Evaluación de ataques de Denegación de servicio DoS y DDoS, y mecanismos de protección

D. Narváez, C. Romero, M. Núñez
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército
manager571@hotmail.com, caromero@espe.edu.ec, mvnunezn@gmail.com

RESUMEN: Una de las grandes amenazas en seguridades informáticas son los potenciales ataques de denegación de servicio Dos y DDos. Ante este problema, el presente artículo propone la evaluación de las técnicas para la ejecución de ataques, basado en herramientas, además del desarrollo de una herramienta personalizada usando tecnología de múltiples hilos o multi-threads, aplicado en un escenario de pruebas reales. En consecuencia, se han implementado mecanismos de monitoreo ante este tipo de ataques, los cuales nos permitirán examinar el tráfico de red con el propósito de decidir que existe un ataque de denegación de servicio por parte de una o varias direcciones realizadas. Se han implementado las seguridades en base de software, específicamente mediante la implementación de políticas de filtrado de tipo IPTables, módulos extras en los servicios levantados que resultan más eficaces a la hora de proteger nuestra red de un posible ataque. Los resultados experimentales muestran que el nivel de eficacia de las protecciones aplicadas frente a este tipo de ataques; si bien es cierto, no serán 100% eficaces en todos los tipos de ataques actuales y probablemente menos los futuros; pero hoy por hoy, resultan ser herramientas de primera mano, conjuntamente con estrategias de seguridad adecuadas.

Palabras clave: Seguridades en Redes, ataques de denegación de servicio, mecanismos de monitoreo

SUMMARY: One of the great threats in computer science securities is the potential attacks of two refusal on watch and DDos. To carry owl this problem, the present article proposes the evaluation of the techniques for the execution of attacks, based on tools, besides the development of a customized tool using thread technology multiple or multi-threads, applied in a scene of real tests, consequently, monitoring mechanisms have been implemented before this type of attacks, which will allow us to examine the network traffic in order to decide that an attack of refusal on watch on the part of one exists or several realised directions. The securities on the basis of software have been implemented, specifically by means of the implementation of filtrate policies of IPTables type, extra modules in the raised services that are more effective at the time of protecting our network of a possible attack. The experimental results show that the level of effectiveness of the protections applied against this type of attacks; although it is certain, they will not be effective 100% in all the types of present attacks and probably except the futures; but at the present time, they turn out to be tools of first hand, jointly with suitable strategies of security.

Keywords: Network Security, Denial of service attacks,

1. INTRODUCCIÓN

El amplio desarrollo de manera exponencial que han venido teniendo las redes de comunicaciones y los sistemas de información actuales plantean inevitablemente la cuestión de su seguridad, que se ha convertido en un tema de preocupación creciente para la sociedad.

Un ataque de denegación de servicio se define como "una acción que priva o interrumpe parcial o totalmente tanto al sistema o a los usuarios, de los recursos requeridos para efectuar su normal funcionamiento" [1]. Por lo general, los ataques DoS son mecanismos que aprovechan la fuerza bruta con el propósito de "echar abajo" el sistema o convertirlo en indisponible o inutilizable, mediante una sobrecarga de la capacidad de procesamiento de paquetes y datos en sus servidores o de la pila de peticiones de la red. El primer tipo de ataque se denomina por vulnerabilidad y el segundo por inundación. Los ataques efectuados a servidores en muchas ocasiones pueden solucionarse aplicando las configuraciones y parches adecuados para limitar o incluso bloquear la excesiva carga del sistema en condiciones poco favorables [2]. Por ejemplo, los ataques mediante el envío de paquetes enmascarados o por difusión, son prácticamente imposibles de detener, a no ser que se desconecte el sistema de Internet. Puede ser que no "echen abajo" el sistema, pero seguramente se logrará saturar la conexión a Internet.

Frente a estos escenarios de pruebas se realiza los ataques a dispositivos como servidores Mandriva implementado servicios de Web (HTTP) Apache, correo (SMTP / POP / IMAP), DNS, FTP. El aporte que presenta este trabajo es darnos una mejor visión acerca de los niveles de seguridad que se deberían tener en cuenta al momento de implementar de los sistemas de información, ya que esta investigación abarca una buena cantidad de aspectos y conceptos de seguridad de redes relativamente nuevos, que además presentan una evolución constante en cuanto a sus contenidos y estrategias.

Sin embargo, es necesario recalcar, que actualmente no existe ningún sistema completamente inmune a todos los ataques de denegación de servicio, especialmente aquellos que se realizan de manera distribuida entre cientos, miles o quizás millones de equipos atacantes también víctimas de manera indirecta.

El resto del documento ha sido organizado de la siguiente manera: La sección 2 muestra los fundamentos de seguridades en las redes de comunicación. La sección 3 detalla el diseño e implementación de los ataques en un escenario real. La sección 4. La implementación y aplicación de una herramienta propia en Java e implementación de las protecciones frente a ataques DoS y DDoS. La sección 5 se evalúa las protecciones implementadas y los resultados experimentales. En la sección 6 se analiza trabajos relacionados y Finalmente en la sección 7, se presenta las conclusiones sobre los resultados obtenidos.

2. LOS ATAQUES DE DENEGACION DE SERVICIO Y LA SEGURIDAD

2.1. Políticas y modelos de seguridad

A las políticas de seguridad se las puede definir como explicitas cuando constituyen unas reglas bien documentadas, registradas y disponibles para su consulta por parte de un potencial ejecutor de la política[3]. Además, existirán las denominadas políticas implícitas, aquellas que establecen criterios que no están documentados pero que se asumen bien por su obviedad, o bien por costumbre. Para garantizar la implementación de los diferentes servicios de seguridad existen tres campos de trabajo que deben ser considerados: prevención, detección y respuesta.

