Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 10, No.6, Mes Junio, 2017
ISSN: 2306-2495 | RNPS: 2343
Pág. 1-10
http://publicaciones.uci.cu

Tipo de artículo: Artículo original
Temática: soluciones informáticas
Recibido: 21/02/17 | Aceptado: 30/04/17 | Publicado: dd/mm/aa

Implementación de servidores seguros contra ataques DDOS

Implementing secure servers against DDOS attacks

Karel Rodríguez Carmenates [1*], Reisel González Pérez [2], Pedro Manuel Puig Díaz[3]

[1] Centro de Tecnologías de Datos, Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas.
[2] Centro de Tecnologías de Datos, Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas.
[3] Departamento de Tecnología, Facultad de Ciencias y Tecnologías Computacionales, Universidad de las Ciencias Informáticas.

[*] Autor para correspondencia: karelr@uci.cu

Resumen

Con el desarrollo de las tecnologías de la Informática y las Comunicaciones, se inicia la era de los procesos digitales donde una o más personas pueden consumir servicios, realizar trámites sin estar presente físicamente. Para soportar dichos procesos se requiere de una robusta infraestructura tecnológica donde la configuración de los servidores dedicados juega un papel importante. Sin embargo en la actualidad existen vulnerabilidades provocadas por malas configuraciones que propician fallas en los servicios. La presente propuesta muestra una panorámica sobre la evolución de los ataques de Denegación de Servicio DoS, así como un conjunto de recomendaciones para mitigar dicha falla.

Palabras clave: Denegación de Servicios, Seguridad Informática, Servidores Seguros.

Abstract

With the development of information technologies and communication, begins the era of digital processes where one or more persons can consume services, perform procedures without being physically present. To support such processes requires a robust technology infrastructure where the dedicated server configuration plays an important role. But today there are vulnerabilities caused by misconfigurations conducive gaps in services. This proposal shows an overview of the evolution of Denial of Service DoS, and a set of recommendations to mitigate such failure.

Keywords: *Denial of Services, IT Security, Secure Servers.*

Introducción

Los inicios de Internet se remontan a mediados de la década de los setenta, bajo los auspicios de la Agencia de Proyectos Avanzados para la Defensa de Estados Unidos (YEZERS´KA 2006). Sus características y facilidades de uso le permitieron convertirse en la tecnología más rápida aceptación de todos los tiempos. Su surgimiento cambió todas las concepciones de la época, partiendo de la disponibilidad de la información, ahora al alcance de todos, las formas de comunicación, las más diversas formas de comercialización de productos y servicios. Su surgimiento le permitió a la Informática convertirse en una ciencia indispensable y de alcance universal.

Con la accesibilidad de la sociedad a las tecnologías, cada vez eran más frecuente la publicación de servicios científicos, comerciales y bancario Internet convirtiéndose así en un atractivo para los piratas informáticos, convirtiéndose así los delitos informáticos en algo común y la Seguridad Informática comenzó a jugar un rol fundamental en la defensa de los activos de las instituciones (GUILLEN-PINTO *et al*. 2017).

Los delitos informáticos se refieren a aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y servicios de Internet (MAYER LUX 2017).

En el documento Norton Cybercrime Report 2011, elaborado y publicado por la prestigiosa compañía Symantec se destacan aspectos fundamentales referidos a los daños financieros causados por delitos informáticos. A continuación se enuncian tres de los principales aspectos del referido documento (PÉREZ PATIÑO and ROBLEDO VELÁSQUEZ 2012):

- 388.000 millones de dólares en pérdidas anuales por ataques informáticos.
- 114.000 millones de dólares en pérdidas financiera y 274.000 millones en tiempo necesario para recuperarse de un ataque.
- 100.000 millones más grande que el mercado combinado de la marihuana, la cocaína y la heroína.

Entre los principales elementos relacionados con la Seguridad Informática que se pueden destacar durante 2011 y el primer semestre de 2012 se pueden citar el "hack-activismo" y la Guerra Cibernética o Ciberguerra (RICO CARRILLO 2013).

