INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY
CAMPUS ESTADO DE MÉXICO

160644

"ESTUDIO DE ATAQUES DE NEGACION DE SERVICIO"

TESIS QUE PARA OPTAR EL GRADO DE
MAESTRO EN CIENCIAS DE LA COMPUTACIÓN
PRESENTA

ARMANDO VALERA PAULINO

Asesor: Dr. JOSÉ DE JESÚS VÁZQUEZ GÓMEZ

Comité de tesis: Dr. ROBERTO GÓMEZ CÁRDENAS
Dr. LUIS ANGEL TREJO RODRÍGUEZ

Jurado:	Dr. ROBERTO GÓMEZ CÁRDENAS	Presidente
	Dr. LUIS ANGEL TREJO RODRÍGUEZ	Secretario
	Dr. JOSÉ DE JESÚS VÁZQUEZ GÓMEZ	Vocal

Atizapán de Zaragoza, Edo. Méx., Marzo del 2002.

RESUMEN

Desde que apareció Internet siempre se han presentando muchos tipos de ataques tales como: worms, sniffers, falsificación, usurpación, paquetes mal formados, etc. Entre estos figuran los ataques de negación de servicio, los cuales tienen como fin dejar fuera de servicio a los sistemas de la red, logrando que los usuarios no puedan acceder a los servicios o recursos que ofrece el sistema, estos ataques son normalmente rápidos y fáciles de generar, los cuales se aprovechan de errores, limitaciones o inconsistencias del protocolo TCP/IP, sistemas operativos, programas o aplicaciones. El principal problema que se tiene es que el protocolo TCP/IP V4 tiene poca seguridad por naturaleza, y los ataques aprovechan estas circunstancias, por lo que luchar en contra de este tipo de ataques no es una tarea sencilla. Dichos ataques son cada día más sofisticados y peligrosos, específicamente el ataque distribuido de negación de servicio mejor conocido como DDOS por sus siglas en inglés (Distribuited Denial of Service), ha sido el más importante en su tipo, este es muy devastador contra su objetivo ya que cientos de máquinas de manera coordinada atacan al mismo tiempo al objetivo.

El ataque DDOS se hizo muy popular en la segunda semana de febrero del 2000, cuando atacó a las principales páginas web que mueven miles de millones de dólares de la industria cibernética (Yahoo, CNN, eBay, Buy, Amazon, ZDNet, eTrade). Según las estadísticas, el rendimiento de Internet se vio reducido en un 26.8% por los ataques DDOS de esa semana, con respecto a la semana anterior, causando además pérdidas económicas considerables. Como el comercio electrónico continuará siendo una parte importante de la economía global, (se prevé que dentro de pocos años, el 20% o 30% de las transacciones comerciales se realizarán a través de Internet), los ataques DDOS tendrán un mayor impacto sobre nuestra sociedad electrónica.

Los ataques DDOS son una constante en Internet, y han aparecido nuevas herramientas y mutaciones para realizarlos. Las respuestas no se han hecho esperar, las compañías y los gobiernos han estado invirtiendo una gran cantidad de recursos para luchar contra estos ataques, en todos los caminos posibles: técnicamente, instalando dispositivos de seguridad; organizacionalmente, contratando a personal especializado en seguridad, y legalmente los gobiernos modificando sus leyes para sancionar severamente a los culpables.

El presente trabajo tiene dos grandes objetivos.

- Primero es proporcionar una guía básica de referencia para defenderse contra los ataques más comunes de negación de servicio, incluyendo el ataque DDOS, esto mediante las recomendaciones y mecanismos que han aportado o utilizado las compañías, gobiernos, grupos y expertos de seguridad.
- Segundo se propone un esquema de protección general para defenderse de los ataques DDOS, con el objetivo de detener los ataques de manera automática, integrando la tecnología que se tiene para defenderse y proponiendo nuevos mecanismos a implementarse para fortalecer la seguridad en Internet. Cabe aclarar que esta propuesta por el momento es un tan sólo un buen deseo, pues muchos de los elementos que la componen no pueden ser materializados; sin embargo, estamos confiados en que un esfuerzo y cooperación de la magnitud planteada es la única forma de limitar este tipo de ataques.

CONTENIDO

GLOSARIO

Abuso.- Comportamiento prohibido o no autorizado.

Administrador.- Una persona encargada de controlar una red.

Algoritmo.- Un algoritmo es una operación matemática que realiza algunos propósitos útiles. Este propósito podría ser superficial, como mostrar páginas web cuando se interpretan, o más critico, como la encriptación y desencriptación de datos sensibles.

Ataque.- Es la actividad cuyo objetivo es causar daño a un sistema, robar información del mismo, o utilizar sus recursos de forma no autorizada.

Amenaza. Es un posible peligro para el sistema; el peligro puede ser una persona (un craker o espía), una cosa (una pieza defectuosa del equipo), o un evento (fuego o inundación) que puede convertirse en una vulnerabilidad del sistema.

Auditoria de Seguridad. Un examen (frecuentemente de terceros) de los controles de seguridad de una organización y mecanismos de recuperación de desastres. El propósito de dicho examen es asegurarse de si actualmente se están utilizando las mejores prácticas. También puede ser una comprobación proactiva de sus controles de seguridad y de su habilidad para sobrevivir, grabar, seguir la pista, analizar e informar de ataques de red.

Autentificación. El proceso de autentificar a un usuario o a un host. Dicha autentificación puede ser sencilla y aplicada en el nivel de aplicación (como puede ser una contraseña) o puede ser compleja (como diálogos de respuesta-desafío entre máquinas que se basan en algoritmos o encriptación en un nivel del sistema discreto).

Autentificador. Cualquier medio por el cual se pueda autentificar a un usuario, nodo o proceso.

Autentificar. Cuando autentifica un usuario o host en particular, está verificando su identidad, su nivel de acceso o ambos.

Autoridad de Certificados.- Una tercera parte de confianza que expide certificados de seguridad y verifica su autenticidad. Probablemente, la autoridad de certificados comerciales más conocida es VeriSign.

Autorización. Los derechos de un usuario para acceder a objetos o recursos.

Buffer Overflow. (*Desboradamiento de Segmento de Memoria).* Tomar ventaja de errores inherentes a una parte específica del código de una aplicación para colocar comandos arbitrarios en la cola de ejecución de procesos.

Bugs *Un bicho*, (Bug) es cualquier error introducido accidentalmente en un programa. Estos errores se vuelven un problema cuando los programas afectados son de vital importancia para el funcionamiento del sistema, por ejemplo: Sistemas Operativos, Protocolo de comunicación, etc.

CERT. El equipo de respuestas para emergencias informáticas (*The Computer Emergency Response Team*), una organización de seguridad que ayuda a las víctimas de ataques.

Certificado Digital. Un documento digital que verifica y garantiza que se ha asignado a una entidad o persona en particular una clave criptográfica particular (normalmente una clave pública).Archivo que contiene información sobre la identidad de una persona, empresa o sistema.

Ciberespacio Conjunto de seres humanos interconectados a través de computadoras y redes de telecomunicaciones sin importar la geografía física.

Cliente. Máquinas o computadoras que realizan la función de solicitar información a un servidor bajo la relación cliente/servidor. Software diseñado para interactuar con una aplicación específica. Por ejemplo, los navegadores WWW como Netscape Communicator e Internet Explorer son clientes WWW. Están específicamente diseñados para interactuar con la Web o con servidores HTTP.

Checksum Conteo de número de bits en una unidad de transmisión utilizada para verificar que el número de bits recibidos sea el mismo que el número de bits enviados.

Contramedidas. Se refiere a las diversas técnicas para proteger los sistemas.

Cracker. Individuo que conoce los detalles de los sistemas y aprovecha las fallas que tengan para causar daños a los mismos.

CRC. CRC es una comprobación de Redundancia Cíclica (*Ciclic Redundancy Check*), una operación utilizada comúnmente para verificar la integridad de los datos.

Criptografía. La criptografía es la ciencia de la escritura secreta. En criptografía, el objetivo principal es codificar sus escritos de manera que no sean legibles para el personal no autorizado. Sólo los usuarios autorizados pueden descifrar un mensaje encriptado.

DDOS *(Distributed Denial of Service).* Ataques de negación de servicio distribuidos. En lugar de una sola computadora, se utilizan cientos o hasta miles de ellas, todas actuando al mismo tiempo contra una misma víctima, un servidor o cualquier computadora conectada a Internet, la que recibe una sucesión de solicitudes de servicio, con tal frecuencia y cantidad, que al no poder ser respondidas van disminuyendo paulatinamente su rendimiento, ocasionando casi siempre la caída del sistema, además de la saturación del ancho de banda asignado.

DES *Data Encription Standard.* Estándar de encripción de criptografía de llave privada

Demonio *(Daemon).* Un demonio es un proceso que se ejecuta en segundo plano, efectuando una función y sin estar ligado a una terminal, tales procesos son espíritus amigables más que demonios maléficos. Por ello la traducción a demonio no es del todo adecuada, lo podemos comprender mejor como un programa residente. Es un termino UNIX, aunque muchos otros sistemas lo soportan, incluso Windows, pero con otros nombres.

Detección de Intrusiones. La práctica de utilizar sistemas automáticos para detectar intentos de intrusión. La detección de intrusiones normalmente implica sistemas o agentes inteligentes.

Dirección IP. Dirección numérica en Internet, como 132.254.8.30

DNS. Sistema de nombres de dominio (Domain Name System). Un sistema de trabajo en red que transforma direcciones IP numéricas (132.254.8.30) en nombres de hosts de Internet (www.cem.itesm.mx), y viceversa.

DOS *(Denial of Service).* Se refiere a los ataques de negación de servicios, una condición que ocurre cuando un usuario provoca maliciosamente que un servidor de información de Internet quede inoperativo, negando el servicio de computadora a los usuarios legítimos.

Eavesdropping Escuchas

Encripción. El proceso de mezclar los datos de forma que sean ilegibles para las personas no autorizadas. En muchos sistemas de encriptación se debe tener una contraseña para volver a ensamblar los datos en un formato legible. La encriptación se utiliza principalmente para mejorar la privacidad o proteger la información sensible, confidencial, privilegiada, clasificada, secreta o de máximo secreto.

Ethernet. Una tecnología de trabajo en red de área local (Local Area Network), originalmente desarrollada por Xerox, que conecta computadoras y transmite datos entre ellas. Los datos se empaquetan en estructuras y se envían por cables.

Extranet Red privada que utiliza los protocolos de Internet y los sistemas de telecomunicaciones públicos para compartir de forma segura, información de negocios y operaciones entre diversas empresas.

Filtrado. El proceso de examinar los paquetes de red para conseguir integridad y seguridad. El filtrado es normalmente un proceso automatizado realizado por ruteadores o software.

Firewall. En general, cualquier unidad que evite que usuarios no autorizados consigan acceso a un host en particular. Con más precisión, una unidad que comprueba la dirección de origen de cada paquete. Si esa dirección está en una lista aprobada, el paquete consigue entrar. Si no, se rechaza.

FTP *(File Transfer Protocol).* Protocolo de transferencia de archivos entre computadoras a través de Internet.

Guerra Cibernética *(Ciberwar).* Se refiere a la guerra de información activa que se lleva a cabo en Internet. Se refiere a la práctica de atacar a un enemigo, con el fin de recoger, procesar, manipular e interpretar comunicaciones e información vital.

Gusanos *(Worms).* Un gusano es un programa que se propaga copiándose a sí mismo en cada host de la red: su propósito es accesar ilegalmente sistemas.

Hacker. Persona que disfruta explorando de los detalles de los sistemas y como obtener el máximo de su capacidad, opuesto a la mayoría de los usuarios que prefieren aprender lo mínimo necesario.

Hash Función unaria que es utilizada para mapear un argumento a un resultado de un tamaño predeterminado.

Host. Una computadora con una dirección de hardware permanente, especialmente en una red TCP/IP.

HTML *HyperText Markup Language.* Conjunto de símbolos y marcas que permiten consultar información en el WWW a través de un navegador como Netscape o Internet Explorer

Incidente. Un evento que pone en riesgo la seguridad de un sistema de cómputo.

Internet Sistema de computadoras conectadas en red pública en todo el mundo. En general, el conjunto de redes informáticas conectadas al sistema telefónico internacional de paquetes conmutados que soporta TCP/IP. Más específicamente, cualquier red informática que soporte TCP/IP y esté interconectada.

Internet II Proyecto de universidades y empresas de EU para el desarrollo de redes y aplicaciones avanzadas para la enseñanza e investigación.

Intranet. Red privada basada en las tecnologías y protocolos de Internet

Intrusión. Una intrusión es una secuencia de acciones realizadas por un adversario malicioso que resulta en una ocurrencia de amenazas de seguridad hacia un equipo o red de cómputo.

IRC *Inter Relay Chat*

Llave privada Llave mantenida en secreto y otorgada por una autoridad certificadora que permite junto con la llave pública realizar operaciones de encripción y decripción.

Llave pública Llave otorgada por una autoridad certificadora la cual se distribuye a las personas que requieran enviar un mensaje, que permite junto con la llave privada realizar operaciones de encripción y decripción.

Negación de Servicio. Una condición que resulta cuando un usuario, maliciosamente, hace que un servidor de información de Internet resulte inoperable, negando así el servicio a usuarios legítimos.

NFS. Sistema de archivos de red (*Network File System*), un sistema que nos permite importar archivos de forma transparente desde hosts remotos. Estos archivos aparecen y actúan como fueron instalados en su máquina local.

Newsgroups Grupos de noticias Discusión de temas específicos a través de comentarios escritos a un servidor de Internet central.

Paquetes. Los datos que se envían a través de la red se parten en porciones manejables llamadas paquetes. El tamaño se determina según el protocolo utilizado.

Pila de Protocolo. Una jerarquía de protocolos utilizada en el transporte de datos, normalmente reunida en una colección llamada suite. (como la suite de TCP/IP)

Políticas de Seguridad. Documentos que describen principalmente el uso adecuado de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios y administradores tienen, y como responder a un incidente.

Portales. Sitio WEB de inicio y punto de entrada hacia otros sitios en Internet.

Proceso. Un programa o trabajo que se está ejecutando en la actualidad.

Protocolo. Un conjunto de normas estandarizadas que gobiernan la comunicación o la forma en que se transmiten los datos.

Puerta Trasera. *(Back door).* Códigos de acceso o procedimientos que permiten el acceso sin la autorización apropiada.

Root *(Raíz).* El superusuario o cuenta administrativa de potencia total en sistemas; el administrador del sistema.

RFC. Petición de comentarios (*Request for Comments*), las notas de trabajo de la comunidad de desarrollo de Internet. Son frecuentemente utilizadas para proponer nuevos estándares.

rhost. El archivo de usuarios y hosts fiables, donde se especifican dichos usuarios y hosts.

Respuesta a Incidentes. Decisiones que los administradores realizan en tiempo real, enfocados a minimizar los efectos de un incidente y mitigar los residuos de riesgos de seguridad basados en evidencia disponible de los eventos relacionados al incidente.

RIP. Protocolo de información de ruta (*Routing Information Protocol*), que permite a los hosts de Internet intercambiar información de ruta.

Ruteador. Una unidad dirige los paquetes hacia dentro y fuera de la red. Muchos ruteadores son sofisticados y pueden funcionar como Firewall.

RSA. Es el sistema y algoritmo de criptografía de claves públicas *Rivest-Shamir-Adleman*. Es extremadamente popular porque puede integrarse sin problemas en muchas aplicaciones.

SET. Transacción electrónica asegurada *(Secured Electronic Transaction)*, un estándar de protocolos seguros asociados con transacciones comerciales y de tarjetas de crédito en línea. (Visa y Master-Card son los punteros en desarrollo del protocolo SET). Su propósito claro es hacer más seguro el comercio electrónico.

Spoofing. Hacer creer al sistema destino que recibe paquetes de un sistema origen, cuando en realidad, un tercer sistema ha modificado la dirección de origen de los paquetes que envía al sistema atacado (destino).

SSL *Socket Secure Layer*

TCP/IP Protocolo de control de transmisión / Protocolo de Internet (*Transmisión Control Protocol/ Internet Protocol*), los protocolo utilizados por Internet.

Troyano o caballo de Troya. Es un programa que al ser introducido en un sistema realiza ciertas funciones no autorizadas y, una vez concluidas éstas, realiza las funciones para las cuales el programa estaba realmente autorizado; el caballo de Troya se presenta, a los ojos del usuario, como un programa que realiza una función legítima.

Tuneleado. La práctica de encerrar un protocolo dentro de otro para trasladar lo entre dos puntos. Utilizada frecuentemente con encriptación para proteger los datos de cualquiera que pudiera estar rastreando la red.

UDP. Protocolo de datagramas de usuario (*User Datagram Protocol*), un protocolo sin conexión de la familia TCP/IP. Los protocolos sin conexión transmiten datos entre dos hosts si no tienen actualmente una sesión activa. Dichos protocolos son considerados no fiables porque no hay garantías absolutas de que los datos lleguen como se deseaba.

Usuario. Cualquier persona que utilice el sistema de computadoras o recursos del sistema.

Virus. Un programa que se autoreplica o propaga (a veces de forma maliciosa) que se une a otros ejecutables, unidades o plantillas de documentos infectando el archivo o host objetivo.

VPN Virtual Private Network. Red privada de datos que utiliza la infraestructura de las redes publicas de datos de forma segura mediante procedimientos de seguridad.

Vulnerabilidad (hueco, agujero). Es un punto en donde un sistema es susceptible de ataque. Este término se refiere a cualquier debilidad del sistema, en hardware o software, que permite a los intrusos obtener acceso no autorizado a servicios negados.

WWW *World Wide Web*

XML *Extensible Markup Language*. Lenguaje que permite integrar además de formato a las páginas WWW, un significado y descripción de la información contenida en el documento.

Zombie - Una computadora generalmente infectada con un troyano de acceso remoto, capaz de recibir órdenes externas, y de actuar, generalmente en actividades maliciosas, sin el conocimiento de sus dueños.

1 INTRODUCCION

1.1 PROPIEDADES DE SEGURIDAD EN LOS SISTEMAS

Antes de describir los ataques de negación de servicio es importante mencionar las propiedades de seguridad que pueden ser afectadas al realizarse esté tipo de ataque u otros, así en lo que tiene que ver con la protección de la información contenida en los sistemas, o con la información que circula entre ellos, la seguridad lógica de un sistema se puede considerar desde cinco perspectivas diferentes.

1.1.1 AUTENTIFICACIÓN.

La autentificación es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información, estas entidades pueden ser personas, procesos o computadoras.

1.1.2 INTEGRIDAD.

La integridad de la información corresponde a lograr que la información trasmitida entre dos entidades no sea modificada por un tercero y esto se logra generalmente mediante la utilización de firmas digitales.

1.1.3 DISPONIBILIDAD

La seguridad de un sistema posee la propiedad de disponibilidad si, la información manipulada por éste, es disponible en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

1.1.4 CONFIDENCIALIDAD.

Es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipular dicha información. Un servicio de confidencialidad es designado para evitar la disponibilidad del tráfico de un mensaje a entidades o usuarios no autorizados. Los usuarios pueden ser una persona, un proceso, un programa, etc.

1.1.5 NO-REPUDIACIÓN.

Los servicios de no-repudiación ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información. Esta característica garantiza que la persona o entidad que envía un mensaje no pueda rechazar el envío o recepción del mensaje.

1.2 ATAQUES DE NEGACIÓN DE SERVICIO

Un ataque de negación de servicio (DOS[1]) es cualquier acción iniciada por una persona o por cualquier otra entidad (proceso, fenómeno natural, etc), que incapacite el hardware, software, o ambos, del host o sistema afectado, y que lleve al atacante a agotar los recursos de este sistema imposibilitando el servicio a los usuarios autorizados. Es decir viola o afecta la propiedad de disponibilidad que todo sistema debe poseer. En un ataque DOS, el objetivo del atacante es sencillo: dejar fuera de servicio a los sistemas de la red, los ataques DOS son maliciosos y, además ilegales, aunque la mayoría de las veces es casi imposible llegar al culpable. [Anónimo01 00]

La negación de servicio es un problema que ocurre frecuentemente por dos razones.

- Primera, los ataques DOS son rápidos y fáciles de generar (pues quienes realmente desarrollan el código de estos ataques los liberan en Internet y así, se encuentran fácilmente en el dominio público) y producen un resultado inmediato y no siempre observable.

- Segunda, muchos de dichos ataques aprovechan errores, limitaciones o inconsistencias en implementaciones de vendedores de TCP/IP que existen hasta que se corrige el problema por el mismo proveedor. [Anónimo01 00]

[1] Denial of Service

Para tener una idea más clara de este tipo de ataques podemos mencionar que el CERT[2] registró 104 incidentes de negación de servicio que sucedieron en Internet entre 1989 y 1995; adicionalmente, otros 39 incidentes reportados en la clasificación de "root-level" o "account-level break-ins"[3] también incluyen un ataque de negación de servicio. Las estadísticas nos indican, de acuerdo a los reportes del CERT, que el número de ataques de negación de servicio se ha mantenido constante con respecto al número de hosts que han aparecido en Internet. Se estima que aparecen periódicamente nuevos ataques DOS, uno cada tres o cuatro meses. [CERT01_95]

De acuerdo a los párrafos anteriores, podemos afirmar que los ataques DOS han tenido una presencia constante en Internet desde sus inicios.

1.3 HISTORIA DE LOS ATAQUES DE NEGACIÓN DE SERVICIO.

Existen muchos ataques negación de servicios (DOS) desde que apareció Internet, sólo basta recordar el primero que hizo caer el sistema ARPAnet el 21 de octubre de 1980 debido a alguna secuencia de paquetes de control defectuosa, éste fue el primer ataque de negación de servicio generalizado de Internet. [Anónimo01 00]

Otro ataque DOS ocurrió en la primera semana de noviembre de 1988 conocido como el worm de Internet, éste fue también el primer ataque extendido o difundido dentro de Internet, sirvió para reconocer la vulnerabilidad de los Sistemas Operativos de aquella época y crear organizaciones para dar respuesta a incidentes como el CERT (Computer Emergency Response Team). El worm a diferencia de un virus, es un programa que es capaz de generar copias de sí mismo, se desarrolló para propagarse a toda computadora que le fuera posible sin que los usuarios se percataran de su presencia (aunque éste no fue el caso, pues resultó en una negación de servicio). En tan sólo 90 minutos más de 6,000 equipos de los 60,000 conectados a Internet fueron infectados y paralizados.[Zakon 01]
El servicio fue denegado en dos formas. Primero, paralizó las máquinas, ya que infectó hosts quedando inútiles debido a que la capacidad de su procesamiento fue agotada por múltiples copias del programa worm; hasta que fueron removidas todas las copias del worm, los hosts no estuvieron disponibles para ser usados. Segundo, aún cuando muchos hosts dentro de Internet no fueron infectados por el worm, muchos administradores de sistemas se vieron en la necesidad de retirar sus máquinas completamente de la llamada "red de redes" por temor de verse infectados, así se desconectaron de la red como una medida de defensa.

Un ataque DOS muy famoso tuvo lugar en septiembre de 1996. Un proveedor de servicios en Internet (ISP) de Nueva York, Public Access Networks Corporation (PANIX), fue aislado durante una semana, negando el acceso a Internet a alrededor de 6000 individuos y mil compañías, según PC Week. Lo más terrible de este ataque fue que se aprovechó de las

---

[2] Computer Emergency Response Team
[3] Ataques a cuentas a nivel de root y usuario

debilidades inherentes en el núcleo del protocolo de Internet (TCP/IP) y el modo en que los sistemas manejaron las peticiones SYN. Esta situación fue exacerbante por que el atacante había falsificado su dirección origen para enmascarar su identidad. Así, en este ataque, y en muchos otros que siguieron, era sumamente difícil capturar a los verdaderos causantes. Este suceso causó un gran impacto sobre la comunidad de Internet y resaltó nuevamente la fragilidad de la red de redes. Aunque este ataque fue predicho años antes, los peligros de llevar a cabo transacciones comerciales en la era de la información eran ahora dolorosamente ciertos. [Stuart 01]

Con el paso del tiempo, y considerando la evolución que ha sufrido Internet, el enfoque sobre posibles ataques ya no es tanto el intentar acceder a un sistema, sino el imposibilitar su acceso. De cara a una empresa, quizás sea más costoso el que su sistema permanezca inaccesible a que accedan al mismo. Sin considerar que cada día resulta más complejo el asaltar sistemas considerados de interés. Es por ello que los *hackers* adoptan una nueva estrategia de ataque: provocar la negación de servicio o imposibilidad de prestar el servicio del sistema atacado. La negación de servicio, por tanto, sólo busca el impedir que los usuarios de un determinado sistema no puedan acceder a él, y por consiguiente a los servicios que proporciona.

En las circunstancias actuales de globalización, el daño económico y de imagen que sufre una empresa por un ataque de este tipo probablemente sea mucho mayor que el derivado de una simple intrusión.

El primer sistema de negación de servicio fue el denominado *mail bombing*, consistente en el envío masivo de mensajes a una máquina hasta saturar el servicio. Resulta curioso recordar que esta práctica se empleaba para castigar a quienes se consideraba hacían un uso incorrecto de Internet.

Hoy en día, los mecanismos de ataque por negación de servicio resultan bastante más sofisticados, empleando debilidades de los protocolos TCP/IP para generar auténticas avalanchas de paquetes sobre un sistema concreto, o simples estados de inconsistencia que provocan que el proceso que atiende el servicio quede inoperante. En algunos casos se han llegado a detectar ataques que generaban más de 1Gbps hacia el sistema atacado. Es cierto que TCP/IP carece de mecanismos de seguridad que permitan detener estas prácticas, pero cuando se diseñó la conectividad era lo importante, pues debía ser capaz de afrontar con éxito ataques externos en la infraestructura de comunicación, y en cualquier caso nadie podía imaginar en qué desembocaría aquella red.

1.4 TIPOS DE ATAQUES DE NEGACIÓN DE SERVICIO.

La realidad es que, frecuentemente, resulta mucho más fácil desorganizar el funcionamiento de una red o sistema que acceder realmente al mismo. Los protocolos de red tales como TCP/IP se diseñaron para su empleo en una comunidad abierta y confiada, y este protocolo tiene defectos propios. Además, muchos sistemas operativos y dispositivos de red tienen defectos en sus pilas de red que debilitan su capacidad para resistir ataques DOS. Se ha comprobado que varios

dispositivos de control de procesos con pilas IP rudimentarias se desmoronan ante un enrutamiento ICMP simple que utilice un parámetro que no sea válido. Aunque hay muchas herramientas disponibles para lanzar ataques DOS, es importante identificar los tipos más probables que puedan encontrarse. En primer lugar, veremos la teoría que se esconde detrás de cuatro tipos comunes de ataques DOS. [Stuart01 01]

1.4.1 CONSUMO DE ANCHO DE BANDA.

La forma más insidiosa de ataque DOS son los ataques de consumo de ancho de banda. Esencialmente, los atacantes consumirán todo el ancho de banda disponible en una red particular. Esto puede suceder sobre una red local, pero es mucho más común que los atacantes consuman recursos remotamente.
Por ejemplo el tráfico ICPM es peligroso, aunque sirve para realizar varios diagnósticos, se puede abusar con facilidad de él, y, con frecuencia, es la "bala" utilizada en los ataques de consumo de ancho de banda. Además, los ataques de consumo de ancho de banda resultan cada vez más peligrosos porque la mayoría de los atacantes falsifica su dirección origen, haciendo sumamente difícil identificar al verdadero culpable.

1.4.2 INANICIÓN DE RECURSOS.

Un ataque por inanición de recursos (resource-starvation) difiere del ataque de consumo de ancho de banda en que está enfocado mas al consumo de recursos del sistema que al de recursos de red. Generalmente, este consumo de recursos esta dirigido a la saturación del CPU, memoria, cuotas del sistema de archivos u otros procesos del sistema. Normalmente, los atacantes tienen acceso legítimo a una cantidad finita de recursos del sistema. Sin embargo, los atacantes abusan de este acceso para consumir recursos adicionales. De esta forma, el sistema o los usuarios legítimos se ven privados de su parte de recursos. El ataque DOS por inanición de recursos, generalmente provoca un fallo general del sistema, por ejemplo que el sistema de archivos se llene o que los procesos se queden colgados.

1.4.3 DEFECTOS DE PROGRAMACIÓN.

Los defectos de programación (programming flaws) son los fallos de una aplicación, sistema operativo o chip lógico que le impiden manejar condiciones excepcionales. Estas condiciones excepcionales, normalmente, ocurren cuando el usuario envía datos imprevistos al elemento vulnerable. Muchas veces, los atacantes enviarán paquetes anormales al sistema objetivo para determinar si la pila de red será capaz de manejar esta excepción o si acabara en un caos y con la caída de todo el sistema. Para aplicaciones especificas que se basan en entradas de los usuarios, los atacantes pueden enviar largas cadenas de datos con miles de líneas. Si el programa utiliza un búfer de longitud fija de, por ejemplo, 128 bytes, los atacantes podrían crear una condición de desbordamiento de búfer y colgar la aplicación. Y, lo que es peor, los atacantes podrían ejecutar mandatos privilegiados. Los ejemplos de defectos de programación son también comunes en los chips lógicos. El infame ataque DOS f00f del Pentium permitía que un proceso en modo usuario colgara a cualquier sistema operativo sin mas que ejecutar la instrucción 0xf00fc7c8 no válida.

Como casi todos sabemos, la existencia de programas, sistemas operativos e, incluso, CPU libres de errores es solo una quimera. Los atacantes también conocen este axioma y sacarán ventaja al colgar aplicaciones críticas y sistemas sensibles. Desafortunadamente y comúnmente, estos ataques ocurren en el momento más inoportuno.

1.4.4 ATAQUE DNS Y DE ENRUTAMIENTO.

Un ataque DOS basado en enrutamiento consiste en que los atacantes manipulan las tablas de distribución o enrutamiento para negar el servicio a redes o sistemas legítimos. La mayoría de los protocolos de enrutamiento, tales como Routing Information Protocol (RIP) v1 y Border Gateway Protocol (BGP) v4, carecen o tienen una autentificación muy sencilla. Esta sencilla autentificación de la que disponen, raramente se utiliza una vez instalados.
Se trata, pues, de un escenario perfecto para que los atacantes puedan alterar las rutas legitimas, frecuentemente falsificando su dirección IP origen para crear una condición DOS. Las víctimas de tales ataques verán cómo se dirige su tráfico a través de la red de los atacantes o hacia un agujero negro, una red que no existe.
Los ataques DOS sobre servidores de nombres de dominios (DNS) son tan problemáticos como los ataques basados en enrutamiento. La mayoría de los ataques DOS DNS convencerán al servidor víctima para que almacene información de direcciones falsa en la caché. Cuando un servidor DNS realiza una búsqueda, los atacantes pueden redireccionarla al sitio que prefieran o, en algunos casos, enviarán la búsqueda a un agujero negro. En los últimos tiempos se han producido algunos ataques DOS de tipo DNS que han provocado que grandes sitios web quedasen inaccesibles durante un tiempo prolongado.

Otra de las características importantes de este tipo de ataques DOS, es que han afectado a diferentes sistemas operativos (Unix, Linux, Windows NT, etc.), aprovechando las vulnerabilidades de cada plataforma.
A los ataques DOS capaces de afectar a diferentes sistemas operativos se le denominan genéricos. Generalmente, estos ataques pertenecen a las categorías de ataque DOS de consumo de ancho de banda y consumo de recursos. Un elemento común a estos tipos de ataques es la manipulación del protocolo. Si se manipula un protocolo (por ejemplo el ICMP) con propósitos mal intencionados, tiene la capacidad de afectar simultáneamente a muchos sistemas operativos.

1.5 PRINCIPALES ATAQUES DE NEGACIÓN DE SERVICIO.

A continuación se describen los principios básicos de como se efectúan los ataques: Sumurfing e Inundación SYN, estos han sido dos de los ataques más importantes en Internet, y a la vez han sido la base de desarrollo para nuevas herramientas de ataque.

1.5.1 ATAQUE SMURFING

El caso del *smurfing*, o amplificación de peticiones broadcast, ha sido ampliamente utilizado en ataques por negación de servicio, y como se verá, es relativamente fácil prevenir el no ser usados en un ataque de este tipo. Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de *ping*. Esta trama lleva como dirección de origen la dirección IP de la víctima, y como dirección de destino la dirección broadcast de la red atacada. De esta forma se consigue que por cada trama que se transmite a la red, contesten a la víctima todos aquellos sistemas que tienen habilitado el poder contestar a paquetes destinados a la dirección broadcast de la red [Huegen 00].

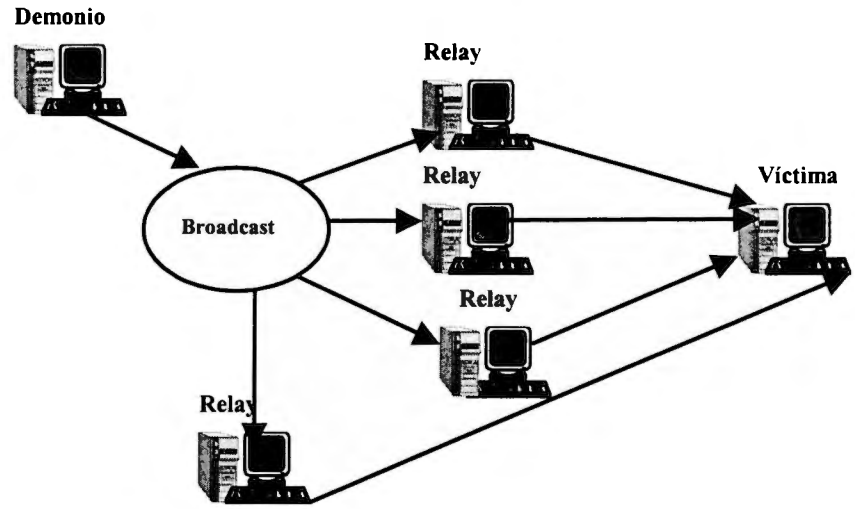


Figura 1.1

Se define como factor de amplificación a la relación entre tramas recibidas por la víctima por cada trama transmitida por el demonio. Podemos averiguar el factor de amplificación de una red mediante el siguiente comando:

/usr/sbin/ping –s <dirección de broadcast de la red> 0 <n>

donde *<dirección de broadcast de la red>* debe ser la dirección de *broadcast* que se utiliza en la red, y que depende del rango de direcciones y la máscara de red, y *<n>* es el número máximo de tramas que esperamos escuchar para finalizar el comando.

Por ejemplo, el comando:
/usr/sbin/ping –s 138.100.15.255 0 10
proporcionaría un resultado:
PING 138.100.15.255: 0 data bytes
8 bytes from panoramix.nw.uam.mx (138.100.8.36): icmp_seq=0.
8 bytes from roble.datsi.nw.uam.mx (138.100.9.10): icmp_seq=0.
8 bytes from r2d3.dia.nw.uam.mx (138.100.11.69): icmp_seq=0.
8 bytes from avellano.datsi.nw.uam.mx (138.100.9.22): icmp_seq=0.
8 bytes from r2d7.dia nw.uam.mx (138.100.11.103): icmp_seq=0.
8 bytes from laurel.datsi.nw.uam.mx (138.100.9.35): icmp_seq=0.

8 bytes from ebano.datsi.nw.uam.mx (138.100.9.108): icmp_seq=0.
8 bytes from r2d6.dia.nw.uam.mx (138.100.11.102): icmp_seq=0.
8 bytes from adelfa.datsi.nw.uam.mx (138.100.9.100): icmp_seq=0.
8 bytes from clip.dia.nw.uam.mx (138.100.11.74): icmp_seq=0.
----138.100.15.255 PING Statistics----
1 packets transmitted, 10 packets received, 10.00 times amplification

Del resultado anterior puede deducirse que esta red tiene, como mínimo, un factor de amplificación de 10. Un análisis más amplio *(n* > 100) nos llevaría a afirmar que esta red tiene un factor de amplificación superior a 100. Puede asegurarse que un ataque empleando esta técnica en una red como ésta sería fatídico. Las contramedidas a este problema son relativamente simples: hay que configurar los sistemas para que no contesten a tramas ICMP cuyo destinatario sea una dirección de broadcast. El problema se convierte en irresoluble cuando los usuarios no quieren o no saben cómo hacerlo. Podemos encontrar más información sobre ataques de tipo *smurf* y las posibles contramedidas para distintos sistemas operativos en el URL: http://www.pentics.net/denial-of-service/

Cuando el sistema a atacar es lo suficientemente potente como para poder absorber la carga extra de trabajo que pudiera generar el atacante, o se buscase crear algo de confusión sobre el origen del ataque, se organizan ataques coordinados, realizándose ésta de forma telefónica o por cualquier otra vía de comunicación, como pueden ser los IRC (Internet Relay Chat). Métodos que en cualquier caso sólo eran útiles para un número limitado de atacantes.