2.2. Servicios básicos de la seguridad

Protege las comunicaciones ante determinadas violaciones de la política de seguridad ante los usuarios. Entre ellos se puede citar: **i)** "Servicio de autenticación o autentificación", garantiza que una entidad comunicante sea realmente quien dice ser; **ii)"**Servicio de confidencialidad de los datos", previene la divulgación no autorizada de los datos del sistema; **iii)**"Servicio de integridad de los datos", detecta

cualquier modificación, inserción, borrado o repetición de los datos, se puede tener integridad de conexión con recuperación, integridad de conexión sin recuperación, integridad de recuperación en campos selectos, integridad en modo no-conexión e integridad en modo no-conexión en campos selectos; **iv)**"Servicio de no repudio", no permite a un emisor negar haber enviado un mensaje, ni permite a un receptor el negar haber recibido un mensaje; **v)**"Servicio de control de acceso", es una protección contra el uso no autorizado del sistema; **vi)**"Servicio de privacidad", consigue que la identidad del elemento que realiza una determinada operación permanezca oculta ante algunos de los sistemas, actores o servicios presentes en dicha operación; **vii)**"Servicio de disponibilidad", se relaciona a la capacidad de la red, sistema o servicio para estar disponible en cualquier momento y para recuperarse con premura a partir de la ocurrencia de un evento de interrupción del mismo.

2.3. Clasificación y tipos de ataque

Se entiende como ataque a la seguridad o amenaza a una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad. Esta señal supone la existencia de un flujo o comunicación desde un origen o emisor de la información a un destino o receptor, utilizando un canal intermedio o una red de comunicación. En este contexto, es posible concebir cuatro categorías generales de ataques a la seguridad: **i)**" Ataques por Interrupción", Un elemento del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.; **ii)**" Ataques por Intercepción", Cuando una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad; **iii)**"Ataques por Modificación", Cuando una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de cambiarlo. Se produce así un ataque contra la integridad; **iv)**"Ataques por Falsificación (Phising)", Cuando una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

2.4. Métodos de defensa contra ataques de negación de servicio

Las maniobras de prevención tienen el propósito de intentar eliminar la posibilidad de que un ataque se realice antes de que este se lleve a cabo de manera real. Estos acercamientos permiten implantar cambios en los protocolos, aplicaciones y sistemas para robustecerlos contra los intentos de ataque. La prevención, referida a los ataques DoS, tiene como objetivo disminuir el riesgo de sufrir algunos de los ataques de vulnerabilidad, además de dificultar al atacante la tarea de conseguir una cantidad de agentes elevados y reduce las probabilidades de éxito del ataque. Pero, aunque la prevención juega un papel primordial para la seguridad, de ninguna manera elimina la amenaza que suponen los ataques de denegación de servicio. En el campo de la prevención de ataques DoS, se podrían clasificar las posibles medidas en cuatro grandes grupos: **i)**" Mecanismos de seguridad del sistema", son mecanismos que tratan de incrementar la seguridad global del sistema, mediante la defensa contra accesos ilegítimos, eliminando bugs en las aplicaciones, actualizando las implementaciones de los protocolos para evitar intrusiones y la utilización del sistema con fines delictivos; **ii)**" Mecanismos de seguridad en protocolos", Son aquellos que abordan el problema de un diseño defectuoso en los protocolos de comunicaciones; **iii)**" Mecanismos de supervisión de recursos", Son aquellos que controlan el acceso de cada usuario a los recursos, fundamentándose en los privilegios que posee dicho usuario y en su conducta; **iv)**" Mecanismos de multiplicación de recursos", Son aquellos que pretenden dotar de abundantes recursos a los sistemas para debilitar la amenaza que supone el agotamiento de los mismos por parte de un posible ataque DoS.

3. ESCENARIO DE PRUEBAS DE ATAQUES DoS.

El escenario fundamental sobre el cual se desarrollarán los ataques, está compuesto por una red de computadoras primaria, que en ciertos casos hará las veces de Internet (red externa); además, se dispondrá de una red interna, compuesta principalmente un Servidor de tipo Mandriva Linux. El mencionado equipo, trabajará implementado como servidor de Web (HTTP) Apache 2.2.1, correo (SMTP / POP / IMAP), DNS,

FTP, entre los servicios más importantes. La red sobre la que será implementado el escenario de pruebas, consiste en un red con topología en estrella de tipo fast-Ethernet con una velocidad de trabajo en modalidad auto negociada 10/100 Mbps. Se trata de una red cableada con dos enrutadores independientes, que servirán para separar igualmente dos redes que servirán para efectuar los ataques respectivos. Para efectuar los ataques externos se utilizará como medio principal, la primera red mencionada anteriormente. En cambio, para los ataques internos a nivel de la intranet, se usará una máquina conectada físicamente a la segunda red. Ya que ambas redes poseen un enrutador independiente para cada una; el enrutador de la primera red fungirá como si se tratase de un ISP, debido principalmente a que estará conectado directamente a Internet, haciendo de Gateway por defecto al enrutador de la segunda red. Finalmente, las dos redes se conectan a través de un switch 10/100 no administrable. Las principales razones por la que se decidió la implementación de este pequeño laboratorio de pruebas de ataques DoS fueron: Por un lado, la facilidad de efectuar cualquier tipo de ataques sin representar una amenaza real a un servicio o proveedor verdadero, ya que se trata de una experimentación con propósitos educativos, además de éticos. Por otro lado, el hecho de poder tener una disponibilidad directa e inmediata de los equipos, facilita enormemente su configuración, monitoreo, activación y desactivación de servicios, etc. Con este escenario se tiene un conocimiento más profundo del funcionamiento de los ataques como se ve en la Fig. 1.