El "hack-activismo" se refiere principalmente a ataques realizados por hackers a modo de protesta contra instituciones y gobiernos. En cambio la Guerra Cibernética se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos

de batalla convencionales (MUÑOZ and RIVAS 2015). A continuación se enuncian algunos de los principales hechos referidos a la Guerra Cibernética (LOBATO and KENKEL 2015):

- 1999 - Guerra de Kosovo : Durante la intervención de los aliados en la Guerra de Kosovo, más de 450 expertos informáticos voluntarios se enfrentaron a los ordenadores militares de los aliados. Lograron penetrar los ordenadores estratégicos de la OTAN, la Casa Blanca y del portaaviones nuclear norteamericano Nimitz.
- 21 de mayo de 2010: es oficialmente activado el Cibercomando de Estados Unidos. Agrupación de Combate de las Fuerzas Armadas de Estados Unidos bajo el mando del Comando Estratégico de Estados Unidos para el dominio del ciberespacio y la Guerra Cibernética. Actualmente radicado en Fort Meade, Maryland.
- 2010 – Irán : A finales de Septiembre de 2010, Irán también registró un ataque a las centrifugadoras del programa de enriquecimiento de uranio -programa nuclear iraní-. El troyano, virus o programa infiltrado recibió el nombre de Stuxnet. Irán acusó a Estados Unidos de su autoría.
- 2010: La primera guerrilla informática global: en defensa de WikiLeaks como respuesta a la Filtración de documentos diplomáticos de los Estados Unidos el 28 de noviembre de 2010 por el portal WikiLeaks, diversas autoridades y empresas de Estados Unidos y otros países boicotean a WikiLeaks, sus canales de financiación y su presencia en la red: EverDNS bloquea el dominio de internet, Amazon.com, el banco suizo PostFinance bloquea las donaciones,PayPal (de la compañía eBay) bloquea las donaciones, Mastercard y Visa (Tarjeta de crédito) bloquean cuentas y donaciones y Twitter y Facebook eliminan perfiles de Anonymous, el grupo visible defensor de WikiLeaks, autodenominado ciberactivista y que se consideran alejados de cualquier actividad relacionada con la Ciberguerra.
- 5 al 12 de noviembre de 2011: La compañía de seguridad Prolexic ha confirmado que el mayor ataque DDoS de 2011 ha tenido implicados a 250.000 ordenadores. el ataque estuvo dirigido a servidores de un compañía asiática de comercio electrónico, generando un tráfico de 45 Gbps con 15.000 conexiones por segundo, durante 7 días.
- El 6 de diciembre de 2011 en defensa de WikiLeaks, el grupo de Internet Anonymous lanza una Operation Payback contra PostFinance y PayPal por el bloqueo de las cuentas de WikiLeaks. El grupo colocó un vídeo en YouTube dirigido al gobierno de Estados Unidos explicando que la Operation Payback es contra la censura en Internet y el Copyright. WikiLeaks ha manifestado que no está ni a favor ni en contra de los ataques cibernéticos, pero ha afirmado que son la expresión de una parte de la opinión pública.

Materiales y métodos

Los Ataques de Denegación de Servicio pueden tener diferentes clasificaciones en dependencia de sus características, pero todos cumplen con un principio de funcionamiento básico y el objetivo a lograr al que nos referiremos a continuación.

Un ataque de denegación de servicio (DoS) es un ataque a un sistema de computadoras o infraestructura que causa que un servicio o recurso sea inaccesible por los usuarios legítimos (FERNANDES 2012). Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado. Cuando el servidor objetivo no es capaz de distinguir entre las peticiones realizadas por usuarios auténticos y las ficticias realizadas por los atacantes, esto provoca la sobrecarga del mismo y posteriormente el colapso, dejando así no disponible el servidor y por tanto los servicios que ofrece.

Una ampliación del ataque DoS es el llamado Ataque Distribuido de Denegación de Servicio, también llamado ataque DDoS el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión (COLÁS TURÉGANO 2016).

Enfoques actuales

En la actualidad se utilizan diferentes enfoques para contrarrestar este tipo de ataque, entre los principales y pudiera considerarse el más popular se destaca el Balanceo de Cargas. Una institución con la infraestructura de red y recursos computacionales necesarios, tales como un considerable ancho de banda y varios servidores, puede permitirse la implementación de un sistema de Balanceo de Cargas.

