Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas

Normandi Rocío Tirado Ríos [1], Dorys Janeth Ramos Reyes [2], Elsa Leuvany Álvarez Morales [3] Stalin Daniel Carreño Sandoya [4]

1 Universidad Técnica Estatal de Quevedo, ntirado@uteq.edu.ec

2 Unidad Educativa "Dr. Manuel Quintana Miranda", dojamipc@hotmail.com

3 Universidad Técnica Estatal de Quevedo, ealvarez@ uteq.edu.ec

4 Universidad Técnica Estatal de Quevedo, sdcarreno@ uteq.edu.ec

RESUMEN

La evolución de los sistemas de información hace necesaria el surgimiento de profesionales en el área informática responsables de evaluar su correcto funcionamiento, detectar aquellos puntos débiles que requieran de medidas preventivas y correctivas para evitar pérdidas de información que podrían causar costes importantes a las organizaciones. En la actualidad, las empresas están expuestas no sólo a robos de material o asaltos en sus instalaciones, sino a delitos de seguridad informática que pueden afectar los datos e información relevante de la organización. El presente artículo tiene como objetivo analizar las técnicas de ataques más usuales aplicadas por los hackers, sus consecuencias y la manera más conveniente de prevenirlas y mitigarlas. La mejor defensa ante un ataque que afecte la seguridad del negocio es implementar redes honeynet, reglas de iptables en el firewall de la organización; el cual permite o deniega el acceso al tráfico y por ende capacitar al recurso humano.

Palabras claves: Ataque, empresa, información, seguridad, vulnerabilidad.

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

Computer Security, a Mechanism to Safeguard the Information of the companies

ABSTRACT

The evolution of information systems necessitates the emergence of computer professionals in the area responsible for evaluating their proper functioning, detect those weaknesses that require preventive and corrective measures to avoid loss of information that could cause significant costs to organizations. At present, companies are exposed not only to material or assaults on their premises theft, but computer security crimes that can affect the data and relevant information from the organization. This article aims to determine the most common techniques applied attacks by hackers, its consequences and the most convenient way to prevent and mitigate them. The best defense against an attack that affects the security of the business is to implement networks honeynet, rules of iptables in the firewall of the organization; which allows or denies access to traffic and thus train human resources.

Keywords: Attack, business, information security vulnerability.

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

1. INTRODUCCIÓN

La seguridad informática ha ganado popularidad en los últimos años y ha pasado de ser considerada un gasto, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial. En algunos países esto ha sucedido de forma acelerada, en otros el paso ha sido más lento; pero en última instancia todos han convergido en un mundo digital en el que la información es el activo intangible más valioso; y por consiguiente debe ser protegido de posibles pérdidas, robos, mal uso, etc (Astudillo, 2013).

La comunidad científica ha investigado e implementado mecanismos que permitan disminuir y mitigar estos ataques de seguridad como hurto, modificación, espionaje, interrupción, falsificación, denegación de servicios, etc., empleando tecnologías de virtualización, cuya aplicación permite disminuir el riesgo a equipos y redes en producción, precautelando la información y servicios de las organizaciones (Fuertes *et al*., 2011).

En Ecuador las redes de computadoras son atacadas y vulneradas, cada año se incrementa la velocidad de propagación, la facilidad de ejecución y el daño que producen estos ataques, por lo tanto, es muy importante para tener una red segura considerar lo que se debe proteger y de quién; luego definir las políticas de seguridad adecuadas en la cual se define las estrategias que permitan la protección, confiabilidad e integridad de la información.

En la actualidad cualquier organización mantiene una red donde los datos viajan de unos equipos permanentemente. Esto es claramente una gran ventaja pero resulta ser también un gran problema debido a las dificultades de seguridad informática que, además, parecen estar empeorando, haciéndose cada vez más complejas; y por consiguiente, produciendo pérdida de dinero o de distintos tipos de información privada (Menéndez *et al*., 2009).

A partir de este antecedente el presente trabajo tiene como objetivo analizar las técnicas de ataques aplicadas por los hackers; para prevenir, controlar o corregir sus efectos en

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

las redes de datos; lo cual contribuye a proteger el activo más valioso de las empresas como es la información.