1.5.2 INUNDACIÓN SYN

Hasta que el ataque Smurf se puso de moda, el ataque de inundación SYN (SYN Flood) había sido el ataque DOS más desvastador existente. Cuando se inicia una conexión TCP, comienza un proceso de tres pasos, como se muestra en la figura 1.2

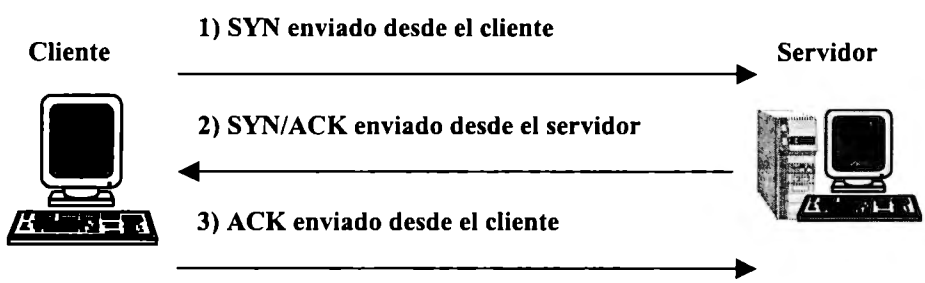


Figura 1.2

En circunstancias normales, un paquete SYN se envía desde un puerto especifico del sistema A a un puerto especifico que esta en estado LISTEN (escuchando) en el sistema B. En esta situación, la conexión potencial en el sistema B esta en un estado SYN_RECV. En este instante, el sistema

B intentará enviar un paquete SYN/ACK como respuesta al A. Si todo va bien, el sistema A volverá a enviar un paquete ACK como respuesta, y la conexión pasará al estado de establecida (established).

Aunque este mecanismo funciona bien la mayoría de las veces, existen algunas debilidades inherentes a este sistema que los atacantes podrían aprovechar para crear una condición DOS. El problema es que la mayoría de los sistemas destinan una cantidad finita de recursos cuando configuran una conexión *potencial*, o sea, una conexión que no ha sido establecida totalmente. Aunque la mayoría de los sistemas pueden mantener centenares de conexiones concurrentes a un puerto especifico (por ejemplo, 80), basta con una docena de peticiones de conexión potenciales para agotar todos los recursos destinados a configurar la conexión. Este es, precisamente el mecanismo que utilizarán los atacantes SYN para inutilizar un sistema.

Cuando se inicia un ataque de inundación SYN, los atacantes envían un paquete SYN desde el sistema A al sistema B; sin embargo, los atacantes falsificarán la dirección de origen asignando la de un sistema inexistente. El sistema B tratará entonces de enviar un paquete SYN/ACK a la dirección falsa. Si el sistema falsificado existe, éste respondería normalmente enviando un paquete RST al sistema B ya que el no inició la conexión. Recuerde, sin embargo, que los atacantes escogen un sistema que es inalcanzable. Así, el sistema B enviará un paquete SYN/ACK y nunca recibirá un paquete RST desde el sistema A. Esta conexión potencial se encuentra ahora en el estado SYN_RECV y se colocará en una cola de conexión. Este sistema intentará ahora establecer la conexión y esta conexión *potencial* sólo se eliminaría de la cola una vez que transcurra el tiempo de establecimiento de conexión. El tiempo de conexión varía de un sistema a otro, pero podría ser tan corto como 75 segundos o tan largo como 23 minutos para algunas implantaciones IP. Como normalmente la cola de conexión es muy corta, los atacantes sólo tienen que enviar unos cuantos paquetes SYN cada 10 segundos para inutilizar completamente un puerto especifico. El sistema que está siendo atacado nunca será capaz de eliminar la cola de espera antes de recibir nuevas solicitudes SYN. [Stuart02 01]

Este ataque es muy desvastador. Primero, porque se requiere muy poco ancho de banda para que se inicie una inundación SYN con éxito. Los atacantes podrían hacer caer un servidor web de gran capacidad utilizando un enlace vía MODEM de solo 14.4 Kbps. Segundo es un ataque silencioso que no deja rastro porque los atacantes falsifican la dirección origen del paquete SYN, dificultando al máximo la identificación del autor. Irónicamente, desde hace muchos años, los expertos de seguridad habían predicho este tipo de ataque y ha sido un instrumento eficaz para conseguir explotar la relación de confianza.
Para determinar si un sistema está siendo atacado, podemos utilizar el comando *netstat, si* lo soporta el sistema operativo. Si observamos muchas conexiones en un estado SYN_RECV. Puede indicarnos que se está llevando a cabo un ataque SYN.

1.6 SPOOFING

Spoofing es un mecanismo de ataque activo en el cual un equipo intruso se hace pasar por otro equipo de la red. Por tratarse de un ataque activo, el spoofing altera la operación normal de la red, inyectando información adicional en una comunicación. El propósito final de este tipo de ataque consiste en que el intruso pueda hacerse pasar por otro equipo y burlar entonces uno de los principios básicos de la seguridad en redes: la identidad de los participantes de una comunicación. Esta técnica puede emplearse para muchas cosas, entre otras para efectuar ataques DOS, aquí la justificación el porque le dedicamos esta sección de la tesis para explicar su funcionamiento.

El spoofing puede ocurrir en cualquiera de las capas del modelo de comunicaciones TCP/IP: en la capa de enlace, en la capa de red, en la capa de transporte o en la capa de aplicación. Sin embargo es importante tener en cuenta que de estar comprometida la seguridad en las capas más bajas, cualquier esquema de seguridad existente estará comprometido.

Dentro de una LAN el mecanismo de spoofing más sencillo trabaja a nivel de protocolo ARP. Por medio de la intercepción de información de broadcast en protocolo ARP un intruso puede fácilmente personificar a un nodo cualquiera de la red y desde ese momento recibir el tráfico de IP destinado al mismo sin que el originador de la conversación se entere de lo que esta sucediendo.

En un contexto de Internet, cada uno de los equipos intermedios toma parte en los procesos de ruteo por medio de los cuales los datagramas puede alcanzar su destino final. Un intruso puede alterar las tablas de ruteo encaminando un datagrama a un destino diferente del deseado en el cual un equipo intruso personifica al nodo final real.

Algunos sistemas basan su confianza en direcciones IP, otros basan su confianza en nombres de DNS. El manejo de nombres de DNS simplifica el reconocimiento de los equipos pero a su vez, al agregar una nueva capa de aplicación al stack de protocolos presenta una nueva oportunidad para un ataque. Los mecanismos de spoofing pueden actuar también a nivel de DNS, permitiendo a un atacante la personalización de un nodo cualquiera de la red.

1.6.1 SPOOFING DNS

Supongamos que un servidor de DNS de Internet se encuentra comprometido por un ataque a su seguridad o simplemente se encuentra en manos no honradas. Este servidor de nombres es autoridad de algunos dominios y todos los hosts de Internet confían en sus respuestas. Estas respuestas pueden llevar a un cliente a conectarse a un servidor falso que en realidad se encuentra bajo el control de un atacante. Algo parecido puede suceder en el campo de las resoluciones inversas en las cuales un servidor DNS falso puede dar información alterada a un nodo que desea autenticar en base al nombre la dirección de un cliente autorizado.

1.6.2 IP SPOOFING

Sucede cuando un atacante hace pasar su máquina como una computadora de la red destino (por ejemplo, engañando a una máquina destino que los paquetes vienen de una máquina confiable de la red interna destino). La política de seguridad que trata el encaminamiento de paquetes debe especificarse claramente para que se actúe correctamente si existe un problema de seguridad. Es necesario que la autentificación basada en direccionamiento fuente se combine con otro esquema de seguridad para protegerse contra los ataques de "spoofing IP". El "spoofing IP" utiliza diversas técnicas para trastornar el control de acceso basado en IP suplantando a otro sistema utilizando su dirección IP.

Sin embargo, el IP spoofing no es una técnica cuyo éxito dependa única y exclusivamente de quién emite el paquete. Es decir, nosotros podemos mandar un paquete con una dirección de origen falseada, pero ese paquete no llegar nunca a su destino.

En redes grandes como Internet existen muchos dispositivos de red que pueden realizar filtrados al tráfico que gestionan. Uno de esos filtros es precisamente la comprobación de la IP de origen. Los dispositivos son normalmente:

- Firewalls
- Ruteadores
- Conmutadores
- Servidores de acceso

Evidentemente, el IP spoofing funciona en una LAN (sobre todo en las que sean tipo bus pasivo). Sin embargo, en Internet no podemos suponer que, a priori, el IP spoofing puede funcionar. Los ISP aplican (o deberían aplicar) filtros en los servidores de acceso y en sus routers para 'paliar' este problema. En el peor de los casos, si no lo hace el ISP, lo hará el carrier, así que estamos en una situación parecida.

1.7 FACTIBILIDAD DE ATAQUES DE NEGACIÓN DE SERVICIO

Llegados a este punto es necesario analizar cuáles son las causas que hacen factible se produzcan este tipo de ataques:

Posibilidad: Existen en estos momentos cientos de miles o millones de sistemas informáticos conectados a la red y configurados con un bajo nivel de seguridad. Sistemas que prácticamente funcionan de forma desatendida las veinticuatro horas al día.

Calidad del software: Cada día el software es más complejo, los tiempos de desarrollo son menores, los programadores poseen menos experiencia (más baratos) y no se dedica el suficiente esfuerzo en controles de calidad.

- **Prestaciones vs Seguridad**: Hasta la fecha los usuarios optan por las prestaciones del producto, sacrificando o no reclamando niveles de seguridad. Se entiende que la seguridad es una complicación añadida, y que no necesariamente debe formar parte de la solución adoptada. De igual manera se diseñan redes pensando en la velocidad y funcionalidad, pero no en la seguridad.

- **Personal no calificado**: La capacidad de formación de administradores de sistemas se ha visto desbordada por la demanda, paralela al crecimiento observado en Internet, contratando como administradores de sistemas a personas no calificadas y sin experiencia.

- **Defensa legal**: La propia Internet facilita que se internacionalice el problema de los ataques, resultando en ocasiones imposible compatibilizar leyes y disposiciones de distintos países, lo que en definitiva juega a favor de los atacantes al existir de hecho una defensa legal. (ver capítulo 6)

1.8 ATAQUE DISTRIBUIDO DE NEGACIÓN DE SERVICIO.

En el mes de febrero del 2000, las principales páginas web que mueven miles de millones de dólares de la industria cibernética (Yahoo, CNN, eBay, Buy.com, Amazon.com, ZDNet, eTrade) fueron afectadas por el ataque distribuido de negación de servicios (DDOS).

Este tipo de ataque, no modifica páginas web ni obtiene listados de claves o de números de tarjetas de crédito, se trata sencillamente de entorpecer el acceso de los usuarios a los servicios de la máquina, estos ataques se basan en fallos de diseño inherentes a Internet o a la aplicación.

El ataque se lleva acabo usando un grupo de máquinas. [Workshop 99]

1. Cliente, (Atacante). Es la máquina que se usa para coordinar el ataque
2. Hosts, (Master). Estas máquinas, entre 3 y 4, están bajo el control directo de quien realiza el ataque
3. Zombies, (Demonios). Alrededor de cien máquinas a las que se les instalo un software responsable de realizar el ataque.

Para llevar acabo los ataques, el atacante pone a trabajar todas estas máquinas. A través de software se escanean los puertos abiertos en las máquinas a las que se puede acceder fácilmente. A estas se les instala un software que realiza los ataques automáticamente y de esta forma el dueño de la máquina no se entera de la utilización de su máquina.

Las máquinas zombies anuncian a las computadoras que actúan como maestros, que ya están preparadas para actuar. Por medio de técnicas de cifrado se distribuye una lista, a las máquinas maestras de las direcciones IP de las computadoras a los que va dirigido el ataque. Las computadoras maestras envían a las máquinas zombies ordenes para comenzar el ataque simultaneo de negación de servicio. Para no ser localizados, quien realiza el ataque utiliza direcciones IP falsas [Workshop 99].

Durante este ataque las máquinas emisoras envían peticiones incompletas a los servidores de la empresa. Vamos, es como llamar a la puerta y salir corriendo. Cuando el servidor de la compañía en cuestión recibe la petición, espera una confirmación para empezar a enviar los datos, confirmación que nunca llega. Debido a que este ataque se hace organizadamente las máquinas se van llenando de procesos que nunca se completan, lo que provoca el colapso del sistema. Es muy difícil defenderse de este tipo de ataques, puesto que no se trata de aprovechar un fallo del servidor, sino de enviar una avalancha de peticiones legítimas de información.

La manera de bloquear a los servidores ha sido similar en todos los casos, desde aproximadamente unos 50 lugares del mundo, y de forma simultanea, se produce un envío masivo de peticiones a los servidores de las respectivas empresas, con flujos de hasta un gigabyte por segundo (una demanda extraordinaria que es desconocida en el mundo del comercio electrónico y que suele producirse no en un día sino en todo un año), que consigue bloquear el sistema hasta dejarlo inutilizado [El Mundo 00].

Una inusual y elevada cantidad de tráfico, servidores repentinamente con promedio de carga por encima de lo normal, son señales que indican que se esta sufriendo un ataque DOS o DDOS.

Para efectuar un ataque DDOS, el atacante necesita tener varios cientos o miles de hosts comprometidos. Los hosts son usualmente computadoras Linux y SUN, sin embargo, las herramientas pueden ser instaladas también en otras plataformas. El proceso de comprometer a los hosts e instalar la herramienta es automático. EL proceso puede ser dividido en cuatro pasos: [Cisco 00]

1. Inicia la fase de escaneo en la cual un número grande de host (del orden de 100,000 ó más) son examinados de acuerdo a alguna vulnerabilidad conocida.
2. Explotando las vulnerabilidades, se compromete a los hosts para ganar acceso.
3. Se instala la herramienta de ataque en cada host comprometido.
4. Se usan los hosts comprometidos, para escanear y comprometer otros hosts.

Debido a que el proceso es automático, los atacantes pueden comprometer e instalar la herramienta en un solo host en 5 segundos, varios miles de hosts pueden ser comprometidos en una hora. [Cisco 00]

A continuación se muestra una figura que ilustra como se lleva acabo el ataque. Un típico sistema de ataque distribuido, el "atacante" controla un pequeño número de "masters" los cuales controlan un gran número de "demonios". Estos "demonios" son usados para lanzar paquetes de inundación contra la víctima, que es el objetivo del atacante.

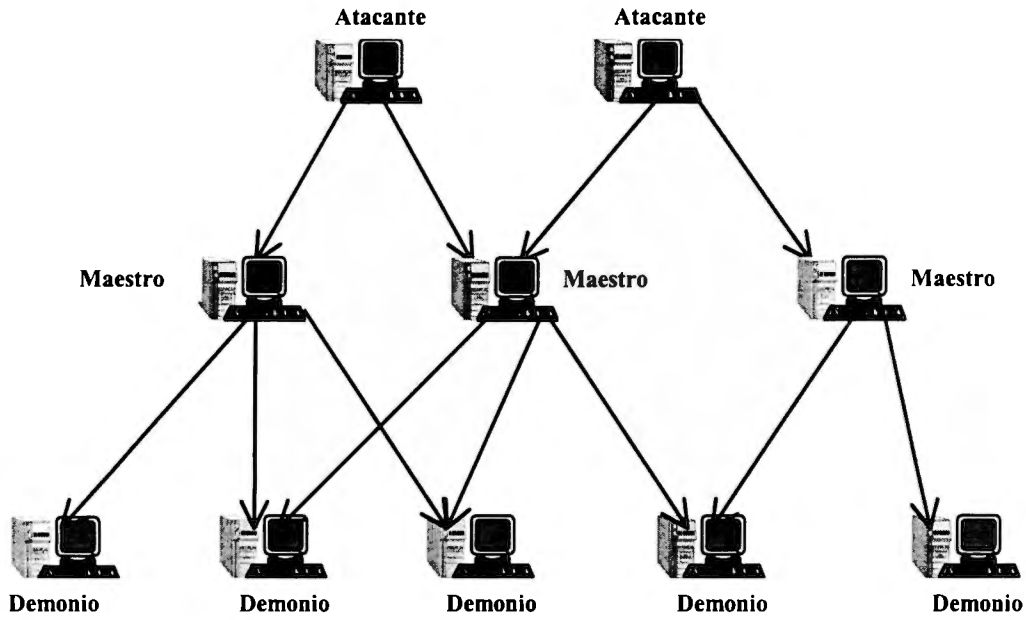


Figura 1.3

Los demonios han sido descubiertos en varios sistemas operativos con diferentes niveles de seguridad y administradores de sistemas. Aunque algunas implementaciones de los programas demonios no requieren privilegios de root para lanzar los ataques, en la práctica muchos demonios fueron ocultados en la instalación de "root kits" diseñados para ocultar la evidencia de intrusión. Los intrusos algunas veces usan recursos del sistema como *cron* para asegurar que un demonio pueda continuar ejecutándose aun cuando una instancia de este fuera borrado o el sistema fuera reiniciado. Cron es el demonio reloj, responsable de planificar otros procesos, como un demonio en algún script de arranque del sistema.

1.9 ATAQUES DDOS MÁS IMPORTANTES EFECTUADOS EN EL 2001.

A continuación describimos los principales ataques DDOS efectuados en el 2001, ordenados cronológicamente.

1.9.1 ATACAN LA RED DE IRC UNDERNET. 11 DE ENERO DEL 2001.

La red de IRC[4] Undernet no estuvo disponible debido a un ataque DDOS. De forma temporal Undernet, una de las mayores redes de IRC de todo el mundo, dejó de prestar servicio a causa de un ataque Distribuido de negación de Servicio. A su vez, un número indeterminado de Proveedores de Servicio de Internet de Estados Unidos, Holanda y Francia -que alojan servidores de IRC de la red Undernet- también sufrieron el ataque distribuido de negación de servicios. Algunos de los servidores fueron bombardeados con 100 Mbytes de datos por segundo. [Ulatina 01]

[4] Internet Relay Chat

1.9.2 ATAQUES DDOS AMENAZAN IRC. 15 DE ENERO DEL 2001.

Debido a la cantidad excesiva de ataques DDOS y la intensa actividad de aspirantes a hacker por probar sus habilidades en un entorno real, las empresas y organizaciones que patrocinan la red IRC donando ancho de banda al servicio, están considerando retirar su apoyo debido a los elevados costos involucrados. El mayor problema es que las actividades de los hackers consumen excesivo ancho de banda. [Diarioti 01]

IRC es un entorno no comercial de clubes virtuales basados en texto. En IRC, los usuarios son motivados a establecer sus propios canales –o salas de "chat"- y muchas de las redes proveen programas previamente configurados los cuales pueden ser usados para mantener el control del canal, o permitir a los usuarios configurar y correr su propio canal.

El protocolo de IRC es de fuente abierta lo cual permite a los usuarios escribir sus propios scripts, sean estos creativos o destructivos. Esto motiva a muchos hackers, en especial aspirantes, a probar sus habilidades maliciosas con propósitos tan dañinos como dividir a la red de servidores para tomar el control de los canales.

Dado que los ataques DDOS consumen mucha banda ancha, los donantes se ven obligados a donar más banda de la que tenían pensado, lo cual se está volviendo excesivamente costoso.

"Mi predicción es que si los ataques DDOS continúan en IRC, no existirá por mucho tiempo", señaló un administrador de IRC. A juicio de muchos, la eventual desaparición de IRC representaría la caída del último bastión no comercial del ciberespacio. [Diarioti 01]

1.9.3 ATACAN SITOS DE MICROSOFT. 26 DE ENERO DEL 2001.

El ataque a los servicios de Microsoft dejó al descubierto las grandes deficiencias que hay en el software de bajo nivel para el manejo de los nombres de dominio, instalados en la mayoría de los sitios a nivel mundial. El Blind, en sus versiones 4 y 8, tiene grandes "huecos" en cuanto a seguridad, mismos que permiten a los hackers realizar fácilmente los ataques denominados (DDOS), que tanto daño han causado a los grandes sitios.

Las graves deficiencias en cuanto a seguridad de todas las versiones de Windows, así como de otros sistemas operativos de red, se suman a los "huecos" citados para crear un ambiente de mucha vulnerabilidad en el ciberespacio, y una oportunidad de negocio a quien se especialice en el ámbito. [Evobonet 01]

1.9.4 NETWORK ASSOCIATES VÍCTIMA DE DDOS POR DESCUBRIR BUG. 12 DE FEBRERO DEL 2001.

Network Associates Inc., una firma de seguridad descubrió un bug[5] en un software básico de Internet, dijo el viernes que su sitio web fue atacado electrónicamente.
La compañía, con sede en Santa Clara, California, productora de software de seguridad y administración de redes, menciono que detectó un intenso ataque DDOS y tomó de inmediato medidas de protección. Este ataque logro la interrupción del acceso a su sitio de Internet mediante el envío de millones de datos. ``No hubo penetración a la red corporativa ni resultaron comprometidos algunos datos", dijo la portavoz de Network Associates, Dana Lengkeep. [Linuxcl 01]

La compañía buscó especialmente un programa que apareció en Bugtraq, una muy difundida lista de correo electrónico relacionada con seguridad informática. "Ese parece ser al menos uno de los problemas", dijo Lengkeep, agregando que el código "maligno" pudo haber sido enviado a otros sitios web. El programa aparecido en Bugtraq estaba orientado supuestamente a explotar un bug en el programa denominado Berkeley Internet Name Domain (BIND), que sustenta hasta 90 por ciento del tráfico en la Internet. Network Associates anunció el pasado lunes su descubrimiento de ese bug en el BIND.

"Es como si los piratas cibernéticos le estuvieran devolviendo la bofetada", dijo Robin Matlock, de la firma Entercept Security Technologies Inc., de San José, California, que desarrolla software para proteger servidores de Internet. Sostuvo que los hackers estaban muy disgustados por el descubrimiento de una vulnerabilidad que ellos habían estado aprovechando para atacar sitios web corporativos y robar información delicada. El supuesto autor del ataque a la compañía de Santa Clara puso en Bugtraq un aviso que decía: ``Gracias NAI (Network Associates Inc.) por la bonita cosa". El programa BIND es usado en las computadoras denominadas servidoras de nombres de dominios (DNS, sigla en inglés), que traducen nombres comunes de sitios, como www.reuters.com, en direcciones numéricas que pueden ser leídas por las computadoras.

1.9.5 HACKERS DE CHINA Y EE.UU. INTERCAMBIAN ATAQUES. 25 DE ABRIL DEL 2001.

La ira causada en China por la colisión del 1 de abril del 2001, entre un avión estadounidense de reconocimiento y un avión caza chino desencadeno ataques contra sitios web de Estados Unidos, dijo el centro de protección de infraestructura. Según dicho organismo, los administradores estuvieron alertas a los denominados ataques distribuidos de negación de servicios, por los cuales los accesos a sitios de la Internet quedan bloqueados por un exceso de tráfico.

Hackers chinos llamaron a una ofensiva de una semana en mayo del 2001 contra las principales compañías de intereses norteamericanos. En el otro bando, un grupo de hackers informáticos llamado Poizo-Box afirma haber bloqueado un centenar de sitios web chinos el cuatro de abril del 2001. [Dinformaticos 01]

---

[5] Un bicho (bug) es cualquier error introducido accidentalmente en un programa.

1.9.6 UN ATAQUE DDOS BLOQUEA AL CERT. 25 DE MAYO DEL 2001.

Un ataque DDOS mantuvo paralizado desde las nueve de la mañana del 22 de mayo del 2001, al mayor centro de alerta de agresiones en Internet, el Computer Emergency Response Team Coordination Center (CERT/CC), ubicado en la estadounidense Universidad de Carnegie Mellon (Pensilvania). El ataque se basa en un potentísimo bombardeo de datos desde cientos de computadoras externas que han sido *esclavizados* por los hackers.

Esa noche se podía acceder, muy lentamente, a la *web* www.cert.org, dónde se informaba, de forma escueta, de que "el CERT/ CC estaba experimentando un ataque DDOS, por lo que el servicio en Internet puede verse interrumpido". El CERT/CC, que tiene centros hermanos por todo el mundo, fue con ellos tan escueto como lo es en su *web*, dónde aseguraban: "Estamos siguiendo los pasos para dejar disponibles los servicios y estamos en contacto con diversas organizaciones, incluidos los proveedores de servicio de Internet, para que nos ayuden a investigar y resolver este ataque".

La tarea de defensa es laboriosa. Primero, según los expertos, hay que contactar con los responsables de cada computadora atacante, que suele haber sido asaltado a su vez para colocarle subrepticiamente el programa para atacar . 'No se puede hacer nada, te lo hacen. Sólo puedes poner filtros y hablar con los proveedores, y eso puede sucederle a un CERT o a una empresa como Amazon', aseguro un especialista del CERT, aludiendo a la primera vez que se usaron estos ataques distribuidos, en febrero del 2000, contra sitios como Amazon o Yahoo. [Internautas 01]

1.9.7 ALLDAS.DE SIN ISP. 17 DE SEPTIEMBRE DEL 2001.

Alldas.de es un sitio que se dedica a llevar estadísticas de páginas hackeadas. Debido a los problemas por ataques DDOS que regularmente tiene, su ISP se ha visto forzado a retirarle el servicio.

El servicio que proporciona Alldas.de como referencia de seguridad es presentar la historia de páginas hackeadas que se les reporta con regularidad. Después de que attrition.org decidió terminar con su servicio análogo, alldas pasó a ser el más importante. Claro, también es foco de atención para hackers y los ataques constantes que ha recibido han obligado a su ISP a suspenderle el servicio. Actualmente buscan a alguien que pueda sostener un tráfico de 300Gb al mes. [cem.itesm 01]

1.10 EFECTOS Y CONSECUENCIAS NEGATIVAS ANTE LOS ATAQUES DDOS

Básicamente se ve comprometida la seguridad de un sistema si se efectúa un ataque DDOS, todo sistema debe poseer la propiedad de disponibilidad tanto en hardware como en software, esto significa que la información manipulada por éste, se encuentre disponible en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

Esta propiedad de seguridad, es elemental en cualquier sistema de computo, la disponibilidad debe mantenerse para trabajar eficientemente o de otra manera esto puede provocar ineficiencia, mala productividad y hasta paralizar la operación completa del sistema, probablemente repercutiendo en otros sistemas dado el carácter distribuido y de interconexión que guardan estos.

La negación de servicio puede concebirse como un ataque intencional o no intencional. La perspectiva más adecuada es que independientemente de la causa, si un servicio no está disponible entonces, el servicio ha sido negado.

Un ataque, no obstante es un acto intencional. Por lo tanto se considera que un ataque de negación de servicio, tiene lugar solamente cuando el acceso a una computadora, a un recurso de la red o a un servicio ofrecido es intencionalmente bloqueado o degradado como resultado de una mala acción realizada por otro usuario o grupo de usuarios. Estos ataques no necesariamente dañan los datos directamente o permanentemente (aunque podría ocurrir), pero estos intencionalmente comprometen la disponibilidad de los recursos, violando así esta parte de seguridad que todo sistema debe tener.

Hace tiempo, la gente consideraba los ataques DOS como meras molestias. Eran realmente problemas que había que evitar, pero no necesariamente importantes o trascendentales. Algunos todavía mantienen ese punto de vista, argumentando que la mayoría de los ataques DOS afectan sólo a algunos servicios que son fáciles de reiniciar. Pero este ya no es el punto de vista que prevalece, los ataques DOS son vistos ahora desde otro prisma, principalmente porque los hábitos de la sociedad sobre las computadoras han cambiado radicalmente. Hoy los servidores son ingrediente indispensable para el comercio electrónico y otros servicios críticos. En este nuevo entorno, en particular, los ataque DDOS pueden degradar o, incluso, destruir los beneficios (sí es cosa de dinero).
Como algunos de los servicios de computación son ahora críticos, que ocurra esto en el futuro podría producir resultados diferentes. Por ejemplo, ahora los investigadores están haciendo comprobaciones de una Internet más rápida (Internet 2), para permitir a los médicos decanos supervisar operaciones remotamente. Imagine que echaran abajo su servidor de vídeo conferencia durante una operación de vida o muerte. En realidad, el paciente sobrevivirá, porque habría un médico experimentado físicamente presente durante todo el proceso. Pero el ataque le quitaría información sensible y temporalmente vital al médico decano.

Como el comercio electrónico continuará siendo una parte importante de la economía global, (se prevé que dentro de pocos años, el 20% o 30% de las transacciones comerciales se realizarán a través de Internet), los ataques DDOS tendrán un mayor impacto sobre nuestra sociedad electrónica. Muchas empresas comienzan a darse cuenta ahora del gran volumen de negocios que suponen transacciones electrónicas en la red. Como resultado, un ataque DDOS tiene la capacidad potencial de llevar a algunas organizaciones a la bancarrota. [Stuart03 01]

Por citar un ejemplo, el costo de este tipo de ataques en el caso de Yahoo, se podrían acercar a casi medio millón de dólares, sólo por las tres horas que los intrusos consiguieron bloquear el acceso a sus páginas. En todos los casos de las empresas atacadas aseguraron que sus archivos

confidenciales, dónde se guardan los números de las tarjetas de crédito de sus clientes, no se vieron afectados, ni sufrieron robo alguno de información. Pero los expertos temen el efecto negativo que los ataques pueden tener en la confianza de quienes realizan transacciones de distinto tipo a través de Internet, un comercio al que se asegura un porvenir enorme una vez que se afiance la seguridad.[Navegante 00]

Es importante mencionar que el ataque afectó no solamente el sitio principal de Yahoo en Estados Unidos, sino también algunos sitios complementarios, como Yahoo Mail y el sitio Web Geocites, el cual es propiedad de Yahoo. Aproximadamente, Yahoo tiene unas 465 millones de páginas web a las que ofrece servicios, lo que le convierte en el mayor operador en Internet y también es el portal más visitado de Internet en Estados Unidos.[Yahoo 00]

Sin embargo, incluso aún cuando existen soluciones para los fallos de seguridad, las empresas no suelen adquirirlas. Para las empresas de comercio electrónico en particular, lo más importante es aumentar su cuota de mercado, y esto significa hacer todo lo posible para atraer el mayor número de visitantes a su página. Lamentablemente, las medidas de seguridad suelen ralentizar los procedimientos, causar interrupciones en el servicio o limitar las operaciones que pueden realizarse desde una página y, puesto que las soluciones suelen ser costosas, absorben fondos que podrían emplearse en otras mejoras más rentables a corto plazo.

Tan importante fue este tipo de ataque DDOS en Estados Unidos en febrero del 2000, que el Presidente Clinton convocó a los expertos y empresas informáticas, con el fin de coordinar una serie de medidas para reforzar la seguridad de los sistemas informáticos, anunciando un considerable incremento del presupuesto de ese país para luchar contra el ciberterrorismo. [Mundo 00].

Por otra parte la Comisión Europea, preocupada por este tipo de ataques contra varios importantes portales de Internet, advirtió a sus Estados miembros acerca de la crucial necesidad de reforzar la seguridad en Internet, esta cuestión se trató en la cumbre especial que se desarrolló en Lisboa en el mes de marzo del 2000. Así mismo, Bruselas preparará un documento sobre la delincuencia en las redes electrónicas, entre otras cosas, este comunicado incidirá en la importancia relativa al uso de medidas efectivas de seguridad.

Otra de las características de este tipo de ataque es que tiene una increíble capacidad para pasar inadvertido, lo que les hace especialmente peligrosos, según las investigaciones las computadoras de la Universidad de California de Santa Bárbara fueron utilizadas en al menos uno de los ataques DDOS efectuados a las compañías dedicadas al comercio electrónico. Esto provoco que la Universidad deshabilitara su conectividad a Internet por varios días.

Inmediatamente después de que se presentó este tipo de ataque considerado el más importante en la historia de Internet, el Departamento de Defensa norteamericano dispuso, como medida de seguridad, la revisión de todas sus computadoras en todo el mundo, como medida preventiva, aclararon que "No hemos sentido nada del ataque y no tenemos motivos para la sospecha de que nuestros sistemas hayan sido utilizados". De todas las áreas gubernamentales estadounidenses, el Pentágono es la que tiene la mayor cantidad de computadoras.

Por último, tampoco nos podemos olvidar de las implicaciones que tendría un ataque DDOS utilizado con propósitos militares. Muchos gobiernos tienen o están en el proceso de desarrollar sistemas ofensivos de guerra electrónica que emplean ataques DDOS en lugar de proyectiles convencionales. Verdaderamente, la era del ciberterrorismo ha llegado. [Stuart03 01]

Dada la importancia de este tipo de ataques, DDOS, mencionada en los párrafos anteriores, surge la necesidad de tener un documento que permita conocer de manera mas detallada y precisa este ataque.

Esta tesis será de gran utilidad para los administradores u operadores de redes cuya responsabilidad es la de mantener seguro su sistema dentro de Internet, también será útil para las personas que son responsables del buen desempeño de algún servicio de Internet en su empresa o institución. Se busca reducir el daño que causa este tipo de ataques dentro de nuestras redes.

El resto de la tesis esta organizada en seis capítulos, ordenados de tal manera que el lector pueda dar un seguimiento al tema sin perderse en él.

En el capítulo dos, se analiza el funcionamiento de las principales herramientas utilizadas para efectuar un ataque distribuido de negación de servicio tales como Trinoo, TFN, TFN2K, Stacheldraht, Shaft, Mstream, Wintrinoo.

El capítulo tres describe las principales medidas que pueden ser adoptadas para protegerse de los ataques DDOS, sugeridas por los expertos en seguridad informática y algunos grupos u organizaciones gubernamentales dedicadas a proteger los sistemas.

En el capítulo cuatro se muestra el funcionamiento de las herramientas que existen para detectar o encontrar herramientas de ataque DDOS instaladas en los sistemas. Básicamente se estudian cuatro herramientas: Zombie Zapper, DDOSPing, Find_ddos y Distributed DoS Scanner. Todas son de libre uso y están disponibles en Internet.

En el capítulo cinco se propone un esquema de protección general para detectar, proteger y detener los ataques DDOS, en tiempo real y de manera automática, integrando la tecnología que se tiene para defenderse y proponiendo nuevos mecanismos a implementarse para fortalecer la seguridad en Internet.

El capítulo seis estudia las leyes contra los delitos cibernéticos en el mundo, resaltando su debida importancia como una medida más de protección, analizando los avances y las propuestas de ley que se tienen en varios países, así como los principales retos y dificultades a los que se enfrentan los gobiernos para aprobar las leyes contra delitos computacionales.

Finalmente el capítulo siete presenta las conclusiones finales a las que se llegaron en la tesis.

2 ANÁLISIS DE LAS HERRAMIENTAS DE ATAQUE DDOS

2.1 INTRODUCCIÓN.

De acuerdo a los expertos que monitorean la propagación de herramientas de negación de servicio, la amenaza de efectuarse múltiples ataques DDOS está creciendo. Por otra parte Phillippe Bourcier, quien mantiene un sitio dedicado a rastrear la actividad de los hackers, mencionó que en el verano del 2000, fue la primera vez que encontraron una gran cantidad de sistemas comprometidos, ejecutando herramientas DDOS. [Knight 00]

Un administrador de sistemas quien se puso en contacto con un afamado experto en seguridad en la lista de correo de Bugtraq, descubrió y deshabilitó cientos de máquinas que tenían instaladas herramientas DDOS, aseguró que el problema se encuentra avanzado y cree que las soluciones que ha dado el CERT[6] son insuficientes y no cubren las expectativas para detener este tipo de ataques. [Knight 00]

2.2 HERRAMIENTAS PARA REALIZAR UN ATAQUE DDOS

Un escenario en el que se disponga de un sistema sofisticado de coordinación, y en el que pudieran involucrarse cientos o miles de computadoras, supondría disponer de una herramienta de ataque por negación de servicio que difícilmente podría combatirse. Si resulta difícil defenderse de un ataque de negación de servicio procedente de un único sistema, puede afirmarse que puede resultar imposible en modo coordinado.

En la actualidad se conocen cinco sistemas básicos de ataque distribuido de negación de servicio: Trinoo, Tribe Flood Network, Stacheldraht, Shaft y Mstream. La información que a continuación se proporciona se basa en los análisis que ha realizado David Dittrich, Universidad de

[6] Computer Emergency Response Team

Washington, sobre copias obtenidas de estas herramientas a finales de 1999 y principios de 2000, por lo que es posible que existan mutaciones sobre el código analizado, y consecuentemente, puedan observarse comportamientos distintos al descrito.

2.2.1. TRINOO

Los primeros demonios de Trinoo se localizaron en abril de 1999 en forma binaria y en varios sistemas Solaris 2.X que habían sido atacados utilizando problemas de *buffer overrun* en rpc.cmsd. [CERT_cmsd 00]

En un análisis preliminar se pensó que era un mecanismo evolucionado, basado en el protocolo UDP, para la recuperación automática de los resultados obtenidos mediante *sniffer*s.
Una vez se obtuvo la primera copia de los fuentes, se vio que el cometido era otro y su funcionamiento era mucho más complejo. El demonio se compiló y ejecutó en Solaris 2.5.1 y Red Hat Linux 6.0. El maestro pudo compilarse y ejecutarse el Red Hat Linux 6.0. [Dittrich_trinoo 99]

El 17 de agosto de 1999 se empleó una red de Trinoo de al menos 227 sistemas, de los que 114 pertenecían a sistemas ubicados en Internet2, para atacar a un único sistema de la Universidad de Minnessota, dejando la red de la Universidad inoperante durante más de dos días. En febrero de 2000, en la Universidad de James Madison (Harrisonburg – Virginia), se detectaron 16 computadoras personales infectadas con una variante para Windows de Trinoo. [Dittrich_trinoo 99]

El escenario típico de un ataque sería: En una cuenta de un sistema atacado se deposita un repositorio de herramientas precompiladas: rastreo, ataque, *sniffers*, *root kits* , así como demonio y maestro de Trinoo. El sistema idóneo para un ataque dispondrá de un gran número de usuarios, y por consiguiente, una gran potencia de proceso y amplio ancho de banda en sus comunicaciones.