Balanceo de Cargas:

El Balanceo de Cargas se refiere básicamente a la acción de compartir el trabajo a realizar entre varios procesos, servidores, discos u otros recursos. Está estrechamente relacionado a los sistemas de multiprocesamiento y a los sistemas de procesamiento distribuidos. Para ello es necesario el uso de un sistema responsable del balanceo de las cargas y servidores (nodos) auxiliares dedicados a atender peticiones.

Novísimo Protocolo Most Knocking First Served (MKFS):

El artículo "*Playing Defense by Offense: Equilibrium in the DoS-attack Problem*" publicado por IEEE Computer Society de los autores A. Lukyanenkot, V. Mazalov, A. Gurtovt y 1. Falko se refiere a la implementación de un novísimo protocolo llamado MKFS. Está basado en estrategias de enfrentamiento a adversarios de la Teoría de Juegos y matemáticamente fundamentado. MKFS parte del principio de que los ataques DoS generan peticiones falsas, desde

direcciones IP generadas aleatoriamente. A diferencia del protocolo estándar que cumple una estrategia FCFS a partir de una estructura de datos FIFO, este protocolo separa las conexiones existentes en el sistema de las conexiones entrantes, y a partir del criterio "Most Knocking First Served", como cada dirección IP es diferente de la anterior, prácticamente es imposible que una dirección atacante pueda acceder a los servicios (COLÁS TURÉGANO 2016).

Inconvenientes

En el artículo "*Evaluating Network-Based DoS Attacks Under the Energy Consumption Perspective"* publicado por IEEE Computer Society de los autores Francesco Palmieri, Sergio Ricciardi y Ugo Fiore se hace referencia por primera vez a una nueva modalidad de ataque DoS (PALMIERI; 2011), esta vez orientados al aumento del consumo energético. Actualmente las Tecnologías de la Información demandan aproximadamente el 8% de la generación energética a nivel mundial y se prevee un crecimiento del 12% cada año. Una entidad con la infraestructura de comunicaciones y los recursos computacionales necesarios para soportar un ataque DoS prácticamente no se preocupará por evitarlos y estará así seriamente amenazada por ataques desde la perspectiva del consumo energético. El atacante haciendo a los servidores a trabajar constantemente intentando satisfacer las peticiones llevará el CPU, la memoria y demás componentes del sistema a modos de alto consumo, provocando así daños económicos considerables en dependencia de la magnitud del ataque y los recursos energéticos de la entidad atacada, así como daños ambientales por la emanación de gases contaminantes GHG.

Partiendo del conocimiento adquirido, la lectura y análisis de los referidos documentos y artículos se puede concluir en que la opción más viable para protegerse de ataques DoS, es precisamente evitarlos. No tratar de manejar la amenaza con Balanceo de Cargas u otros mecanismos existentes que pueden verse afectados desde ópticas tan novedosas como el aumento del consumo energético.

Resultados y discusión

Servidores Seguros

En el presente trabajo se propone una solución que sea capaz de evitar este tipo de ataques mediante la combinación efectiva de software profesional y un conjunto de configuraciones que permiten la implementación de servidores seguros contra ataques DDoS y otros tipos de ataques comunes. Todo el software a utilizar en el presente trabajo está disponible en el repositorio de Debian Squeeze (stable) y en versiones superiores. Para mejor acabado de este trabajo se tuvo en cuenta el cubrimiento de los principales Mecanismos de Defensa establecidos en Seguridad Informática:

- Preservación, Detección, Recuperación.

Preservación

En el artículo "Preventing of SYN Flood attack with iptables Firewall" publicado por IEEE Computer Society de los autores Sara Mirzaie, Alireza Karimi Elyato y DR.Mehdi Agha Sarram (MIRZAIE 2010) se hace referencia a la potencia de Iptables Firewall para la protección de sistemas, así como las ventajas que ofrece al permitir escribir reglas con fines específicos ganado en flexibilidad. Teniendo en cuenta su potencia, en el presente trabajo será la Preservación el principal mecanismo de defensa a utilizar.

Netfilter/Iptables Firewall v1.4.8-3: Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Iptables permite al administrador definir políticas de filtrado del tráfico que circula por la red, con cadenas y reglas almacenadas.