2. METODOS

Se realizó previamente una revisión de la bibliografía referente a algunos escenarios de ataques a sistemas informáticos, para tener una referencia sobre las herramientas que utilizan los distintos autores y los resultados que obtienen, así como la recopilación de estadísticas de los últimos 5 años sobre incidencias que atentan a la seguridad informática. El método estadístico empleados es el analítico descriptivo donde se describen en valores absolutos y porcentuales por año.

3. RESULTADOS

El término seguridad informática ha sido objeto de estudio por algunos autores, lo que permite tener una definición más exacta; por lo tanto es un conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, la confidencialidad y disponibilidad de la información (Escrivá *et al.*, 2013). Por otra parte, consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información, su respectiva modificación, sólo sea posible a las personas que se encuentren autorizadas y dentro de los límites de su autorización (Costas, 2014).

En definitiva estas definiciones complementan el término de seguridad informática como un conjunto de medidas y procedimientos con la finalidad que los datos siempre estén disponibles, salvaguardar la información, asegurando los recursos del sistema de información; por lo tanto, los procesos deben cumplir con estándares de seguridad; y por consiguiente, sólo el personal autorizado pueda acceder a la información.

Para Zapata (2012) las redes teleinformáticas están expuestas a ataques e intrusiones que pueden dejar inoperativos los recursos y causar pérdidas de la imagen, productividad, credibilidad y competitividad, provocando perjuicios económicos que podrían comprometer la continuidad del negocio. Esta incertidumbre sigue agravándose, pues continúan apareciendo diversas amenazas, vulnerabilidades y ataques; perjudicando

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

directamente a los negocios que son altamente dependientes de sus sistemas y redes de información.

De todos modos los daños producidos por la falta de seguridad pueden causar pérdidas económicas, falta de credibilidad y prestigio en una organización; por consiguiente, se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información.

El escaneo de puerto o rastreo de sistema consiste en el envío de una serie de señales (paquetes) hacia una máquina víctima que responde reenviando paquetes, que el atacante decodifica y traduce a fin de conseguir información sobre: direcciones IP activas, puertos TCP y UDP activos y; reconocimiento del tipo de sistema operativo del equipo como elemento de una red, además la herramienta más empleada para realizar el escaneo de puertos es Nmap (Network Mapper) (Zapata, 2012).

El escaneo de puertos es una técnica de monitorización y es el primer paso en la obtención de información básica de una red; su objetivo es acceder a información valiosa que le permitirá al hacker reunir todos los detalles para acabar con la seguridad del equipo y extraer información importante y confidencial del mismo.

Este término se utiliza para designar a una red de ordenadores controlados por el atacante (denominados “ordenadores zombies”) a través de la red. La finalidad de estas redes de ordenadores suele ser el envio de spam o la realización de ataques de denegación de servicio sobre servidores (Gascó *et al*., 2013).

Los Botnets tratan de controlar un número masivo de máquinas o servidores infectados de manera remota con la finalidad de capturar datos bancarios, cuentas de correos; por consiguiente estos equipos son controlados a través de un BotnetMaster.

Por su parte Gil & Martínez (2016) propone la detección y mitigación de las redes mediante un doble análisis de las fuentes de información. Primero a través de la monitorización de los flujos del tráfico de red y una vez confirmado el ataque se realiza una inspección más profunda de los paquetes de red. La propuesta es la creación y despliegue de una honeynet en donde se llega a aislar en una red virtualizada de cara a

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

que los bots gestionados remotamente por el botmaster no sean capaces de ejecutar su ataque final; es decir, el ataque distribuido de denegación de servicios.

Lo anterior muestra la ventaja que tiene la implementación de las redes honeynet; que tiene como objetivo reunir datos sobre la actividad del intruso con la finalidad de detectar las vulnerabilidades antes de que sean explotadas.

Si alguien intenta acceder a un sistema informático protegido con contraseña, previamente deberá averiguar esta. Cuanto más robusta sea una contraseña, más difícil será averiguarla. Una combinación de cifras, números y otros caracteres hace que sea más fuerte, pero hay que tener en cuenta que los usuarios son seres humanos y tienden a establecer contraseñas fáciles de recordar, por lo que es habitual que los sistemas establezcan restricciones que obliguen a los usuarios a cumplir unas determinadas normas a la hora de seleccionar sus contraseñas.