Se realiza un rastreo buscando posibles nuevos destinos para posteriores ataques. Suelen buscarse sistemas Solaris y Linux, dada la disponibilidad de herramientas (sniffers y root kits) para estos entornos. Se elabora una lista de sistemas vulnerables que posteriormente se utiliza en un procedimiento de comandos que realiza el ataque. El resultado es una lista de sistemas comprometidos dispuestos para alojar sniffers o demonios y maestros Trinoo. Se seleccionan aquellos sistemas más idóneos para incorporarse a la red y se crea otro procedimiento de comandos que automatiza la instalación de los procesos Trinoo. De esta forma crece la red Trinoo. Una red Trinoo esta formada por Atacantes, Maestros, Demonios y Víctimas, y tendría una estructura como la reflejada en la figura 2.1. [Dittrich_trinoo 99]

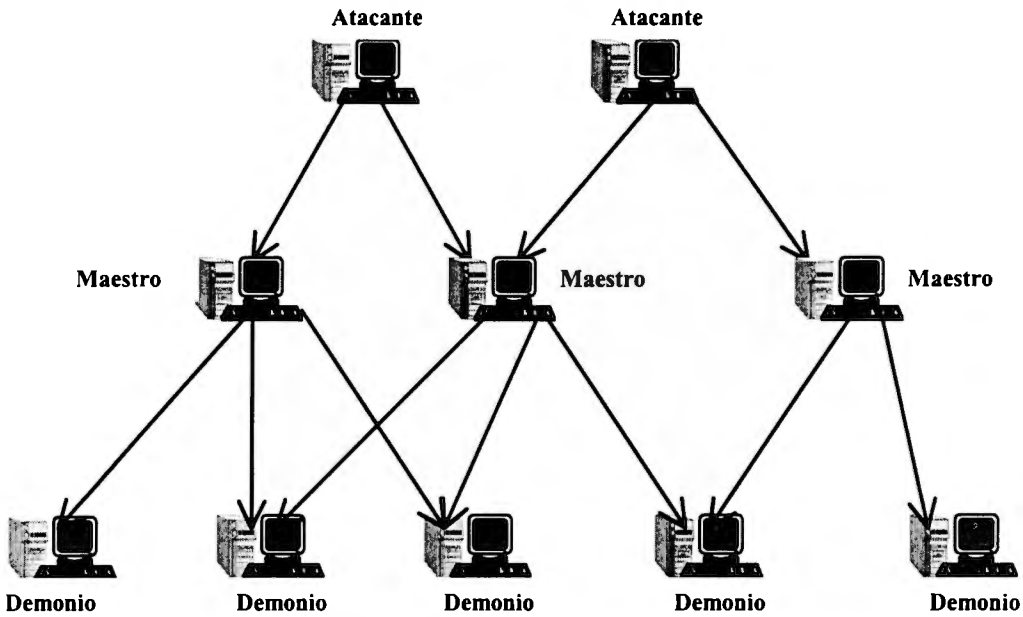


Figura 2.1

El atacante controla uno o más maestros. Cada maestro controla a gran cantidad de demonios. Los demonios son los que reciben la orden coordinada de realizar un ataque contra una o más víctimas. La comunicación entre los distintos niveles se realiza de la siguiente forma: [Dittrich_trinoo 99]

Atacante a Maestro: puerto 27665/TCP
Maestro a Demonio: puerto 27444/UDP
Demonio a Maestro: puerto 31335/UDP

La comunicación entre el atacante y el maestro, así como la del maestro y el demonio están protegidas por claves de acceso. En las primeras versiones estas claves se almacenaban en claro en los archivos de programa. En versiones posteriores se ha detectado el empleo de mecanismos de criptografía para el manejo de claves, siendo éstas del tipo *crypt()*. Las claves se emplean en forma simétrica, de manera que se almacenan cifradas tanto en el maestro como en el demonio, procediéndose a su comparación con la clave que se proporciona y transporta sin cifrar por la red. Ciertos comandos enviados por el maestro al demonio también están protegidos por claves, que igualmente se transmiten sin cifrar por la red. El maestro mantiene una lista de demonios activos, que se almacena y cifra mediante el sistema Blowfish (ver anexo 1 para detalles de este algoritmo)

El ataque de Trinoo es del tipo de *inundación por tramas UDP*.

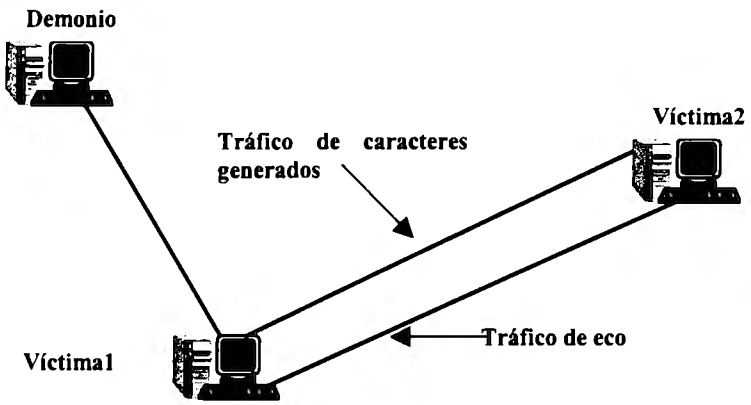


Figura 2.2

En los ataques de este tipo, el atacante (que en este caso en particular sería el demonio) envía tramas UDP con dirección de origen falsa y que consigue enlazar el servicio de generación de caracteres *(chargen)* de una de las víctimas con el servicio de eco *(echo)* de la otra. La primera comienza a enviar caracteres que la segunda responde. El volumen de tráfico se va incrementando hasta que los dos sistemas terminan por inundar la red.

2.2.2 TRIBE FLOOD NETWORK.

Desarrollada por un hacker denominado Mixter, TFN, fue la primera herramienta distribuida de negación de servicio para Unix que se hizo pública (ataca principalmente equipos Solaris y RedHat). Compuesto por un conjunto de programas clientes y demonios que implementan una herramienta de negación de servicio distribuida, capaz de generar ataques por generación masiva de paquetes ICMP, SYN o UDP, así como ataques del tipo *smurfing*. Las tramas SYN, o tramas de sincronización, representan el inicio de una comunicación TCP: [Dittrich_tfn 99]

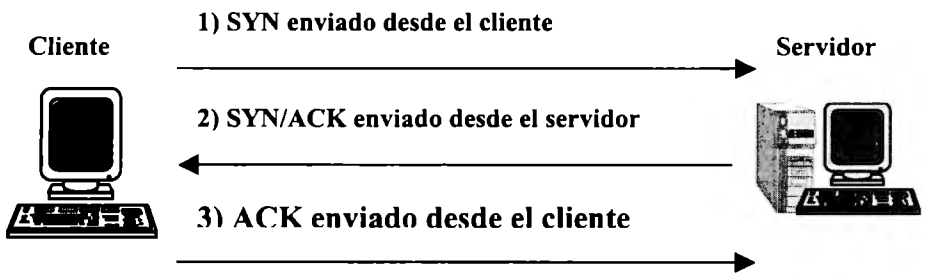


Figura 2.3

dónde el Sistema 1 solicita iniciar una comunicación (SYN), el Sistema 2 contesta afirmativamente (SYN ACK) al establecimiento de la misma, y el primero termina confirmando el comienzo de sesión (ACK).

En el caso de ataques por inundación con tramas SYN, el sistema atacante, utilizando una dirección inexistente o inoperante, envía multitud de solicitudes de establecimiento de conexión (SYN) al sistema víctima del ataque. Tantas como para llenar la cola de solicitudes pendientes al

no contestar los supuestos peticionarios. Esta situación lleva a que las solicitudes reales no puedan ser atendidas, consiguiéndose de esta forma la negación de servicio. [Dittrich_tfn 99]

Una red TFN esta formada por Atacantes, Clientes, Demonios y Víctimas, y tendría una estructura como la reflejada en la siguiente figura:

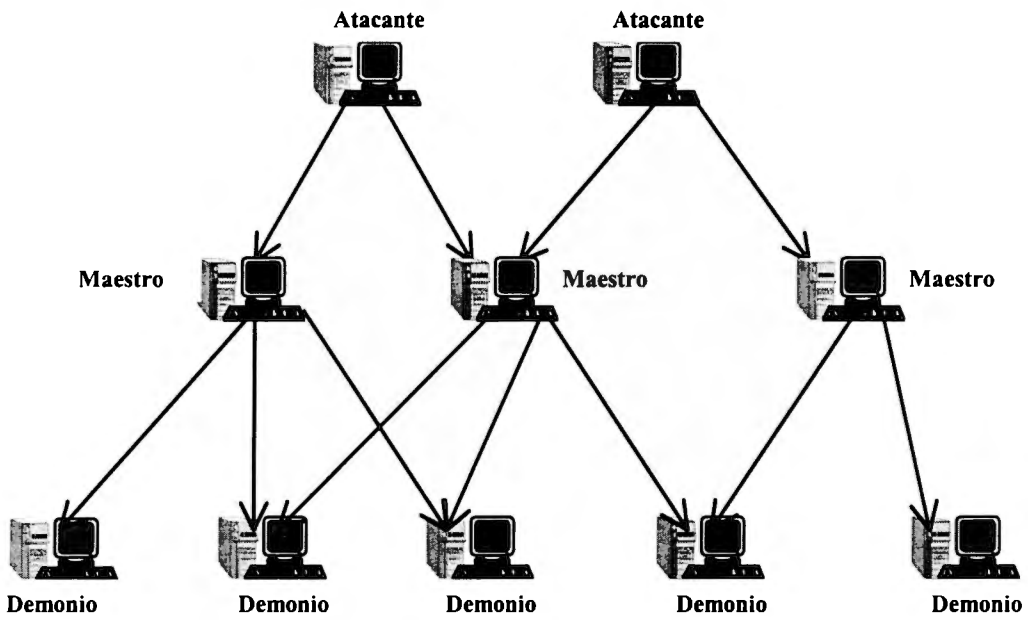


Figura 2.4

El atacante controla uno o más maestros. Cada maestro controla una gran cantidad de demonios. Los demonios son los que reciben la orden de realizar un ataque coordinado contra una o más víctimas.

El control de la red TFN se realiza mediante comandos enviados al programa maestro. Estos comandos pueden transmitirse mediante diversos métodos de conexión: shell remoto a un determinado puerto TCP, shell remoto basado en conexiones UDP cliente/servidor, shell remoto basado en conexiones ICMP cliente/servidor, sesión SSH, o un simple Telnet a un puerto TCP.

La comunicación entre los clientes y los demonios se realiza mediante paquetes ICMP_ECHOREPLY, por lo que no existe comunicación del tipo TCP o UDP entre ambos tipos de procesos. [Dittrich_tfn 99]

Uno de los puntos fuertes de esta herramienta de ataque por negación de servicio es que muchas herramientas de monitorización de redes no analizan toda la gama de paquetes de tipo ICMP o simplemente no muestran la parte de datos de estos paquetes, por lo que la detección de esta comunicación puede resultar compleja. Aunque el acceso a los clientes no está protegido por palabra clave, los comandos que el cliente envía a los demonios van codificados en forma de número binario en dos *byte*s, siendo fijo el número de secuencia del paquete: 0x0000, lo que puede hacer que parezca como el primer paquete generado por un comando *ping*. [Dittrich_tfn 99]

Tanto los clientes como los demonios necesitan ejecutar con privilegio de root, pues utilizan *sockets* del tipo SOCK_RAW. Por otra parte, el cliente necesita disponer del archivo conteniendo la lista de direcciones IP de los demonios (iplist), por lo que, una vez localizado el cliente se dispone de la relación de demonios. En las últimas versiones se ha detectado tratamiento criptográfico en el archivo iplist mediante el sistema Blowfish.

2.2.3 TRIBE FLOOD NETWORK 2000 (TFN2K)

TFN2K es una evolución del anteriormente comentado TFN. Esta última herramienta DDOS se encuentra bastante mas perfeccionada que el original, permitiendo comunicaciones aleatorias en los puertos (eliminando por lo tanto el bloqueo de puertos en sus routers frontera como una contramedida preventiva) y el cifrado (eliminando la posibilidad de aplicar el Sistemas de Detección de Intrusos basados en red como contramedida de detección). La estructura es similar, aunque cambia la terminología. De esta forma, se denomina Maestro al sistema informático en el que corre el Cliente, y Agente al sistema informático dónde se ejecuta el Demonio. El TFN2K permite a los Maestros explotar los recursos de un determinado número de Agentes con el fin de coordinar un ataque a una o más víctimas. El Maestro configura a los Agentes para atacar a una determinada lista de víctimas. Los Agentes atacan a las víctimas por inundación de paquetes. [Barlow 00]

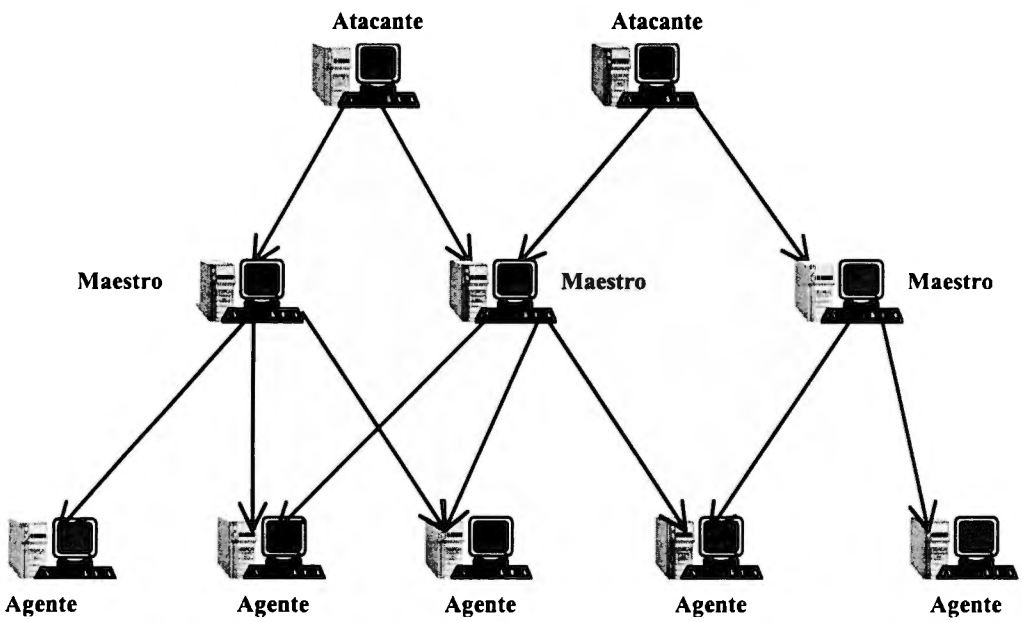


Figura 2.5

La comunicación entre el Maestro y el Agente se realiza de forma cifrada mediante el algoritmo CAST-256. [RFC_2612 99]. La clave se define en el momento de realizar la compilación, y se utiliza como clave de acceso cuando se ejecuta el cliente. Todos los datos cifrados se codifican en Base 64 antes de ser transmitidos. Con el fin de complicar un posible rastreo de la comunicación entre Maestro y Agente, ésta se mezcla con una serie de tramas trampa enviadas a direcciones IP aleatorias.[Barlow 00]

Tanto la comunicación Maestro-Agente como el ataque en sí mismo puede realizarse utilizando de forma aleatoria paquetes TCP, UDP o ICMP. Para finalizar hay que añadir el hecho de que el Maestro falsifica su dirección IP *(spoof)* en las tramas que envía. Al contrario de su predecesor, TFN2K es absolutamente silencioso y no contesta a los comandos que recibe. Los comandos no se basan en secuencia de caracteres, sino que van codificados en un *byte*, viajando como datos de la trama los parámetros particulares de cada comando.

El agente de TFN2K intenta ocultarse cambiando el contenido de *argv[0]*, es decir, cambiando el nombre del proceso. El nombre falso se define en el momento de compilación y puede variar de unas instalaciones a otras. Esto le permite camuflarse como un proceso normal, por lo que difícilmente podrá detectarse en una simple revisión de la tabla de procesos activos. [Barlow 00]

En cualquier caso ha de destacarse lo sofisticado y complejo del desarrollo del TFN2K, así como la dificultad que implica su localización. Se han encontrado Agentes en plataformas Linux, Solaris e incluso Windows NT. En cualquier caso, la herramienta es fácilmente portable a otras plataformas. Por lo que se ha visto, la detección de TFN2K resulta a priori muy compleja por no decir que imposible, pero como todo en la vida, también tiene su "talón de Aquiles". Puede ser que por un descuido, o por un simple error, en la codificación a Base 64 siempre aparece una marca al final de cada paquete. No se tiene claro el objetivo, pero al final de cada trama se introduce una colección de ceros (entre 1 y 16) que al ser codificados en Base 64 quedan como 0x41 (carácter A). De esta forma, el número de 0x41 que aparece al final de cada paquete es variable, pero siempre aparece por lo menos uno. La presencia de esta marca permite rastrear y localizar los paquetes de comandos. Otros errores que pueden ayudar en la detección de tramas generadas por TFN2K son:

- . La longitud de los paquetes UDP (la que aparece en la cabecera UDP) es tres bytes mayor que la real.
- . La longitud de las cabeceras TCP (la que aparece en la cabecera TCP) es siempre cero, lo que nunca podría ocurrir.
- . Los *checksums* de las tramas UDP y TCP no incluyen los 12 bytes de las pseudo-cabeceras y por lo tanto son incorrectos.

2.2.4. STACHELDRAHT.

Esta herramienta de ataque por negación de servicio fue detectada entre finales de septiembre y principios de octubre de 1999 [CERT_inc 99]. Tanto en sistemas europeos como norteamericanos El término de origen alemán Stacheldraht podría traducirse por *"alambre de púas"*. Combina características de Trinoo y TFN, y añade mecanismos de cifrado en la comunicación entre el cliente y el conductor, así como mecanismos de actualización automática de los agentes. [Dittrich_stach 99]

Su estructura, similar a los anteriores sería:

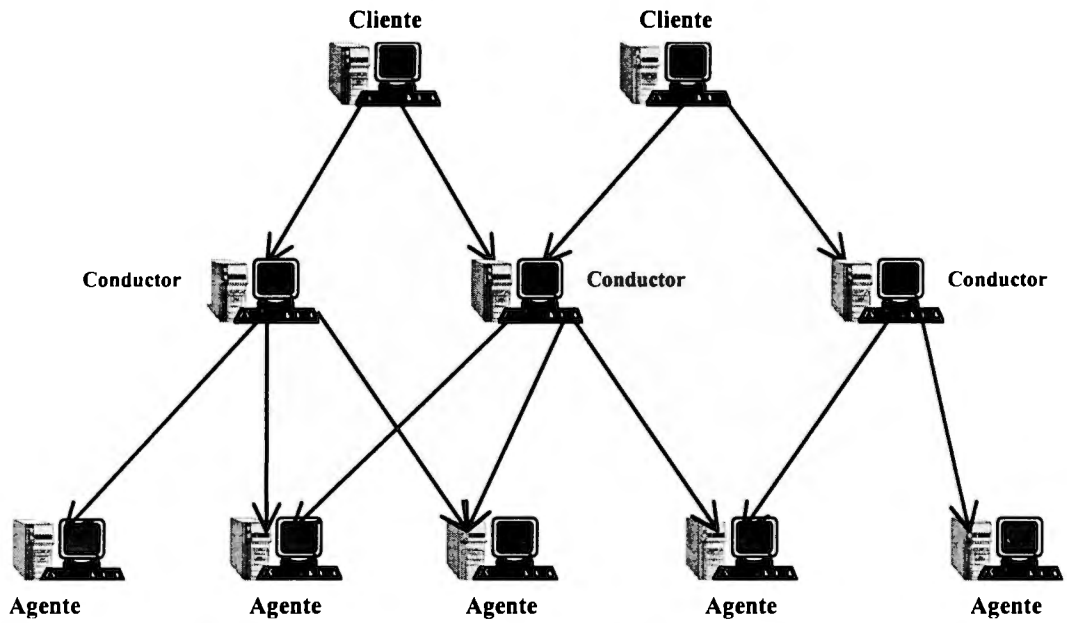


Figura 2.6

Algunos analistas consideran Stacheldraht como la competencia a TFN2K, pues presentan muchas similitudes en cuanto a comportamiento y facilidades: negación de servicio mediante avalancha de tramas ICMP, SYN y UDP, así como ataques mediante técnicas de amplificación de *broadcast (smurf)*. [Dittrich_stach 99]

Al contrario que la primera versión de TFN, en dónde la conexión entre el atacante y el cliente se transmitía sin cifrar, Stacheldraht dispone de un mecanismo similar a un Telnet (Stacheldraht Term) para la comunicación del cliente con el conductor que incluye cifrado mediante el uso de clave simétrica. Una vez establecida la comunicación entre el cliente y el conductor, se solicita un password que está cifrado mediante *crypt()*. A partir de ese momento toda la comunicación se realiza de forma cifrada mediante el algoritmo Blowfish.

El Stacheldraht se localizó inicialmente en forma binaria en sistemas Solaris. Un posterior análisis de los fuentes ha demostrado que también puede ejecutarse en entornos Linux, aunque no parece funcionar demasiado bien. [Dittrich_stach 99]

La comunicación entre los distintos niveles de realiza de la siguiente forma:
Cliente a Conductor: puerto 16660/TCP
Conductor a/desde Agente: puerto 65000/TCP, ICMP_ECHOREPLY

La mayor novedad que presenta Stacheldraht respecto a otras herramientas anteriormente analizadas, es la posibilidad de ordenar a los agentes su actualización. Para ello se utiliza el comando *rcp* (514/tcp) sobre una cuenta robada en cualquier máquina de la red. Los agentes borran la actual copia del programa, descargan la nueva versión y arrancan ésta usando *nohup*. En ese momento finaliza la ejecución de la antigua copia. En el momento de arranque de un agente, éste intenta leer un archivo de configuración en el que se le indica qué conductores le pueden

controlar. Este archivo contiene una relación de direcciones IP y está cifrado mediante Blowfish. Para los casos en que falle la localización del mencionado archivo, el propio agente lleva definido en el código una serie de direcciones que debe usar por omisión.

Una vez que el agente ha arrancado y dispone de la lista de conductores, comienza a transmitir tramas del tipo ICMP_ECHOREPLY con ID 666 y conteniendo en el campo de datos la palabra "skillz". Todos aquellos conductores que reciben esta trama contestan con otra del mismo tipo, con ID 667 y en el campo de datos la palabra "ficken". El diálogo entre conductor y agente se mantiene de forma periódica, lo que permite detectar la presencia de Stacheldraht mediante la monitorización pasiva de la red a través de un *sniffer*.

2.2.5. SHAFT.

Puede considerarse de la misma familia de herramientas que las analizadas anteriormente, y aunque ha sido de las últimas en detectarse, se piensa es contemporánea a TFN por su modo de operar y mecanismos de control. De hecho, su estructura básica es similar: [Sven_shaft 00]

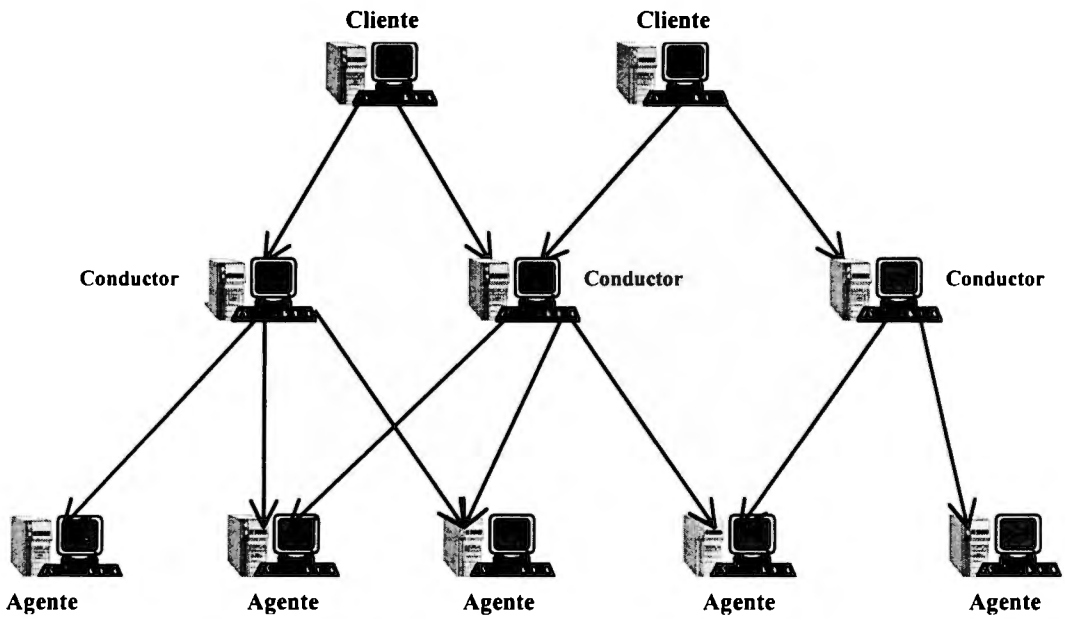


Figura 2.7

El Shaft fue localizado a finales de noviembre de 1999, y sólo se dispone de los fuentes del módulo agente, por lo que hay ciertas opciones que no se conocen con exactitud, por lo que ha sido necesario deducir su utilidad. La comunicación entre los distintos niveles de realiza de la siguiente forma: [Sven_shaft 00]

Cliente a Conductor: puerto 20432/TCP
Conductor a Agente: puerto 18753/UDP
Agente a Conductor: puerto 20433/UDP
Una de las novedades que presenta esta herramienta es el uso de *tickets* para garantizar el control sobre los agentes. Tanto el *password* como el *ticket* deben ser correctos para que un agente acepte

las peticiones que le puedan llegar. Tanto el conductor como el agente disponen de su propio conjunto de comandos. Aunque el atacante sólo interactúa con el conductor mediante comandos a través de una conexión Telnet. A través del análisis del código fuente se ha podido detectar la existencia de un cliente por defecto, y definido de la siguiente forma:
#define MASTER "23:/33/75/28"
que restando 1 al valor decimal de cada carácter Cifrador de Cesar (que funciona reemplazando cada carácter por otro del mismo alfabeto que ocupa un número fijo de posiciones adelante o atrás) obtendremos la dirección IP 129.22.64.17, que corresponde a electrochem1.echem.cwru.edu.

Por otra parte, el programa por sí mismo intenta camuflarse como un proceso habitual de un sistema Unix, como puede ser por ejemplo httpd. Los autores de Shaft han demostrado tener un interés muy especial por disponer de estadísticas. En concreto, el radio de generación de paquetes de cada uno de los agentes. Es posible que esta información les permita optimizar el número de agentes necesarios para ejecutar un ataque, o añadir más en caso de disminuir el nivel estimado de carga para que el ataque proporcione los resultados esperados.

2.2.6. MSTREAM.

En el segundo trimestre del año 2000 apareció esta herramienta distribuida de negación de servicio, y se ha detectado en Universidades Americanas. Ha sido diseñada para bloquear una red ahogando determinados sistemas mediante la generación de gran cantidad de tramas.
Su estructura es muy similar a los sistemas anteriormente citados: un módulo controlador y un módulo agente. El controlador es el encargado de gestionar las relaciones con los agentes. De esta forma, un atacante se conecta con el controlador mediante una sesión Telnet para controlar a los agentes. [Dittrich_mst 00]

El tipo de ataque que generan los agentes es una modificación del ataque conocido como "stream.c", pues la mayor parte del código del agente se basa en dicho programa. El agente envía paquetes TCP ACK al sistema que es objeto del ataque, aunque con la particularidad que dichas tramas se encaminan a puertos seleccionados de forma aleatoria y conteniendo una dirección IP de remitente falsa. Un ataque de este tipo presenta los siguientes síntomas: El sistema objeto del ataque baja su rendimiento debido al consumo de CPU por el tráfico de red que debe atender. Se observa un consumo elevado de ancho de banda en la red como consecuencia del propio ataque. El sistema atacado ocupa aún más ancho de banda al intentar contestar con tramas TCP RST a los falsos remitentes de las tramas TCP ACK. Los *routers* contestarán a la víctima con tramas ICMP indicando que el destinatario de la trama TCP RST no existe, lo que también consume aún más ancho de banda.

Aunque este tipo de ataque proviene de un único sistema no suele producir grandes efectos en el sistema atacado, pero cambia el panorama cuando son varios los sistemas atacados y muchos los atacantes, pues sólo tiene un desenlace: la saturación de la red, si no la caída del sistema atacado, y por consiguiente la negación de servicio, que es el objetivo final. La arquitectura de este sistema es similar a los anteriormente vistos:

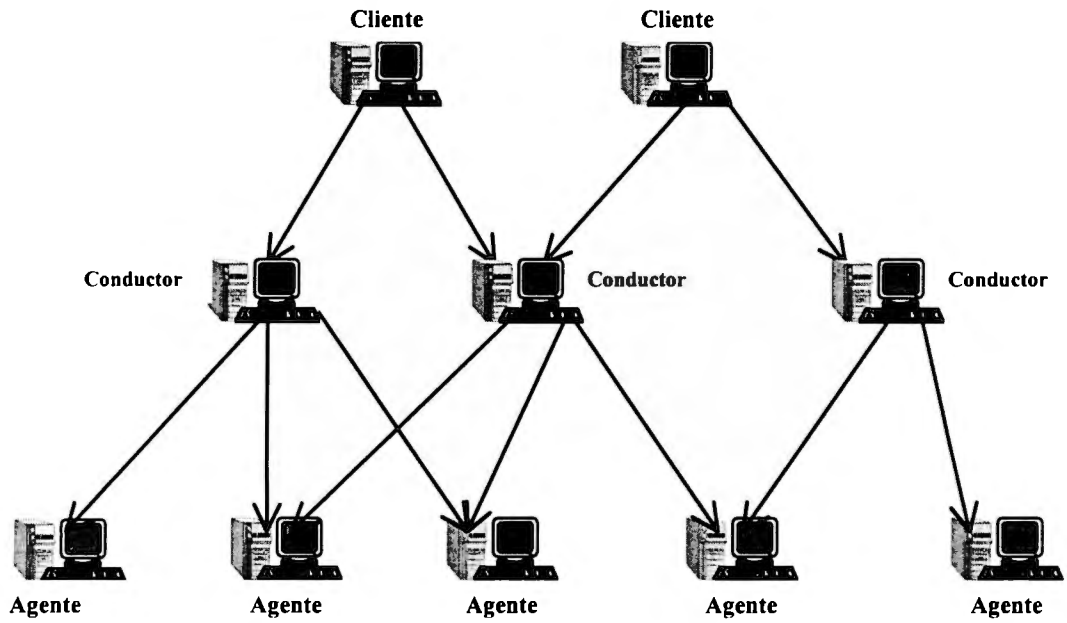


Figura 2.8

El cliente es la máquina que el atacante emplea para lanzar el ataque. El conductor coordina a todos los agentes. Y son éstos los que realizan el ataque a la víctima. Cada conductor puede coordinar un número indeterminado de agentes, y cada agente puede estar coordinado por un número indeterminado de conductores. Los agentes necesitan ejecutar con privilegio de root dado que utilizan *sockets* del tipo SOCK_RAW.

Se han encontrado tres versiones de esta herramienta, y en cada una de ellas varían los puertos y los passwords utilizados para la comunicación entre los distintos componentes.
Basándonos en la versión que de forma anónima se publicó en BugTraq, el conductor escucha por el puerto 6723/TCP, y el password de identificación es "sex". El conductor también escucha por el puerto 9325/UDP para permitir que los agentes puedan registrarse. [Dittrich_mst 00]

Los agentes pueden transmitir dos tipos distintos de paquetes. Uno es un "pong", como respuesta a una petición "ping". El otro es un "newserver", indicando que la dirección IP indicada se añade a la lista de agentes. Dicha lista se mantiene en el archivo".sr". Las direcciones IP se codifican añadiendo 50 al valor ASCII de cada carácter de la dirección IP (Cifrador de Cesar):
"138.100.14.35" -> "cej`cbb`cf`eg"
Mediante el comando *cat .sr | tr 'b-k`' '0-9.' | sed 's/<$//'* podrá ver en claro el contenido del archivo.sr.
En la versión a la que se ha tenido acceso la gestión de la lista de agentes es bastante deficiente, dado que si un agente arranca varias veces éste aparecerá otras tantas veces en la lista. Por otra parte, cada agente lleva incluido en el propio código la lista de posibles conductores autorizados, con un máximo de tres, lo que obliga a definirlos en el momento de compilar.

Los agentes atienden por el puerto 7983/UDP los posibles comandos que les puedan transmitir los controladores. A parte del comando "ping" anteriormente citado, pueden recibir el comando "mstream", cuyo formato es:

mstream/a1.b1.c1.d1:a2.b2.c2.d2: .../T

dónde ax.bx.cx.dx representan las direcciones IP de los sistemas que deben ser atacados, y T representa la duración del ataque expresado en segundos.
Existe también el comando "stream", que es similar a "mstream", pero que sólo permite lanzar el ataque a una única dirección IP, y en este caso la dirección IP del atacante es la real y no una falsa.

2.2.7. WINTRINOO

WinTrinoo fue anunciado públicamente por primera vez por el equipo Razor de Biendview. WinTrinoo es la versión para Windows de Trinoo y es capaz de realizar casi todos los ataques que efectúa Trinoo. La herramienta es un Troyano que, normalmente, recibe el nombre de service.exe (si no ha sido renombrado) y su tamaño es de 23,145 bytes. Tenga cuidado de no confundir el archivo "service.exe" de WinTrinoo con el archivo "services.exe" [Stuart04 01]

Una vez que se haya puesto en marcha el ejecutable, añadirá un nuevo valor a la clave Run del Registro de Windows para permitir que se reinicie el ataque cada vez que haga lo propio con el equipo:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run System Services: REG_SZ: service.exe

Naturalmente, este valor en particular sólo se podrá ejecutar si el archivo "service.exe" se encuentra en algún lugar de la ruta de acceso. WinTrinoo escucha en los puertos TCP y UDP 34555. [Stuart04 01]

Para detectar WinTrinoo, podrá escanear su red (por ejemplo con nmap), en busca de los puertos TCP o UDP 34555 que estén abiertos o intentar localizar un archivo en sus sistemas que tengan el nombre "service.exe" (aunque también podrá adoptar otros nombres) y un tamaño aproximado de 23,145 bytes. Además de esta técnica manual, podrá emplear un programa antivirus como el Norton Antivirus de Syamantec, que eliminará automáticamente dicho archivo.

2.3 MUTACIONES DE ATAQUES DDOS

A continuación describimos las principales características de algunas herramientas o programas DDOS (diferentes a las convencionales Trinoo, TFN, TFN2K, Stacheldraht, Shaft Mstream), que están siendo utilizados para efectuar nuevos ataques distribuidos de negación de servicio en Internet.

2.3.1 TRINITY V3

Trinity v3, es una poderosa herramienta DDOS, fue encontrada en más de 400 servidores, lo que representa una amenaza de potenciales ataques, según el grupo de investigación de Internet Security Systems Inc.'s X-Force. [Diarioti_Tri 00]

Trinity v3 no es un virus, por lo que se cree que hackers instalan la herramienta forzando su entrada en el sistema de Linux que desean usar a modo de "zombie" para efectuar el ataque.

"Cuatrocientos zombies son suficientes para tumbar un gran sitio de comercio electrónico, si es que no tienen las herramientas de detección de intrusión apropiadas", dijo Chris Rouland, director de X-Force. [Diarioti_Tri 00]

De acuerdo a X-Force, Trinity es controlado vía IRC (Internet Relay Chat), y en la versión que fue examinada, el agente binario es instalado en un sistema Linux en /usr/lib/idle.so.

Cuando idle.co es iniciado, se conecta a un servidor Undernet IRC en puerto 6667.

Debido a que Trinity no escucha en ningún puerto, es difícil de detectar las actividades de las herramientas a menos que los administradores de los sistemas busquen el tráfico sospechoso en IRC.

2.3.2 I-WORM.FOG

Tipo: Gusano[7] de Internet y Caballo de Troya

Comportamiento: Este gusano en formato Win32, posee habilidades de troyano de acceso remoto por la puerta trasera (backdoor), y puede utilizarse para participar de ataques del tipo DDOS. Es un ejecutable en formato PE EXE, escrito en Delphi, de unos 180 Kb, comprimido con la utilidad UPX. Descomprimido, ocupa unos 500 Kb. [Zonaluz 01]
El gusano se envía a si mismo a otras computadoras, adjunto a mensajes como un archivo con el nombre de AntiVirus.exe, y es en esa forma que puede llegar a nuestra computadora:

Asunto: I think that you sent me a virus.. heres a cleaner Texto: I took my computer to the shop and they ran this, and told me to send it to you.. hope this helps.Archivo adjunto: AntiVirus.exe (180 Kb) Para propagarse, utiliza rutinas MAPI para conectarse a las aplicaciones de correo electrónico.