Una vez instalado se procede a la configuración de las reglas del mismo. A continuación se muestra un conjunto de reglas que permiten proteger el sistema servidor contra algunos de los principales tipos de ataques existentes:

```
#!/bin/bash
#
# Script de configuración del firewall Iptables
# camino: /etc/init.d/iptables
# version 0.06
# fecha 2012-03-10

### BEGIN INIT INFO
# Provides:          iptables
# Required-Start:    $all
# Required-Stop:     $remote_fs $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Iniciar el iptables al iniciar el sistema
# Description:       Habilita el firewall iptables.
### END INIT INFO

do_start () {
   # Borrar configuraciones
   iptables -F
   iptables -X

   # Política Restrictiva: Denegar por defecto entrada y permitir salida.
   iptables -P INPUT DROP
   iptables -P FORWARD DROP
   iptables -P OUTPUT ACCEPT

   # Recordar estado de conexión
   iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

   # Permitir conexiones locales desde interface Loopback
   iptables -A INPUT -i lo -j ACCEPT
```

```
### Configurar Puertos Específicos ###

#DNS
iptables -A INPUT -p UDP --dport 53 -j ACCEPT
iptables -A INPUT -p TCP --dport 53 -j ACCEPT

#SSH
iptables -A INPUT -p TCP --dport 22 -s 10.0.0.0/16 -j ACCEPT
iptables -A INPUT -p TCP --dport 22 -s 10.56.18.0/24 -j ACCEPT
iptables -A INPUT -p TCP --dport 22 -s 10.128.60.0/24 -j ACCEPT

#HTTP, HTTPS
iptables -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -A INPUT -p TCP --dport 443 -j ACCEPT
#iptables -A INPUT -p TCP --dport 8080 -j ACCEPT
#iptables -A INPUT -p TCP --dport 8090 -j ACCEPT

#FTP (Passive and non-Passive) (data port, control (command) port)
iptables -A INPUT -p TCP --dport 20:21 -j ACCEPT

#FTPS  (FTP Protocol over TLS/SSL) (data, control)
iptables -A INPUT -p TCP --dport 989:990 -j ACCEPT

#SMTP
iptables -A INPUT -p TCP --dport 25 -j ACCEPT

#POP3
iptables -A INPUT -p TCP --dport 110 -j ACCEPT

#IMAP
iptables -A INPUT -p TCP --dport 143 -j ACCEPT
iptables -A INPUT -p UDP --dport 143 -j ACCEPT

#PostgreSQL
iptables -A INPUT -p TCP -s 10.36.17.0/24 --dport 5432 -j ACCEPT

#MySQL
iptables -A INPUT -p TCP --dport 3306 -j ACCEPT

#Bacula
iptables -A INPUT -p tcp --dport 9101:9103 -j ACCEPT

#Webmin
iptables -A INPUT -p TCP --dport 10000 -j ACCEPT
iptables -A INPUT -p TCP --dport 5666 -s 10.128.60.0/24 -j ACCEPT

### Configuraciones Avanzadas ###

#Permitir solo un ping por segundo
iptables -A INPUT -p icmp --icmp-type 8 -m limit --limit 1/second -j ACCEPT

# Protección Anti-flooding o Inundación de tramas SYN.
iptables -N syn-flood
iptables -A INPUT -p tcp --syn -j syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
```

```
    # Evitar ataques de tipo Tiny Fragment Attack.
    iptables -A INPUT -f -m length --length 0:40 -j DROP

    # No responder broadcast.
    echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

    # Evitar ataques de Spoofing (para asegurar que el origen del paquete)
    for interface in /proc/sys/net/ipv4/conf/*/rp_filter; do
    echo "1" > ${interface}
    done

    # Deshabilitar la redirección del ping. Los ICMPs redirigidos pueden alterar la tabla de rutas.
    for interface in /proc/sys/net/ipv4/conf/*/accept_redirects; do
    echo "0" > ${interface}
    done

    # Asegurar, aunque no tenga soporte el núcleo, que no haya "Forward".
    echo "0" > /proc/sys/net/ipv4/ip_forward
}

do_stop () {
    iptables -F
    iptables -X
    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT
}

case "$1" in
  start)
    echo 'Starting iptables...'
    do_start
    ;;
  restart|reload|force-reload)
    do_stop
    do_start
    ;;
  stop)
    echo 'Stopping iptables.'
    do_stop
    ;;
  force-stop)
    echo 'Stopping iptables...'
    do_stop
    ;;
  status)
    iptables -L
    ;;
  fullstatus)
    iptables -L -n
    ;;
  *)
    echo "Usage: $0 start|stop|force-stop|restart|reload|status|fullstatus" >&2
    ;;
```

esac

exit 0

Detección

En el artículo "*Using Nagios to monitor faults in a self-healing environment* " publicado por IEEE Computer Society del autor Mikko A.T. Pervilä se evidencian las ventajas y potencia que ofrece Nagios como sistema de monitorización de recursos computacionales de hardware, software y servicios (ISSARIYAPAT 2012).