El Ataque de fuerza bruta trata de explorar todo el espacio posible de claves para romper un sistema criptográfico. Los “ataques de diccionario”, que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario, etcétera. (Álvaro, 2014).

En efecto esta técnica permite averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Existen un sinnúmero de herramientas disponibles en Internet que permiten efectuar ataques de clave de fuerza bruta entre ellas se mencionan las siguientes: Jhon The Ripper, Medussa, Hydra, etc.

Según Guijarro *et al*. (2016) el análisis de riesgos se lo realiza para obtener un registro de todos los posibles ataques y sus potenciales consecuencias. 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.

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

Hay que tener en cuenta que en los últimos años este ataque de fuerza bruta es uno de los más utilizados por los hacker para violentar la seguridad en las organizaciones y una manera de contrarrestarlos es a través del bloqueo del acceso a una cuenta después de varios intentos de inicio de sesión fallidos, generalmente tres.

Otra técnica es la Denegación de servicios también conocida como DoS (Denial of Services), tiene como principal objetivo atacar un grupo o red de computadoras causando que los servicios sean inaccesibles para los usuarios que acceden de una forma legítima a los mismos, dicho ataque normalmente ocasiona la pérdida total de conectividad a la red, por el aumento excesivo del consumo del ancho de banda de la víctima o también una sobrecarga de los recursos de los sistemas informáticos (Duque & Gómez, 2015).

Es decir esto provoca que un servicio, equipo o recurso sea inaccesible para usuarios legítimos; el cual se lleva a cabo mediante el uso de herramientas que envían una gran cantidad de paquetes con la finalidad de desbordar los recursos del servidor, logrando de esta manera que el servicio quede inoperable.

Para contrarrestar este tipo de ataque, Avalos & Gómez (2015) desarrollaron un demonio en Shell script, el mismo que neutralizó la amenaza del ataque dentro del ambiente de producción. La implementación se lo realizó en el Firewall que es donde se ejecuta el script con reglas de iptables, las cuales son una herramienta poderosa para filtrado, denegación o aceptación de paquetes. En definitiva, si existen varias peticiones de un mismo servicio con el mismo direccionamiento IP el script bloquea al equipo que está atacando a dicho puerto.

Una variante de DoS, son los ataques distribuidos de denegación de servicios DDoS, es una de las técnicas más eficientes y difícil de detectar por su naturaleza distribuida. En un ataque de este tipo, el atacante compromete un gran número de computadores conectados a la red mediante la explotación de vulnerabilidades de software de red, el volumen de tráfico malicioso generado es tan alto que la víctima no puede gestionar y se paraliza al instante el servicio. Una forma de ataque es UDP Flood, éste es posible cuando el atacante envía un gran volumen de paquetes IP con datagramas UDP a un puerto

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

aleatorio de la víctima y por ende el envío excesivo de datagramas UDP puede producir la caída del sistema (Molina *et al*., 2015).

Con referencia a lo anterior estos ataques se convierten en un desafío para los administradores de la redes de datos, quienes deben garantizar la disponibilidad del servicio mediante políticas que integren los aspectos básicos de seguridad incluyendo hardware, software y recurso humano como los componentes estratégicos que contribuirán a mantener la seguridad de la información

Por lo que se refiere a la suplantación mediante el protocolo ARP (Address Resolution Protocol), ésta técnica modifica el flujo de datos enviado desde la víctima hacia la pasarela (Gateway) haciendo un ataque de tipo hombre en el medio, de esta forma consigue que este tráfico pase a través de la máquina atacante sin que la víctima se percate de ello, entre las herramientas que permiten ejecutar un envenenamiento ARP están: Cain y Abel, Arpspoof, Ettercap, Arpoison; y los mecanismos de detección ante un ataque ARP son: Arpwatch, Snort y ArpGuard (González *et al*., 2016).

Cabe agregar que este ataque se desarrolla en la capa de acceso a la red y trabaja modificando la dirección física de la tabla ARP, debido a que en el protocolo ARP un host puede suplantar a otro host; obteniendo toda la información que le corresponde a su víctima; para proteger la red se deben implementar políticas en el switch que bloqueen el acceso del atacante, además de configurar mecanismos de detección que monitoricen la red.