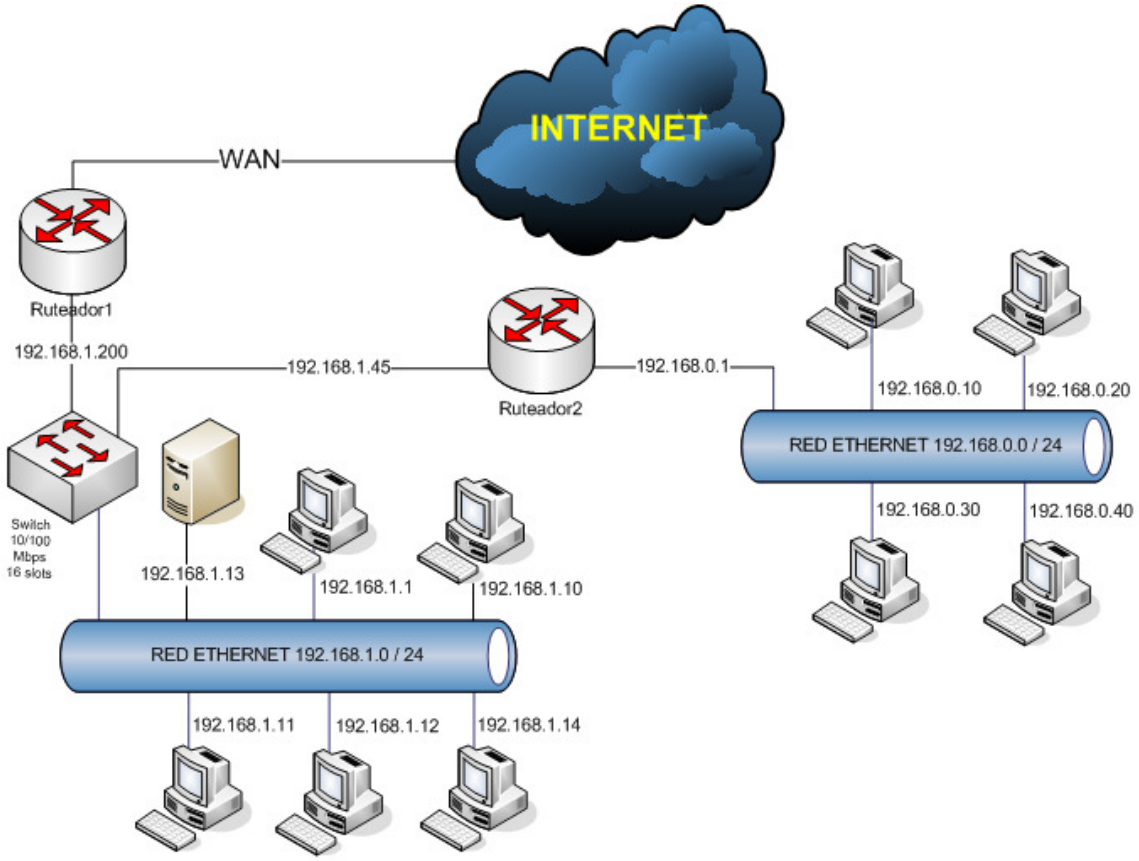

Figura 1:Diagrama del escenario de pruebas

Con el propósito de obtener un esquema de monitoreo del rendimiento inicial de nuestro servidor, se utilizó la herramienta de monitoreo de red Wireshark. La Fig. 2 muestra la captura de pantalla del rendimiento y el nivel de carga normal del servidor antes de efectuar los ataques. Se puede observar que el

pico promedio oscila en un valor cercano a 100 paquetes con tendencia a la baja, con una carga pico máxima de alrededor de 300 paquetes y una mínima de 50 paquetes.

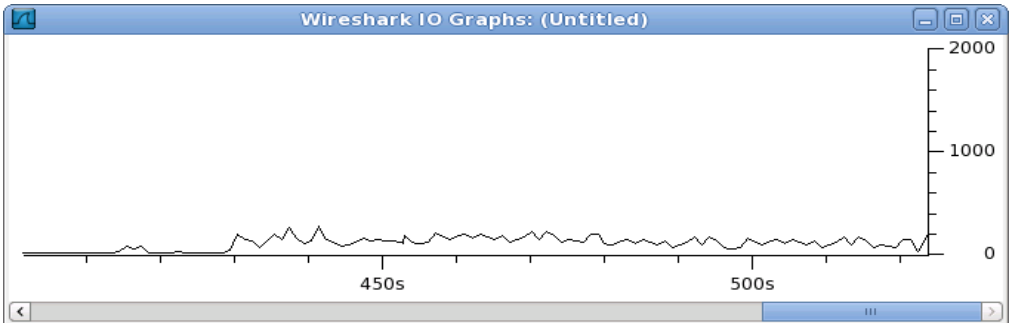

Figura 2. Captura de pantalla antes del ataque DoS y DDoS

3.1. Ejecución de los ataques con diferentes herramientas a diferentes servicios y protocolos.

En los tipos de ataques que se realizaron se utilizaron herramientas para los ataques de inundación y vulnerabilidad, para el ataque a través del protocolo ARP se realizó sin ninguna herramienta especializada, sino únicamente con el comando ARP, mediante la alteración de las tablas ARP. Este protocolo, se encarga de almacenar dentro de una caché interna, la lista de equivalencias MAC – IP de los diferentes equipos o hosts con quienes se ha comunicado. Este ataque está basado en modificar la tabla de traducción, a medida que se va estableciendo contacto con los hosts de la LAN específicamente con la Mac de la maquina atacada. Una vez que ya no se ha vuelto a establecer contacto con un determinado host, dentro de un tiempo prudencial, ARP automáticamente elimina el registro de su tabla de traducciones, con el propósito de dejar espacio a nuevas direcciones de otros hosts.

3.2. Ataque por Inundación HTTP (Flood)

Con el propósito de desarrollar un ataque más efectivo, se utilizo la herramienta [4] DoSHTTP v2.5.1 desde varias máquinas (DDoS), de tal manera que, se obtuvo una denegación de servicio de manera casi inmediata, ya que, por un lado el ancho de banda del objetivo fue inferior al ancho de banda de los atacantes, y por otro lado el ataque simultáneo de manera distribuida complico aún más la situación de la víctima. Una vez inicializado la herramienta en algunas máquinas atacantes, se ingresa la dirección correspondiente a la víctima, se escoge el agente de usuario o cliente Web que será visible en el momento de efectuar el ataque. Suministrada esta información, se especifica la cantidad de Sockets que abrirá nuestra herramienta, además que el envío de paquetes fue de manera continúa. La Fig. 3 muestra los componentes de la herramienta. Una vez configurado se procede a iniciar el ataque. Al acceder hacia el servidor HTTP de tipo Apache, la pagina Web de pruebas, ya no se encuentra disponible. Ya que el servicio fue saturado de peticiones, teniendo como resultado la demora del tiempo de respuesta del servicio (véase Fig. 3).

