un ataque de diccionario, y aplicar reglas específicas al IDS con el objetivo de reducir las probabilidades de que se concrete el ataque, y alertar al administrador de la red de la ejecución del mismo.

Como método de prevención ante ataques de ingeniería social, se deben dar charlas internas sobre los potenciales riesgos que supone un ataque de ingeniería social, tanto para la empresa afectada como para el usuario.

El área de seguridad informática debe mantener un régimen de actualización constante, es decir, estar al tanto de las nuevas tecnologías que se desarrollan, y las nuevas amenazas que se dan a conocer.

Aplicar firewall de aplicación para los servicios más vulnerables de la empresa, esto como contramedida a los ataques de diccionario que siempre se efectúan a los protocolos o servicios desactualizados o con menos garantías a de seguridad [19].

REFERENCIAS

[1] Y. Marrero Travieso, “La Criptografía como elemento de la seguridad informática,” *Acimed*, vol. 11, 2003.
[2] L. F. Herrera Quintero, “Viviendas inteligentes (Domótica),” *Rev. Ing. e Investig.*, vol. 25, no. 2, pp. 47–53, 2005.
[3] M. A. Flórez de la Colina, “Hacia una definición de la domótica,” *Inf. la construcción*, vol. 56, no. 494, pp. 11–18, 2004.
[4] A. Chavez, “Seguridad Informática,” p. 218, 2009.
[5] H. Herrera, “SIMULACIÓN DE ATAQUES A REDES IP EN UN ENTORNO CORPORATIVO REAL,” 2015.
[6] L. Zapata, “Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución,” *Ingenius.Ups.Edu.Ec*, pp. 11–19, 2012.
[7] H. Avalos and E. Gómez, “Seguridad de la información, Generación y Mitigación de un Ataque de Denegación de Servicios,” vol. 28, no. Diciembre, pp. 54–72, 2015.
[8] L. Salvador, “INGENIERÍA SOCIAL Y OPERACIONES PSICOLÓGICAS EN INTERNET,” *Inst. Español Estud. Estratégicos*, pp. 1–21, 2011.
[9] UNAM-CERT, “Estadísticas de incidentes en 2015,” 2015. [Online]. Available: http://www.cert.org.mx/estadisticas.dsc.

[10] K. Linux, "KALI LINUX," 2016. [Online]. Available: http://docs.kali.org/introduction/what-is-kali-linux.
[11] Ubuntu, "Ubuntu Server 14.04," 2016. [Online]. Available: http://www.ubuntu.com/server.
[12] H. Fernández, J. Sznek, and E. Grosclaude, "Detección y limitaciones de ataques clásicos con Honeynets virtuales," 2008.
[13] L. V, "Papel de la explosión combinacional en ataques de fuerza bruta," vol. 1, pp. 28–32, 2013.
[14] U. Culhuacan, Q. U. E. Para, and O. El, "'ESTUDIO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN A SISTEMAS INFORMÁTICOS,'" 2011.
[15] "NMAP-ORG," 2015. [Online]. Available: https://nmap.org/man/es/.
[16] "THC-HYDRA," 2016. [Online]. Available: https://www.thc.org/thc-hydra/.
[17] C. P. C and C. G. Galindo, "Prácticas de Seguridad para el Laboratorio de Simulación de Telecomunicaciones," no. 1, 2013.
[18] J. Duque, "ANALISIS COMPARATIVO DE LAS PRINCIPALES TECNICAS DE HACKING EMPRESARIAL," no. x, pp. 1–6, 2010.
[19] G. Flament, J. Vera, and A. I. Aranda, "Implementación de un web application firewall basado en mod_security," 2012.
[20] "Fail2Ban," 2016. [Online]. Available: http://www.fail2ban.org/wiki/index.php/Main_Page.
[21] W. Flórez R, C. A. Arboleda S, and J. F. Cadavid A, "Solución Integral De Seguridad Para Las Pymes Mediante Un Utm," *Ing.USBMed*, vol. 3, no. 1, pp. 35–42, 2012.