También se reporta a un canal de IRC, en donde informa de su presencia junto a otros datos de la máquina infectada, de modo que permite activar sus rutinas de troyano del tipo backdoor, y sus habilidades para producir ataques DDOS. Todo ello es administrado en forma remota por el atacante que controle el troyano luego de recibir esa información. Para propagarse, el gusano

---

[7] Un gusano es un programa que se propaga copiándose a sí mismo en cada host de la red: su propósito es accesar ilegalmente sistemas.

examina la bandeja de entrada en busca de todos los mensajes que contengan al menos un archivo adjunto, y los responde con un mensaje infectado con el archivo AntiVirus.exe, y con las demás características vistas anteriormente. [Zonaluz 01]

Para protegerse y hacer más difícil su detección y limpieza, el gusano borra los archivos NETSTAT.EXE y REGEDIT.EXE del directorio de Windows. El primero es una implementación del comando Netstat de los protocolos TCP/IP, que permite mostrar estadísticas de estos protocolos y sus conexiones actuales, pudiendo ser usado para detectar la actividad de un troyano. El segundo es el editor del registro de Windows, lo que impedirá la modificación del mismo.

El gusano también busca antivirus, así como otros procesos que estuvieran activos, e intenta finalizarlos.

2.3.3 DDOS/APBOT@MM. ATAQUE DDOS, BORRADO DE ANTIVIRUS, ETC.

Nombre: DDoS/Apbot@mm
Tipo: Gusano de Internet y Caballo de Troya
Alias: I-Worm.Fog.B
Fecha: 1/jul/01
Variante: 27/jul/01
Tamaño: 380,416 bytes, 421,888 bytes

Este troyano fue reportado primeramente como I-Worm.Fog , pero una nueva variante ha sido identificada en algunos grupos de noticias según reporto el AVERT (McAfee).
Se trata de un bot de IRC, y un gusano de envío masivo a través del correo electrónico. También es capaz de borrar varios programas de seguridad (antivirus y firewalls).Compromete la seguridad de la computadora infectada, y de otras computadoras conectadas a Internet, ya que puede ser utilizado para participar de ataques del tipo DDOS. [Tripod 01]

Puede ser recibido en un mensaje con la siguiente característica:

Asunto: Virus Alert! Texto: Businesses of all kinds have suffered today as a virus has been unleashed, please find the attatched cleaner and run it. You cannot tell if you have this virus until you run the cleaner.Archivo adjunto: Regsrv32.exe

Si el usuario ejecuta el archivo adjunto, el troyano se copia a si mismo en la carpeta correspondiente al sistema de Windows:
C:\WINDOWS\SYSTEM\regsrv32.exe

Es importante notar que en esa misma ubicación, existe un archivo legítimo de Windows, de nombre parecido (REGSVR32.EXE), y la única diferencia (que puede pasar desapercibida), es el intercambio de sólo dos letras, RV por VR.

Luego, el troyano modifica la siguiente rama del registro, para ejecutarse en el reinicio de Windows:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
RegPath = C:\WINDOWS\SYSTEM\regsrv32.exe

Para protegerse y hacer más difícil su detección y limpieza, el gusano también borra los archivos NETSTAT.EXE y REGEDIT.EXE del directorio de Windows:

C:\Windows\NETSTAT.EXE & C:\Windows\REGEDIT.EXE

El primero es una implementación del comando Netstat de los protocolos TCP/IP, el cual permite mostrar estadísticas de estos protocolos y sus conexiones actuales, pudiendo ser usado para detectar la actividad de un troyano. El segundo es el editor del registro de Windows, la falta del cual impedirá la modificación del mismo. Un archivo de texto, conteniendo nombres de usuarios de IRC y contraseñas, es descargada desde el sitio http://c0ntrol.virtualave.net. Esta información es utilizada para conectarse a un servidor de IRC. Una vez conectado, el sistema infectado se mantiene a la escucha de instrucciones enviadas por el atacante desde el mismo servidor de IRC, a través del puerto 6667. [Tripod 01]

2.3.4 TROJ/SLACK

Alias: Backdoor.Slackbot, DDOS/Slack
Tipo: Backdoor Trojan
Comportamiento: Troj/Slackbot es un acaballo de troya "de puerta trasera" el cual puede ser configurado para conectarse a cualquier servidor IRC. Cuando se conecta, ensambla un canal preconfigurado de IRC y espera por futuras instrucciones. [Zonaluz 01]

2.3.5 W32/NIMDA

Esté virus afecta sistemas Microsoft Windows 95, 98, ME, NT, y 2000. [CERT_Nim 01]

El pasado 17 de septiembre del 2001, el virus NIMDA comenzó a atacar las redes públicas de México.

El virus catalogado como "de alto riesgo" tiene la particularidad de propagarse a través del correo electrónico y de sitios que utilicen tecnología Microsoft, sin que el usuario lo note y sin que el usuario siquiera tenga que abrir el correo electrónico infectado. [Activamente 01]

Aunque existe la sospecha de que se trato de un ataque a los Estados Unidos, relacionado a los actos terroristas en Nueva York y Washington, el FBI aún no encuentra relación directa entre ambos sucesos.

2.3.5.1 Funcionamiento de NIMDA

El virus de tipo "gusano" se propaga especialmente de dos formas:

1) los correos generados por el gusano (NIMDA) se especifican como contenido de tipo "audio/x-wav", con un archivo ejecutable adjunto (Attachment). Cuando el correo es abierto el archivo adjunto es ejecutado aún sin que el usuario se haya dado cuenta (no es necesario que el usuario ejecute el archivo). [Activamente 01]

2) Una vez infectado, el virus agrega un breve código HTML con un programa Javascript que abre una nueva ventana que contiene el correo maligno (tomado del archivo README.EML). Sucedido esto, cuando el código HTML es visto (local o remotamente) por otra computadora, ésta queda infectada también.

Una vez infectado, el sistema es utilizado para buscar otros usuarios de computadoras para ser infectadas vía Internet. Como esto genera procesos de red muy intensos, las redes y ruteadores acaban por saturarse.

2.3.5.2 Daños que ocasiona

Aunque las computadoras infectadas no se ven afectadas sustancialmente, los perjuicios que NIMDA ocasiona son enormes porque satura las redes al intentar propagarse a través de ellas, ocasionando lentitud en redes en todo el Mundo. [Activamente 01]

A continuación se muestran gráficas de la sobrecarga de tráfico global obtenidas por el sistema de monitoreo de tráfico de datos (http://www.internettrafficreport.com):

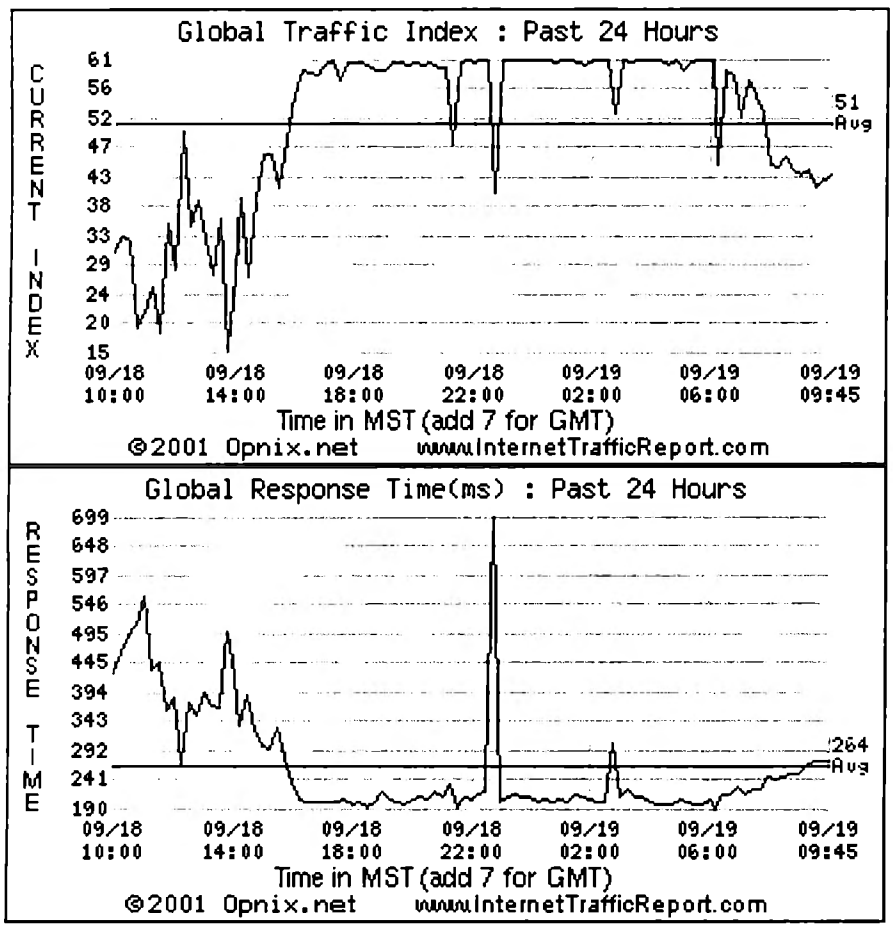


Figura 2.9

Internet Traffic Report monitorea el flujo de datos alrededor del mundo. Los datos son actualizados cada 15 minutos. Una prueba llamada "ping" es usada para medir el tiempo en un viaje redondo a lo largo de una ruta en Internet. Existen varios servidores en diferentes áreas alrededor del mundo que realizan el mismo ping al mismo tiempo. Cada servidor compara la respuesta actual con la pasada para determinar si la respuesta es buena o mala es una escala de 1 a 100.

"Traffic Index" es un número entre 0 y 100 donde 0 es el mas "lento" y 100 el mas "rápido". Esto es determinado al comparar la actual respuesta de un ping echo con todas las respuestas previas realizadas desde el mismo ruteador en los últimos 7 días. El número asignado de 0 a 100 depende si las repuestas fueron mejores o peores con respecto a las anteriores repuestas desde un mismo ruteador. El tiempo de respuesta esta dado en milisegundos y es el tiempo que tarda un paquete de datos en viajar de un punto A a B en viaje redondo. El número que se muestra en las gráficas (51 y 264 avg) indican los valores promedio en el lapso de tiempo indicado, es decir de las 10 hrs. del día 18 de septiembre a las 9:45 hrs. del 19 del mismo mes.

2.3.6 CODE RED.

Según la rutina que desempeña Code Red, a partir de las 20:00 horas en EEUU del día 19 de agosto del 2001 se lanzaron, supuestamente, ataques distribuidos de negación de servicio, al site de la Casa Blanca. No obstante, todo pareció indicar, y así lo confirmaron los expertos del Centro de Protección de Infraestructura Nacional (NIPC) dependiente del FBI, que su efecto fue relativamente reducido. Muchos administradores a principios del mes de agosto del 2001 instalaron los parches recomendados por Microsoft lo que provocó, que se haya limitado la propagación del virus y como consecuencia una reducción considerable en el número de servidores infectados. Por este motivo, los equipos "zombies" que le ayudaron a lanzar ataques distribuidos de negación de servicio carecieron de fuerza y se prevé que su actuación no llegue muy lejos. [Virusprot Red 01]

Contra Code Red toda prevención es poca. Microsoft, además de recomendar el uso del parche que corrige las vulnerabilidades del software ISS[8], puso a disposición de todos los usuarios dos nuevas herramientas[9] que facilitan la detección de agujeros en equipos y sistemas y facilita su reparación. Los usuarios en casa, pueden escanear sus equipos utilizando el botón de "Scan Now" que se encuentra en la página web http://www.microsoft.com/TechNet/mpsa/content.asp

En cuanto a los últimos afectados por Code Red II, un virus similar a Code Red pero cuya misión no es lanzar ataques DDOS sino dejar puertas traseras abiertas en los servidores que infecta, destaco la intrusión en sites del gobierno de Japón. En los últimos días de agosto del 2001, algunos proveedores por cable estadounidenses como Time Warner Cable, AT&T y Cox Communications experimentaron una mayor lentitud en sus conexiones puesto que analizaron la red en busca del gusano lo que genero un retraso en el tráfico. [Virusprot Red 01]

2.3.7 CODE BLUE.

Este gusano exploto un agujero de seguridad del software ISS de Microsoft diferente a la elegida por Code Red y para ésta hay parche desde del año pasado. [Virusprot Blue 01]

Coincidiendo con la publicación de un estudio de la consultora de seguridad Netcraft sobre el aumento de seguridad en la Red aparece Code Blue, un hermano de Code Red que exploto el agujero de seguridad conocido como "Web server folder traversal vulnerability".

Volviendo al estudio, para el cual se observo el comportamiento de miles de servidores desde finales de julio del 2000, se afirmo que Code Red constituyo un "catalizador de seguridad en Internet" puesto que "obligo" a los administradores a revisar sus sistemas y estar mucho más alertas de lo que antes lo estaban para evitar que se repitieran las pérdidas económicas cercanas a los 2.600 millones de dólares. Pese a estas conclusiones, las medidas contra los gusanos nunca son suficientes. Así lo demuestra la acción de Code Blue, que desde su aparición ya ha sumado un buen número de víctimas. [Virusprot Blue 01]

---

[8] Por sus siglas en inglés: Internet Information Server
[9] Disponibles en http://www.virusprot.com/Nt170822.html

En principio, Code Blue sólo afecta a servidores que trabajen con Windows NT y 2000 que tengan instalado el software ISS 4 o 5 de Microsoft. La diferencia estriba, como ya hemos explicado, en la vulnerabilidad que aprovecha para introducirse en el sistema cuyo parche está disponible desde el mes de octubre del 2000. El agujero de seguridad permite al código el acceso a carpetas y archivos de un equipo a través de una dirección URL construida para ese fin. A partir de ese momento, se permite el acceso remoto de la computadora afectada, incluyendo la capacidad de poder modificar o eliminar los archivos que se deseen, tanto del equipo como del servidor.

El virus se transporta en los archivos SVCHOST.EXE, HTTPPEXT.DLL y D.VBS, que se copian en el directorio raíz del equipo. El primero de ellos modifica el registro de Windows para poder ejecutar el gusano cada vez que se reinicie el sistema. D.VBS va más allá y borra los restos de Code Red que puedan quedar en la memoria de la PC e incluso crea ciertas defensas que luchen contra posibles futuros ataques de este gusano. Los expertos consideran a Code Blue una mayor amenaza que Code Red puesto que absorbe muchos más recursos del sistema lo que implica irremediablemente la caída del servidor.

Otra novedad que presenta estaría en que, utiliza las computadoras que infecta para convertirlos en "zombies" desde los cuales lanza ataques distribuidos de negación de servicio a una empresa de seguridad china cuya dirección web es http://www.nsfocus.com. El ataque DDOS se realizo todos los días de diez a once de la mañana, el resto del tiempo lo dedicaba a propagarse buscando servidores vulnerables. [Virusprot Blue 01]

Las principales casas de software de seguridad ya han incluido a Code Blue en sus bases de datos. El origen de este gusano es desconocido pero hay quien habla de una posible venganza puesto que, expertos norteamericanos confirmaban el nacimiento de Code Red en una universidad china.

3 DEFENSAS CONTRA LOS ATAQUES DDOS

3.1 PROPUESTA BASADA EN EL RFC-2827

"Filtrado de entrada a red: Cómo minimizar los ataques de negación de servicio que emplean una técnica de falsificación de direcciones fuente IP" [RFC_2827]

3.1.1 INTRODUCCIÓN

Esta técnica es de gran utilidad para protegerse contra los ataques de negación de servicio y especialmente contra los ataques DDOS ya que entre los ataques disponibles con Tribe Flood Network (TFN) y Trinoo se encuentran: ICMP, Smurf, UDP e inundaciones SYN, los cuales utilizan falsificación de direcciones IP.
De manera análoga la herramienta Stacheldraht combina las características de Trinoo con aquellas presentes en TFN para realizar sus ataques, (ver capítulo dos , para un análisis de estas herramientas).

Esta técnica describe un simple y efectivo método para filtrar el tráfico de ingreso a la red y prohibir a los atacantes que usen direcciones IP falsas en nuestras instalaciones o ser propagadas detrás de un Proveedor de Servicios de Internet ISP.

Aunque los ataques DOS han sido bien conocidos desde hace ya un buen tiempo, defenderse de ellos ha sido una constante preocupación. La técnica propuesta no hace absolutamente nada contra ataques flooding[10] los cuales se originan desde direcciones IP validas, pero si prohíbe a un atacante dentro de su red lanzar un ataque utilizando direcciones IP falsas, que no se ajustan a las reglas del filtrado de entrada. Todos los proveedores de conectividad a Internet deben implementar el filtrado descrito aquí ya que prohíbe a los atacantes usar direcciones de origen falsas que no están en un rango legítimo de sus direcciones IP válidas. [RFC_2827]

[10] Inundación

El beneficio adicional de implementar este tipo de filtrado es que esto habilita al origen y se puede seguir fácilmente su rastro hasta el origen verdadero, dado que el atacante tendrá que utilizar una dirección IP válida, legitima y alcanzable.

3.1.2 PLANTEAMIENTO DEL PROBLEMA

Un simple diagrama simplificado del problema TCP SYN flooding es descrito abajo:

204.69.207.0/24
host <----- router <--- Internet <----- router <-- attacker

TCP/SYN
<----------
Source: 192.168.0.4/32
SYN/ACK
no route

TCP/SYN
<----------
Source: 10.0.0.13/32
SYN/ACK
no route

TCP/SYN
<----------
Source: 172.16.0.2/32
SYN/ACK
no route

[etc.]

Asumimos que :

- "host" es la máquina víctima.
- El atacante reside dentro del prefijo "valido", 204.69.207.0/24.
- Se lanza el ataque utilizando direcciones de origen cambiadas aleatoriamente, en este ejemplo las direcciones de origen no están generalmente presentes en las tablas de los ruteadores en Internet, y por lo tanto, son inalcanzables. Sin embargo, cualquier prefijo inalcanzable puede ser utilizado para perpetrar este ataque.

Algo digno de mencionarse es que en caso de que la dirección origen sea falsificada para aparentar ser originada desde una red legítima, en tal caso, un atacante utilizando una dirección válida de red podría causar estragos haciendo que el ataque aparentase provenir de una organización que, de hecho no originó el ataque y es completamente inocente. En tal situación el

administrador del sistema bajo ataque puede inclinarse por filtrar todo el tráfico proveniente del aparente origen de ataque. Agregando tal filtro provocará una negación de servicio a sistemas legítimos, no hostiles. En este caso el administrador del sistema bajo ataque se convierte involuntariamente en cómplice del atacante. [RFC_2827]

Para complicar más los problemas, los ataques TCP SYN flood podrían resultar en paquetes SYN-ACK paquetes enviados a uno o varios hosts que no tienen participación en el ataque, pero se convierten en víctimas secundarias. Esto permite al atacante abusar de dos o más sistemas al mismo tiempo.

Ataques similares se han llevado acabo usando UDP y ICMP flooding.

UDP flooding ataca utilizando paquetes falsificados para probar y conectar el servicio de carga UDP con el servicio de eco UDP en otra localización. Los administradores de sistemas nunca deben permitir que paquetes UDP destinados a puertos de diagnóstico alcancen sus sistemas desde fuera de su dominio administrativo.

El otro ataque (ICMP flood), utiliza una herramienta insidiosa en los mecanismos IP de replica de broadcast de subred. Este ataque se vale de un ruteador sirviendo una gran red multiacceso de broadcast para estructurar una dirección IP de broadcast (como una destinada para 10.255.255.255) en una capa 2 de trama (frame) broadcast (para ethernet, FF:FF:FF:FF:FF:FF). El NIC físico de ethernet (capa MAC física, específicamente) sólo escuchará un número selecto de direcciones en una operación normal. La dirección MAC que comparten todos los dispositivos en operaciones normales es la difusión del medio, o FF:FF:FF:FF:FF:FF.
En este caso, un dispositivo tomará el paquete y enviará una interrupción al proceso. Así, un flood de estos marcos de difusión consumirán todos los recursos disponibles en un sistema final. Es recomendable que los administradores aseguren sus ruteadores frontera para que no permitan entregar paquetes broadcast directamente a través de sus ruteadores por omisión.

Cuando un ataque TCP SYN es lanzado utilizando direcciones de origen inalcanzables, el host víctima intenta reservar recursos a la espera de una respuesta. El atacante repetidamente cambia la dirección de origen falsa en cada paquete nuevo enviado, agotando así los recursos adicionales del host. [RFC_2827]

Alternativamente, si el atacante utiliza algún otro host valido como dirección de origen, el sistema bajo ataque enviará un gran número de paquetes SYN/ACK a lo que cree que es el autor de la secuencia de establecimiento de conexión. De está forma, el ataque hace daño a dos sistemas: el sistema víctima destino, y también el sistema que cuya dirección falsificada está utilizando realmente en el sistema de ruteado global.

Es decir en los ataques ICMP flooding, los atacantes envían peticiones ICMP a la víctima utilizando también direcciones falsas. Esta dirección es casi siempre la propia dirección de la víctima. La petición ICMP es transmitida a múltiples hosts de la red víctima. Estos responden en su momento, inundando a la víctima con sus respuestas. Esto puede ser pésimo si la red víctima contiene muchos hosts.

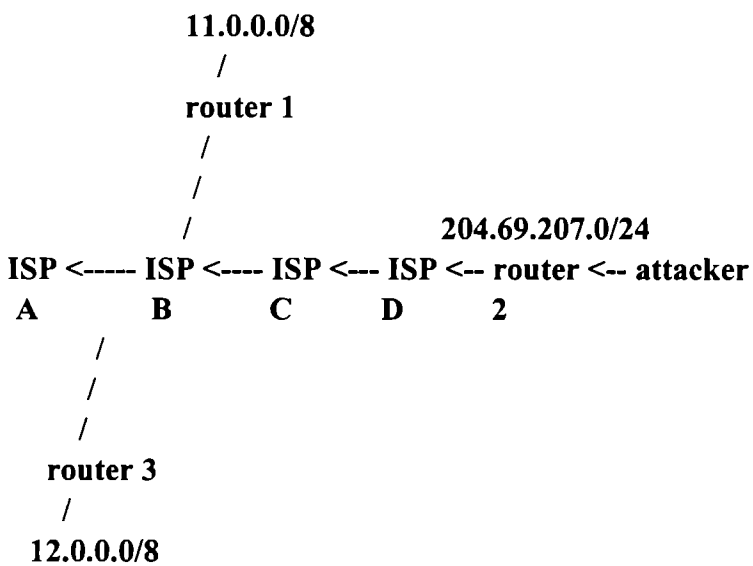
El resultado de ambos métodos de ataques es una disminución en el desempeño, o en el peor de los casos, una caída del sistema.

En respuestas a estas amenazas, muchos vendedores de sistemas operativos han modificado su software permitiendo a los servidores sostenerse ante los ataques con altos intentos de conexión o manteniendo bastantes conexiones en estado "semiabierto". Esto obviamente es bienvenido y es una parte necesaria de la solución general del problema. La filtración de ingreso puede tomar un buen tiempo en ser implementada completa y efectivamente, pero las extensiones del sistema operativo deben ser implementadas rápidamente.

3.1.3 RESTRINGIR EL TRÁFICO FALSIFICADO

Los problemas encontrados con este tipo de ataques son numerosos e incluyen limitaciones y defectos en las implementaciones de software del host, metodologías de ruteo, y el propio diseño del protocolo TCP/IP. [RFC_2827]

El problema de falsificación de direcciones origen puede ser virtualmente eliminado en un escenario de ataque como este:



En el ejemplo de arriba , el atacante reside dentro de 204.69.207.0/24, y tiene conectividad a Internet por el ISP D. Una entrada de tráfico en el enlace de ingreso de "router 2", que provee conectividad con la red del atacante, la técnica restringe el tráfico para permitir únicamente tráfico originado por direcciones de origen en el prefijo 204.69.207.0/24, y prohíbe a un atacante usar direcciones origen "invalidas" que residan fuera de su rango de prefijos.

En otras palabras, el filtro de ingreso en el "router 2" deberá checar:

IF Los paquetes de la dirección origen provienen dentro del rango **204.69.207.0/24**
THEN se envía como adecuado.

IF Los paquetes de la dirección origen provienen de cualquier otra dirección
THEN negar el paso del paquete.

Los administradores de la red deberán de registrar la información de los paquetes los cuales fueron detenidos. Esto provee una base para monitorear cualquier actividad sospechosa en la red.

Si no estamos seguros de que espacio de direcciones estamos usando en un site, entonces, se deberán filtrar al menos las direcciones origen IP privadas y reservadas. (RFC 1918). La "Autoridad de Números Asignados en Internet", Internet Assigned Numbers Authority (IANA), ha reservado los tres siguientes bloques de direcciones IP para el uso en Internet privadas:

10.0.0.0 - 10.255.255.255 (prefijo 10/8)
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)

Nos referiremos al primer bloque como "bloque de 24 bits", al segundo como "bloque de 20 bits" y al tercero como "bloque de 16 bits". Observe que (en la notación anterior a CIDR) el primer bloque no es más que un único número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos, y el tercer bloque es un conjunto de 256 números de red de clase C contiguos.
Una empresa que decida usar direcciones IP del espacio de direcciones definido en este documento puede hacerlo sin tener que coordinarse con la IANA o con un registro de Internet. De está manera el espacio de direcciones puede ser usado por muchas empresas. Las direcciones de este espacio de direcciones privado sólo serán únicas dentro de la empresa, o el conjunto de empresas que elijan colaborar sobre este espacio para que puedan comunicarse con las demás en su propia Internet privada.

La siguiente es una lista de direcciones origen que también deberán ser filtradas:

0.0.0.0/8 - Historical Broadcast
127.0.0.0/8 - Loopback
169.254.0.0/16 - Link Local Networks
192.0.2.0/24 - TEST-NET
224.0.0.0/4 - Class D Multicast
240.0.0.0/5 - Class E Reserved
248.0.0.0/5 - Unallocated
255.255.255.255/32 - Broadcast

Si usamos Network Address Translation (NAT), necesitamos ejecutar este filtro entre el mecanismo NAT y el ISP, debemos verificar también que la configuración del mecanismo NAT solamente traduzca direcciones usadas y autorizadas en el espacio de direcciones interno.

3.1.4 RESPONSABILIDADES

Un filtrado de está naturaleza puede interrumpir algunos servicios "especiales". Esta técnica está considerada con el objetivo de ofrecer dichos servicios especiales ISP; de cualquier modo, se necesitan considerar métodos alternativos de implementación de estos servicios, que eviten ser afectados por el filtrado de tráfico de entrada.

IP móvil , se ve específicamente afectada por filtros de tráfico de entrada, ya que el tráfico al nodo móvil es tuneleado, pero el tráfico desde el nodo móvil no es tunelizado. Esto resulta en paquetes del nodo móvil que tienen direcciones de origen que no concuerdan con la red dónde la estación está ligada. Para acomodar los filtros de entrada y otros asuntos, el grupo de trabajo de IP móvil desarrollo una metodología para "túneles inversos", esto provee un método para los datos transmitidos por el nodo móvil, para ser tuneleado al agente local antes de su transmisión a Internet. Existen beneficios adicionales al esquema de tuneleado inverso, incluyendo mejor manejo del tráfico de múltiple asignación. Estos sistemas de IP móvil son motivados para implementar este método de tuneleado inverso. [RFC_2827]

Como se mencionó anteriormente, mientras se filtra el tráfico de entrada se reduce drásticamente el éxito del falsificar la dirección de origen, esto no evita que un atacante use direcciones de origen falsificadas de otro host dentro del rango de prefijos permitidos en el filtro. Sin embargo asegura que cuando un ataque de está naturaleza ocurre, un administrador de red puede estar seguro de que el ataque se esta originando realmente dentro de los prefijos conocidos que están siendo mostrados. Esto simplifica el rastreo del culpable y en el peor de los casos el administrador tendrá que bloquear un rango de direcciones de origen, hasta que el problema sea resuelto.

Si el filtro de entrada es usado en un ambiente dónde se cuenta con DHCP o BOOTP, el administrador de red debería ser advertido para asegurar que los paquetes con dirección de origen de 0.0.0.0 y un destino de 255.255.255.255 sean permitidos para llegar al agente de

retransmisión en los ruteadores cuando sea apropiado. El alcance de la replicación de difusiones dirigidas debe ser controlado, de cualquier modo, y no arbitrariamente reenviados.

3.1.5 RESUMEN

El filtrado de tráfico de entrada en la periferia de las redes conectadas a Internet reducirá la efectividad de la falsificación de direcciones de origen en los ataque de negación de servicio. Los proveedores de servicios de red y administradores están implementando este tipo de filtro en sus ruteadores de su periferia, y se recomienda que todos los proveedores de servicio realicen esto tan pronto como sea posible. Además de ayudar a la comunidad de Internet en conjunto a vencer este método de ataque, esto puede ayudar a proveedores de servicios a localizar el origen del ataque si estos proveedores pueden demostrar categóricamente que su red ya tiene colocados filtros de ingreso en los enlaces con los clientes.

Los administradores de redes corporativas deben implementar filtros para asegurar sus redes corporativas no son la fuente de tales problemas. En efecto, el filtro puede utilizarse dentro de una organización para asegurar que los usuarios no causan problemas insertando incorrectamente direcciones de red equivocadas.

El filtro puede también, en la práctica, disuadir a un empleado disgustado de realizar ataques anónimos.

Es responsabilidad de todos los administradores de redes asegurarse de no ser, inconscientemente, la fuente de un ataque de esta naturaleza.

3.1.6 CONSIDERACIONES DE SEGURIDAD

La intención primordial de estas recomendaciones es incrementar las prácticas de seguridad e informar a toda la comunidad de Internet como pueden ser los Proveedores de Internet, Administradores de Redes Corporativas, etc. Si tenemos implementado un filtro de entrada, la oportunidad de un atacante de usar direcciones de origen falsificadas como un método de ataque serán reducidas significativamente. Aunque esto no detiene un ataque, permite fácilmente seguir el origen de un ataque y terminarlo rápidamente. Rastrear el origen de un ataque se simplifica cuando dicho origen es mas probable de ser "valido". Reduciendo el número y la frecuencia de ataques en Internet en conjunto, habrá mas recursos para rastrear los ataques que últimamente ocurren.
Se deberá filtrar también todo el tráfico que no tenga nada que ver con los servicios que se ofrecen.

3.2 EVITAR QUE LA RED SEA USADO COMO UN SITE DE AMPLIFICACIÓN BROADCAST.

El propósito de estas recomendación es asegurar que nuestra red no sea utilizada como un Site de amplificación broadcast para inundar otras redes con ataques DOS como Smurf.

Las acciones que deben ser llevadas acabo son la configuración del sistema (ruteadores, estaciones de trabajo, servidores, etc), con el propósito de que no reciban o reenvíen tráfico broadcast.

3.2.1 DESHABILITAR EL TRÁFICO IP BROADCAST EN TODOS LOS SISTEMAS

Los siguientes sistemas tienen por omisión deshabilitado el direccionamiento broadcast, sin embargo cuentan con la opción de habilitarlo.

- Cabletron SSR
- FreeBSD

- Microsoft Windows Workstation & Server 3.5 & 3.5.1

Para Windows NT 4, el comportamiento por omisión era responder a todos los paquetes broadcast, esto puede ser solucionado al instalar el Servicie Pack 4. La ultima versión de Service Packs para NT, puede ser obtenida en Microsoft. [Spack 01]

3.2.2 COMO PROBAR LA RED PARA DETERMINAR SI ES UN SITE DE AMPLIFICACIÓN.

Para saber si una red esta actuando como un site de amplificación, se puede usar el comando ping para enviar un paquete ICMP Echo Request a la dirección IP base de red y broadcast de la red o redes.

Quizás necesitemos conocer o verificar cuales son las direcciones IP base de red y broadcast. Podemos encontrar ayuda de gran utilidad para determinar estas direcciones para la red. en la tabla CIDR (Enrutamiento Interdominio Sin Clase). [CIDR 00]

A continuación se describe como usar y analizar la salida del comando ping para determinar si una red es un site de amplificación broadcast, en los Sistemas Operativos Solaris y Linux

Solaris
% /usr/sbin/ping -s <Network-or-Broadcast-IP-Address> 0 10

Este comando envía paquetes ICMP Echo Request con tamaño 0, espera 10 respuestas.

Si la red está actuando como un site de amplificación veremos algo como esto:
----PING Statistics----
2 packets transmitted, 10 packets received, 5.00 times amplification

Si la red no está actuando como un site de amplificación debemos ver esto "100% paquetes perdidos"
---PING Statistics----
10 packets transmitted, 0 packets received, 100% packet loss

Linux
% /bin/ping -c 10 -s 1 -q -b <Network-or-Broadcast-IP-Address>

Este comando envía paquetes ICMP Echo Request con un tamaño de datos de 1 byte, y espera 10 respuestas.

Si la red está actuando como un site de amplificación veremos algo como esto:
--- ping statistics ---
10 packets transmitted, 10 packets received, +369 duplicates, 0% packet loss

3.2.3 EXIGIR A LOS FABRICANTES QUE DESHABILITEN EL TRÁFICO BROADCAST DIRIGIDO IP.

Al comprar un nuevo sistema, debemos exigir al vendedor que deshabilite la recepción y el envío de paquetes dirigidos broadcast como se especifica en el RFC 2644. [RFC_2644]

De acuerdo al RFC 2644 un ruteador debe tener una opción de configuración que permita recibir paquetes broadcast dirigidos, sin embargo esta opción debe ser deshabilitada por omisión, en consecuencia el ruteador no debe recibir paquetes broadcast dirigidos a la red al menos que sean configurados específicamente por el usuario final. [RFC_2644]

Un ruteador debe tener una opción para habilitar el envío y recepción de paquetes broadcast dirigidos con prefijos de red. Las opciones por omisión deben bloquear el envío y recepción de broadcast dirigidos con prefijos de red.

Aplicar estas medidas de seguridad para el tráfico broadcast y las recomendaciones de filtrado de ingreso en la red (RFC 2827), reducirán significativamente la oportunidades y amenazas de que una red pueda ser dañada por los ataques DOS. Y los mas importante estas medidas pueden ser aplicadas inmediatamente y no requiere de grandes recursos para ser implementadas.

3.3 UNA PROPUESTA BASADA EN RUTEO

La siguiente técnica puede ser usada para incrementar la defensa contra los ataques DDOS en tiempo real, la solución esta basada en el ruteo y requiere infraestructura de red adicional. [Schapachnik 00]

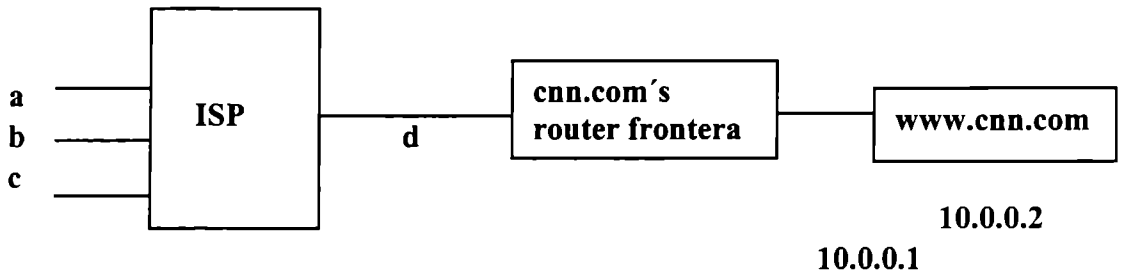
El problema con los ataques DDOS es que generalmente los paquetes vienen desde direcciones "spoofed" o falsificadas (cuando un atacante se hace pasar por la dirección IP de otro usuario) y poder rastrear la fuente se vuelve una tarea muy compleja, que por lo mismo requiere una enorme cantidad de tiempo.

Algunas medidas han sido propuestas, pero ellas están basadas en filtrar paquetes falsos en la red de origen del ataque como lo describe el RFC 2827, esta acción es importante para mitigar los ataques DDOS y debe implantarse antes de que se efectué un ataque DDOS. Sin embargo se confía la seguridad a terceros.

La técnica que se describe a continuación tiene el propósito de detener el ataque cuando éste ocurre, en un tiempo razonable. Esta propuesta se ilustra mediante el siguiente ejemplo.

Supongamos que cnn.com es un importante sitio web, asumimos que no estamos interesados en cualquier otro servicio mas que www, aunque este método puede ser aplicado para proteger otros servicios. Otra simplificación es que cnn.com tiene solamente un enlace a Internet.

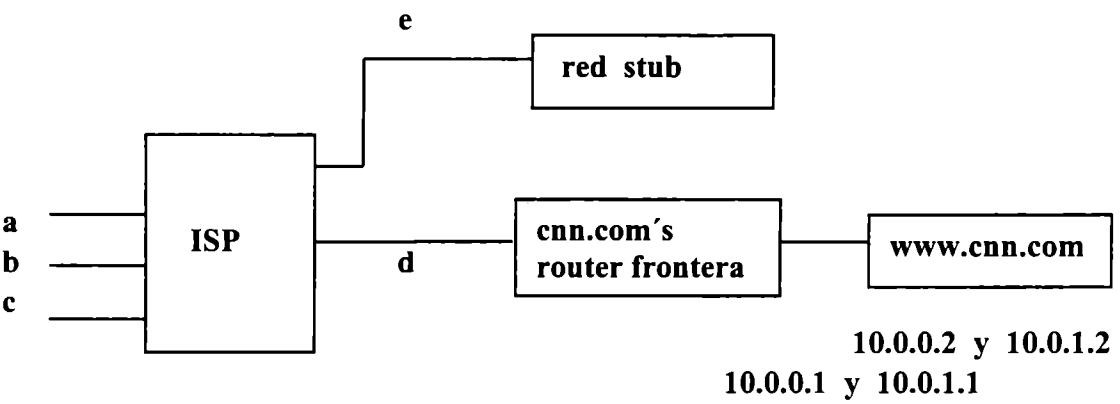
El dibujo de la infraestructura descrita es:



Siendo: *a, b y c* los enlaces ISP a Internet, y *d* un enlace entre el ISP y cnn.com.
10.0.0.1 es a la IP asignada a la interface interna del ruteador frontera y 10.0.0.2 es la IP asignada al servidor web público: www.cnn.com. Puede asumirse que existe un firewall entre ellos, pero esto no es relevante para el ejemplo. [Schapachnik 00]

El propósito de la técnica es cómo cambiar la dirección IP del host cuando es atacado y desviar la IP bajo ataque a una red stub, dónde el tráfico pueda ser analizado y rastreado.