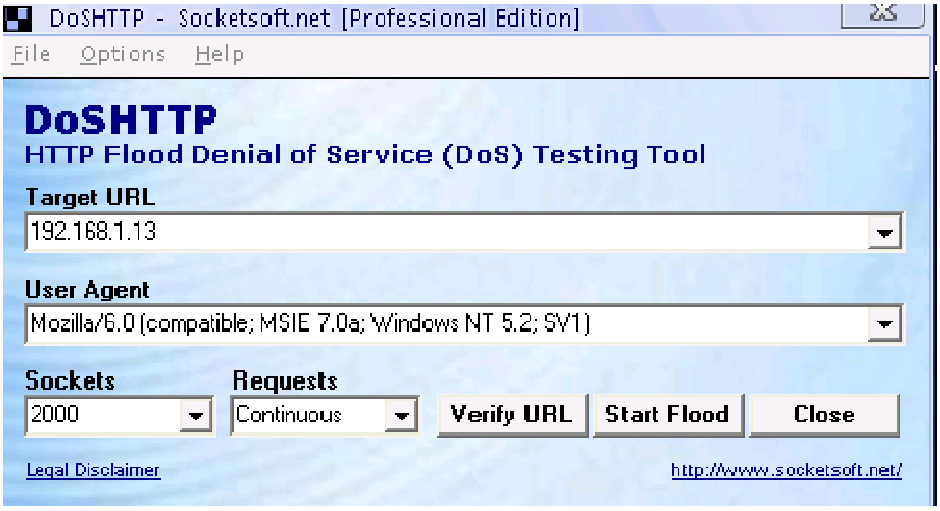

Figura 3. Inicializando la herramienta DoSHTTP

3.3. Ataque DoS por suplantación de direcciones con EtterCAP

Para efectuar este tipo de ataque, se utilizo una eficaz herramienta, que efectúa una inyección de paquetes de manera arbitraria hacia una máquina víctima, la misma que automáticamente alterará su tabla de direcciones ARP, capturando su tráfico mediante un ataque de tipo "Man in the Middle" o redirigiendo su tráfico a un punto muerto de una red o host no existente. Para que este ataque funcione se uso las herramientas: La conocida interfaz Winpcap 2.0, estándar de la industria para acceder a la conexión entre capas de red en entornos Windows y EtterCAP 0.7.3 para inyectar los paquetes. La Fig. 4 muestra los componentes y procedimiento para realizar el ataque.

En este ataque su nivel de efectividad fue muy elevado, pero también depende mucho del esquema de protección del que disponga el equipo o víctima a ser atacada. De hecho, este mismo tipo de ataque puede tener ciertas variantes o combinaciones dependiendo del tipo de resultado que se quiera obtener.

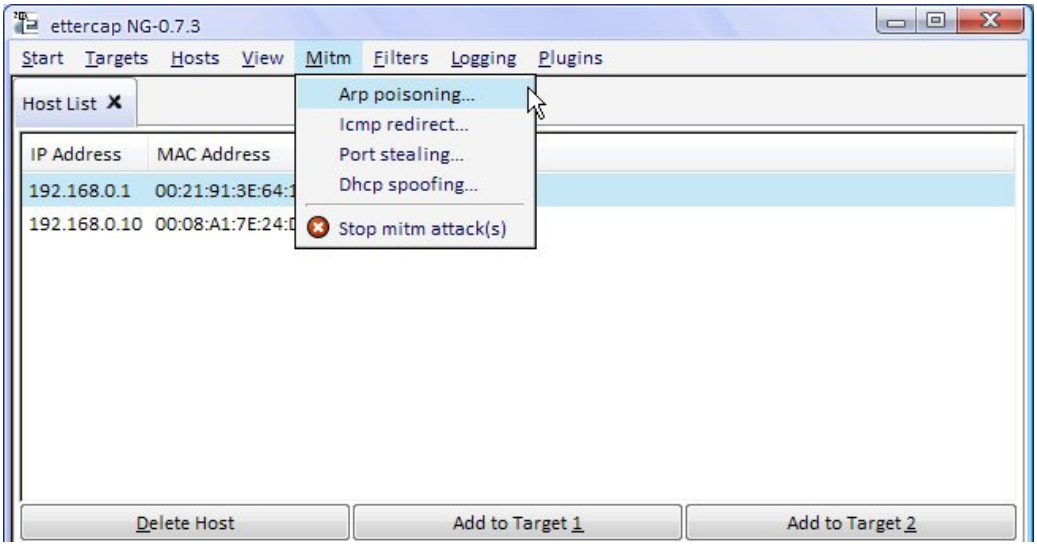

Figura 4. Iniciando el ataque MitM

3.4. *Ataques a DNS por medio de DNS Spoofing.*

Este ataque se realizo con el elementos DNS Spoofing, es un mecanismo muy poderoso de suplantación de un servidor de nombres de dominio; mediante esta característica se hizo pasar por un determinado host de Internet, y la víctima nunca se dio cuenta que en realidad está accedió a una dirección falsa forjada por la herramienta EtterCAP que trabajo con algunos plug-ins, que extiende ciertas funcionalidades del programa que normalmente no son posibles. Se suplanto una dirección específica apuntada en el servidor DNS legítimo. En este caso, se suplanto de manera temporal en la víctima la conexión de acceso hacia la página www.microsoft.com, de tal manera que se mostro otra página diferente en lugar de aquella, o también se puede realizar que aparezca bloqueada o fuera de servicio. En este tipo de ataque todo el resto de páginas no fueron afectadas, de tal manera que el usuario piensa que su conexión no ha sido intervenida de manera alguna, pasando de esta forma el ataque prácticamente desapercibido.

3.5. Ataques de redirección falseada del Servidor SMTP

Para lograr este ataque se manipulo el direccionamiento de los registros DNS impactando de esta manera las actividades normales, la productividad y por ende, la seguridad de las víctimas de este tipo de ataque. Utilizando el DNS Spoofing contra los registros hacia los cuales apuntan los servidores de correo electrónico de Google, atacando los puertos de una cuenta de gMail creada a propósito para esta tesis. Efectivamente, después de haber efectuado el ataque, el servidor SMTP de pruebas, apunto a una dirección no existente, por lo cual, el servidor de envío de mensajes gMail aparece como fuera de servicio o inaccesible; confirmándose de esta manera la denegación del servicio para la víctima del ataque.

3.6. Ataque a enrutador por medio de inundación

Para llevar a cabo este objetivo, se trabajo con dos herramientas, se utiliza Angry IP escanner v 2.2 como un eficaz escaneador de direcciones y puertos disponibles en nuestra red, podiendo observarla en la Fig. 5 donde nos despliega los puertos abiertos. Y una herramienta para ataques por inundación, llamada Server Attack. Se sometió a la red de pruebas al proceso de escaneo de puertos abiertos; excepto el caso del enrutador mismo que ha sido habilitado para redireccionar mediante NAT hacia una máquina ubicada dentro de la red local.