Las vulnerabilidades de seguridad de la red datos de una empresa es susceptible a un sinnúmero de ataques cuando no se aplican las medidas de prevención, con la finalidad de coadyuvar a mejorar la seguridad de los sitios, en la tabla 1 se observa las estadísticas generales de los ataques a las redes informáticas en los últimos seis años según Universidad Nacional Autónoma de México y su Equipo de Respuesta a Incidentes de Seguridad en Cómputo (UNAM-CERT).

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

Tabla 1. Estadísticas de los ataques desde el 2011 al 2016

Año	Fuerza Bruta	Botnets	Denegación de Servicio	Phishing
2011	297	21.220	2	10
2012	24.811	58.125	16	16
2013	8.812	4.067	20	3
2014	13.712	13.712	13	20
2015	5.650	859	20	1
2016	45.903	308	45	26

Fuente: UNAN-CERT, la primera columna indica el año, la segunda hasta la quinta columna indican el número de ataques por año.

En el año 2012 el ataque de mayor relevancia es de botnets con 58.125 en relación a los ataques en estudio y en menor presencia se observó phishing en el año 2016 con un incidente.

Comparando cada uno de los ataques por año, fuerza bruta, denegación de servicio y phishing en el año 2016 presentaron 45.903; 45 y 26 respectivamente. Seguido por botnets que en el año 2012 presentó el mayor ataque.

UNAN-CERT considera que el ataque de mayor relevancia en los últimos años es el ataque de fuerza bruta, debido a 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. Mientras que Duque *et al*. (2016) concuerda que el ataque antes mencionado es muy fácil de aplicar 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.

Tabla 2. Estadísticas del porcentaje de incidencia anual de los ataques desde 2011-2016

Año	Total Incidentes	Fuerza Bruta (%)	Botnets (%)	Denegación de Servicio (%)	Phishing (%)
2011	26.989	1,10%	78,62%	0,01%	0,04%
2012	115.851	21,42%	50,17%	0,01%	0,01%
2013	15.963	55,20%	25,48%	0,13%	0,02%
2014	21.119	64,93%	64,93%	0,06%	0,09%
2015	6.825	82,78%	12,59%	0,29%	0,01%
2016	46.803	98,08%	0,66%	0,10%	0,06%

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

Fuente: UNAN-CERT, la primera columna indica el año, la segunda la cantidad de incidentes por año y desde la tercera hasta la sexta columna indican es el porcentaje de incidencia que representa los ataques por año.

Es incuestionable que desde el año 2016 el ataque de fuerza bruta con el 98,08% ha significado la principal amenaza para los sistemas informáticos y en menor presencia el ataque de denegación de servicio y phishing con el 0,01% en el año 2011 y 2012 respectivamente.

Comparando estadísticamente cada uno de los ataques por año, el ataque de fuerza bruta representa 98,08% en el año 2016; los botnets 78,62% en el 2011, denegación de servicio 0,29% en el 2015 y el ataque de phishing en el año 2014 con 0,09%.

Según UNAN-CERT el ataque de fuerza bruta desde el año 2013 ha tenido un crecimiento exponencial lo cual ha significado la principal amenaza para los sistemas informáticos, esto se debe a la falta de políticas seguridad por parte de los administradores de la red y por consiguiente; se deben fortalecer las políticas de contraseñas para disminuir el riesgo que puede presentar en una organización frente a el ataque de fuerza bruta. Sin embargo Domínguez *et al*. (2016) considera que es importante que la sociedad conozca cómo funcionan las técnicas de ataques de Fuerza Bruta con Diccionario de Datos, ya que con el avance de las tecnologías como los GPU (Unidad de Procesamiento de Gráficos) se puede llegar a descifrar contraseñas de 8 caracteres en 5.5 horas, comprobando de ésta manera que es cuestión de tiempo y de recursos llegar a vulnerar los métodos de autenticación simple “Contraseñas”.