Para estar preparado a un ataque masivo DDOS, Schapachnik propone cambiar la anterior estructura de red de cnn.com a una como la siguiente:



cnn.com's DNS server donde: www=10.0.0.2 y TTL=0

Bajo el supuesto de que un ataque DDOS contra cnn.com sea detectado, las siguientes acciones podrían ser ejecutadas:

1. Cambiar la tabla del servidor DNS de cnn.com, para que www.cnn.com apunte a 10.0.1.2

2. llamar al ISP para que enrute el tráfico 10.0.0.x a la red stub e inicie el ruteo a la red 10.0.1.x El ISP puede también dejar de publicar la ruta 10.0.0. esto probablemente tiene un costo en el BGP (Border Gateway Protocol) en la disgregación y actualización del ruteo, pero puede darnos una ventaja, debido a que conforme se propague la actualización del ruteo, el ataque se detendrá cerca de su origen. [Schapachnik 00]

Estos simple pasos podrían separar el ataque a un lugar dónde no se rompa la funcionalidad de cnn.com y dónde éste pueda ser rastreado.

Por supuesto quien realiza el ataque puede notar el cambio y ejecutar las siguientes acciones:

a) *Atacar también la nueva red (10.0.1.x).* En este caso la potencia de dicho ataque contra cada red se verá disminuida a la mitad. Podría ser útil que cnn.com tenga muchas redes stub que puedan ser usadas para tales casos. Un número suficiente de redes deberá manejar la cantidad de tráfico recibido y deberá ser lo suficientemente grande para ser soportada por la infraestructura.

b) *Ataca solamente la nueva red.* En este caso cnn.com puede cambiar hacia la red anterior o incluso hacia una nueva. Quizás este es el mejor movimiento que el atacante pueda realizar, pero las máquinas que tiene comprometidas podrían crear un patrón de tráfico muy fácil de identificar por un scanner distribuido de red, que puede estar consultando a un site central para patrones o diseños actualizados periódicamente por ISPs preocupados por la seguridad en Internet.

En cada caso el atacante deberá estar consultando los servidores DNS continuamente. Los *clientes* pueden hacer esto automáticamente, así en los logs se podría ver esta acción, o incluso el "evil master" detrás del ataque podría realizar un error y consultar el DNS frecuentemente. Si su software debe atacar una dirección IP y tiene alguna experiencia, deberá consultar el servidor DNS desde una de las máquinas comprometidas, o algún otro, pero entonces nuevamente puede ser perseguido desde aquí, así debe usar IPs reales para conseguir esa máquina.

Como se señala, el ruteador frontera del ISP (el único que conecta al ISP y cnn.com) es aún el punto débil. Esta identidad puede ser ocultada configurándolo para que no responda a ICMP y traceroutes. [Schapachnik 00]

Para que esta técnica sea efectiva, el ancho de banda total del ISP deber ser varias veces el ancho de banda que se vende a los clientes. Si el ISP no puede sobrevivir a los ataques, tampoco podrán sobrevivir sus clientes.

4 DETECCIÓN DE ATAQUES DDOS

4.1 INTRODUCCIÓN.

Contar con herramientas que nos permitan encontrar en nuestros sistemas la presencia de ataques del tipo: Trinoo, TFN, TFN2K, Shaft, Stacheldraht y ataques semejantes, es de gran importancia ya que nos abre la posibilidad de poder detectar y eliminar con anticipación los demonios ya instalados, y en el peor de los casos, cuando el ataque se está produciendo, podemos enviar comandos a los zombies y ordenarles que detengan el ataque en el mismo momento en que se efectúa éste.

A continuación describimos cuatro herramientas que nos serán de gran utilidad para tal fin, dichas herramientas pueden bajarse de la red gratuitamente y algunas están disponibles para aplicarse en diferentes sistemas operativos.

4.2 ZOMBIE ZAPPER

Zombie Zaper (ZZ), envía comandos a los zombies y les ordena detener el ataque cuando éste está ocurriendo. [Razor 00]

ZZ funciona contra Trinoo, TFN, Stacheldraht, Shaft y Troj_Trinoo (el demonio trinoo que ataca windows). En Trinoo, esto no detiene al demonio completamente (normalmente configurado para ser reiniciado por cron, silenciosamente, esperando más comandos), y con Troj_Trinoo el demonio raramente permanece hasta que se reinicia, pero con el resto de las herramientas DDOS la inundación solamente es detenida. Esto proporciona la ventaja de poder ordenarle al demonio detener la inundación sin detener al demonio, con esto tenemos más tiempo para rastrear el ataque, y lo más importante, llegar hasta el lugar donde se inicia el ataque.

Existen muchos ejemplos de detección de código que hacen lo mismo, excepto que simplemente avisan la presencia de zombies dentro de la red. Todo depende de cómo sean los passwords por omisión.

Se menciona esto ya que el software podría no funcionar contra TFN2K, el cual obliga a usar un nuevo password durante su uso. [Razor 00]

Al ejecutar ZZ con la opción –h muestra lo siguiente.

USAGE: *./zz [-a 0-3] [-c class C] [-d dev] [-f sec] [-h] [-s src] [-u sport] [-v] hosts*
Zombie Zapper v1.2 - DDoS killer
Bugs/comments to thegnome@razor.bindview.com
More info and free tools at http://razor.bindview.com
Copyright (c) 2000 BindView Development
USAGE:
./zz [-a 0-5] [-c class C] [-d dev] [-h] [-m host] [-s src] [-u udp] [-v] hosts

-a antiddos type to kill:
0 types 1-4 (default)
1 trinoo
2 tfn
3 stacheldraht
4 trinoo on Windows
5 shaft (requires you use the -m option)
-c class C in x.x.x.0 form
-f time in seconds to send packets (default 1)
-d grab local IP from dev (default eth0)
-h this help screen
-m my host being flooded (used with -a 5 above, only one host)
-s spoofed source address (just in case)
-u UDP source port for trinoo (default 53)
-v verbose mode (use twice for more verbosity)
host(s) are target hosts (ignored if using -c)

Explicaremos cada una de estas opciones con más detalle. [Razor 00]

- La opción *–a* es especifica el tipo de ataque DDOS que deseamos detener. No especificar la opción *–a* o usar *–a 0* asume los tipos 1 hasta 4 puesto que ellos no requieren una entrada adicional. Usar la opción *–a 5* requerirá que especifiquemos el nombre del host del sistema que se encuentra inundado.

- La opción *–c* permite especificar direcciones clase C para enviar paquetes. Direcciones desde x.x.x.0 hasta x.x.x.255

- La opción *–d* permite especificar en cual dispositivo grabar la dirección local IP. sólo desde Unix. (default eth0).

- La opción *–f* establece un cronometro para enviar paquetes. ZZ permite enviar 50 paquetes por segundo y podemos modificar el tiempo con esta opción.

- La opción *–m* permite especificar el nombre del host para detener la inundación del agente Shaft (solamente un host). Usado con *–a 5*.

- Con la opción *–s* podemos falsificar la dirección origen (en Unix solamente). Esto es útil dentro de una DMZ[11], y también nos ayuda a ocultarnos, para aquellos casos en los que el atacante tenga ejecutado sniffers.

- La opción *–u* nos permite alterar el puerto fuente UDP dentro de trinoo (por omisión 53). Útil también dentro de una DMZ

- Con la opción *–v* se aplica el modo verbose. Para aquellos curiosos quienes deseen ver parte de los efectos que suceden cuando el programa esta en ejecución.

- En la línea de comandos, todo aquello que no es una opción es considerado un host objetivo. Se recomienda que usemos nuestras direcciones IP, pero con los nombres de hosts también se trabaja adecuadamente. Si se usa la opción *–c*, los host en la línea de comandos son ignorados.

4.2.1 VERIFICANDO LA RED.

Es necesario verificar los logs del firewall, si notamos una lentitud al accesar a Internet, observamos una cantidad de paquetes transportándose hacia otro site. En alguna otra parte dentro de la red un número de máquinas son el objetivo de inundación.

¿Donde comenzar a buscar los zombies para detenerlos?
Ejecutamos ZZ contra nuestras propias direcciones IP, y asumimos los passwords por omisión, si el código no ha sido cambiado en el ataque DDOS, podemos pararlos inmediatamente.

Por ejemplo, si tenemos las direcciones 192.168.1.x y 192.168.2.x, podemos hacer lo siguiente:

./zz -c 192.168.1.0
./zz -c 192.168.2.0
Si tenemos una lista de direcciones en un archivo, intentaremos lo siguiente:
./zz `cat ip_file.txt | tr '\n' ' '`
Entonces los zombies serán rápidamente detenidos.

[11] Zona desmilitarizada

4.2.2 PROTEGERSE DE OTROS SITES.

Es posible que ejecutemos ZZ contra un site que está inundado, pero, existen algunas cosas que debemos considerar:

- En el site inundado podemos tener reglas en el firewall y en los ruteadores que prevengan ejecutar ZZ contra ellos.

- Los paquetes pueden ser falsificados, así podemos ejecutar equivocadamente ZZ en contra de un site.

- Es muy posible que puedan pensar que nosotros somos los atacantes, y podremos tener visitas de los agentes del gobierno.

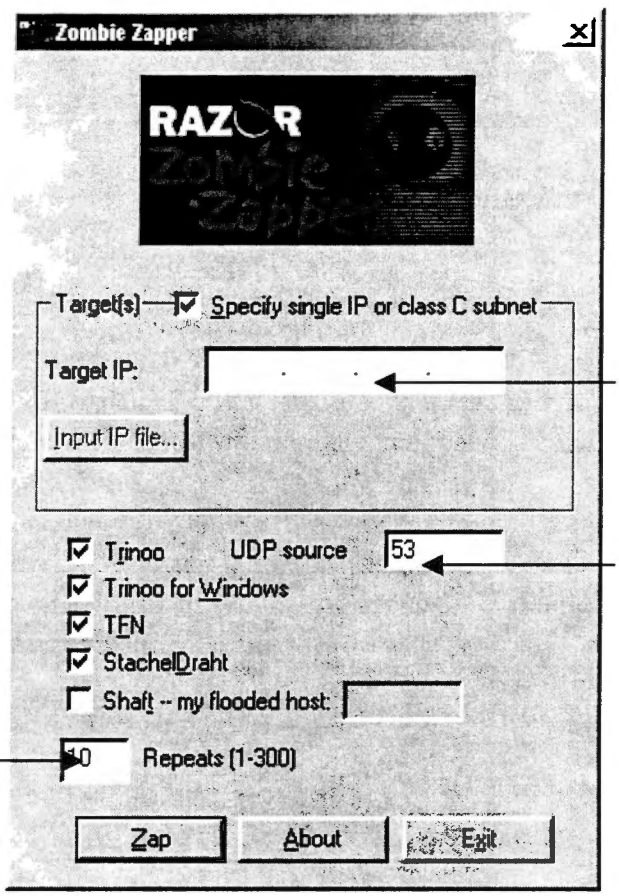
- No debemos hacer mal uso de la opción *–f*.

En otras palabras, usar esto en contra de otro site es bajo nuestro propio riesgo. No existe nada que pueda prevenir que nos envíen paquetes desde direcciones falsificadas. Si reunimos las direcciones en los logs, podemos fácilmente enviar comandos a estas direcciones e intentar detener las inundaciones.

Podemos usar ZZ junto con Sistemas de Detección de Intrusos y Firewall. Especialmente en soluciones de código abierto que soportan o pueden ser modificadas para soportar otras soluciones de código abierto.

ZZ tiene diferentes versiones que pueden ser utilizadas en diferentes Sistemas Operativos Unix y Windows NT.

4.2.3 INTERFACE DEL PROGRAMA



Entrada del objetivo.

Puerto fuente para paquetes UDP

Número de veces que se envía el paquete para eliminar los zombies.

4.3 DDOSPING

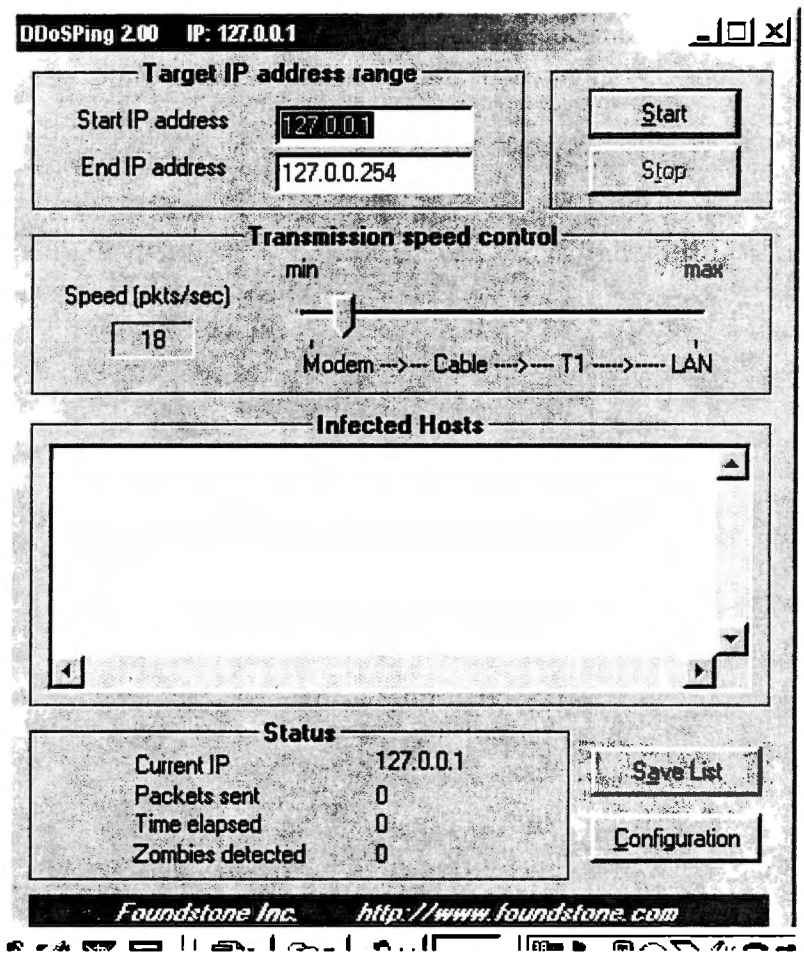
DDOSPing es un scanner de red remoto para detectar los programas más comunes que se utilizan para llevar acabo un ataque DDOS. [Foundstone 00]

Esta herramienta detecta Trinoo, Stacheldraht y Tribe Flood Network cuando dichos programas se ejecutan con sus configuraciones por omisión, aunque es posible cambiar la configuración de cada tipo de programa para detectar alguna variación de éstas, desde la pantalla de configuración de la herramienta DDOSPing.

El escaneo es realizado al enviar los mensajes adecuados ICMP y UDP a un rango de direcciones y velocidad que nosotros especifiquemos. DDOSPing requiere Winsock 2 para ejecutarse. Si tenemos Windows 95 sin el Winsock actualizado, necesitamos visitar el site web de Microsoft para actualizarlo. [Foundstone 00]

4.3.1 INTERFACE DEL PROGRAMA

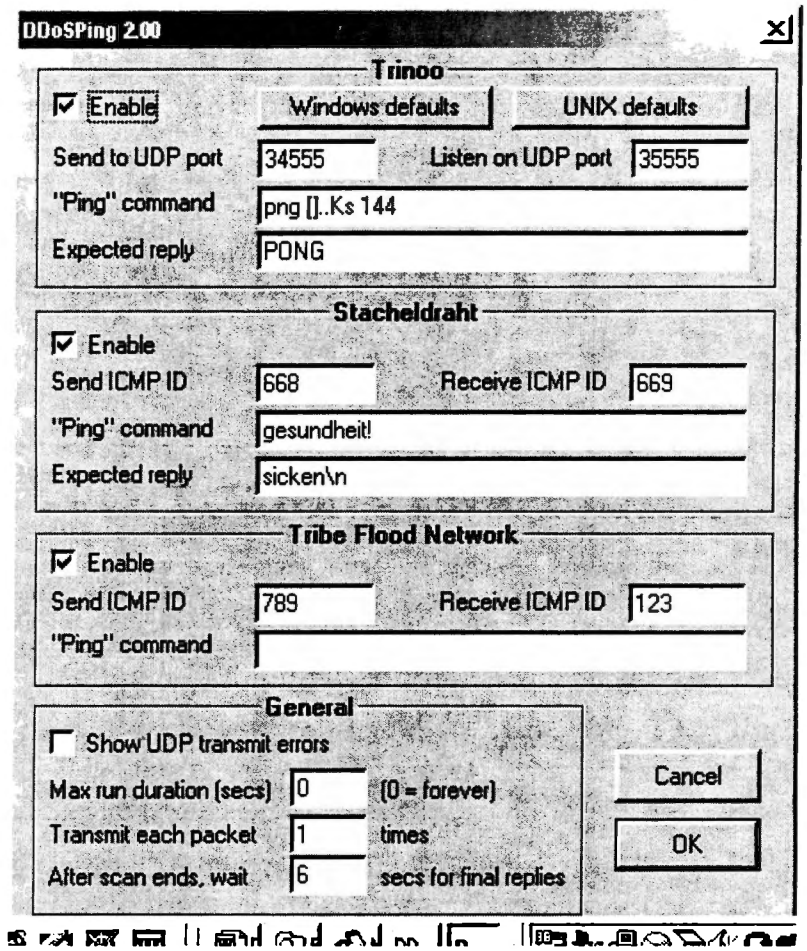
En esta pantalla podemos especificar el rango de direcciones que deseamos probar, así como la velocidad de transmisión de los paquetes, una vez configurados los valores podemos iniciar el escaneo, adicionalmente contamos con la opción de salvar la lista de los hosts que se encontraron infectados. [Foundstone 00]



Con la opción *Configuración* de la pantalla anterior, podemos seleccionar las herramientas de ataque que deseamos detectar durante el escaneo (Trinoo, Stacheldraht y Tribe Flood Network), se puede cambiar entre UNIX o Windows, para tener las configuraciones por omisión de Trinoo.

Es posible cambiar los comandos y puertos de cada herramienta, esta característica puede ser de gran interés ya que podemos detectar algunas otras herramientas que han sido instaladas en nuestros sistemas y que son mutaciones de las herramientas de ataque originales.

Dicha pantalla se muestra a continuación.



4.4 FIND_DDOS

En respuesta a los numerosos ataques DDOS que se presentaron, el Centro de Protección a la Infraestructura Nacional de Estados Unidos (NIPC) y la Unidad de Aplicaciones de Tecnología Especial (STAU), desarrollaron esta herramienta para ayudar a combatir la amenaza de éstos ataques. La herramienta puede ser utilizada para escanear sistemas locales que sean sospechosos o que se conozca contienen programas DDOS. Find_ddos es capaz de escanear procesos ejecutándose en Sistemas Solaris 2.6 o superior y archivos locales en Sistemas Solaris 2.x o superior y Sistemas Linux. [Nipc 01]

Find_ddos detecta varias herramientas de ataque DDOS, la forma en que los encuentra es revisando todos los archivos de formato ELF[12] de 32-bits dentro del árbol de directorio que especifiquemos y comparando los strings (cadenas de caracteres) y tabla de símbolos contra un patrón ya conocido "fingerprints" para TFN y Trinoo. Si luego de examinar la identidad entre éstos datos, el resultado muestra que son lo suficientemente cercano comparado con uno de estos fingerprints Este archivo es identificado como posible causante de ataques. La herramienta podría opcionalmente realizar una copia de todos los archivos relacionados con este último. Si el

[12] Formato Binario usado por sistemas Unix

archivo fue encontrado en un proceso de ejecución, la utilidad tomará la parte principal de este para luego de concluido el curso de la acción analizarla con los patrones. Algunos de estos patrones se utilizan también para examinar cualquier dirección IP integrada a los archivos que puedan utilizarse para tener acceso al sitio de esa dirección. Todos los resultados son mostrados en la terminal del usuario o almacenados en un archivo log (archivo que registra las instrucciones realizadas desde el momento de conexión a Unix).

La herramienta también busca archivos ".sr", "...", "mservers", y opcionalmente realiza una copia de ellos para su análisis posterior. Estos son los nombres comunes de archivos que contienen una lista de direcciones IP encriptadas con blowfish. La llave de encripción blowfish puede ser encontrada al examinar los binarios.

Las herramientas DDOS que son detectadas por Find_ddos son: [Nipc 01]

* mstream master
* mstream server
* stacheldraht client
* stacheldraht daemon
* stacheldraht master
* tfn-rush client
* tfn client
* tfn daemon
* tfn2k client
* tfn2k daemon
* trinoo daemon
* trinoo master

La herramienta debe ser ejecutada como root. La sintaxis es:

./find_ddos [-g grabdir] [-l logfile] [-p] [-v] [-V] [-x exclude1] [scandir]

- O - *./find_ddos*

Donde:

- *"-g grabdir"* Especifica una localización opcional para guardar el archivo de comparaciones, imágenes core, y nombres de archivos : ""..." o "mservers". Este directorio será creado si no existe y no será escaneado por la herramienta.
- *"-l logfile"* Especifica un archivo opcional para guardar los resultados. (en tal caso los resultados no serán mostrados).
- *"-p"* Le dice a la herramienta que también escane los procesos ejecutándose.
- *"-v"* Proporciona mayor información cuando se está escaneando. Modo Verbose
- *"-V"* Muestra información acerca de la versión.
- *"-x exclude1"* Le dice a la herramienta que se salte un archivo o directorio cuando se está realizando el escaneo. Múltiples exclusiones pueden ser proporcionadas al repetir la bandera *"-x"*, si se excluye un directorio, también se excluyen todos sus subdirectorios.

- *"scandir"* Especifica uno o más archivos o directorios para escanear.

Si la herramienta se ejecuta sin parámetros, se asumen los siguientes parámetros por omisión:

./find_ddos -g files -l LOG -p /tmp /

Si algún parámetro es proporcionado, los parámetros por omisión no son usados. Por lo tanto:
"./find_ddos -v -x /mymount" no realiza nada. Mas bien debemos de ejecutar:
./find_ddos -v -x /mymount -g files -l LOG -p /tmp /

La herramienta está diseñada para ser capaz de ejecutarse desde un disco flexible, y puede escanear el sistema y salvar los resultados en el mismo disco para su análisis posterior.
Para realizar estó, entramos como root, colocamos una copia de la herramienta en un disco flexible vacío, y montamos el disco en el sistema. La herramienta puede entonces ser ejecutada al dar doble clic en el icono del administrador de archivos o ejecutarse desde la línea de comandos. Una vez que la herramienta termina de ejecutarse, el disco debe ser desmontado y removido para su análisis posterior. [Nipc 01]

Advertencias:

* La herramienta es rápida pero consume muchos recursos. Si somos un usuario que se queja cuando el sistema se vuelve lento, se recomienda usar el comando "nice"

* La herramienta fue escrita en C para tener un mínimo de seguridad suficiente dentro de un sistema binario, de esta manera no puede ser afectada por la mayoría de los "root kits".

*Algunas diferencias en la tabla de símbolos puede ser el resultado de la forma que compilaron los programas DDOS, más que un cambio en el código fuente del programa. Esto no ocasiona que el programa falle, pero causa que las diferencias sean reportadas, aunque no sean significativas.

4.5 DISTRIBUTED DOS SCANNER (DDS)

Dave Dittrich y otros especialistas han desarrollado esta herramienta especializada en la detección de agentes Trinoo, TFN y Stacheldraht. No detecta agentes TFN2K. [Dittrich_dds 01]

Este programa se puede compilar y ejecutar, al menos, en los siguientes Sistemas Operativos:

* Linux (kernel 2.2.x)
* Solaris 2.6 o superior
* Digital Unix 4.0d
* IBM AIX 4.2
* FreeBSD 3.3

* OpenBSD 2.6
* IRIX 6.5

Quizás necesitemos editar el archivo Makefile para definir las librerías necesarias para compilar el programa. Por default trabaja para sistemas Sun Solaris.

Debemos ejecutar DDS como root, Existe un retraso de 30 segundos por omisión después de mandar todos los paquetes, para permitir a los paquetes retrasados ser recibidos antes de que el programa termine. [Dittrich_dds 01]

Las redes son especificadas usando la notación de Enrutamiento Interdominio Sin Clases (CIDR). Las máscaras de red comunes y sus CIDR equivalentes, son:

255.255.0.0	/16
255.255.255.0	/24
255.255.255.255	/32

Si tenemos una red de subredes, todas compartiendo una red común de direcciones en 198.162. para escanear esta red /16 completamente, debemos usar el comando:

#./dds 198.162.0.0/16

Si en lugar de eso tenemos una subred de 24 bits 198.162.1, debemos usar el comando:
#./dds 198.162.1.0/24

Para escanear un host, sólo necesitamos dar la dirección IP:
#./dds 198.162.1.1

Si DDS encuentra algún agente activo, reportará lo siguiente:

 # ./dds 192.168.1.0/24
Received 'PONG' from 192.168.1.17 - probable trinoo agent
Received TFN Reply from 192.168.1.153 - probable tfn agent
Received 'sicken' from 192.168.1.202 - probable stacheldraht agent

Si DDS no encuentra ningún agente activo, este no regresará nada. Podemos usar el modo verbose, si realmente queremos ver el reporte cada vez que se envía un paquete, de esta manera:

 # ./dds -v 192.168.1.0/24
Mask: 24
Target: 192.168.1.0
dds $Revision: 1.3 $ - scanning...

Probing address 192.168.1.1
Probing address 192.168.1.2

. . .
Received 'PONG' from 192.168.1.17 - probable trinoo agent
. . .
Probing address 192.168.1.152
Received TFN Reply from 192.168.1.153 - probable tfn agent
. . .
Received 'sicken' from 192.168.1.202 - probable stacheldraht agent
Probing address 192.168.1.203
. . .
Probing address 192.168.1.254

Si hacemos esto, realizar el escaneo a una subred clase C, generaría 254 líneas de salida, probablemente necesitemos ejecutar un script para capturar toda la salida.

Si DDS recibe un paquete ICMP_ECHOREPLY con el mismo valor ID (669) como el que produce un agente Stacheldraht, pero sin la palabra "sicken" en la porción de datos del paquete, o un paquete UDP dentro del manejador de Trinoo sin escuchar el puerto "PONG" en la porción de datos del paquete, se reportaría algo como esto:

Unexpected ICMP packet from ...
Unexpected UDP packet received on port ... from ...

Esto no es lo mismo que detectar agentes Trinoo o Stacheldraht.

Cualquier paquete ICMP_ECHOREPLY con un ID 123 recibido por DDS, podría ser un agente TFN. Es muy improbable que esto sea un falso positivo.

4.6 CONCLUSIONES

De acuerdo al análisis de las herramientas recomendamos Zombie Zaper para detectar ataques convencionales del tipo: Trinoo, TFN, TFN2K, Shaft, Stacheldraht , cuenta con opciones muy interesantes como verificar redes remotamente falsificando nuestra dirección IP, es muy recomendable utilizarla, está disponible para sistemas Unix y Windows. Una herramienta muy parecida a está es DDOSPing con la ventaja de que es posible cambiar la configuración de cada tipo de programa para detectar alguna variación de estás (por ejemplo números de puerto), la desventaja es que la información y soporte para este tipo de herramienta es escasa.

Por otra parte si deseamos detectar mutaciones de ataques DDOS, la mejor herramienta para verificarlo es Find_ddos, ya que está herramienta desarrollada por el NIPC se encuentra en constante actualización, por ejemplo en su última versión detecta Trinity v3 (descrita en el capítulo uno), y algunas variantes de Stacheldraht denominadas "Stacheldraht 1.666+antigl+yps" y "Stacheldraht 1.666+smurf+yps". La desventaja es que sólo está disponible para sistemas Linux y Solaris.

Por lo tanto dependiendo de que herramientas DDOS necesitemos detectar y al sistema operativo con que estemos trabajando, las utilizaremos de acuerdo a nuestros sistemas y necesidades. Se recomienda una combinación de ambas. Desafortunadamente, si contamos con sistemas Windows, no podremos detectar mutaciones de herramientas DDOS, al menos con las herramientas libres que tenemos hasta el momento.

Por otra parte, en la medida en que los sistemas detectores de intrusos alcancen madurez, estos permitirán realizar detecciones más confiables, como por ejemplo reducir el número de falsos positivos que estos generan.

5 PROPUESTA DE UN ESQUEMA GENERAL DE PROTECCIÓN CONTRA ATAQUES DDOS

A continuación se describe un esquema de protección general que tiene como fin detectar y detener los ataques DDOS, antes de que se lleven acabo o en el momento mismo en que se efectúan. Se previene al lector que muchas de las consideraciones y recomendaciones aquí expuestas no son necesariamente actualmente realizables; sin embargo, es muy probable que con el avance de la tecnología, la seguridad y la legislación lleguemos a este esquema en un futuro.

5.1 DEFINICIÓN DEL PROBLEMA.

Como se analizó en los capítulos anteriores de esta tesis, no existe una solución única y total para enfrentar este tipo de ataques sino que, más bien, existe un conjunto de medidas preventivas y recomendaciones, que en caso de implementarse, nos permitirán ser menos vulnerables y enfrentar de mejor manera los diferentes tipos de ataques de negación de servicio a los que estamos expuestos.
Ante tal situación se propone un esquema de protección basado en un protocolo que integre varios de los elementos ya analizados, para detectar y detener este tipo de ataques de manera automática.

Básicamente, a grosso modo, los elementos que se requieren para implementar este esquema son de tres tipos:

- Un conjunto de herramientas.
- Un protocolo que permite coordinar los esfuerzos para detectar y detener un ataque.
- Un conjunto de normas globales de coordinación a nivel mundial en Internet.

5.2 SERVICIO PROPUESTO POR EL PROTOCOLO.

El objetivo del protocolo es la comunicación y cooperación entre los diferentes elementos de una red (servidores, hosts, switches, ruteadores, gateways, repetidores, etc) que tengan la capacidad de abrir y cerrar puertos de manera dinámica, para recibir, responder y reenviar alertas verificadas, hasta llegar al origen o cerca del origen del ataque DDOS y detenerlo.

5.3 REQUISITOS PREVIOS

A continuación se presenta una lista de varios requisitos previos que se deberán cumplir para garantizar que el esquema de protección funcione de manera adecuada, algunas sólo existen como recomendaciones, otras ya se encuentran implementadas de manera parcial y unas más son características nuevas que deberán establecerse en los dispositivos de ruteo.

1. Se cuenta con un NIDS[13] y un Firewall[14], colocados entre la red de los ISP o Compañías y el resto de Internet y carriers como Telmex, AT&T, satelitales, etc. Un NIDS examina individualmente todos los paquetes que viajan por la red y es capaz de comprender todas las diferentes banderas y opciones que pueden coexistir dentro de estos paquetes, puede vigilar el tráfico de red dentro de la red protegida por nuestro firewall y detectar los tipos de ataque, por ejemplo, de "desborde de buffer", también es capaz de detectar cambios de archivos y directorios. Podemos analizar los flujos, buscando "firmas" que se asemejen a la de los ataques conocidos. Mientras que un Firewall está diseñado para filtrar el tráfico normal de la red, basándose en atributos tales como las direcciones de origen, destino, números de puerto y los tipos de mensajes ICMP, así como protocolos específicos de nivel de aplicación (FTP, HTTP, Telnet, etc.). Es muy probable que estas tecnologías se fusionen en el futuro cercano. Dado que los elementos de detección de intrusos son la fase inicial para detener un ataque DDOS, es necesario que se trabaje en la investigación para que estas herramientas generen verdaderas alertas y no falsos positivos. Es decir en nuestro esquema propuesto necesitamos mejoras y avances en los IDSs actuales para realmente poder detectar de manera confiable los ataques de negación de servicio.

2. Los dispositivos de comunicaciones permitirán especificar el ancho de banda máximo que puede consumir cierto tráfico. Está posibilidad nos permitirá detectar cuando se está produciendo una anomalía y consecuentemente, antes de que ocurra algo grave podremos tomar las contramedidas oportunas. En Cisco esta característica es conocida como "Committed Access Rate" (CAR, o Tasa de acceso comprometido). Esta función nos permite limitar el tráfico ICMP a un valor razonable, tal como 256K ó 512K. [Stuart05 01]

3. Se da por hecho que todos los Proveedores de Servicio de Internet y las grandes compañías con redes corporativas conectadas a Internet utilizan filtrado de tráfico entrante para prohibir ataques DDOS que utilizan direcciones IP falsificadas (RFC2827, descrito en el capítulo 3). Aunque esta

[13] Network Intrusion Detection System
[14] "muralla cortafuegos"

medida no garantiza el que podamos ser víctima de este tipo de ataques, facilitará el análisis y seguimiento de éstos en caso de producirse. Esto es de suma importancia para que podamos seguir el rastro hasta el origen del ataque.

4. Se considera que se tiene deshabilitado, en la medida de lo posible, el tráfico IP Broadcast en todos los Sistemas y también se tiene deshabilitada la recepción y el envío de paquetes dirigidos Broadcast en todos los ruteadores como se especifica en el RFC 2644 (descrito en el capítulo 3). El propósito de esta recomendación es asegurar que ninguna red sea utilizada como un Site de amplificación Broadcast para inundar otras redes con ataques DoS como Smurf.

5. Cada sistema dispone de las herramientas que se describieron en el capítulo cuatro, con el objetivo de que una vez que sea detectado un posible ataque, las herramientas puedan ser ejecutadas para detener los ataques y eliminar los zombies y maestros.

6. Los ruteadores, switches, gateways, etc., sobre todo de los grandes ISP, deberán tener una gran capacidad de canal para no ser saturados mientras consumen tiempo filtrando comunicaciones.

5.3.1 NUEVAS CARACTERÍSTICAS

7. Todos los dispositivos de ruteo deberán contar con una nueva característica de registro de paquetes y logs a nivel capa dos (enlace) y en tiempo real, que se describe a continuación.

La característica que proponemos sea implementada en todos los dispositivos de ruteo, consiste en que cada uno de estos dispositivos pueda guardar registro de un identificador de cada uno de los paquetes que recibió (enrutó) en las últimas tres horas, donde deberá registrarse la dirección origen y destino de cada paquete, la hora de recepción local y el dispositivo de ruteo por donde se recibió dicho paquete.

Dirección Origen	Dirección Destino	Hora de recepción	Equipo de dónde se recibió (puerto en el dispositivo)

Se deberá ir registrando de manera automática la información descrita de cada uno de los paquetes conforme vayan llegando y deberán irse borrando aquellos paquetes que cumplan las tres horas señaladas. La justificación de tomar un tiempo aproximado de tres horas, es que para efectos de análisis, es el tiempo aproximado en que se efectúan los ataques DDOS, nulificando a su víctima. Es por esta razón que consideramos suficiente el tiempo de tres horas y por otra parte limitamos el uso de recursos que utilizaremos para implementar esta característica. Este tiempo se estimó a partir de los ataques DDOS acontecidos a inicios del año 2000.

El objetivo de implementar esta característica en los dispositivos de ruteo, es que el esquema de protección propuesto en esta tesis se basa en alertas y éstas generalmente se propagan hasta llegar cerca del origen del ataque, la manera en que se propagan esta

alertas se basará en checar las direcciones origen y destino de los paquetes para conocer por qué dispositivo llegaron y, en base a esto, reenviárselo al dispositivo de ruteo correspondiente; sólo en el caso de que enfrentáramos algún problema y no estuviese registrado por dónde llegó un paquete dado, no se propagará más la alerta.

Con respecto a los requisitos arriba mencionados, dos importantes aspectos que vale la pena mencionar son:

- Primero, en realidad algunas de estas recomendaciones, son fáciles de implementar (configurar) y no requieren de grandes recursos para ser llevadas acabo, por ejemplo, actualmente la mayoría de los ruteadores se venden deshabilitando por omisión el tráfico broadcast.

- Segundo, la dificultad más grande que encontramos es que se requiere forzosamente la colaboración de toda la comunidad de Internet, especialmente de los grandes proveedores de carriers, ISP, y en general compañías que proveen servicios a través de Internet o simplemente se encuentran conectadas a Internet, esto es indispensable para lograr que el esquema planteado sea exitoso, no basta con que sólo algunos se preocupen por la seguridad en los sistemas. Por citar un ejemplo, si un ISP, no implementa la característica de filtrado de tráfico entrante en su red, un cliente en Internet puede realizar el ataque usando direcciones IP falsificadas, y con el esquema planteado se dificultará llegar al origen verdadero del ataque.

Elementos Implicados y Abreviaturas Empleadas.

- (FW) Firewall
- (DI) Sistema de Detección de Intrusos de Red, también conocido como NIDS
- (R) Equipos ruteadores (switches, gateways, ruteadores, repetidores, etc.)
- (ISP) ISP's que son o requieren de proveedores de Carriers
- (V) Hosts Víctimas
- (C) Clientes de un ISP, o de una red corporativa
- (Z) Zombies o máquinas comprometidas para atacar
- (H) El Hacker o Hackers que lanzan el ataque
- (T) Tools, Herramientas para detener y eliminar los zombies.