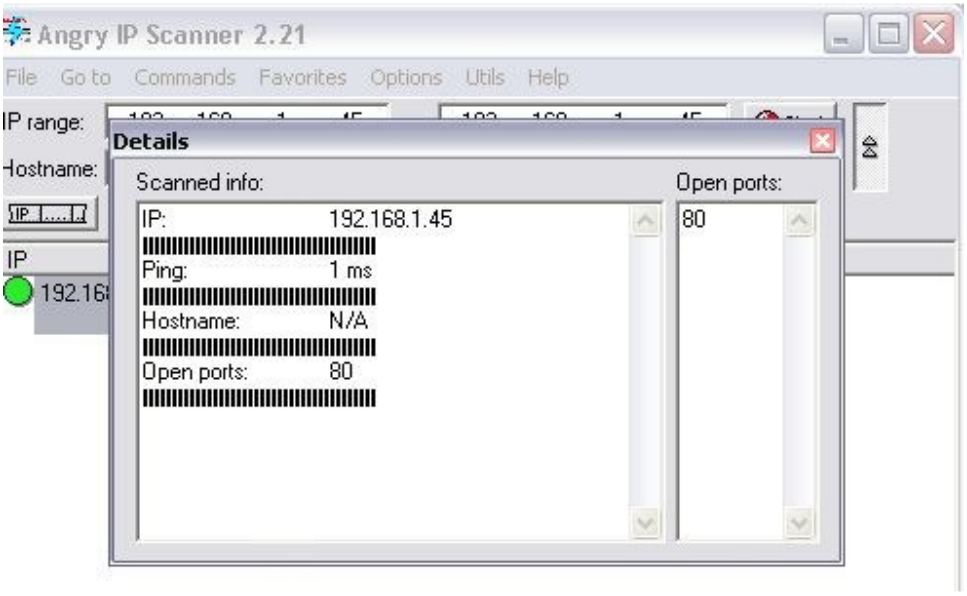

Figura 5. Escaneado de puertos con Angry IP

Dado que se conoce como se encuentra distribuida la red, se espero que el escaneador de puertos aparezca con el resultado. A continuación se ejecuto la aplicación Server Attack, con el cual, se realiza el ataque por inundación hacia el puerto abierto en el enrutador. Para tal efecto, se ingreso la dirección Ip como el puerto de la víctima que se ataco.

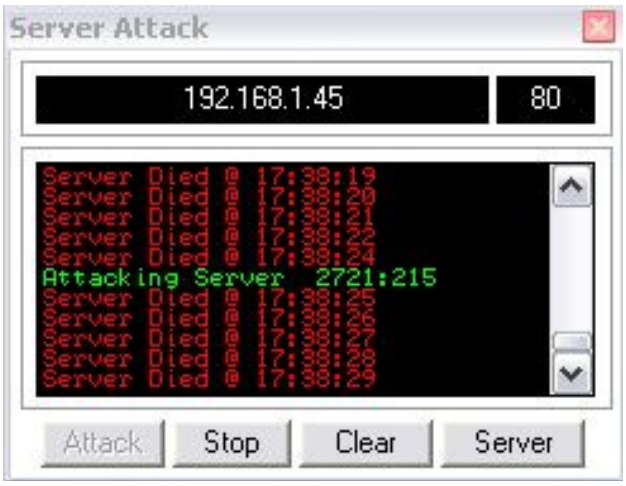

Figura 6. Ataque con la herramienta Server Attack

En la Fig. 6, se demuestra que el ataque se está llevando a cabo, se observa que aparecen unos mensajes de estado en color rojo; estos mensajes indican claramente que el ataque está siendo exitoso ya que no hay respuesta de parte del servidor, y por esa razón el log o bitácora de seguimiento de procesos aparece pintado de rojo, este ataque se desarrolla desde diferentes maquinas ejecutando algunos procesos en cada equipo atacante. Con el propósito de efectuar una verificación sobre el éxito del ataque, se procede a realizar un intento de acceso hacia el servidor y los resultados son negativos.

4. DISEÑO E IMPLEMENTACION DE UNA HERRAMIENTA Y SU APLICACION

La herramienta creada utiliza el Framework de desarrollo Java NetBeans IDE v 6.8 de Sun. El nombre del paquete de aplicación en cuanto se refiere a la clase base sobre la cual está definido este proyecto Java es URLFlooder. Adicionalmente, aprovecha la característica del trabajo con múltiples hilos o threads para efectuar su ataque de manera simultánea a medida que se procesan los Threads, dándole a la herramienta una capacidad de procesamiento paralelo, si se la ejecuta desde una máquina con 2 o más procesadores trabajando a la vez.

La interfaz de trabajo de la herramienta está compuesta por cinco campos de ingreso de datos, cuatro campos de visualización o resumen, un campo para controlar la duración de ataque en curso y tres botones que permitirán iniciar un ataque, detenerlo o cerrar la aplicación. Dentro del campo denominado URL o IP a atacar, se deberá ingresar la URL o dirección IP de la víctima a la que deseamos atacar, se tiene los campos para ingresar la cantidad de Threads (hilos) que se va a ejecutar, así como también la cantidad de Sockets por cada Thread que se ejecute, el indicador del número de puerto (por defecto 80), y finalmente, el tiempo de espera máximo permitido, mostrado en la Fig. 7.