Nagios v3.2.1-2: Sistema de monitorización de redes de código abierto. Permite la monitorización de los recursos de sistemas de cómputo. Permite además la monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Snort v2.8.5.2-8: es el más antiguo y popular Sistema de Detección de Intrusiones de código abierto. Permite el Monitoreo constante de los servicios de Red y Logs se seguridad del sistema. Existen variantes de Snort para diferentes sistemas basados en Linux, así como una versión para Windows.

Tripwire v2.4.2-9: herramienta de seguridad destinado a chequear la integridad de ficheros. Es útil para monitorizar y alertar de cambios específicos en ficheros del sistema. Funciona cotejando los archivos y directorios con una base de datos de la ubicación y las fechas en que fueron modificados, además de otra serie de datos.

Recuperación

Bacula v2.4.2-9: herramienta de seguridad destinado a chequear la integridad de datos. Es útil para monitorizar y alertar de cambios específicos en ficheros. Funciona cotejando los archivos y directorios con una base de datos de la ubicación y las fechas en que fueron modificados, además de otra serie de datos.

Conclusiones

Los Ataques de Denegación de Servicio, sin importar su tipo son un problema cada vez más frecuente a enfrentar por las instituciones que ofrecen servicios en Internet. Dada la dificultad para proteger toda una infraestructura de comunicaciones, es imprescindible al menos garantizar la disponibilidad de los servicios que se ofrecen asegurando la protección del servidor donde han sido publicados.

Con la selección y combinación del software y con configuraciones adecuadas se puede proteger un servidor de un gran número de ataques, en particular de este tipo DDoS, sin que implique un gran coste económico para la institución atacada.

Referencias

COLÁS TURÉGANO, A. El delito de intrusismo informático tras la reforma del CP español de 2015 *Iuris Tantum Revista Boliviana de Derecho*, 2016: 210-228.

FERNANDES, J. P. T. A ciberguerra como nova dimensão dos conflitos do século xxi *Relações Internacionais (R:I)*, 2012: 53-69.

GUILLEN-PINTO, E. P.; L. RAMÍREZ-LÓPEZ, *et al.* Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles *Universidad y Salud*, 2017, 19: 280-292.

ISSARIYAPAT, C. Using Nagios as a groundwork for developing a better network monitoring system *2012 Proceedings of PICMET '12: Technology Management for Emerging Technologies*, 2012.

LOBATO, L. and K. M. KENKEL A Ciberguerra É Moderna! Uma Investigação sobre a Relação entre Tecnologia e Modernização na Guerra *Contexto Internacional*, 2015, 37: 629-660.

MAYER LUX, L. EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS *Revista chilena de derecho*, 2017, 44: 261-285.

MIRZAIE, S. Preventing of SYN Flood Attack with Iptables Firewall *Communication Software and Networks, 2010. ICCSN '10. Second International Conference on*, 2010.

MUÑOZ, M. and L. RIVAS Estado actual de equipos de respuesta a incidentes de seguridad informática *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 2015: 1-15.

PALMIERI;, F. Evaluating Network-Based DoS Attacks under the Energy Consumption Perspective: New Security Issues in the Coming Green ICT Area *2011 International Conference on Broadband and Wireless Computing, Communication and Applications*, 2011.

PÉREZ PATIÑO, A. L. and J. ROBLEDO VELÁSQUEZ Crecimiento de firmas entrantes tardías en la industria de software: un modelo desde la difusión multigeneracional de productos con efectos de red *Revista Facultad de Ingeniería Universidad de Antioquia*, 2012: 60-73.

RICO CARRILLO, M. Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos *Revista IUS*, 2013, 7: 207-222.

YEZERS´KA, L. *Los Cibermedios en Perú*, 2006. [Disponible en: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=81996106