5.4 DESCRIPCIÓN DEL ESQUEMA DE ALERTAS PARA MITIGAR LOS EFECTOS DE UN ATAQUE DDOS

Para la explicación del funcionamiento del protocolo, asumiremos que R_i es el ruteador actual donde se está analizando la alerta y R_{i+1} es al que se enviará la alerta, un servidor que ya recibió una alerta se convierte en R_i.

De manera informal las directivas del protocolo son:

1. Un equipo (DI) detecta un posible ataque en un host víctima (V), analizando el tráfico que entra o sale de la red que protege, examina los paquetes individuales que viajan por ella, detectando paquetes armados maliciosamente o sospechosos y genera la alerta de manera reactiva, es decir, responde ante una posible actividad ilegal, por ejemplo, sacando al usuario del sistema o mediante la configuración remota del Firewall, para impedir tráfico de red desde una fuente presumiblemente hostil, guardando la información correspondiente en un archivo log. La primera alerta se envía hacia su ruteador de frontera (R_{i+1}). La alerta contiene los datos que se indican en el siguiente punto. Es necesario mencionar que existe "confianza" entre (DI) y Ri, es decir, ambos aceptan a una autoridad certificadora común[15], y han intercambiado sus llaves públicas (certificados). Esta confianza ocurrirá de la misma forma en cada Ri en la red, básicamente cada Ri debe aceptar la autoridad que certifica a sus vecinos, con los que mantiene una conexión directa, y posee las llaves públicas de cada uno de ellos.

2. **Primer conjunto de datos del protocolo.** La alerta llevará como información la dirección de la víctima, la supuesta dirección del origen del ataque (ya que esta puede haber sido falsificada), la hora GMT (que permitirá a R_{i+1} saber que la alerta es reciente) y un hash de los datos anteriores, todo esto es cifrado primero con la llave privada del emisor (DI), lo que constituye su firma, y posteriormente con la llave pública del receptor R_{i+1} (para que sólo este pueda interpretarla) . Después de recibir un aviso del (DI), el equipo R_i observa de qué dirección proviene la comunicación o paquete malicioso y preparará una alerta para R_{i+1}.

3. **Segundo conjunto de datos del protocolo.** Con el objetivo de seguir el rastro del atacante este segundo conjunto de datos contendrá la siguiente información: dirección del dispositivo R_i (donde se está generando o ruteando la alerta) y dirección del dispositivo R_{i+1} (por donde llegó el paquete a R_i). Si R_{i+1} está recibiendo la alerta de (DI), inicia un contador de saltos a 50, el cual estará incluido también en el segundo conjunto de datos. Si se recibió la alerta de Ri , decrementará el contador en un salto antes de reenviarlo (el contador tiene una función semejante al campo TTL de TCP/IP). A este conjunto de datos se le va aplicar un tratamiento semejante al del primer conjunto de datos. Nótese

---

[15] Aunque para el enfoque propuesto, basta con que los dispositivos confíen en los dispositivos a los que están directamente conectados, lo ideal sería contar con una autoridad global que permitiese a cualquier dispositivo en internet, verificar las credenciales de cualquier otro dispositivo en la red mundial. Eventualmente, está verificación proveerá la confianza entre cualesquiera dos dispositivos en Internet. La implantación de un esquema de certificación mundial estaría sujeto a un sinnúmero de acuerdos, políticos, legales, tecnológicos, e incluso la definición de una política de certificación global. La descripción de un esquema de tal magnitud queda abierto a investigaciones futuras. Foros como las Naciones Unidas podrían tomar a cargo la especificación de este esquema. De hecho, ya están trabajando en documentos como **Ley Modelo de la CNUDMI sobre las firmas electrónicas** , que puede ser consultado en: http://www.uncitral.org/spanish/texts/electcom/ecommerceindex-s.htm. Por otra parte la Comisión Europea aprobó la Identrust, una sociedad que reúne más de veinte bancos mundiales en una red de autenticación de rúbricas electrónicas, y de otros servicios que garantizan las transacciones asociadas al comercio electrónico. Cada participante podrá desarrollar la propia tecnología de modo independiente, con base en la infraestructura de la Identrust, ofreciendo servicios que van de la identificación del socio de la transacción a la autenticación de los mensajes electrónicos, hasta la definición de las reglas contractuales aplicables en caso de controversias, dicho sistema no hará cualquier restricción a la competencia, y no amenaza restringir el mercado, a partir del momento que está constantemente abierto a nuevos miembros, afirmo la Comisión Europea. Mas información puede ser consultada en: http://www.ansa.com.br

que en este caso, las direcciones de los dispositivos R van cambiando conforme se reenvían, es decir este conjunto de datos no es fijo, por lo que la firma digital en está parte será diferente en cada salto; sin embargo, el primer conjunto de datos nunca cambia. Aquí radica la importancia de distinguir y separar cada conjunto de datos.

Como el segundo conjunto de datos tiene la huella (hash) de la primera alerta, no será posible para alguien que haya interceptado la primera alerta, intentar reenviarla a otros R, haciéndoles perder tiempo. Resumiendo, la alerta enviada de Ri a R_{i+1} contiene los campos siguientes:

a. La dirección de Ri
b. La dirección de R_{i+1}
c. Contador
d. Dirección de la víctima
e. Dirección del atacante
f. Tiempo GMT (original)
g. El hash de (Dirección de la víctima, Dirección del atacante, Tiempo GMT)

Todo lo anterior es cifrado primero con la llave privada de Ri y después cifrado con la llave pública de R_{i+1} finalmente este conjunto de datos es enviado a R_{i+1}.

4. Una vez preparada la alerta con los dos conjuntos de datos descritos en los pasos 2 y 3, El procedimiento realizado es el siguiente: R_i tiene la alerta, verifica en sus tablas de ruteo si se encuentra conectado directamente con la dirección del atacante, en caso positivo, ejecuta el paso 7. En caso contrario, checa los logs para conocer por dónde llegó el paquete y envía la alerta al correspondiente dispositivo R_{i+1}, en el peor de los casos que no tenga registrado por dónde le llegó el paquete ya no lo propaga.

5. Una vez que un equipo R recibe una alerta, primero la descifra y autentifica la alerta verificando su firma y corroborando los datos de la alerta contra el hash, desencriptando ambos conjuntos de datos con las llaves públicas y privadas correspondientes. Verifica la huella, también checa el contador de saltos y si este aún no es cero lo decrementa para enviarlo al siguiente R. De ser cero, se descarta la alerta y ya no se propaga. En caso de que la verificación sea exitosa se continua con el paso 6, en caso contrario R desecha la alerta y no se propaga más, registrando sólo un log de lo sucedido.

6. Recibida la alerta y después de verificarla, existen dos posibilidades, Si algún R_i recibe más de una vez una alerta con la misma firma del primer conjunto de datos, la desecha y ya no la propaga, en caso contrario R_i en el segundo campo de datos, checa sus logs y agrega la dirección correspondiente R_{i+1}, el primer conjunto de datos no cambia, repite nuevamente el paso 4, este procedimiento continua hasta que se haya suspendido la comunicación con el atacante o se deje de propagar de forma natural las alertas, por recibirla más de una vez, porque ya no hay a quien redirigirla, o porque el contador de tiempo ha expirado.

7. Desde el servidor donde tenemos instaladas las herramientas para combatir a los zombies, (en el site donde se encuentra el zombie) se ejecuta la orden correspondiente para detener y matar a los zombies que realizan el ataque, todo esto se registra en un log y se desecha la alerta. Eventualmente, el administrador de esos sistemas puede investigar en sus logs para tratar de rastrear al hacker que realmente lanzó el ataque. Por ejemplo, el administrador del site donde se hallan los zombies puede checar las bitácoras para identificar la posible dirección o direcciones desde donde el o los zombies recibieron el comando de ataque. Si esta dirección es determinada con suficiente precisión, puede procederse a un protocolo semejante al anteriormente descrito y propagar alertas hacia el site donde se encuentra el "maestro" que lanzó el comando de ataque. Una vez realizado esto, una tercera fase sería, a partir del site donde está el "maestro", analizar las bitácoras buscando la posible dirección del hacker que lanzó el ataque. Evidentemente, los esquemas en que operan los ataques DDOS podrían hacer muy complicado realizar estas dos últimas fases, y sólo convendría llevarlos a cabo en casos muy particulares. De hecho, tal vez convendría que estas dos últimas fases fuesen delegadas a un organismo internacional dedicado exclusivamente a la investigación de estos casos.

8. Una vez detenido el ataque, y corregidas las vulnerabilidades, el site donde radicaban los zombies envía un mensaje informando a su ruteador que el problema ha sido eliminado. Con lo cual el ruteador podrá notificar al ruteador de la víctima que puede abrir de nuevo su comunicación a la supuesta dirección del atacante. Obviamente, estas comunicaciones están nuevamente basadas en confianza (autenticación y confidencialidad).

5.5 CONSIDERACIONES RELEVANTES.

Primeramente con la combinación del Sistema de detección de intrusos y el Firewall, se detecta y cierra el camino por donde se está efectuando el ataque, se genera la alerta y se propaga hasta llegar cerca del origen del ataque. La importancia del esquema presentado no consiste únicamente en evitar el ataque, si no llegar hasta el origen mismo del ataque para detener completamente a los zombies y evitar que estos puedan ser utilizados nuevamente para atacar el mismo objetivo u otros sistemas en Internet.

Con el esquema planteado, en lo que se refiere a la propagación de alertas para encontrar al atacante, las alertas se irán propagando de manera innecesaria por la red con el consecuente consumo de recursos y tal vez alertas cayendo en ciclos en la red, por está razón se propuso un contador de saltos y una vez que este número se mayor a 50, es decir una misma alerta que haya circulado por más de 50 dispositivos de ruteo, se destruye o desecha automáticamente al cumplirse esta condición.

Por otra parte es importante mencionar y aclarar que seguramente tendremos varías alertas diferentes, que un mismo dispositivo de ruteo podrá generar y propagar ya que normalmente los ataques se realizan desde varios puntos en la red hacia un mismo objetivo.

Sin embargo, gracias a que las alertas contienen poca información y son rápidas de propagar de acuerdo a los mecanismos planteados para lograr la mayor eficiencia posible, automáticamente esperamos un cierre de caminos de manera gradual en los diferentes puntos de la red donde se producen los ataques, hasta llegar a detener el ataque completamente.

Generalmente los ataques DDOS necesitan cierto tiempo para lograr inundar al objetivo y dejarlo fuera de servicio, al mismo tiempo nuestro esquema de protección trabajará cerrando la comunicación en los diferentes puntos de la red donde se originan los ataques, buscando que el ataque sea más débil conforme transcurra el tiempo, hasta lograr finalmente que el objetivo atacado se libere completamente del ataque y opere de manera normal. Además, con las diferentes medidas sugeridas, sobre todo con la de Broadcast o CAR se esperan ataques menos intensos, ya que los atacantes contarán con menos sistemas que podrán utilizar para llevar a cabo sus ataques.

El protocolo en sí no se ha validado, ya que no se generan e inspeccionan todos los estados posibles que pueden presentarse en nuestro sistema a partir del estado inicial, por lo que puede ser motivo de tema a desarrollar en otros trabajos.

5.6 FORMATO DE LOS MENSAJES PROPUESTOS

A continuación se describe de manera detallada los formatos de mensajes propuestos para enviar y recibir cada uno de los dos conjuntos de datos del protocolo, cumpliendo las propiedades de autentificación, confidencialidad, integridad y no repudio de la información. (véase capítulo uno, para consultar las definiciones de cada una de estas propiedades).

5.6.1 ESPECIFICACIÓN DEL ALGORITMO

Primer conjunto de datos del protocolo.

El mensaje M está constituido por la dirección de la víctima, dirección del origen del ataque, la hora y la huella digital de los campos anteriores.
Sean A y B dos equipos Rs, y A desea comunicar una alerta a B, veamos qué es lo que sucede durante la comunicación.

La forma más común de firmar digitalmente un mensaje es utilizando un algoritmo de clave pública. Algunos de estos algoritmos permiten cifrar tanto con la clave pública como con la privada. Esto resulta muy útil, pues un mensaje encriptado con la clave privada de A sólo puede haber sido generado por A ya que es la única entidad (ruteador) que conoce la clave. Con esto se autentifica la identidad de A. Estas funciones toman un mensaje de un largo arbitrario y computan lo que se llama un "message digest" (MD) de un largo fijo establecido (generalmente mucho menor que el largo del mensaje). Una propiedad que debe cumplir una función de hash es que, dado un mensaje M y su imagen H(M) en la función de hash, sea computacionalmente

imposible encontrar un mensaje M' distinto de M que cumpla H(M)=H(M'). A este tipo de funciones se les llama en-un-sentido ("one-way"). Si H cumple esta propiedad, un atacante no podrá encontrar un mensaje distinto de M con el mismo compendio del mensaje.

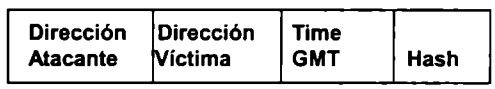
Veamos como funciona este protocolo:

1) A calcula la huella digital que será incluida en M.
2) A firma el mensaje M incluyendo el hash del paso 1, encriptándolo con su clave privada, obteniendo CApriv(M)
3) A cifra todo con la llave pública de B y el resultado es enviado a B
4) B usa su clave privada y la clave pública de A para desencriptar el mensaje recibido.

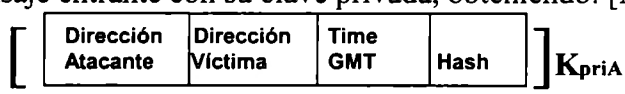
Si obtiene un mensaje con sentido (en el formato especificado), sabe que fue enviado por A pues es la única persona que puede haberlo encriptado usando Apriv. Además B debe verificar la huella digital del mensaje recibido y que la alerta sea reciente.

Entonces el protocolo de firma sería el siguiente:
1. El mensaje M llevará los siguientes datos:

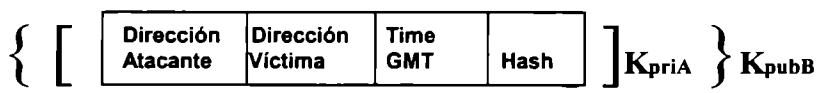
2. A le aplica la función de hash H al mensaje M, obteniendo H(M), un compendio del mensaje.



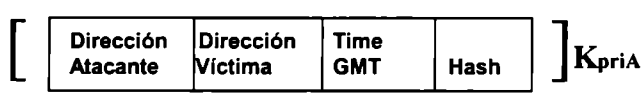
3. A encripta el mensaje entrante con su clave privada, obteniendo: $[M, H(M)]_{KpriA}$



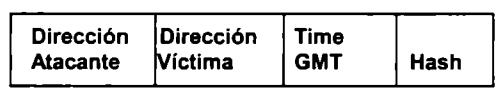
4. A encripta el mensaje entrante con la llave pública de B obteniendo: $\{[M, H(M)]_{KpriA}\}_{KpubB}$ y lo envía a B.



5. B recibe M y desencripta $\{[M, H(M)]_{KpriA}\}_{KpubB}$ con la clave privada de B, KpriB y obtiene:



6. B desencripta $[M, H(M)]_{KpriA}$ con la llave pública de A y obtiene el mensaje original:



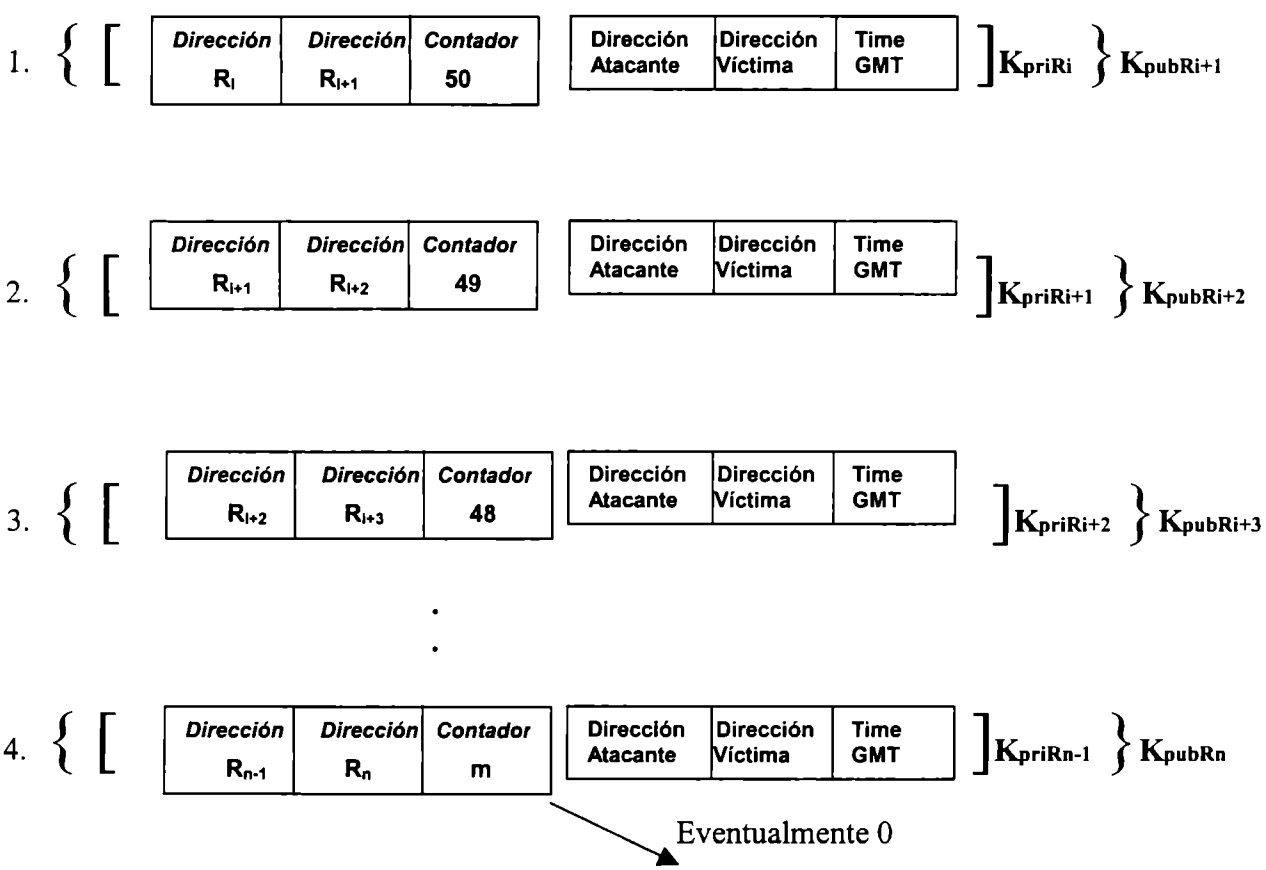
7. B le aplica la función de hash H al mensaje M recibido para obtener nuevamente H(M).

8. B compara el compendio del mensaje recibido en el paso 6 con el obtenido en el paso 7. Si son iguales quiere decir que la firma es válida.

Segundo conjunto de datos del protocolo.

Solamente requiere agregar tres datos, estos son: (Dirección del dispositivo R_i, Dirección del dispositivo R_{i+1}, y un contador de saltos) , no describiremos nuevamente el algoritmo ya que es el mismo de la primera parte del conjunto de datos, pero si mostramos a continuación cómo van cambiando los datos conforme se propaga la alerta por la red.

Cada paso representa un punto en la red conforme se va propagando la alerta.



A diferencia del primer conjunto de datos, el segundo no es constante, si la alerta se encuentra en el dispositivo de ruteo R_i el segundo campo tendrá las direcciones R_i y R_{i+1}, posteriormente, una vez que la alerta llega al dispositivo R_{i+1}, se conserva la dirección R_{i+1} sustituyendo a la dirección

del dispositivo R_i; la dirección R_{i+2} ocupará el lugar que tenía R_{i+1}. Esto se repite hasta llegar al sitio del origen del ataque.

Una situación importante de resaltar es que una vez que se llega al origen del ataque, es decir hasta el zombie que está atacando, en este punto, el último ruteador debe notificar al servidor de herramientas del site afectado que se ejecuten acciones, para detener y matar a los zombies.

5.6.2 RASTREO DEL MAESTRO

Una vez realizado esto se genera una nueva alerta, con la diferencia de que, ahora la dirección de la víctima será la del zombie que estaba recibiendo órdenes para atacar del maestro y la dirección del origen del ataque será la del maestro. Y se vuelve a repetir el mismo algoritmo hasta encontrar y detener ahora al maestro. La condición para realizarlo es que aún exista en los logs, la dirección del maestro. (ver punto 7, en página 64)

5.6.3 INFRAESTRUCTURA DE SEGURIDAD

Hemos mencionado que nuestro esquema utiliza sistemas criptográficos basados en clave pública, por tal motivo se requiere una tecnología basada en PKI, que representa el proceso de emisión de certificados digitales por medio de una Autoridad de Certificación y la administración de estos certificados; para el esquema de alertas presentado necesitamos que exista un acuerdo para conformar una PKI para manejo de alertas en Internet. (que es uno de los requerimientos más ambiciosos para contrarrestar los ataques en Internet). Ver anexo 2, para más detalles de estos estándares de criptografía de llave pública.

5.7 RUTEO EN LOS DISPOSITIVOS

A continuación se muestra una red, con el fin de ilustrar qué ocurre en el esquema propuesto al tener una alerta en R.

a) Red con cuatro redes y tres ruteadores

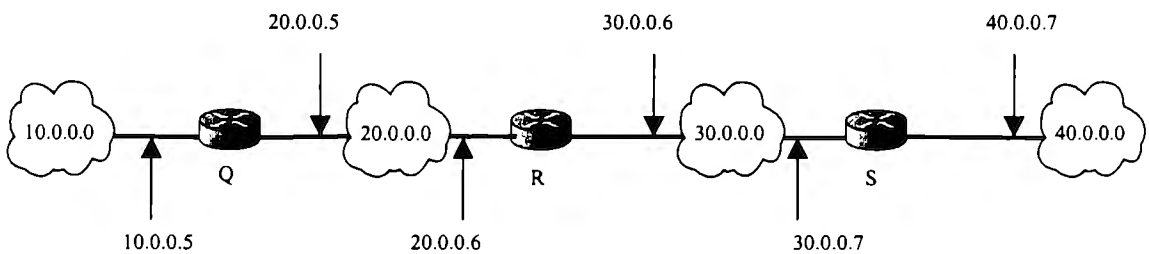


Figura 5.1

b) Tabla de ruteo en el ruteador R

PARA ALCANZAR LOS ANFITRIONES EN LA RED	RUTEAR A ESTA DIRECCION
20.0.0.0	ENTREGAR DIRECTAMENTE
30.0.0.0	ENTREGAR DIRECTAMENTE
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

Cuando a R le llegue una alerta verificará en su tabla de ruteo, si está conectado directamente con la red de donde el atacante la envía, si no checa en sus logs para observar por dónde le llega el paquete (que fue utilizado en el ataque), y lo envía a la red correspondiente, en el peor de los casos en que no conozca por dónde le llegó el paquete, deja de propagar la alerta.

5.8 EJEMPLO DE UN ATAQUE DDOS

De acuerdo a la figura 5.2, el esquema propuesto funcionaría de la siguiente manera.

1. El zombie atacante con la dirección IP 21.2.34.90, que se encuentra en la Subred 1.3 , no logra tener éxito en su ataque, ya que el ISP tiene implementado el filtro de ingreso a la red para evitar direcciones IP falsificadas. La dirección debiera ser 1.3.X.X y ésta es falsificada ya que tiene la dirección 21.2.X.X. Además el Firewall tiene la capacidad de filtrar mensajes salientes con direcciones que no pertenecen a su red interna.

2. Los ataques desde las direcciones IP 1.2.24.55 y 2.4.24.70, logran tener éxito, logrando salir desde sus respectivas redes para efectuar el ataque. Pues usan direcciones internas correctas (tal vez haciéndose pasar por alguien en su propia red)

3. En la subred 2.1, el sistema de detección de intrusos detecta un flujo de datos anormal, provenientes de la dirección IP 2.4.24.70, reacciona coordinándose con el Firewall y cerrando todo el flujo de paquetes que llega desde esa dirección.

4. Se genera la alerta correspondiente el router R6 con el primer conjunto de datos, (dirección del atacante 2.4.24.70, dirección de la víctima 2.1.30.12, hora y el hash), observa si está conectado directamente con la dirección 2.4.24.70 de donde proviene el ataque, la prueba resulta negativa, procede a verificar en sus logs, para saber por dónde le llegó el paquete, observa que proviene del router R7, prepará el segundo campo de datos (dirección del router R6, dirección del router R7, contador=50), encripta la alerta con las llaves públicas y privadas correspondientes, y envía la alerta a R7.

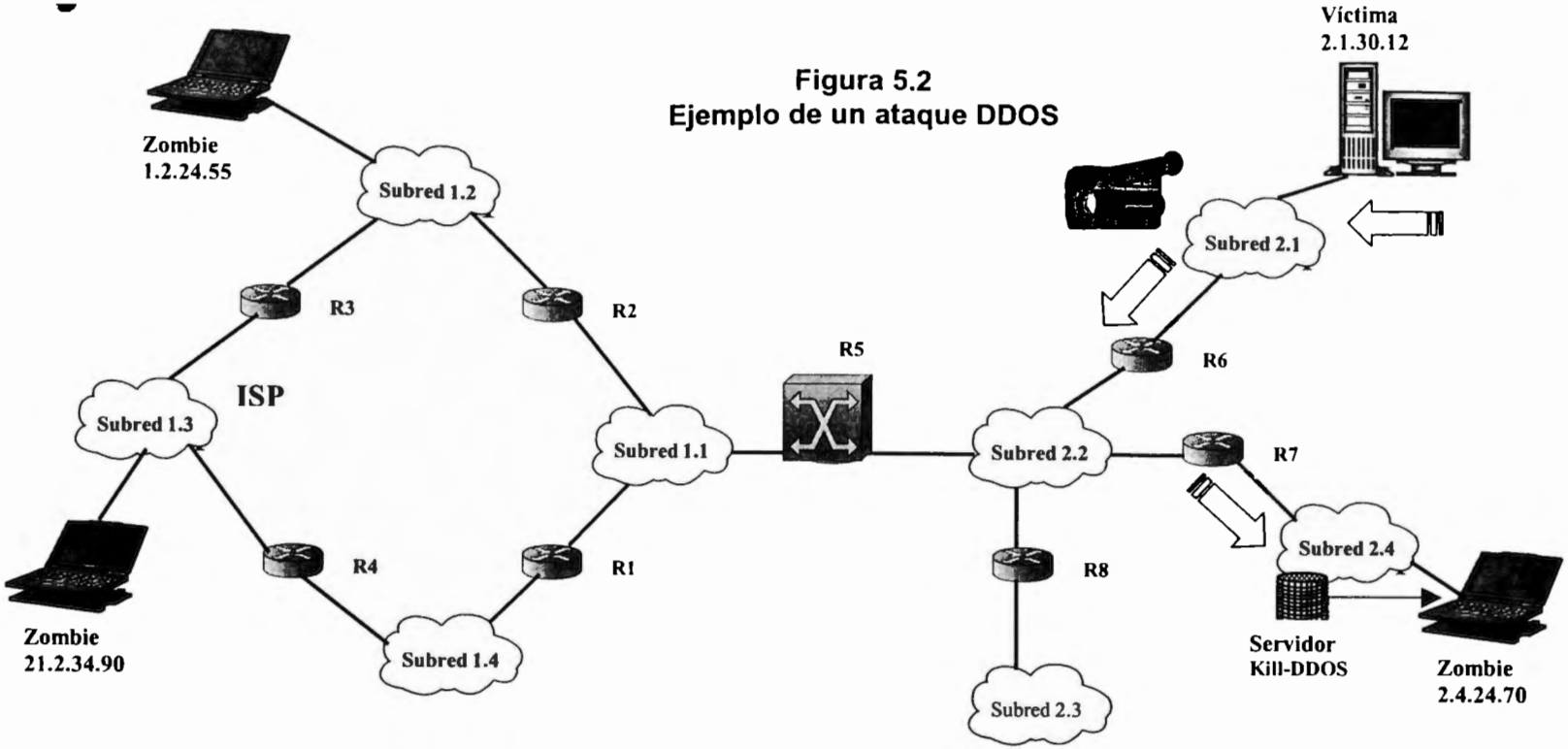
5. En el paso anterior, en el peor de los casos, que el router R6 no encontrase en sus logs por donde le llegó el paquete proveniente de la dirección del atacante 2.4.24.70, dejará de propagar la alerta.

6. Una vez que el router R7 recibe la alerta primero la autentifica, en caso de que la autentificación falle desecha la alerta y ya no la propaga más, si la autentificación resulta positiva checa con el hash para comprobar si no le ha llegado una misma alerta con la misma huella digital, en caso positivo desecha esta alerta, en nuestro caso la huella es nueva, entonces continúa el proceso.

7. El router R7, observa que se encuentra directamente (en la misma red) conectado con la dirección IP de donde proviene el ataque, entonces procede a dar las ordenes al servidor que contiene las herramientas para detener y matar al zombie con la dirección IP 2.4.24.70. Beneficiando quizá, a otras redes que estaban siendo atacadas utilizando el mismo zombie.

8. El mismo procedimiento se repite para el zombie con la dirección IP 1.2.24.55 y otros cientos más, en caso de existir.

Figura 5.2
Ejemplo de un ataque DDOS



S I M B O L O G I A	
Máquinas comprometidas con Zombies, las Cuales realizan el ataque desde la dirección X.X.X.X	Máquina objetivo del ataque, con la dirección X.X.X.X
Subred X.X — Subred X.X, dentro de Internet	Firewall y NIDS (Network Intrusion Detection System) Utilizados para detectar el ataque.
Dispositivo de Ruteo Exterior BGP (Border Gateway Protocol).	Servidor con herramientas para detener y matar a Los zombies que realizan el ataque.
Alerta	Dispositivos de ruteo Interior - Router

5.9 RECOMENDACIONES GENERALES PARA DISMINUIR LOS ATAQUES DDOS

Ante la delicada situación que puede presentarse ante este tipo de ataques, el Centro de Coordinación del CERT (CERT/CC) reunió a finales de 1999 a treinta expertos de todo el mundo con el fin de analizar la situación y proponer una serie de medidas. En los primeros días de diciembre de 1999 se publicó el documento que contenía los resultados obtenidos http://www.cert.org/reports/dsit_workshop.pdf y que básicamente contemplan una serie de recomendaciones dirigidas a Responsables de Informática, Administradores de Sistemas, Proveedores de Servicios de Internet y Grupos de Respuesta a Incidentes.

Desgraciadamente, y más que nunca, es necesario insistir en que la mejor medida adoptable es la prevención. Le versión de los protocolos IP actualmente en uso (IPv4) no permite mayores mecanismos de seguridad, y hasta que se generalice el uso de IPv6, si es que algún día sucede, seguiremos sufriendo ataques como los descritos. En general, puede decirse que el primer paso que tiene que tomar una organización para detener un ataque DDOS es identificar los demonios que lo están generando y filtrarlos individualmente en el router principal. Esto es una labor lenta, pero hasta la fecha es la única que se ha mostrado efectiva.

En la línea de la prevención, y mientras se implementan nuevos protocolos en los dispositivos de comunicación que permitan mejorar los niveles de seguridad, podrían recomendarse las siguientes medidas:

5.9.1 LIMITAR ALGÚN RANGO PARA EL TRÁFICO EN LA RED.

Algunos ruteadores tienen la característica que permite limitar el ancho de banda que cierto tipo de tráfico puede consumir. En Cisco esta característica es conocida como "Committed Access Rate" (CAR, o Tasa de acceso comprometido). Esta función le permitirá, por ejemplo, limitar el tráfico ICMP a un valor razonable, tal como 256K ó 512K. Otro ejemplo puede ser el configurar el límite del rango de paquetes SYN. [Hackers2 01]

5.9.2 MANTENER LAS MÁQUINAS ACTUALIZADAS Y SEGURAS.

Mantener actualizados nuestros sistemas, aplicando los parches destinados a eliminar vulnerabilidades. Es una labor que puede resultar tediosa, más cuantos más sistemas deben mantenerse, aunque se está avanzando en sistemas automáticos de aplicación de parches que facilitarán esta labor.
Esto implica tener también personal especializado en cuestión de seguridad (o subcontratarlo). Estar al día de los parches de seguridad de los proveedores y de las actualizaciones de kernel. Se deberán configurar adecuadamente los permisos de archivos y directorios del sistema. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, pues puede emplearla en un DDOS coordinado o para ocultar su verdadera dirección.

5.9.3 AUMENTAR EL ANCHO DE BANDA.

La forma más insidiosa de ataque DoS son los ataques de consumo de ancho de banda. Esencialmente, los atacantes consumirán todo el ancho de banda disponible en una red particular. Esto puede suceder cuando el atacante está sobre la red local atacada, pero es mucho más común que los atacantes consuman recursos remotamente.
Los atacantes son capaces de inundar la conexión de la red de la víctima porque tienen más ancho de banda disponible. Un escenario probable es alguien que tiene una conexión T1 (1.544-Mbps) u otra conexión de red más rápida, que inunda un enlace de red de 56 ó 128 Kbps. Por esta razón es recomendable aumentar el ancho de banda.

5.9.4 ADQUIRIR SISTEMAS DE DETECCIÓN.

Disponer de una política de implantación y actualización de sistemas antivirus y software para detección de intrusiones. Para esto son de gran utilidad herramientas de auditoria de sistemas y auditoria de redes.

Las herramientas que posibilitan ataques coordinados tienen una serie de huellas en la red local cuando, por ejemplo, se comunican con su "dueño". Existen herramientas de seguridad que permiten reconocer estas huellas, con lo que el administrador sabrá que ha sido contaminado antes de que su sistema sea empleado en un ataque masivo.

5.9.5 FILTRADO

Los administradores deben filtrar todos los puertos, dejando únicamente operativos aquellos que sean estrictamente necesarios. Se deben establecer filtros de entrada en la red que permitan parar ataques mediante la utilización de direcciones falsificadas. Se recomienda la lectura del RFC-2827, descrito en el capítulo 3.

Es fundamental la existencia del Centro de Emergencia de Datos como medida de prevención de desastres, pero también es fundamental que los ataques del tipo DDOS entren dentro de lo que podría denominarse desastre, teniendo previstos los mecanismos que permitan continuar la actividad en un plazo mínimo de tiempo.

5.10 CONCLUSIONES

En el esquema de protección propuesto, el cifrado de clave pública y PKI resuelven los problemas de autenticación, autorización y privacía de las alertas. Ya que los mensajes de las alertas las codificamos dos veces para autenticar al emisor así como para reforzar la privacía. Luego de que un emisor codifica el mensaje utilizando la clave privada del emisor, el emisor codifica nuevamente el resultado por medio de la clave pública del receptor. El receptor primero

aplica su propia clave privada para obtener de nuevo el primer nivel de cifrado y luego aplica la clave pública del emisor para decodificar el mensaje original.

El principal inconveniente que tiene el esquema de protección propuesto es que requiere de la cooperación de toda la comunidad en Internet, en la medida en que se exista dicha cooperación, interés y preocupación por proteger los sistemas, el esquema será mas robusto y eficiente. Independientemente de la seguridad de los sistemas que están actualmente conectados a Internet (muy inseguros y vulnerables), cada proveedor de servicios de Internet y Compañías corporativas conectadas a Internet deben proteger sus sistemas al menos con las recomendaciones arriba mencionadas, en la medida que realicen esto, serán "buenos vecinos" en la red, además de protegerse, evitarán que sus sistemas puedan ser utilizados para atacar a terceros, limitando el número de sistemas que los atacantes puedan utilizar, evitando incluso problemas o demandas legales.

6 LEYES CONTRA DELITOS CIBERNÉTICOS EN EL MUNDO

6.1 INTRODUCCIÓN

En el capítulo cinco, analizamos las medidas técnicas que podemos emplear para detectar, proteger y detener los ataques DDOS, pero hasta el momento no hemos mencionado un aspecto que es vital e indispensable: *Las leyes contra los delitos cibernéticos en el mundo.*

Inclusive algunas de las recomendaciones propuestas en el capítulo cinco, requieren del aval de los gobiernos para convertirse en normas o leyes, no sólo en ciertos países, si no en todo el mundo, de esta manera contaremos con más elementos para disuadir a los criminales cibernéticos de efectuar ataques en la red, aumentando también las posibilidades de llegar y castigar a los culpables.

En este capítulo estudiamos este tema, resaltando su debida importancia como una medida más de protección, analizando los avances y las propuestas de ley que se tienen en varios países, así como los principales retos y dificultades a los que se enfrentan los gobiernos para aprobar las leyes contra delitos computacionales.

Esta medida va orientada a desanimar a los terroristas cibernéticos de cometer delitos.

Este capítulo no pretende proponer regulaciones o normas, pues amerita un estudio profundo que está fuera del alcance de esta tesis. Este estudio resume el trabajo de la consultora McConnell.

6.2 PANORAMA GENERAL

El creciente peligro de delitos cometidos contra computadoras, o contra información contenida en computadoras, está comenzando a reclamar la atención de todas las naciones en el mundo.

En la mayoría de los países alrededor del mundo, existen leyes cuya aplicación es muy improbable, para combatir tales delitos. Esta falta de aplicación legal lleva a empresas y gobiernos a apoyarse exclusivamente en medidas técnicas para protegerse de quienes roban, *niegan acceso* o destruyen información.