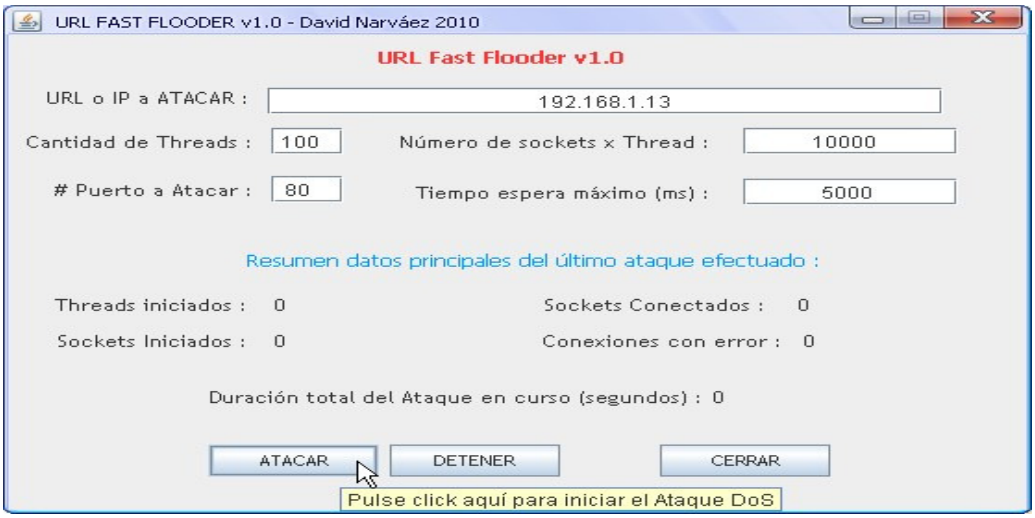

Figura 7. Ejecución de la herramienta Java

En el diagrama de secuencia que se muestra en la Fig. 8, se describen los eventos generados por los actores externos y su orden. El usuario ingresa los datos en el sistema y este envía la petición al servidor. El servidor envía los resultados y los despliega en pantalla al usuario (véase Fig. 8).

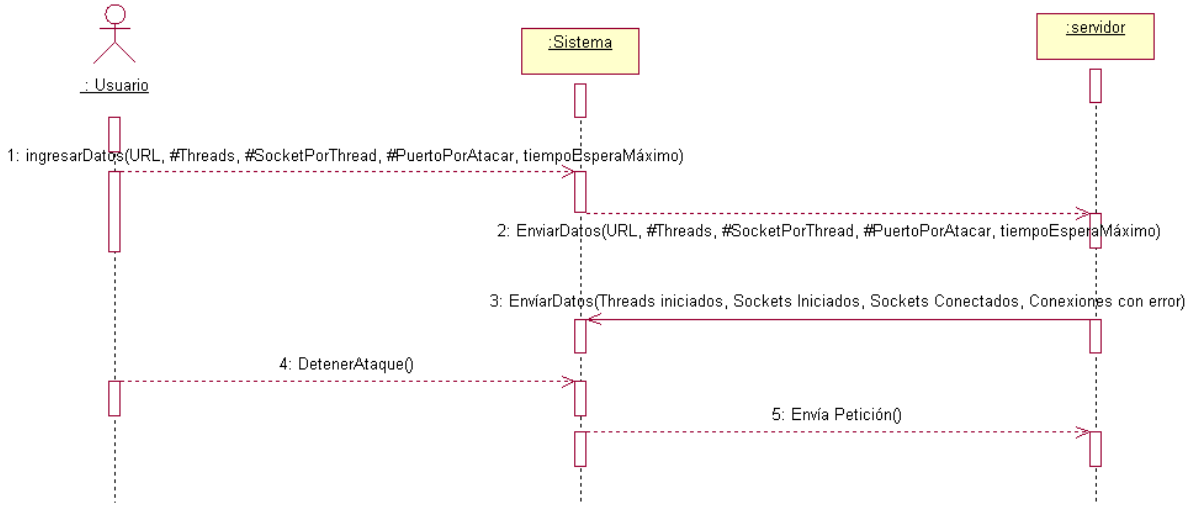

Figura 8. Diagrama de Secuencia de la herramienta

4.1. Implementación de Protección frente a ataques DoS y DDoS

Frente a estos ataques bien efectivos se optaron por mecanismos que se tiene dentro del servidor, es el firewall, con IPTABLES, que es el firewall más poderoso y difundido a nivel de servidores. Después de configurar del firewall con las reglas más adecuadas para establecer un nivel de seguridad óptimo para el servidor; se configura también las opciones inherentes a la distribución Linux sobre la cual se encuentra instalado y trabajando el Servidor de pruebas. Para lo cual, hay que dirigirse al centro de control principal de la interface Gnome instalada en este sistema, e ingresar a las opciones de seguridad correspondientes al servidor y configurarlas en niveles altos. Se limito los recursos utilizados por los usuarios en el sistema

como el uso de la memoria, la cantidad de procesos y sesiones concurrentes permitidos a éstos, incluso se limita las cuotas de espacio de disco disponibles para cada uno. Habilitar las entradas Proc y bloqueos de seguridad, básicamente corresponde a las opciones que se configuran mediante /proc/sys/net/ipv4, este set de entradas es un grupo de comandos para activar funcionalidades de seguridad que protegen al sistema contra varios tipos de ataques y vulnerabilidades conocidas; entre ellas el envenenamiento de ARP o la suplantación de direcciones y DNS basado en spoofing. Además de agregar seguridades extras como la instalación y configuración del módulo de Apache llamado MOD_EVASIVE, es una contribución desarrollada de manera independiente por Jonathan Zdziarski's[6]. Un científico e investigador que ha hecho este y otros aportes a la comunidad GNU. Además se activo algunos complementos que son paquetes de instalación RPM disponibles en la configuración de Mandriva Linux. Los paquetes, corresponden explícitamente a apache_devel y glibc_devel, los mismos que son requeridos obligatoriamente para poder compilar el archivo fuente suministrado por el creador de mod_evasive. Por último, y para dar por finalizado el proceso de aseguramiento del servidor de pruebas, se efectuó una protección extra hacia los ataques DNS Spoofing, activando la configuración que dentro del archivo de control al servidor DNS.

5. EVALUACION DE RESULTADOS

Con la implementación de políticas de filtrado de tipo IPTables configuradas, y módulos extras en los servicios levantados se volvió a realizar todos los ataques. Por lo cual, en todos los intentos de ataque, la configuración aplicada a MOD_EVASIVE, procedió a limitar la carga de la misma página hasta un máximo permitido de 2 veces por segundo. De sobrepasarse ese intervalo de tiempo, MOD_EVASIVE procedió a bloquear todos los paquetes cuyo origen sea el host que está sobrecargando las peticiones y que estén destinados al puerto 80 (http) del servidor. El equipo sospechoso de ser un atacante, ingresa automáticamente a la lista negra de MOD_EVASIVE por un intervalo de 10 minutos. Una vez transcurrido el período de cuarentena de un host puesto en lista negra, vuelve a permitir acceso nuevamente; En el caso de que el equipo atacante volviese a reincidir en la sobrecarga de paquetes, volverá a estar bloqueado de nuevo, hasta un máximo de 10 bloqueos sucesivos; posterior a lo cual, será bloqueado del servidor. Paralelamente al mecanismo de bloqueo, MOD_EVASIVE envia un e-mail de advertencia al administrador del servidor, con el propósito de informarlo acerca de las direcciones que fueron bloqueadas de los posibles atacantes, ya que probablemente se tratase de un ataque DDoS. Realizando una evaluación entre la activación de MOD_EVASIVE, se desprenden las siguientes diferencias:

En la Fig. 9 donde MOD_EVASIVE no está activo; el pico promedio oscila en un valor cercano a 800 paquetes / segundo, con una carga pico máxima de alrededor de 1500 paquetes / segundo y una mínima de 100 paquetes / segundo. En este ataque se registró el contingente de algunas máquinas atacantes.