4. CONCLUSIONES

El ataque de botnets es un software que una vez introducido en el PC sirve para que los hackers tomen control remoto del mismo y puedan realizar diferentes acciones, como el envío de spam, virus, gusanos y troyanos; por consiguiente para mitigar este ataque se propone la creación de una red honeynet. El ataque de fuerza bruta con diccionario se efectúa a través de diferentes herramientas que permite acceder a un host de la red; por tal razón, para contrarrestar se crea una regla que bloquee los tres intentos fallidos conocida como "regla de los tres strikes". La técnica de Denegación de Servicios Distribuidos está integrada por componentes efectivos y diversos, que la convierten en un

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

ataque complejo, difícil de detectar y detener. La técnica de hombre en el medio dispone de diferentes herramientas que permiten al atacante, suplantar la dirección MAC en la tabla ARP de los equipos de la red, situarse en el medio de una comunicación e interceptar los mensajes, ésta se puede evitar monitoreando el tráfico de la red y configurando políticas de defensa en el switch.

A partir del 2013 el ataque de fuerza bruta ha tenido un crecimiento vertiginoso en comparación con el ataque de botnets, denegación de servicio y phishing; motivo por el cual en la actualidad se ha convertido en una principal amenaza para las redes de datos de las empresas.

5. REFERENCIAS BIBLIOGRÁFICAS

Álvaro V. (2014), *Gestión de Incidentes de Seguridad Informática*, Madrid, España, Editorial RA-MA, Pag.43.

Astudillo, K., (2013), *Hacking Ético 101*, Guayaquil, Ecuador, Editorial RA-MA, Pag.8.

Avalos H. y Gómez E. (2015). Seguridad de la información, Generación y Mitigación de un ataque de Denegación de Servicios. Revista Tecnológica de la ESPOL, 28(5), 54-72.

Costas J., (2014), *Seguridad Informática*, Madrid, España, Editorial RA-MA, Pag.19.

Domínguez, H, Maya, E., Peluffo, D., Crisanto, Ñ. (2016). Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación. *Revista Científica Maskana*, 7(1), 87-95.

Duque, J., Silva, L. y Rentería, E. (2011). Análisis comparativo de las principales técnicas de Hacking Empresarial.Scientia et Technica, 2(1), 1-6.

Fuertes, W., Rodas, F. y Toscano, D. (2011). Evaluación de ataques UDP Flood utilizando escenarios virtuales como plataforma experimental. *Facultad de Ingeniería*, *20*(31), 37-53.

Gascó Escriva, Romero G y Ramada D. (2013), *Seguridad Informática*, Madrid, España, Editorial Macmillan Iberia S.A. Pag.7.

Revista Publicando, 4 No 10. (2). 2017, 462-473. ISSN 1390-9304

González, D. A., Pérez, M. E. G., & Bernal, L. P. (2016). Detección y mitigación de ataques ARP en la red corporativa de la división territorial holguín, ETECSA. *Revista Telem@ tica*, *15*(1), 62-68.

Guijarro, A., Lorenzo, C. y Cárdenas, D. (2016). Análisis, Incidencia y Mitigación de un ataque basado en diccionario. International Journal of Innovation and Applied StudiesScientia et Technica, 17(3), 872-883.

Menéndez, E., Díaz, G. y Castro, M.,(2009), Herramientas individualizadas para la formación en Seguridad de la Información Simulador de Ataques y Sistema de Detección de Intrusiones. TICAI 2009, 4(11), 75-82.

Molina, L., Furfaro, A., Malena, G., & Parise, A. (2015). Ataques Distribuidos de Denegación de Servicios: modelación y simulación con eventos discretos.

Orozco, A. L. S., Vidal, J. M., & Villalba, L. J. G. (2015). Sistema Inmunitario Adaptativo para la mitigación de ataques de Denegación de Servicio. In Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad: León, 14, 15, 16 de septiembre de 2015: I JNIC2015 (pp. 26-31). Servicio de Publicaciones.

Zapata, L. (2012). Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de virtualización de libre distribución. *Revista de Ciencia y Tecnología INGENIUS*, *20*(8), 11-19.

UNAN-CERT, (2017). Estadísticas de incidentes en RedUNAM durante 2016 Recuperado de ***http://www.cert.org.mx/estadisticas.dsc***