La autoprotección, aún cuando es esencial, no es suficiente para hacer del ciberespacio un lugar seguro para conducir negocios. Las normas legales deben ser aplicadas. Los países donde los resguardos legales son inadecuados se volverán cada vez más incapaces en la nueva economía. Los gobiernos deben revisar sus actuales códigos para determinar si son suficientes para combatir los delitos que se presentan en Internet. En donde existan brechas, los gobiernos deberán adoptar de otras naciones las mejores medidas y trabajar estrechamente en conjunto con la industria para promulgar resguardos legales aplicables contra estos delitos.

En un informe donde se analiza el estado de la ley en 52 países. Devela que sólo diez naciones han modificado sus leyes para cubrir más de la mitad de los tipos de delitos que se deben combatir. Otras naciones tienen iniciativas en curso, es claro que se requiere de mucho más trabajo antes que las organizaciones y personas sientan que los criminales cibernéticos lo pensarán dos veces antes de atacar sistemas e información de alto valor. [McConnell 00]

6.3 ¿QUÉ HACE DIFERENTE AL DELITO CIBERNÉTICO?

No disuadidos por la posibilidad de arresto o enjuiciamiento, los delincuentes cibernéticos en todo el mundo acechan en la red como una amenaza omnipresente a la salud financiera de las empresas, a la confianza de sus clientes, y como una amenaza emergente para la seguridad de las naciones.

Los titulares de ataques cibernéticos llaman nuestra atención con mayor frecuencia. De acuerdo al Centro de Coordinación del Equipo de Respuesta a Emergencias Computacionales (CERT/CC), el número de incidentes denunciados sobre violaciones a la seguridad en el primer trimestre del año 2000 aumento en un 54 por ciento con respecto al número total de incidentes denunciados en 1999[16]. [CERT_STS 01]

Más aún, innumerables instancias de acceso ilegal y daño a la información, alrededor del mundo permanecen sin ser denunciados por las víctimas por temor a ver expuestas sus debilidades, consecuentemente el delito no es perseguido legalmente, y se va perdiendo la confianza del público.

Las grandes compañías sólo hacen públicas las agresiones en casos extremos, por las repercusiones negativas que su conocimiento público pueda tener para el prestigio del negocio.

---

[16] Ver www.cert.org. Aún cuando las siguientes organizaciones también rastrean incidentes denunciados, aún no se han compilado las estadísticas globales: El Centro Nacional para la Protección de Infraestructura (NIPC), www.nipc.gov, El Instituto de Seguridad Computacional (CSI), www.gocsi.com, y el Centro de Denuncias de Fraude en Internet, www.ifccfbi.gov.

Según un estudio de la compañía International Data Group (IDG), experta en investigaciones sobre Tecnologías de la Información, el cibercrimen merma la imagen de una empresa y le puede hacer perder hasta un 30% de sus ganancias. [Tablón 01]

El 2 de abril del 2001, en un estudio realizado por el FBI publican que durante los últimos 12 meses, el 70 por ciento del empresariado estadounidense ha informado sobre vulnerabilidades en la seguridad informática. Sin embargo sólo el 25 por ciento de las compañías que fueron atacadas por hackers reportaron el incidente a la justicia. [Tablón 01]

Aunque el número de casos de ataques cibernéticos se ha incrementado enormemente, el Departamento de Justicia (DOJ), señaló que espera que la gente reporte tales incidentes a la justicia, con el fin de generar un efecto preventivo que los reduzca. Sin embargo, el DOJ reconoce la imposibilidad de investigar en detalle todas y cada una de las denuncias sobre crimen cibernético. En tal sentido, explica que "Los daños tienen que ser al menos de 5,000 dólares para que sea considerado un crimen". [McConnell 00]

Los delitos cibernéticos – actos dañinos cometidos contra una computadora o red computacional – se diferencian de la mayoría de los delitos en cuatro aspectos.

1.- Su cometido es fácil de aprender
2.- Requieren pocos recursos en relación al daño potencial provocado
3.- Pueden ser cometidos en una jurisdicción sin estar físicamente en ella
4.- Con frecuencia su ilegalidad no es clara.

Desafortunadamente, las leyes de la mayoría de los países no prohibe los delitos cibernéticos de manera clara. La existencia de leyes contra actos físicos como invasión de propiedad o irrupción o allanamiento de morada, a menudo no contemplan sus contrapartes "virtuales". Las páginas web, tales como los sitios de negocios electrónicos afectados por ataques distribuidos de negación de servicio[17], no pueden ser cubiertos por leyes obsoletas como las formas de resguardo de la propiedad. Nuevos tipos de delitos pueden encontrarse entre los crackers, como sucedió en Filipinas cuando intentaron procesar al autor del virus del amor en mayo del 2000, el cual produjo millones de dólares de pérdidas a nivel mundial. [McConnell 00]

La efectiva aplicación de la ley se complica debido al carácter global del ciberespacio. Los mecanismos de cooperación inter-fronteras nacionales para resolver y procesar delitos son complejos y lentos. Los delincuentes cibernéticos pueden desafiar los dominios jurisdiccionales convencionales de naciones soberanas, originando un ataque desde casi cualquier computadora en el mundo, pasándolo por múltiples límites nacionales, o diseñando ataques que parecen provenir de fuentes extranjeras. Tales técnicas aumentan de modo dramático las complejidades tanto técnicas como legales de investigación y procesamiento de los delitos cibernéticos.

---

[17] Las víctimas de los ataques incluyen: Yahoo, CNN Interactive, Amazon.com, eBay, Datek Online, E*Trade, ZDNet, y Buy.com..www.mcconnellinternational.com

El futuro del mundo conectado en redes exige un enfoque más proactivo, mediante el cual los gobiernos, la industria y el público trabajen unidos para elaborar leyes aplicables que disuadan de manera efectiva si no a todos, al menos a los delincuentes cibernéticos más osados.

Tanto las leyes como los reglamentos obsoletos, sumados a débiles mecanismos de aplicabilidad para proteger información procesada en redes, crean ambientes inhóspitos para conducir sistemas claves de información dentro de un país o a través de límites nacionales. La inadecuada protección legal de información digital puede crear barreras a su intercambio y detener el crecimiento del comercio electrónico o poner en riesgo la seguridad nacional de cualquier país. A medida que se expanden los negocios electrónicos y las aplicaciones en línea, crecerá la necesidad de medios consistentes para proteger la información en redes.

6.4 EMPRESAS O GOBIERNOS ¿QUIÉN DEBE IMPEDIR LOS CIBERDELITOS?

Una vez más la eterna pregunta: ¿quién debe poner orden al enorme flujo de información que circula por Internet? ¿Debe ser el gobierno aprobando leyes más restrictivas? ¿Deben ser las empresas las que se preocupen de mantener protegidos sus sites y así impedir que atenten contra ellas?. Aunque la mayoría de las compañías son conscientes del descenso considerable de beneficios y el daño a su imagen que supone ser hackeados, también conocen los elevados costos que conlleva evitar los ciberdelitos. Esto explicaría como, según datos del estudio, los gastos en los que éstas incurren para protegerse no alcanzan el 10% y la mayoría de este presupuesto se destina a contratación de personal experto.[Tablón 01]

El problema cae entonces en los gobiernos u organismos públicos. En esta línea, la Unión Europea (UE) y el FBI ya han tomado cartas en el asunto para reducir el índice de criminalidad, tarea difícil si se tiene en cuenta que en el 2002 habrá más de 150 millones de usuarios conectados a la Red. En esta línea, un experto en seguridad informática afirma que no existen medidas organizadas para combatir el crimen organizado en Internet algo que se podría solucionar aplicando sanciones más elevadas y permitiendo que las leyes sean aplicadas tanto por la policía como por el poder judicial. [Tablón 01]

6.5 LAS LEYES CONTRA DELITOS CIBERNÉTICOS EN LAS NACIONES

En base a un estudio, y ante la incapacidad filipina para procesar al estudiante responsable del virus del amor, McConnell International[18] encuestó su red global de ejecutivos de políticas de tecnología de la información para determinar el estado de las leyes de seguridad cibernética en el

[18] McConnell International es una firma consultora en políticas globales de tecnología y administración que ayuda a sus clientes a aprovechar las oportunidades en la nueva economía. En la actualidad administra la red global de cooperación de políticas gubernamentales patrocinada por las Naciones Unidas, en donde participan 120 Naciones.

mundo. Se solicitó a los países proporcionar leyes que sean usadas para procesar actos criminales que involucren computadoras tanto del sector privado como del público. [McConnell 00]

Respondieron más de cincuenta gobiernos[19] con leyes recientes, copias de códigos actualizados, proyectos de ley, o declaraciones de que no se había planificado ningún curso de acción concreto para responder a un ataque cibernético al sector público o privado.

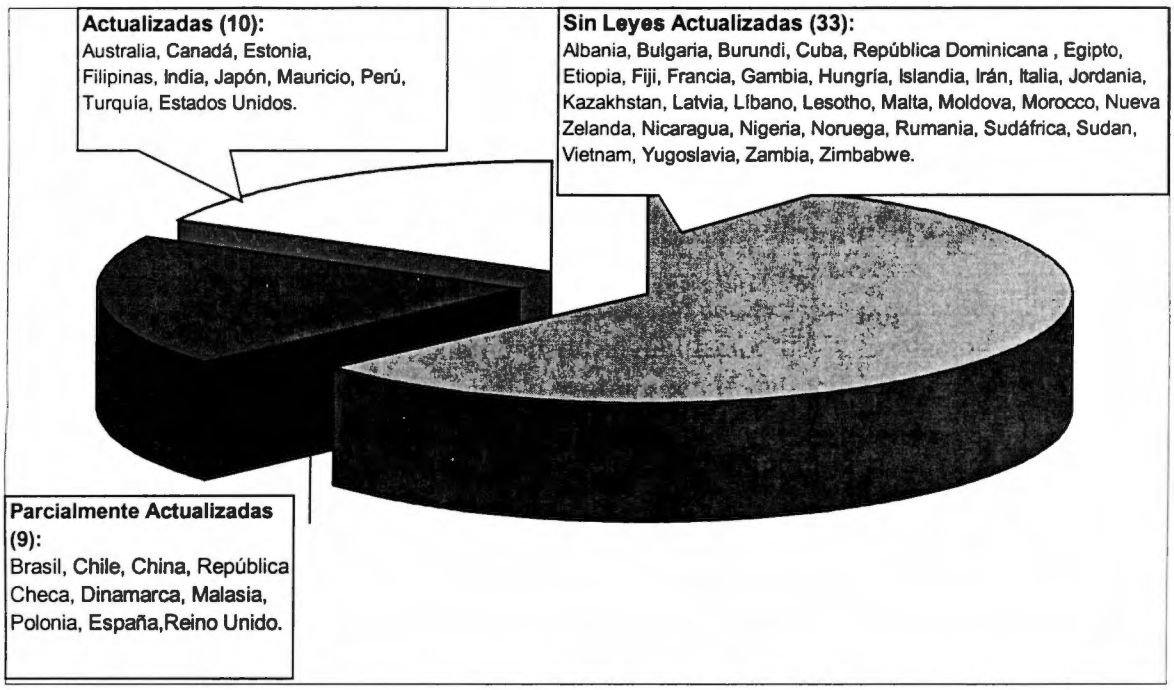
Los países que proporcionaron legislación fueron evaluados para determinar si sus códigos criminales habían sido ampliados al ciberespacio para cubrir diez distintos tipos de delito cibernético en cuatro categorías: delitos relacionados con datos, incluyendo intercepción, modificación, y robo; delitos relacionados con redes, incluyendo interferencia y sabotaje; *delitos de acceso*, incluyendo hacking y distribución de virus; y delitos relacionados con computadoras, incluyendo colaborar y encubrir a delincuentes cibernéticos, fraude computacional, y falsificación computacional. [Schjolberg 01]

Treinta y tres de estos países encuestados aún no han actualizado sus leyes para enfrentar algún tipo de delito cibernético. De los países restantes, nueve han promulgado leyes para enfrentar cinco o menos tipos de delito cibernético, y diez han actualizado sus leyes para penalizar seis o más de los diez tipos de delito cibernético. La Figura 6.1 muestra una categorización de los 52 países encuestados. [McConnell 00]

[19] Los países evaluados son: Albania, Australia, Brasil, Bulgaria, Burundi, Canadá, Chile, China, Cuba, la República Checa, Dinamarca, República Dominicana, Egipto, Estonia, Etiopia, Fiji, Francia, Gambia, Hungría, Islandia, India, Irán, Italia, Japón, Jordania, Kazakhstan, Latvia, El Líbano, Lesotho, Malasia, Malta, Mauricio, Moldovia, Marruecos, Nueva Zelanda, Nicaragua, Nigeria, Noruega, Perú, Filipinas, Polonia, Rumania, Sudáfrica, España, Sudán, Turquía, El Reino Unido, Estados Unidos, Vietnam, Yugoslavia, Zambia, y Zimbabwe.

Figura 6.1

Grado de Avance en la Actualización de Leyes Contra Delitos Cibernéticos



La Figura 6.2 detalla cuáles de los diez tipos de delitos cibernéticos son penalizados por la ley en cada uno de los 19 países con legislación en vigor, substancial o parcialmente, actualizada.

Los extractos o el texto completo de códigos pertinentes se encuentran a disposición en el sitio web de McConnell International, www.mcconnellinternational.com, para cada uno de los países señalados en la Figura 6.2 [McConnell 00]

En Canadá, los procesamientos acertados del fraude computacional han puesto al día la ley. Canadá también ejemplifica un fenómeno en muchos países, los funcionarios tienen mucha confianza que las leyes existentes serán suficientes contra "delitos relacionados con computadoras," incluyendo colaborar y encubrir a delitos cibernéticos, fraude computacional, y falsificación computacional. [Zyberk 00]

Incluso entre estos países, los delitos no son tratados de manera uniforme. En algunos, el acceso no autorizado es un delito sólo si existe la intención de producir daño; en otros, el robo de datos es un delito sólo si la información se relaciona específicamente con la religión o salud de una persona, o si la intención es cometer fraude. Las leyes tienden a favorecer la protección de computadoras del sector público. Muchas de las leyes analizadas para preparar la figura 6.2, declaran ilegales delitos cometidos con o contra computadoras gubernamentales, pero no proporciona una protección recíproca a computadoras del sector privado.

Existen discrepancias incluso dentro de países. Por ejemplo, en Septiembre del año 2000, el Partido Demócrata Australiano criticó al gobierno australiano del sur (estatal) por crear un paraíso para delincuentes cibernéticos al no actualizar sus leyes para combatir el delito computacional en conformidad con las leyes de otros estados de Australia. Más aún, como lo

indica la Figura 6.2, existe poca uniformidad en las naciones en términos de qué tipos de delitos han sido abordados a través de códigos actualizados.
Las penas aplicadas por códigos criminales actualizados varían ampliamente. Mauricio, Filipinas y los Estados Unidos aplican penas más fuertes por convicciones de delitos cibernéticos cubiertos.

Figura 6.2. Países con Leyes Actualizadas [McConnell 00]

País	Delitos de Datos			Delitos en Redes		Delitos de acceso		Delitos relacionados		
	Intercepción de Datos	Modificación de Datos	Robo de Datos	Intervención de Redes	Sabotaje de Redes	Acceso No Autorizado	Diseminación de Virus	Colaborar Y Encubrir Delitos Cibernéticos	Falsificación Computacional	Fraude Computacional
Australia	☼	☼	☼	☼		☼			☼	☼
Brasil		☼			☼	☼		☼		
Canadá	☼	☼	☼	☼	☼	☼	☼			☼
Chile	☼	☼	☼	☼	☼					
China		☼		☼			☼			
República Checa		☼	☼		☼	☼				☼
Dinamarca		☼		☼						☼
Estonia		☼	☼	☼	☼	☼	☼	☼		☼
India		☼	☼	☼	☼	☼	☼	☼		☼
Japón	☼	☼	☼	☼	☼	☼		☼	☼	☼
Malasia		☼				☼		☼		☼
Mauricio	☼	☼		☼	☼	☼	☼	☼	☼	
Perú	☼	☼	☼	☼	☼	☼				☼
Filipinas	☼	☼	☼	☼	☼	☼	☼	☼	☼	☼
Polonia		☼	☼	☼				☼		
España	☼	☼	☼					☼		☼
Turquía		☼	☼	☼	☼		☼	☼	☼	☼
Reino Unido		☼		☼	☼	☼		☼		
Estados Unidos	☼	☼	☼	☼	☼	☼	☼	☼		☼

Significado.
Intercepción de Datos: Intercepción de datos en transmisión.
Modificación de Datos: Alteración, destrucción, o eliminación de datos.
Robo de Datos: Sustraer o copiar datos, independientemente de si está protegida por otras leyes, por ejemplo, derechos de privacidad, etc.
Intervención de Redes: Impedir o evitar acceso para otras personas. El ejemplo más común de esta acción es realizar un ataque distribuido de negación de servicios(**DDOS**), inundando sitios web o Proveedores de Servicios de Internet. Los ataques **DDOS** se lanzan a menudo desde numerosos computadoras que han sido objeto de hacking para obedecer los comandos del autor.
Sabotaje de Redes: Modificación o destrucción de una red o sistema.
Acceso No Autorizado: Hacking o cracking para obtener acceso a un sistema o datos.

Diseminación de Virus: Introducción de software dañino en sistemas o datos.
Colaboración y Encubrimiento: Posibilitar la omisión de un delito cibernético.
Falsificación Computacional: Alteración de datos con la intención de representarlos como auténticos.
Fraude Computacional: Alteración de datos para obtener un beneficio económico.

Finalmente, de los 33 países sin leyes actualizadas en vigor, 13 indicaron el avance hacia la adopción de leyes actualizadas para combatir delitos cibernéticos está en curso. Siete de estos 13 países están en África o el Medio Oriente, lo que indica que, aún cuando estas regiones aún no han abordado adecuadamente el tema del delito cibernético, muchos países están conscientes de la necesidad de acciones. La siguiente sección, ofrece un resumen del trabajo en curso. [McConnell 00]

6.6 AVANCE EN CURSO EN 13 PAÍSES SIN LEYES ACTUALIZADAS

Albania La Autoridad para la Regulación de las Telecomunicaciones comenzó a debatir este año, acerca del tema de la ciber leyes, con el objetivo de elaborar protocolos de colaboración e intercambio de información.

Cuba* Un Grupo de Trabajo del Ministerio de Justicia ha planificado modificaciones al Código Penal.

Gambia está planificando una iniciativa nacional de tecnología de la información, aún cuando la capacidad para elaborar un marco legal es limitada. Gambia puede acudir a organismos internacionales en busca de orientación en torno a este esfuerzo, de modo de poder replicar o mejorar las leyes necesarias.

Irán Durante los últimos seis años, Irán ha examinado diversos aspectos de la ciber ley, aún cuando no se han implementado leyes o reglamentos en relación a delitos computacionales. Las áreas que se han considerado han sido: delitos computacionales, temas de propiedad intelectual, protección de la privacidad de datos y libertad de información.

Kazakhstan. Organismos estatales de Kazakhstan están desarrollando actualmente una ley acerca de los delitos cibernéticos. Además se encuentra en desarrollo un programa estatal especial para la protección de los recursos de información, incluyendo la protección técnica y de software.

Latvia* Se han diseñado modificaciones al Código Penal que contemplan graves castigos para actos delictivos relacionados con computación. Se añadirán las adiciones correspondientes al Código de delitos Civiles.

Lesotho ha establecido grupos especiales de interés para analizar diversos aspectos de seguridad de la información en relación con el comercio electrónico.

Malta* En el mes de mayo de 2000, Malta anunció su objetivo de brindar un sólido marco legal para el comercio electrónico, protección de datos, y mal uso computacional. Los Proyectos relevantes para desarrollar un marco legislativo para prácticas de la información fueron publicados en septiembre de 2000 y serán analizados en el Parlamento en los meses venideros.

Marruecos En Marruecos, existe un comité interministerial patrocinado por el Primer Ministro y que trabaja en temas de seguridad.

Nueva Zelanda* En la actualidad no hay delitos computacionales generalizados en Nueva Zelanda. Sin embargo, en la actualidad el país está elaborando un Proyecto de Enmienda Ley (No. 6).

Sudán tiene la intención de invitar a abogados, legisladores y profesionales de la computación a talleres de trabajo en los cuales se intercambiarán ideas acerca de la naturaleza de los delitos computacionales y las formas de enfrentarlos mediante códigos legales adecuados.

Vietnam está en proceso de recopilar información para realizar propuestas de enmienda a sus leyes.

Zambia* a puesto a disposición un anteproyecto de su Código del Consejo para las Telecomunicaciones y Tecnología de la Información.

* Copias de los respectivos documentos se pueden obtener en www.mcconnellinternational.com.

6.7 LAS LEYES CONTRA DELITOS CIBERNÉTICOS EN MÉXICO

En México los delitos informáticos están regulados por el artículo 211 bis del Código Penal Federal, que fue reformado en mayo de 1999 para "penar el acceso, uso o apoderamiento de información, la entrada sin autorización, así como la modificación o destrucción de datos que esté en un sistema informático protegido". "Las sanciones van desde 6 meses hasta dos años de prisión y multas de 100 a 300 días de salario mínimo si se trata de un ataque dirigido a particulares", si el objetivo del ataque es equipo de información del Estado las penas pueden aumentar hasta 4 años de prisión y 200 días de multa. La gravedad del castigo está en función, en gran parte, de la intenciones del atacante, ya que depende de si la intromisión se hizo con el afán de robar, modificar o provocar la pérdida de información. [Reforma 00]

Existe una nueva iniciativa de reformas y adiciones a diversas disposiciones del código penal para el distrito federal en materia del fuero común, y para toda la republica en materia de fuero federal (delitos informáticos), a cargo del C. Dip. Francisco Suárez Tanori, del grupo parlamentario del Partido Acción Nacional, la cual fue presentada el 22 de marzo del 2000. [Gaceta 00].

Los objetivos que se desea lograr con este tipo de normas son:

1.- Respeto a la integridad humana en los espacios virtuales, evitando la intromisión de agentes externos no deseados, como el abuso de la publicidad no solicitada, o el recibir correos electrónicos que no se desean, etc.

2.- Protección a los menores, evitando en la medida de lo posible que se comercie con la pornografía infantil, la violencia, formas abusivas de mercadeo, etc, que lesionan los derechos humanos fundamentales de la niñez.

3.- Fomentar la protección, independientemente de los sistemas particulares que para este fin se determinen, de la información confidencial generada por el Gobierno Federal, las fuerzas armadas, la marina, etc. (Instrucciones para la fabricación de bombas, producción de drogas, actividades terroristas, etc).

4.- Salvaguardar la propiedad intelectual. Distribución no autorizada de trabajos protegidos mediante derechos reservados. (copyright de software, música, etc.)

La Iniciativa de Reformas y Adiciones sobre diversas disposiciones del Código Penal son: [Rktconsulting 00]:

Artículo Unico: Se reforma del Título quinto, el capítulo I, artículo 167 párrafo VI; y del capítulo II del mismo título, se reforman los artículos 173 y 174, y se adiciona el artículo 174 bis. Se adiciona al Título Vigésimo segundo, capítulo III, con el artículo 389 ter, se adiciona el capítulo VII del mismo título con el artículo 399 ter, párrafos I al VIII, así como una reforma al título Vigésimo sexto, artículo 424, del Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la república en materia de fuero federal, para quedar como sigue;

Titulo Quinto
Capítulo I

Artículo 167.- Se impondrá de uno a cinco años de prisión y multa de quinientos a cincuenta mil pesos:

> VI.- Al que interrumpiere la comunicación *de una red pública de telecomunicaciones, de un espectro radioeléctrico*, telegráfica o telefónica, alámbrica o inalámbrica, o el servicio de producción, o transmisión de alumbrado, gas o energía eléctrica, destruyendo o deteriorando uno o más postes o aisladores, el alambre, *un equipo de computo*, una máquina o aparato de un telégrafo, de un teléfono, de una instalación de producción, o de una línea de transmisión de energía eléctrica.

Capítulo II
Violación de la correspondencia

Artículo 173.- Se aplicarán de tres a ciento ochenta jornadas de trabajo a favor de la comunidad:

I.- Al que abra indebidamente una comunicación escrita, *o la accese a través de medios electrónicos, electromagnéticos, u ópticos*, que no esté dirigida a él.

Artículo 174.- No se considera que obren delictuosamente los padres que abran o intercepten las comunicaciones escritas, *a través de medios manuales, electrónicos, electromagnéticos, u ópticos*, dirigidas a sus hijos menores de edad, y los tutores respecto de las personas que se hallen bajo su dependencia.

Título Vigésimo segundo
Delitos en contra de las personas en su patrimonio

Capítulo III
Fraude

Artículo 389 ter.- Comete delito de fraude, y se sancionará con prisión de tres meses a doce años y multa de cincuenta a quinientos días, al que actuando en calidad de usuario, intermediario, empresa proveedora de información, banco, o cualquier empresa comercializadora, utilice el intercambio electrónico de datos para obtener con engaños ganancias indebidas, como dinero, valores, o cualquier otra cosa, aprovechándose de su acceso a los sistemas de redes computacionales, adquiriendo, enajenando, transfiriendo, depositando, o dando en garantía productos y servicios de toda índole.

Capítulo VII
Delitos informáticos

399 ter.- *Se aplicará la pena de prisión de dos a cinco años, y de cien a trescientos días de multa al que:*

I.- Sin estar autorizado, se apodere, altere, utilice o modifique, en perjuicio de un tercero, datos reservados de carácter personal, familiar o de negocios que se hallen registrados en ficheros programas, códigos, comandos, soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

II.- Difunda, revele o ceda a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren el apartado anterior.

III.- Con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta descrita en el párrafo anterior.

IV.- Teniendo la calidad de encargado o responsable de los ficheros, programas, códigos, comandos o soportes informáticos, electrónicos o telemáticos, archivos o registros, incurra en lo descrito en los apartados I y II, se le impondrá la pena de prisión de tres a seis años de prisión.

V.- Afecte con los hechos descritos en los apartados anteriores datos de carácter personal, que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad, se impondrán las penas de cuatro a siete años de prisión.

VI.- Realice los hechos descritos de la fracción I a la III con fines lucrativos, se le impondrán penas de cinco a diez años de prisión.

VII.- Siendo proveedor de acceso a Internet, que proporcione servicios informativos que contengan material apto solo para mayores de edad, o que puedan afectar la integridad de la familia, o herir la sensibilidad de algún sector de la población, omita identificarse totalmente, incluyendo nombre o razón social, domicilio, y número telefónico, y no especifique claramente en su página de entrada la siguiente advertencia: " estas páginas contienen materiales aptos solo para adultos, si usted tiene menos de 18 años, deberá salir de esta página, si usted es un adulto que está interesado en evitar que menores de edad que manejan su équipo de cómputo, tengan acceso a estas páginas, póngase en contacto con el proveedor de la información para su cancelación."

VIII.- Siendo proveedor de acceso a internet, solicite de los usuarios el derecho de uso de sus datos personales para determinados fines como inscripción para obtener un servicio, o comprar o vender un producto, y los utilice para fines distintos sin su aprobación.

Título Vigésimo Sexto
De los delitos en materia de Derechos de autor

Artículo 424.- Se impondrá prisión de seis meses a seis años y de trescientos a quinientos días multa:

III.- A quien produzca, reproduzca, importe, almacene, transporte, distribuya, ceda o arriende copias de obras, fonogramas, videogramas, *programas computacionales*, o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Es importante resaltar que aún cuando está iniciativa es la última que se ha presentado ante el congreso, no contempla los castigos correspondientes para los atacantes que intervengan redes (que consiste en impedir o evitar el acceso a otras personas a redes), por lo tanto no se están considerando los castigos para quienes efectúen ataques DDOS. Otras Naciones si contemplan los castigos para este tipo de ataques como se describe en la sección 6.5.

6.8 INICIATIVA EUROPEA PARA FORMAR POLICÍAS POR INTERNET

Todo agente de policía (ciberpolicía) debe dominar la informática a nivel de usuario avanzado, y las unidades especializadas en delito informático deben contratar a los mejores expertos. Esta es

la idea que hay detrás del proyecto Falcone, una iniciativa de la Comisión Europea destinada a acondicionar los conocimientos de los policías a las necesidades de la era de Internet.[El País 00]

Dentro del proyecto, unos 200 agentes de España, Italia y Alemania acaban de recibir, de diciembre a febrero, un curso sobre Criminalidad Informática Organizada. La originalidad de dicho curso ha sido que se ha desarrollado, a través de Internet, en el campus electrónico de la Universitat Oberta de Catalunya (UOC). Las clases se han desarrollado en cuatro idiomas y han tratado desde los problemas técnicos y de seguridad de las redes a las distintas legislaciones nacionales sobre el delito cibernético, así como los modelos de cooperación policial y judicial en entornos nacionales e internacionales. La evaluación continua ha incluido análisis de casos reales.

La labor policial contra el crimen organizado por Internet se ve dificultada por la inexistencia de una legislación uniforme en Europa, aseguró Fermín Morales, profesor de derecho penal, en la clausura del curso. El programa Falcone podría servir "para fijar las bases de un debate común que pueda desembocar en cooperación policial y judicial y tratados internacionales", apuntó.

El proyecto Falcone podría seguir extendiéndose a otros países, incluyendo una posible colaboración con cuerpos de seguridad de Estados Unidos.

6.9 ÚLTIMAS NOTICIAS EMITIDOS PARA COMBATIR LOS CIBERDELITOS

Desde el año pasado, el gobierno norteamericano ha promovido la creación de centros para compartir y analizar información contra el ciber terrorismo (llamados ISAC por su nombre en inglés). Los tres primeros centros fueron el de servicios financieros y los de las industrias de telecomunicaciones y de suministro de energía. En diciembre del 2000, se creó el cuarto, para la propia industria de tecnologías de la información, el IT-ISAC.

Con una aportación de casi 40,000 dólares por cada una de las 19 compañías fundadoras, el centro ya opera y está abierto a la participación de más empresas, aunque dentro de las 19 ya están las más grandes del mundo. [evobo.net 01]

Por otra parte, después de los atentados terroristas del 11 de septiembre del 2001, las fuerzas armadas de Estados Unidos, Gran Bretaña y Australia anunciaron su cooperación para mejorar y desarrollar medidas de seguridad que protejan sus respectivas redes informáticas de los ataques electrónicos. Fuentes de la inteligencia militar estadounidense aseguraron a *DefenseNews.com* que China y Rusia están desarrollando programas informáticos para invadir las redes de otros ejércitos.

La preocupación del gobierno estadounidense por el ciberterrorismo, aumentó tras los ataques al Pentágono y a las Torres Gemelas. El presidente George Bush creó el 17 de octubre un equipo especial para proteger las redes de información del gobierno y del sector privado.

El acta contra el terrorismo (ATA), que propuso Bush, equipara las actividades de los hackers con los actos terroristas. De esta forma, el gobierno se propone evitar interrupciones de sistemas clave de información y, "en consecuencia, ayudar a proteger al pueblo, la economía, servicios humanos y gubernamentales esenciales y la seguridad nacional de Estados Unidos". "La protección de estos sistemas es esencial para los sectores de telecomunicaciones, energía, servicios financieros, manufactura, agua, transporte, cuidado de la salud y servicios de emergencia", añade el decreto. [La Jornada 01]

Bush ordenó a la Casa Blanca asegurar los sistemas de información, excepto los del Pentágono y las agencias de inteligencia, que están a cargo del secretario de Defensa y del director de la Agencia Central de Inteligencia (CIA). El Equipo de Protección de Infraestructura Crítica será presidido por Richard Clarke, nuevo asesor de Bush en cuestiones de Seguridad en el ciberespacio.

Expertos en computación dibujaron en el Congreso un escalofriante panorama sobre la posibilidad de ataques terroristas combinados con ciberataques en Estados Unidos.

Los especialistas mencionaron que las principales amenazas a la seguridad son los virus, el pirateo, *la negación de servicio*, la intervención, la identidad falsa y los desastres naturales o técnicos, como los apagones.

Hablando ante la Comisión de Ciencias del Congreso, la experta en seguridad informática Terry Benzel afirmó que el potencial de un ataque a la red de computación estadounidense es "más que atemorizante". "¿Qué ocurriría si los terroristas también pudieran golpear nuestros sistemas de comunicación, afectando nuestros esfuerzos de rescate?" se preguntó Benzel. [La Jornada 01]

Un informe dado a conocer un día antes del 11 de septiembre resaltó la vulnerabilidad de las redes informáticas de Estados Unidos. Según la investigación, ordenada por el gobierno, los sistemas informáticos oficiales presentan fallas que ponen en riesgo operaciones de máxima seguridad.

Los expertos han venido advirtiendo por algún tiempo sobre lo que describieron como un "Pearl Harbour electrónico", un ataque que podría causar una destrucción masiva, y pérdida de vidas. [La Jornada 01]

El día 23 de noviembre del 2001, 30 países firmaron un tratado internacional controversial para combatir el delito cibernético, 26 de estos países pertenecen al CoE[20], además se agregaron Estados Unidos, Canadá, Japón y Sudáfrica, el encuentro internacional tuvo lugar en Budapest. [Convention 01]
La convención del ciberdelitos, criminaliza actividades como la pornografía de niños, fraude y hacking, y establece reglas de cómo mantener el orden en Internet. Una nota de pie de página, agregada a principios de este mes buscaba eliminar webs racistas y de odio, pero fue eliminada del tratado para acomodar a Estados Unidos.

[20] Council of Europe

Grupos de derechos Civiles y proveedores de servicios de Internet, han rechazado el tratado, ya que dicen contiene un lenguaje vago, imponiendo fuerte castigos y fue realizado en forma secreta el cual no permitió la participación de la comunidad en general.
El tratado está abierto para cualquier país que lo desee firmar y surtirá efecto cuando 5 países lo ratifiquen, incluyendo al menos 3 miembros del CoE. [Perera 01]

6.10 CONSIDERACIONES RELEVANTES

a) La confianza en las leyes terrestres es un enfoque no evaluado.
A pesar del avance alcanzado en muchos países, la mayoría de ellos aún confía en la ley tradicional para procesar delitos cibernéticos. La mayoría de los países descansan en códigos arcaicos que anteceden el nacimiento del ciberespacio y aún no han sido puestos a prueba en los tribunales.

b) Penas bajas limitan el disuasivo.
Las bajas penas en la mayoría de los códigos actualizados producen un disuasivo limitado a delitos que pueden tener efectos económicos y sociales de gran escala.

c) La auto-protección sigue siendo la primera línea de defensa.
La debilidad general de los códigos aumenta la importancia de los esfuerzos del sector privado para desarrollar y adoptar fuertes y eficientes soluciones técnicas y prácticas de gestión para la seguridad de la información.

d) Un trabajo temporal en las leyes crea una baja certidumbre.
Existe poco consenso entre los países en cuanto a exactamente sobre qué delitos se debe legislar. La Figura 6.2 ilustra los tipos de brechas que aún existen, incluso en los 19 países que ya han tomado medidas para abordar delitos cibernéticos. En el mundo interconectado por redes, ninguna isla es una isla. A menos que los delitos sean definidos de una manera similar en las distintas jurisdicciones, los esfuerzos coordinados de los cuerpos legales para combatir el delito cibernético serán complicados.

e) Se requiere un enfoque modelo.
La mayoría de los países, particularmente aquellos en el mundo en desarrollo, están buscando un modelo a seguir. Estas naciones reconocen la importancia de declarar ilegales los actos computacionales maliciosos de una manera oportuna para promover un ambiente seguro para el comercio electrónico. Pero pocos tienen los recursos legales y técnicos necesarios para abordar las complejidades que significa adaptar códigos criminales tradicionales al ciberespacio. Se requiere una coordinación de todos los países para producir un modelo de enfoque en cuestión de leyes, que permita eliminar el potencial peligro de la inadvertida creación de paraísos para los delitos cibernéticos.

6.11 RECOMENDACIONES

El débil estado de los resguardos legales globales contra el delito cibernético sugiere tres tipos de acciones.

6.11.1. LAS EMPRESAS DEBIERAN ASEGURAR SU INFORMACIÓN PROCESADA EN REDES.

Las leyes para proteger el trabajo de derechos de autor sólo funcionan cuando sus dueños toman adecuadamente medidas para proteger su propiedad en primer lugar. Como ha señalado un observador, si los dueños de casa no compran cerradura para sus puertas a la calle, ¿debieran las ciudades solucionar el problema promulgando más leyes o contratando más policías? Incluso donde las leyes son las adecuadas, las empresas que dependen de la red deben asegurar sus propios sistemas e información.

6.11.2. LOS GOBIERNOS DEBIERAN ASEGURAR QUE SUS LEYES SE APLICAN A LOS DELITOS CIBERNÉTICOS.

Los gobiernos siguen siendo la autoridad dominante para regular el comportamiento criminal en la mayor parte del mundo. Una nación que ya ha luchado y establecido sus leyes contra los delitos cibernéticos, es crucial para que otras naciones saquen provecho de esta lección, y examinen sus actuales leyes para discernir si están compuestas de una forma tecnológicamente neutra que no excluye el procesamiento de delitos cibernéticos. En muchos casos, las naciones encontrarán que las leyes deben ser actualizadas. La promulgación de leyes contra delitos computacionales que también respeten los derechos de las personas son el siguiente paso en la batalla contra esta amenaza emergente.