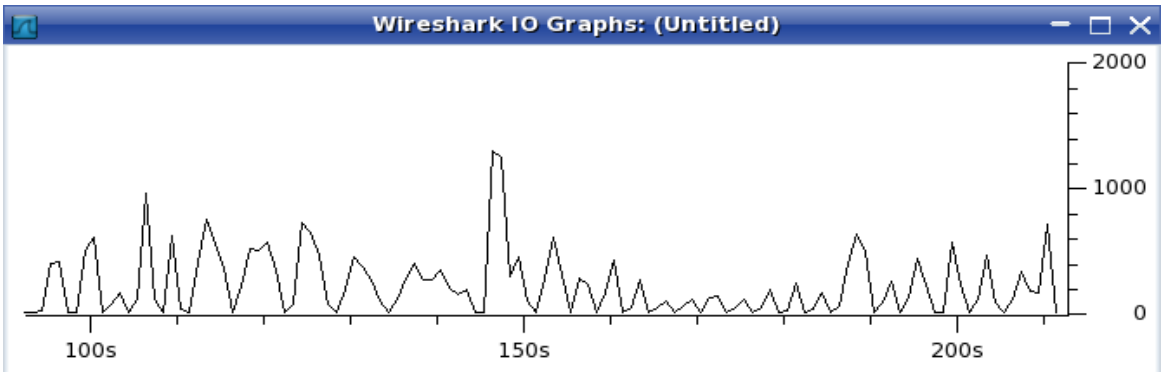

Figura 9. Ataque al Servidor Apache sin MOD_EVASIVE

En la Fig. 10 donde MOD_EVASIVE si está activo; se observa que el pico promedio oscila en un valor cercano a 250 paquetes/segundo con tendencia a la baja, con una carga pico máxima de alrededor de 550 paquetes/segundo y una mínima de 100 paquetes/segundo. En este ataque se registró igualmente el contingente de algunas máquinas atacantes.

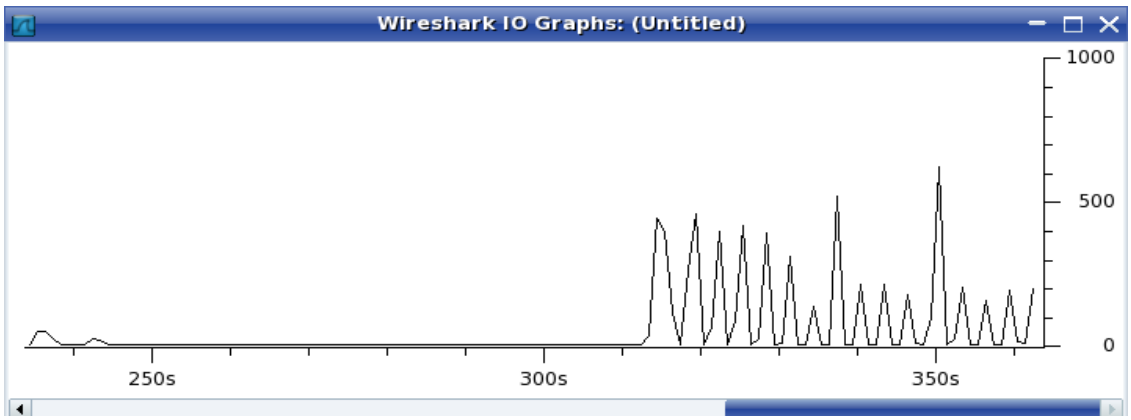

Figura 10. Ataque al Servidor Apache con MOD_EVASIVE activo

En efecto MOD_EVASIVE resultó eficaz para frenar los paquetes atacantes, reduciendo prácticamente en un 80% el nivel de carga del servidor mostrado en la Fig. 11, debido principalmente al bloqueo de los atacantes en base a la restricción de la cantidad de peticiones permitidas a un mismo host por segundo.

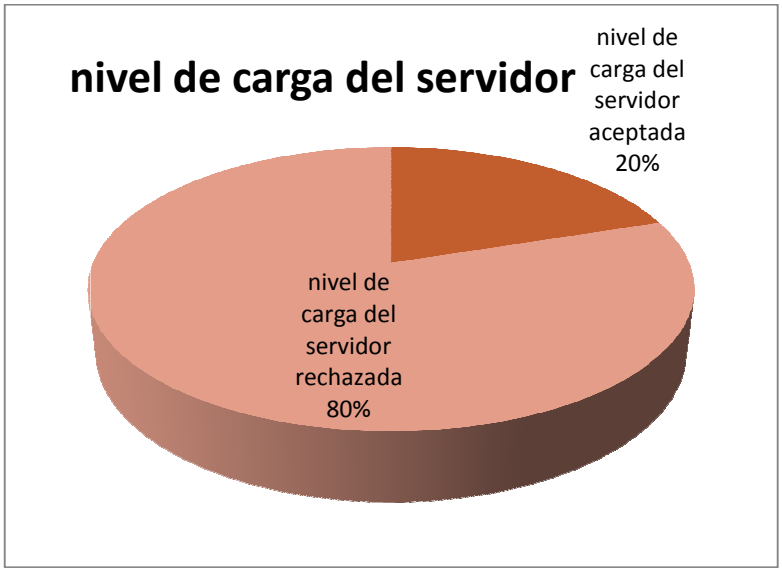

Figura 11. Conexiones rechazadas por MOD_EVASIVE

Se comprueba el nivel de eficacia de las protecciones aplicadas a nivel del servidor frente a este tipo de ataques; si bien es cierto, no serán 100% eficaces en todos los tipos de ataques actuales y probablemente menos los futuros; pero hoy por hoy, resultan ser herramientas de primera mano, conjuntamente con estrategias de seguridad adecuadas como análisis y monitoreo periódico del tráfico de red, mantenimiento, actualización de servicios y parches, respaldo de datos sensibles, protección de antivirus, malware y rootkits, entre otras.

6. TRABAJOS REALACIONADOS

Aunque exista una diversidad de trabajos relacionados, en esta sección se han incluido los más relevantes, que se han encontrado durante la investigación:

En lo que se refiere al tema de seguridad y ataques de DoS en redes IPv6, el trabajo presentado en [7] describe que el tráfico IPv6 está empezando a ser notable y la tendencia irá en aumento a medida que los operadores y proveedores de contenidos lo implementen en sus redes y servicios. IPv6 no es más inseguro que su predecesor IPv4, todo lo contrario. Sin embargo como cualquier otra tecnología, IPv6 ofrece la posibilidad de que gente maliciosa idee diversas formas de sacarle partido para realizar actividades fraudulentas. En lo que se refiere a métodos planteado por RR. Talpade [8] que consiste en el planteo de un sistema escalable de monitorización NOMAD, el cual, detecta los absurdos realizando un análisis estadístico de la información contenida en las cabeceras IP. Se puede utilizar para detectar anomalías en una red local, pero no nos permite clasificar el tráfico agregado que venga procedente de diferentes fuentes. Por los resultados obtenidos, se puede deducir que, como el método no reconoció en base a la información en las cabeceras de otras redes, podría no ser muy efectivo, en razón de que los ataques por inundación saben cómo saturar el ancho de banda.

Respecto a investigaciones basadas en técnicas de minería de datos (data minning) planteada por Stolfo [9], que revela los patrones en las características de un sistema que evaluara el comportamiento de los programas y los usuarios. Mediante aquello, se creó un clasificador que reconoció anomalías e intrusiones. Este procedimiento utiliza como información base a las variables o parámetros medidos en el propio sistema y no en los paquetes de información que viajan por la red. Con el propósito de mejorar esta técnica se utilizan los resultados provenientes de múltiples modelos para corregir la detección. Esta es una investigación a gran escala y aporto mucho para mi tesis ya que realiza las pruebas en escenarios reales. Respecto a investigaciones basadas detección de estructura de ataques de red, hicieron la formulación de que una estructura de datos heurística [10] recopila información fundamentándose en las direcciones IP de origen o destino. Cada elemento de una red recopila información estadística en una estructura de tipo multinivel, de tal forma que únicamente cuando una dirección o rango de direcciones supera un cierto nivel de tasa de tráfico dado se inician a compilar datos con mayor nivel de detalle. Es así que este sistema permite detectar el origen del ataque y a su vez las máquinas víctimas de un ataque. Una de sus desventajas es que requiere la reconfiguración de los encaminadores, mucha memoria y que no es capaz de detectar ataques con spoofing aleatorio generado por una sola fuente, o por un número lo suficientemente elevado de agentes, en nuestro proyecto el MOD_EVASIVE realiza el mismo trabajo sin usar tantos recursos. Para finalizar se recalca que todas las herramientas usadas fueron evaluados con algunos prototipos existentes, pero la gran diferencia fue la funcionalidad y eficacia para ejecutar los ataques, son herramientas súper básicas en su programación aprovecha la característica del trabajo con múltiples hilos para efectuar su ataque.

7. CONCLUSIONES Y TRABAJO FUTURO

En este artículo, se ha presentado la metodología general a seguir para la ejecución del ataque, ilustrando las implicaciones que ello conlleva, tanto en el lado del servidor atacado como en el del atacante. Con la aplicación creada, se ha probado y evaluado la alta capacidad y eficiencia obtenida por estos ataques, como se ha demostrado a través de la experimentación aportada en el trabajo. Para ello, una vez desarrollada las soluciones prácticas que posibilita dicha ejecución, se han propuesto mejoras a la misma y se ha comprobado el beneficio de sus efectos para el escenario de pruebas atacado.

Como trabajo futuro se podría evaluar los ataques en tráfico IPv6. Por tanto IPv6 sólo representa un nuevo canal por el que se podrían aprovechar vulnerabilidades de equipos, aplicaciones y también la seguridad en la Web 2.0.

Referencias Bibliográficas

[1] Macías Fernández Gabriel, "Ataques de denegación de servicio a baja tasa contra servidores". Tesis Doctoral Universidad de Granada ,2007. Pp(s): 115 – 139.

[2] Mieres Jorge, "Buenas prácticas en seguridad informática". Analista ESET La, [online:], abril 2010. http://www.eset-la.com/press/informe/buenas_practicas_seguridad_informatica.pdf.

[3] Limón Martínez Fernando, "Sistemas Distribuidos de Denegación de Servicio". Madrid, Junio de 2000, [online:] http://fi.upm.es/~flimon

[4] Web de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), [online,]http://www.enisa.europa.eu/, varios temas consultados

[5] Modelo de Clases , Objetos y Secuencia, [online:]http://www.dcc.uchile.cl/~psalinas/uml/modelo.html

[6] Jonathan Zdziarski's, "mod_evasive", [online:]http://www.zdziarski.com

[7] Miguel Angel Díaz Fernández, Cesar Olvera y Álvaro Vives, "Seguridades y ataques de DoS en redes IPv6". XII Congreso iberoamericano de Internet, telecomunicaciones y sociedad de la información, octubre 2009.

[8] Talpade R.R. Kim. S Khurana, "Simposium IEEE. Computers and Comm.",Pp(s): 324 – 335, 2006 [online] http://portal.acm.org/citation.cfm?id=1100973

[9] J. Stolfo Salvatore, Lee Wenke, Chan Philip K., Wei Fan, Eleazar Eskin. "Data mining-based intrusion detectors: an overview of the columbia IDS project". ACM Portal, December 2007, [online], http://www.cc.gatech.edu/~wenke/publications.html

[10] Thomer M. Gil y Massimiliano Poletto," MULTOPS" Simposium de Redes y Sistemas Distribuídos, November 2006 [online:] http://portal.acm.org/citation.cfm?id=1179542.1179557&coll=GUIDE&dl=GUIDE&CFID=93496650&CFTOKEN=73142641