6.11.3. LAS EMPRESAS, GOBIERNOS, Y LA SOCIEDAD CIVIL DEBEN TRABAJAR DE MANERA COOPERATIVA PARA FORTALECER LOS MARCOS LEGALES PARA LA SEGURIDAD CIBERNÉTICA.

Para procesar en otras jurisdicciones, un acto debe ser un delito en cada jurisdicción. Así, no obstante se deben respetar las tradiciones legales locales, las naciones deben definir delitos cibernéticos de forma similar. Un importante esfuerzo para crear un modelo de enfoque está en curso en el Consejo de Europa (ver www.coe.int), que reúne a 41 países. El Consejo está redactando una Convención internacional sobre el Delito Cibernético. La Convención aborda el acceso ilegal, intervención ilegal, intervención de datos, intervención de sistemas, falsificación computacional, fraude computacional, y la ayuda y encubrimiento de estos delitos. También aborda materias de investigación relacionadas con jurisdicción, extradición, intercepción de comunicaciones, y la producción y preservación de datos. Finalmente, promueve la cooperación entre los funcionarios judiciales a través de fronteras nacionales. En la etapa final de su proceso, el Consejo comenzó a considerar las opiniones de la industria y sociedad civil afectadas. Este proceso está volviendo el producto del Consejo más realista, práctico, eficiente, equilibrado y

respetuoso del debido proceso que protege los derechos individuales. En este punto, la mayoría de los observadores apoyan disposiciones que mejoran la cooperación para la aplicación de la ley inter-fronteras. Sin embargo, La Alianza Mundial de Servicios y Tecnologías de la Información (ver www.witsa.org/press/), argumenta que los requerimientos a los proveedores de servicios para monitorear las comunicaciones y para proveer asistencia a investigadores, como se esboza en el Borrador de la Convención, serían indebidamente pesados y costosos. Otra disposición considerada como objetable podría penalizar la creación y uso de software intrusivo, o programas de hacking, los cuales son diseñados para legitimar propósitos de testeo de seguridad. Esta acción podría reprimir los avances en tecnología vitales para enfrentar exitosamente las amenazas cibernéticas en evolución. Los partidarios de la privacidad y de los derechos humanos (ver www.gilc.org) objetan al Borrador de la Convención de su falta de resguardos procesales y del debido proceso para proteger los derechos de las personas, y la posibilidad de que las inminentes leyes nacionales impongan de manera efectiva restricciones sobre la privacidad, anonimato y encripción.[WITSA 00]

En este año 2001, un proceso político que involucra gobiernos determinará el alcance y cobertura de la Convención final. Debido al potencial internacional del delito cibernético, todos los países, y todas las empresas, se ven afectadas. Partes interesadas, incluyendo gobiernos no europeos, y empresas y organizaciones no gubernamentales de todo el mundo, debieran participar de manera vigorosa en un proceso de consenso para desarrollar medidas que apoyen efectivamente la aplicación de leyes internacionales y promuevan un continuo crecimiento e innovación.

7 CONCLUSIONES

La gran cantidad de aplicaciones y servicios que se prestan hoy en día a través de Internet, como el comercio electrónico, y sobre todo de los servicios críticos en redes financieras y empresariales, requieren que el servicio que se presta no se vea suspendido en ningún momento, y su principal amenaza son los ataques de negación de servicio. Situación que ha provocado que gobiernos y empresas inviertan considerables recursos para evitar esta amenaza constante que se tiene en Internet.

En este estudio analizamos el funcionamiento de los principales ataques de negación de servicio, centrando nuestro estudio en el ataque distribuido de negación de servicio (DDOS), el cual combina algunos de los principales ataques de negación de servicio (como smurfing e inundación SYN) con otras técnicas, por ejemplo falsificación de direcciones IP y cifrado en sus comunicaciones, lo cual hace al ataque complejo y con gran capacidad para dejar fuera de servicio al objetivo atacado. El otro factor que lo hace muy eficaz es que se realiza desde cientos de máquinas previamente comprometidas siendo realmente difícil de detener una vez que se ha iniciado el ataque. Podemos afirmar que los ataques DDOS ocurridos en febrero del 2000, son los más importantes ataques de negación de servicio conocidos hasta hoy y uno de los más trascendentales ataques que se presentan en Internet.

Este tipo de ataques no ha disminuido, por el contrario han ido en aumento y son un riesgo latente al que se debe prestar atención y no menospreciarlo. Desgraciadamente la versión de los protocolos IP v4, no permite mayores mecanismos de seguridad, y hasta que se generalice el uso de IP v6 (donde al menos contaríamos con autenticación, confidencialidad e integridad a nivel de capa de red), si es que algún día sucede, seguiremos sufriendo considerables ataques de esté tipo. Aunado a esto, los sistemas operativos y los programas de aplicación siempre tienen vulnerabilidades, es decir, la tecnología y algunas veces las personas favorecen, intencional o descuidadamente, a quienes realizan los ataques. Por lo tanto el panorama hacia el futuro para evitar o erradicar los ataques de negación de servicio, no es muy halagador, ya que siempre aparecen nuevos ataques de este tipo y son cada vez más peligrosos. Sin lugar a dudas los ataques distribuidos de negación de servicio han dejado al descubierto las grandes deficiencias que existen aún en materia de seguridad computacional en la red, a pesar de que muchas de las vulnerabilidades han sido identificadas (más no corregidas) desde mediados de los 80's.

Por las razones expuestas en el párrafo anterior, desarrollamos un esquema de protección general para mitigar este tipo de ataques, el cuál requiere de nuevas características que deberán implantarse en los dispositivos de ruteo, y que además considera algunas propuestas de los RFC de Internet (por ejemplo RFC 2827). Otro punto fuerte e interesante, mas difícil de lograr, es que, para que este esquema sea eficaz, se requiere la cooperación de toda la comunidad de Internet. Principalmente todos los proveedores de servicios de Internet y las empresas conectadas a Internet mediante sus redes corporativas, deben preocuparse y tomar las medidas adecuadas para proteger sus sistemas, en el grado en que cada uno de los sistemas conectados a Internet carezca de vulnerabilidades para ser explotadas, la posibilidad de ataques de negación de servicio disminuirá considerablemente. Consideramos que, aunque un tanto futurista, tarde o temprano (cuando existan mayores intereses en Internet), se normarán tecnológica y legalmente los usos que demos a esta tecnología. Esto conducirá igualmente a acuerdos y cooperación para proteger de manera mundial los servicios y facilidades ofrecidas en Internet.

Una ventaja del esquema planteado, es que al lograr detener los zombies, éstos en ocasiones pueden estar atacando a varios objetivos y no sólo uno, al detener los zombies muy probablemente ayudaremos a otros sistemas que también pueden estar siendo atacados utilizando los mismos zombies para efectuar otros ataques, de esta manera el esquema planteado, que necesita como requisito la cooperación de la comunidad de Internet, como recompensa todos se *verán* también favorecidos con las medidas aplicadas y no sólo las víctimas de los ataques, creando sobre todo, un sistema robusto y altamente cooperativo.

Con respecto a los programas y herramientas con que se cuenta para detectar y detener los ataques DDOS, no debemos olvidar que éstas normalmente actúan contra las herramientas convencionales de ataque DDOS como son: Trinoo, TFN, TFN2K, etc. Por lo tanto es posible que las mutaciones que aparezcan de herramientas para efectuar ataques DDOS no las detecten.

Quizás nunca seamos víctima de un ataque DDOS, pero puede ser problemático el hecho de que nuestros sistemas pudieran ser utilizados como vía para llevarlos a cabo, llegando incluso a contraerse problemas legales, sobre todo con las nuevas leyes más severas que se están proponiendo y aplicando hoy en día en la mayoría de los países.

Por otro lado, las leyes son sólo una parte de la respuesta, el ampliar el alcance de la ley al ciberespacio es un paso crítico para crear un ambiente confiable tanto para la gente como para las empresas. Puesto que tal expansión continúa siendo un trabajo en estudio, hoy en día las organizaciones deben antes que nada defender sus sistemas e información de ataques. Sólo pueden confiar de manera secundaria en el disuasivo que puede proporcionar la efectiva aplicación de la ley.

Para proporcionar esta auto-protección, las organizaciones deben centrar sus esfuerzos en implementar planes dirigidos a la gente, procesos y temas tecnológicos. Las organizaciones deben comprometer los recursos para educar a sus empleados sobre prácticas de seguridad, desarrollar planes rigurosos para manejar información, registros y transacciones sensibles, e incorporar una fuerte tecnología de seguridad -- tales como firewalls, software anti-virus, herramientas detectores de intrusiones, y servicios de autentificación -- a través de los sistemas

computacionales de las organizaciones. Aún cuando un administrador de sistemas no pueda prevenir completamente los ataques, algunas medidas de seguridad básicas como las presentadas en este documento, pueden disuadir a quienes las cometen, haciendo que los ataques sean mucho más difíciles de realizar. Aunque algunas medidas si requieren más recursos, las grandes empresas, seguramente no escatimarán esfuerzos para proteger sus sistemas, considerando que para algunas de éstas, el estar fuera de servicio un par de horas, representaría pérdidas económicas considerables.

Finalmente, este estudio presentó un panorama de los ataques de negación de servicio, se concentraron los mecanismos de defensa propuestos de manera aislada por la tecnología actual, y por último se esbozó un esquema que presenta de manera conjunta las medidas de protección y trata de aglutinarlas con los aspectos que consideramos faltantes, como son algunas características de cooperación entre dispositivos de comunicación, tanto de los grandes proveedores de portadoras, como de los ISP y las redes corporativas. Asimismo se señaló la necesidad de perfeccionar las herramientas de detección de este tipo de ataques, pues son ellas el punto de arranque para poder minimizar los daños que éstos puedan causar. Puesto que el atacante puede estar prácticamente en cualquier parte del globo, y estar sujeto a una jurisdicción completamente diferente a la de su víctima, se presentó un panorama del marco de legislación electrónica actual en el mundo y en México, y se resaltó la necesidad de homologar las leyes entre los diferentes países participantes en Internet.

BLIOGRAFÍA

[Anónimo01 00] Anónimo, Linux Máxima Seguridad, Prentice Hall, 2000. p 486.

[Douglas 96] Douglas E. Comer, Redes Globales de Información con Internet y TCP/IP Prentice Hall, 1996.

[Stallings 97] William Stallings, Comunicaciones y Redes de Computadores, Prentice Hall, 1997.

[Stephen 99] Stephen Northcutt, Network Intrusion Detection: An Analyst's Handbook New Riders, 1999, 267 p.

[Stuart 01] Stuart McClure, Joel Scambray, George Kurtz
Hackers 2. Secretos y soluciones para la seguridad de redes
McGraw-Hill, 2000, p. 538.

[Stuart01 01] Idem [Stuart 01], p.539.
[Stuart02 01] Idem [Stuart 01], p.547.
[Stuart03 01] Idem [Stuart 01], p.563.
[Stuart04 01] Idem [Stuart 01], p.560.
[Stuart05 01] Idem [Stuart 01], p.545.

REFERENCIAS ELECTRÓNICAS

[Activamente 01] Virus Nimda. Septiembre del 2000.http://www.activamente.com/nimda/

[Barlow 00] Jason Barlow, Woody Thrower, AXENT Security Team. TFN2K – An Analysis. 7 de marzo del 2000. http://packetstorm.decepticons.org/distributed/TFN2k_Analysis-1.3.txt

[cem.itesm 01] Alldas.de sin ISP. 17 de septiembre del 2001. http://dsc01.cem.itesm.mx/seguridad/article.php?sid=85

[CERT_csmd 00] CERT Advisory CA-99-08 Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd. http://www.cert.org/advisories/CA-99-08-cmsd.html

[CERT_inc 99] CERT Incident Note IN-99-04. 9 de Diciembre de 1999. http://www.cert.org/incident_notes/IN-99-04.html

[CERT_Nim 01] CERT Advisory CA-2001-26 Nimda Worm. 18 de septiembre del 2001. http://www.cert.org/advisories/CA-2001-26.html

[CERT_STS 01] CERT/CC Statistics 1988-2001, http://www.cert.org/stats/cert_stats.html,

[CERT01 95] "Denial of Service Incidents" Un capítulo de CERT Coordination Report que revisa los ataques DoS de 1988 a 1995. Gran Documentación Histórica sobre ataques DoS. http://www.cert.org/research/JHThesis/Chapter11.html

[CIDR 00] Sans Institute Resources, CIDR Table 23 de marzo del 2000. http://www.sans.org/dosstep/cidr.htm

[Cisco 00] Strategies to Protec Against Distributed Denial of Service (DDoS) Attacks February 17, 2000. http://www.cisco.com/warp/public/707/newflash.html

[Convention 01] Convention on Cybercrime, Budapest, 23 de noviembre del 2001. http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm

[Diarioti 01] Ataques DDOS amenazan IRC. 15 de Enero del 2001. http://www.diarioti.com/noticias/2001/ene2001/15193861.htm

[Diarioti_Tri 00] Surgen nuevas Herramientas DoS, Trinity V3, 7 de septiembre del 2000. http://www.diarioti.com/noticias/2000/sep2000/15193446.htm

[Dinformaticos 01] Hackers de China y EE.UU. Intercambian Ataques. 25 de abril del 2001. http://www.delitosinformaticos.com/noticias/98818797137295.shtml

[Dittrich_dds 01] David Dittrich Program to scan for a limited set of distributed denial o f service (ddos) agents. http://staff.washington.edu/dittrich/misc/ddos_scan.tar.

[Dittrich_mst 00] David Dittrich, George Weaver, Sven Dietrich, Neil Long. The "mstream" distributed denial of service attack tool 1 de mayo del 2000. http://staff.washington.edu/dittrich/misc/mstream.analysis.txt

[Dittrich_stach 99] David Dittrich, The "stacheldraht" distributed denial of service attack tool, 31 de Diciembre de 1999. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[Dittrich_tfn 99] David Dittrich , The "Tribe Flood Network" distributed denial of service attack tool, 21 de octubre de 1999. http://staff.washington.edu/dittrich/misc/tfn.analysis.txt

[Dittrich_trinoo 99] David Dittrich, The DoS Project's "trinoo" distributed denial of service attack tool, 21 de octubre de 1999. http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt

[El País 00] Iniciativa europea para formar policías por Internet http://www.granavenida.com/prehackers/prensa/2002201.htm

[Evobotnet 01] Atacan Sitos de Microsoft. 26 de Enero del 2001. http://www.evobo.net/noticia_det.asp?not=17

[Foundstone 00] DDoSPing v2.0 - A network admin utility for remotely detecting the most common DDoS programs.by Foundstone, Inc. 20 de noviembre del 2000. http://www.foundstone.com/rdlabs/proddesc/ddosping.html

[Gaceta 00] Gaceta Parlamentaria, año III, número 474, miércoles 22 de marzo de 2000. http://gaceta.cddhcu.gob.mx/Gaceta/2000/mar/20000322.html

[Huegen 00] Craig A. Huegen, The latest in denial of service attacks: "smurfing" Description and information to minimize effects, Febrero del 2000. http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

[Internautas 01] Un ataque DDOS bloquea al CERT. 25 de mayo del 2001. http://social.internautas.org/articulo.php?sid=9

[Knight 00] Will Knight, Experts warn of multiple computer attacks, 4th October 2000. http://news.zdnet.co.uk/story/0,,t269-s2081778,00.html

[La Jornada 01] Jesús Ramírez Cuevas, Los frentes de la ciberguerra, domingo 18 de noviembre del 2001, sección masiosare, pg.3-5

[Linuxcl 01] Network Associates víctima de DDOS por descubrir Bug. 12 de febrero del 2001. http://www.linux.cl/article.php?sid=68

[McConnell 00] Cyber Crime ... and Punishment? Archaic Laws Threaten Global Information, December 2000, By McConnell International. http://www.mcconnellinternational.com/services/CyberCrime.htm .

[Mundo 00] Oleada de ataques en Internet....¿quién será el siguiente? 9 de Febrero del 2000. http://www.el mundo.es/navegante/diario/2000/02/09/ataques.html

[Navegante 00] Diario el Navegante, Oleada de ataques en Internet, 9 de febrero del 2000 http://www.el mundo.es/navegante/diario/2000/02/09/ataques.html

[Nipc 01] Find Distributed Denial of Service (DDOS), by NIPC. http://www.nipc.gov

[Perera 01] Rick Perera. Thirty Countries sign cybercrime treaty , Computerworld 23 de noviembre del 2001. http://computerworld.com/nlt/0%2C3590%2CNAV65-663_STO66012_NLTSEC%2C00.html

[Razor 00] Zombie Zaper, Open source tool that can tell a zombie system flooding packets to stop flooding. 29 de marzo del 2000. http://razor.bindview.com/tools/ZombieZapper_form.shtml

[RCF_2612 99] C. Adams, J. Gilchrist The CAST-256 Encryption Algorithm. Junio de 1999. http://sunsite.dk/RFC/rfc/rfc2612.html

[Reforma 00] Máximo Curi, Adriana Vizcaíno, Hackers en la era de la globalización. 20 de mayo del 2001. http://www.reforma.com/internacional/articulo/096398/

[RFC_2644] D. Senie, Amaranth Networks Inc. "Changing the Default for Directed Broadcasts in Routers". Agosto de 1999. http://www.rfc-editor.org/rfc/rfc2644.txt

[RFC_2827] P. Ferguson, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". Mayo del 2000. http://www.faqs.org/rfcs/rfc2827.html

[Schapachnik 00] Fernando Schapachnik, Distributed Denial Of Service attacks A proposal based on routing. 3 de abril del 2000. http://rootprompt.org/article.php3?article=297

[Schjolberg 01] Stein Schjolberg, Penal Legislation in 42 Countries, 27 de noviembre del 2001. http://www.mossbyrett.of.no/info/legal.html

[Schneier 01] B. Schneier , Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). http://www.counterpane.com/bfsverlag.html.

[Spack 01] Microsoft, Windows NT Server 4.0, Service Pack (Q152734), 9 de agosto del 2001. http://support.microsoft.com/support/kb/articles/Q152/7/34.ASP

[Sven_shaft 00] Sven Dietrich, Neil Long, David Dittrich, An analysis of the ``Shaft" distributed denial of service tool. !3 de Marzo del 2000. http://www.adelphi.edu/~spock/shaft_analysis.txt

[Tablón 01] Empresas o Gobiernos ¿Quien debe impedir los ciberdelitos?, 17 de Julio del 2001. http://www.virusprot.com/Tablon.html

[Tanenbaum 97] Andrew S. Tanenbaum, Redes de Computadoras, Prentice Hall, 1997.

[Tripod 01] DDoS/Apbot@mm Ataque DDOS. VSantivirus No. 387 - Año 5, 30 de julio de 2001 http://videosoft.tripod.com/apbot.htm

[Ulatina 01] Atacan la red de IRC Undernet, 11 de enero del 2001. http://www.unionlatina.org/noticias/enero.html

[Virusprot Blue 01] Code Blue, ¿el virus vengativo?.Virusprot. 10 de septiembre del 2001. http://www.virusprot.com/Nt100921.html

[Virusprot Red 01] ¡Alerta! Code Red, ¿al ataque?, Virusprot. 20 de agosto del 2001. http://www.virusprot.com/Nt200822.html

[WITSA 00] World Information Technology and Services Alliance (WITSA) Statement on the Council of Europe Draft Convention on Cyber-Crime http://www.witsa.org/papers/COEstmt.pdf

[Workshop 99] Distributed-Systems Intruder Tools Workshop, Pittisburgh, Pennsylvania USA, November 2-4, 1999. http://www.cert.org/reports/dsit_workshop.pdf

[Yahoo 00] Diario el navegante, Yahoo! sufre el peor ataque informático de su historia. 8 de febrero del 2000. http://www.el-mundo.es/navegante/diario/2000/02/08/yahoo.html

[Zakon 01] Hobbes' Internet Timeline, 1993-2001 by Robert H Zakon
http://www.zakon.org/robert/internet/timeline/

[Zonaluz 01] Sistema de alerta de virus, I-Worm.fog, Julio del 2001.
http://www.zonaluz.com.mx/sav/2001/julio01.htm

[Zyberk 00] Helena Plater-Zyberk, Canadian Cyber Crime Laws Are Among the Strongest, 2 January 2000
http://www.mcconnellinternational.com/pressroom/20010102.cfm

ANEXOS

ANEXO 1. ALGORITMO BLOWFISH

Describiremos el algoritmo Blowfish por ser utilizado para cifrar la lista de demonios activos en Trinoo, también se utiliza para cifrar el archivo que contiene la relación de direcciones IP en TFN y Stacheldraht, así como las comunicaciones entre el cliente y el conductor en Stacheldraht, es un algoritmo diseñado por Bruce Schneier, y está diseñado para ejecutarse preferentemente en microprocesadores y satisfacer los siguientes criterios: [Schneier 01]

1. Rapidez. Blowfish encripta datos en procesadores de 32 bits a razón de 26 ciclos de reloj por byte.
2. Escaso consumo de recursos. Blowfish necesita como mínimo sólo 5 Kb de 1memoria.
3. Simplicidad. Blowfish usa operaciones simples: suma, XOR, y manejo de tablas con operandos de 32 bits. Su diseño es fácil de analizar, y por tanto pueden descubrirse fácilmente errores de implementación.
4. Seguridad configurable. La longitud de la clave de Blowfish es variable, y puede llegar hasta 448 bits.

Blowfish maneja bloques de datos de 64 bits. El algoritmo tiene dos partes: expansión de la clave y encriptación de los datos. Se utiliza un array P, formado por 18 subclaves de 32 bits, y 4 S-boxes de 32 bits con 256 elementos cada una. La expansión de la clave convierte una clave de 448 bits en varios arrays de subclaves que totalizan 4168 bytes. Explicaremos más adelante el proceso de cálculo de las subclaves. [Schneier 01]

El proceso de encriptación está formado por 16 rondas, siendo la entrada un bloque de datos de 64 bits, x. El algoritmo consiste en:

Dividir x en dos mitades de 32 bits: x_L, x_R
Para $i = 1$ hasta 16
  $x_L = x_L$ XOR P_i
  $x_R = F(x_L)$ XOR x_R
  Pasar x_L a la "derecha" y x_R a la izquierda
Pasar x_L a la "derecha" y x_R a la izquierda (deshace el intercambio de posición de la última ronda)
$x_R = x_R$ XOR P_{17}
$x_L = x_L$ XOR P_{18}
Unir x_L y x_R

Para la función F se divide x_L en cuatro partes de 8 bits, a, b, c y d, y se calcula:

$$F(x_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \text{ XOR } S_{3,c}) + S_{4,d} \bmod 2^{32}$$

El proceso de desencriptación sigue el mismo algoritmo, salvo que P_1, P_2,... P_{18} se usan en orden inverso. El cálculo de las subclaves se realiza utilizando el algoritmo Blowfish:

1. Inicializar el array P y las cuatro S-boxes con una cadena fija, formada por dígitos hexadecimales del número pi.
2. Hacer el XOR de P_1 con los primeros 32 bits de la clave, el XOR de P2 con los siguientes 32 bits... y así con toda la clave, hasta llegar a P_{18}. Si se terminan los bits de la clave antes de haber completado el array P, se vuelve a empezar con el primer bloque de 32 bits.
3. Encriptar una cadena formada por ceros según el algoritmo Blowfish, utilizando las subclaves obtenidas en los pasos 1 y 2.
4. Sustituir P_1 y P_2 por la salida del paso 3.
5. Encriptar la salida del paso 3 usando el algoritmo Blowfish con las nuevas subclaves.
6. Sustituir P_3 y P_4 por la salida del paso 5.
7. Continuar con el proceso, sustituyendo todos los elementos del array P, y después todos los elementos de las S-boxes.

Hace falta un total de 521 iteraciones para obtener todas las subclaves.
Serge Vaudenay ha atacado Blowfish utilizando S-boxes conocidas y r rondas; un ataque con criptoanálisis diferencial podría obtener el array P con 2^{8r+1} textos no encriptados seleccionados (lo que en la bibliografía en inglés se conoce como "chosen plaintext attack", es decir, un ataque en el que se utilizan para el análisis parejas de textos no encriptados y el correspondiente texto encriptado, seleccionando aquellas parejas que podrían revelar más contenido de la clave que otros). Con algunas claves débiles que generan S-boxes de peor calidad, el mismo ataque necesita 2^{4r+1} textos no encriptados seleccionados. La posibilidad de dar con una de estas claves es de 1 entre 2^{14}. Si se realiza el ataque sin conocer las S-boxes, se puede detectar si se está usando una clave débil, pero no si se trata de una S-box o del array P. El ataque sólo funciona con versiones de Blowfish que usaran pocas rondas, siendo completamente inútil contra la versión con 16 rondas. [Schneier 01]

Así pues, no existe por ahora ningún ataque contra Blowfish basado en criptoanálisis que sea efectivo. Quedaría entonces el ataque de fuerza bruta, que en el caso de utilizar la mitad de los bits para la longitud de la clave de Blowfish, es decir 224 bits, necesitaríamos hacer frente a 2^{224} posibles claves.

De acuerdo a la descripción del algoritmo Blowfish podemos concluir que ésta se utiliza en las principales herramientas de ataque DDOS por su rapidez, poco consumo de memoria 5 Kb y la simplicidad de implantación. Además, es considerado como uno de los algoritmos mas seguros.

ANEXO 2 AUTORIDADES DE CERTIFICACIÓN

En nuestro esquema vimos que nuestros servicios de seguridad utilizan técnicas criptográficas de clave pública. En el contexto esto implica que los receptores deben tener acceso a la clave pública de los emisores y viceversa. El problema que surge es cómo se realiza dicho intercambio en forma segura.

Una solución evidente es un intercambio previo en forma personal o por un canal "seguro", pero ésta no es aplicable a un uso generalizado de nuestras comunicaciones entre dispositivos R´s, ya que muchas veces las partes que intercambian mensajes no tienen un canal de comunicación seguro alternativo para el intercambio de claves. Al diseñar un protocolo aplicable a nuestro sistema de comunicación, se debe tener en cuenta que las partes no disponen de una conexión (en el sentido de canal de comunicación *conectado*) entre ellas. Esto limita enormemente el tipo de protocolos a utilizar. Una segunda alternativa sería que el intercambio se haga en forma electrónica, utilizando el mismo medio que utilizan para intercambiar los mensajes de correo. Esto implicaría que primero A y B intercambian sus claves públicas vía e-mail y luego intercambian mensajes utilizando estas claves. El problema que presenta esta solución es que ni A ni B tienen la certeza de que la contraparte sea realmente quien dice ser. Ya que es relativamente fácil impersonificar a otros vía email, por lo que este esquema es altamente susceptible a un *"man in the middle attac*k".

Nosotros necesitamos disponer de un proceso en el cual puede obtener la clave pública de algún dispositivo en forma segura, en el momento en que la necesite, sin intervención explícita de este dispositivo. Surgen como solución general a este problema las *Autoridades de Certificación (CA* por sus siglas en inglés). Una CA es una tercera entidad en el intercambio de mensajes, en la cuál confía tanto quien envía como quien recibe. Es tarea de la CA proveer los mecanismos necesarios para el intercambio de claves públicas en forma segura. El concepto básico que utilizan es la *Certificación de Clave*s. El principal cometido de una CA es *certificar* que la relación entre una entidad (para nuestro caso un dispositivo de comunicación) y su clave pública es válida, de la misma manera en que un escribano certifica que una firma en papel de una persona es válida.

A modo de ejemplo, supongamos que los ruteadores A y B desean hacer un intercambio de mensajes, para lo que necesitan intercambiar sus claves públicas, el procedimiento general a seguir es el siguiente:

a) A genera su pareja de claves Apriv y Apub. Lo mismo hace B.
b) A entrega a la CA su clave pública junto con documentación que acredite que sea

realmente A. La CA certifica la autenticidad de esta relación entregándole un certificado.
c) B hace lo mismo, obteniendo su propio certificado.
d) A y B intercambian certificados
e) A y B pueden ahora intercambiar mensajes en forma segura, suponiendo que la certificación sea válida.

Es importante destacar que todo esto funciona si A y B confían en la autoridad de certificación y en los certificados que ésta entrega. La duda que surge es cómo hacen A y B para tener la certeza de que los certificados son válidos. Veremos posteriormente en que consiste un certificado y como pueden hacer A y B para verificar la autenticidad de estos.

El método es muy general y de hecho se utiliza para autenticar no sólo a dispositivos de red sino cualquier entidad como puede ser, una persona, un servidor de web, un rol dentro de una organización, un software, etc.

Durante el resto de este anexo hablaremos de autoridades de certificación, pero hay una estructura que engloba sus actividades llamada PKI: *Public Key Infraestructure.* Esta comprende a las propias autoridades de certificación, a las autoridades de registro (RAs), el software para la generación y respaldo de claves, además de los protocolos ligados a esta actividad como son el acceso a directorios de datos (por ejemplo, LDAP, donde se almacenan listas de certificados válidos y revocados), los servicios de timestamping y software cliente/servidor PKI-enabled que hace uso de estos servicios.

LOS CERTIFICADOS

Un identificador digital *(Digital ID)* es un documento electrónico que representa en forma digital la identidad de una entidad, de la misma manera que la cédula de identidad relaciona una persona física con un nombre, una foto, fecha de nacimiento, etc.
El identificador digital no certifica nada, y es por sí solo fácilmente falsificable. En el mundo físico esto es combatido mediante técnicas de impresión y afines difícilmente reproducibles, como lo son las marcas de agua y los sellos holográficos. Esto no es aplicable directamente al mundo digital. Es aquí donde entran los certificados.

Cuando una autoridad de certificación desea hacer legítima la relación entre un identificador digital de una entidad y su clave pública, emite un *certificado*, que es firmado digitalmente por ella. El certificado es entonces una declaración digital hecha por la CA, donde esta certifica la relación entre una entidad (dada por su identificador digital) y su clave pública, información que es "sellada" con la pareja de claves de la propia CA. Cada vez que una entidad necesite darle su clave pública a otra entidad, le entregará su certificado y la entidad receptora podrá verificar la autenticidad de este conociendo la clave pública de la autoridad certificadora, suponiendo que confía en la autoridad certificadora y sus métodos de certificación. En forma general, un certificado es un conjunto de datos compuesto por:

*Información que describe a la entidad dueña del certificado

*La clave pública de esa entidad, junto con información que describe el tipo de clave pública
*Firma de este certificado, o sea, los dos ítems anteriores cifrados con la clave privada de la entidad certificadora.

En el esquema propuesto, será necesario establecer la confianza en una o una serie de autoridades de Internet.

Veremos a continuación un estándar propuesto para codificar certificados utilizado ampliamente hoy en día, llamado X.509.

EL ESTÁNDAR X.509

La *ITU-T (International Telecommunication Unio*n) estableció un estándar para codificar los certificados digitales, llamado *X.509*. Fue inicialmente desarrollado para resolver la autenticación en el estándar de directorio *X.500*. Este último nunca se desarrollo como se suponía, principalmente por problemas en la rigidez de sus entidades y el modelo jerárquico de nombres que propone, no siempre aplicable a la realidad. Para no limitar el *X.509* al estándar de directorio, surge el *X.509v3* (versión 3) que establece extensiones de forma de hacerlo aplicable a otras entidades por fuera del modelo *X.500*. Entre otras cosas, fija un criterio para darle nombres a las entidades que es aplicable a la realidad. Es este el estándar que se esta utilizando hoy en día. X.509v3, define los campos que deben figurar en el certificado y establece extensiones posibles (aunque sin restringir). En cuanto a los algoritmos de cifrado utilizados, no establece cuál debe ser usado pero sí recomienda el uso de claves RSA. Para permitir la variedad de algoritmos, incluye un identificador de algoritmo.

El certificado tiene entre otros, los siguientes campos de información:

- Versión del formato utilizado Número serial (único dentro de la CA) del certificado
- Identificador del algoritmo de firma utilizado
- Nombre X.500 (DN: *Distinguished Name*) de la CA emisora del certificado
- Período de validez del certificado (inicio y fin)
- Información de la entidad dueña del certificado:
- Nombre X.500
- Identificador del algoritmo de clave pública usado
- Su clave pública
- Extensiones
- Firma digital del certificado

Las extensiones son un conjunto de datos del tipo (clave, valor) con una bandera opcional de *dato crític*o. Dado que no existe un uso estandarizado de las extensiones, se incluye la bandera para señalizar que esa clave no debe ser pasada por alto y en caso de que un software reciba un certificado con una extensión marcada como crítica que no conoce (y por lo tanto no sabe interpretar) deberá declarar que no sabe manejar ese certificado. Hay dos tipos de extensiones: las informativas y las restrictivas. Las primeras proveen información adicional acerca del certificado

así como de su dueño. También pueden incluir tipos de, usos deseados para el certificado (por ejemplo autenticación pero no firma digital). Las restrictivas establecen criterios adicionales que deberán cumplirse para que el certificado sea válido. Permiten que una CA restrinja el uso del certificado dentro de un país o empresa. Algunas de las extensiones posibles son las siguientes:

Uso de la clave
Define el uso que se le dará a la clave pública, por ejemplo para firmas, no repudiación, intercambio de claves privadas, autenticación, correo electrónico, firma de código ejecutable, etc.
Nombre alternativos
Se incluye aquí todo nombre que no encaja en el modelo X.500, como ser nombres tipo RFC822 *(tuba@fing.edu.uy)*, nombres tipo DNS (viola.fing.edu.uy), URLs (http://www.fing.edu.uy/), un IP, nombre EDI, etc.

Políticas de uso de la CA para este tipo de certificados.
Permite que una CA emita certificados para un uso determinado, como puede ser uso personal sin fines de lucro, y que por lo tanto permite a quien recibe el certificado saber que criterios utilizó y cuán exigente fue la CA al emitirlo. Esto permite que una misma CA emita distintos tipos de certificados de distinta "calidad".

Mapeo de seguridad entre CAs
Aquí la CA puede incluir información sobre como se mapea este certificado y los procedimientos tomados al emitirlo contra otros certificados de la misma CA u otra CA. Dada la cantidad de extensiones que se proponen y la falta de un criterio único para establecerlas, surgieron distintas familias de certificados, llamados *X.509v3 profiles*. Estos son propuestos y utilizados por grupos de organizaciones con necesidades similares sobre los certificados. Cada *profile* utiliza un subconjunto de extensiones, a los que le asigna una semántica precisa.

EL PROCESO DE CERTIFICACIÓN

Por proceso de certificación se entiende el proceso que debe seguir un usuario para obtener su certificado, así como las acciones que la CA deberá tomar durante el proceso.

1. Generación de claves
El usuario deberá generar una pareja de claves (pública y privada) compatible con los métodos criptográficos de su CA preferido.

2. Generación y firma de identificación digital
En este paso, el usuario crea un registro digital con la información que considera que deberá ser parte de su identificador digital (en común acuerdo con las políticas de uso impuestas por la CA para este certificado) y, junto con su clave pública lo firma (utilizando su clave privada) y se lo entrega a la CA. En forma paralela, le entrega su clave pública sin cifrar.

3. Verificación de identificación
La CA descifra los datos entregados utilizando la clave pública obtenida.

En este paso verifica dos cosas: primero que el usuario dispone de la pareja de claves y no sólo de la parte pública. Si no dispusiera de la clave privada, no hubiera podido generar el cifrado correcto. Por otro lado verifica que la información sea correcta, exigiendo algún otro tipo de documentación. Es aquí donde más se diferencian las CAs, especialmente ante los criterios utilizados al evaluar la información. Hablaremos de esto más adelante. Notar que la información es cifrada no sólo para verificar la tenencia de ambas claves sino también para protegerla durante la transmisión.

4. Generación del certificado
Aquí la autoridad de certificación genera el certificado X.509 descrito anteriormente. Esto es, empaqueta los datos del usuario, sus propios datos y los firma con su clave privada.

5. Verificación del certificado
El usuario puede verificar la correctitud del certificado, de sus datos y de su clave pública descifrándolo con la clave pública de la CA .

6. Publicación del certificado
Para que otras personas puedan usar el certificado, tanto la CA como el propio usuario pueden publicarlo en directorios.
Este es un proceso en teoría. En la práctica muchas veces son las propias CAs quienes generan las claves, utilizando distintos tipos y largos de claves según el uso que se le dará a esa clave. Para no comprometerse con el mal uso de las claves, la CA incluye información en el certificado que describe el uso para el que fue generada esa clave. Otra variante posible es que la persona se tenga que presentar físicamente ante la autoridad certificadora, en cuyo caso se pueden omitir los controles sobre la transmisión de datos, aunque aún es útil que el usuario presente su clave pública y sus datos personales cifrados con su privada.

CUESTIONES DE CONFIANZA

El esquema presentado se basa en la confianza que guarden entre sí los elementos en la red, es por ello importante que esta confianza pueda ser garantizada en todo Internet.

Mencionamos que es tarea de una autoridad de certificación establecer el nexo entre una entidad y su clave pública, pero nunca establecimos un método que deberá seguir una autoridad de certificación para verificar la identidad de esa entidad. Un problema con el que se enfrenta el sistema aquí planteado es que no existe tal método: cada entidad certificadora exige lo que ella considera necesario para acreditar a esa entidad (persona) y emite el certificado en base a eso. La pregunta que uno se hace aquí es ¿qué valor tiene un certificado de una CA si uno no sabe que procedimientos siguió esa CA para verificar la identidad del portador del certificado?. La solución parcial que utilizan las CAs es primero establecer distintos "planes" de certificación, o sea, emitir certificados distintos para distintos usos, y segundo hacer públicos sus métodos de verificación de identidades.