Introducción

En este trabajo de investigación denominado "**Seguridad en redes IP**" se pretende dar una visión profunda de los riesgos existentes en las redes conectadas a Internet así como de los principales sistemas de seguridad existentes.

Internet, denominada también la red o red de redes, se ha convertido en la última década en un fenómeno que ha revolucionado la sociedad. Desde la aparición de la televisión no se ha observado ningún otro fenómeno social de tal envergadura o que evolucione tan rápido.

De los muchos factores que han convergido en este nuevo fenómeno para catapultarlo de forma masiva a la sociedad actual, podemos destacar tres principalmente:

- La expansión de los ordenadores en todos los ámbitos de la sociedad (empresas, universidades, gobiernos…) ha contribuido a informatizar casi cualquier aspecto de nuestra vida.

- La rápida evolución de la tecnología de las comunicaciones (más rápido, más barato, mejor) ha acelerado aún más el despegue de Internet.

- El carácter universal de Internet que permite la conectividad global y permanente de todo el planeta de forma económica y prácticamente instantánea, lo convierten en una herramienta imprescindible para prácticamente cualquier tipo de comunicación.

En consecuencia, cada día cientos de millones de personas en todo el mundo utilizan Internet como parte de su trabajo y ocio. De igual forma que en cualquier otro servicio utilizado por gran cantidad de personas (como el metro o las carreteras), la seguridad es un factor básico que siempre debe ser tenido en cuenta.

> **Seguridad** (*l. securitate*) : **1** *f.* Calidad de seguro [WWW1].
> **Seguro, -ra** (l. *securu*) : **1** *adj.* Exento de todo peligro o riesgo [WWW1].

Desde un punto de vista sociológico, en cualquier grupo social un pequeño porcentaje de su población es malévolo [CZ95]. Internet ha alcanzado en el año 2002 más de 160.000.000 de ordenadores conectados [WWW5] sumando un total estimando de 580.000.000 de usuarios en todo el mundo [WWW6][WWW7]. Si tan sólo el 1 por cien de la población pertenece a este sector tenemos casi 6 millones (5.800.000) de posibles atacantes. Incluso suponiendo sólo un uno por mil tenemos la cantidad de casi seiscientos mil (580.000) peligros potenciales.

El objetivo de este estudio se centra precisamente en el análisis de los peligros y amenazas más comunes que existen en Internet así como en los nuevos mecanismos de seguridad que pretenden darles solución.

1.1 Resumen de los capítulos

La estructura que presenta este trabajo se divide en cinco capítulos que se agruparán en dos bloques. La primera parte hace referencia al trabajo de investigación teórica y se compone de los primeros cuatro capítulos, mientras que la segunda parte se compone del capítulo cinco dónde se presenta la parte experimental realizada.

1. **Los protocolos IP**: En el primer capítulo se realiza una explicación en profundidad de la familia de protocolos TCP/IP versión 4. Se describen las características y funcionalidades más importantes que presentan los protocolos IP, ICMP, UDP y TCP así como su interrelación y papel que juegan en la comunicación de sistemas conectados a Internet.

   También se explica el proceso de traslado de los datagramas por Internet (rutado de paquetes) hasta llegar a la red local de destino (LAN), dónde es entregado al ordenador especificado por la dirección IP gracias a los protocolos ARP/RARP.

2. **Denegación de servicio (DOS / DDOS)**: En este segundo capítulo realizaremos un repaso histórico de la evolución de los ataques a redes de ordenadores en Internet, centrándonos en el estudio y clasificación de los ataques de denegación de servicio o DOS.

   Los ataques DOS son aquellos destinados a conseguir de forma total o parcial el cese de un servicio existente. Estos ataques se basan en el uso de diferentes técnicas que intentan colapsar el servicio en sí mismo o el ordenador que lo soporta mediante una inundación de peticiones fraudulentas.

   Los ataques DOS distribuidos (DDOS) se caracterizan por la sincronización de varios ordenadores distintos que focalizan sus ataques de forma coordinada hacia un mismo destino.

   En la parte final de este capítulo realizaremos un análisis exhaustivo de un ataque DDOS real registrado en Internet el 11 de enero de 2002.

3. **Sistemas de detección de intrusos** (IDS): En este tercer capítulo realizaremos una explicación de los sistemas de detección de intrusos o IDS. Comentaremos la taxonomía en la que se dividen los sistemas de detección de intrusos: sistemas de ordenador (HIDS) y sistemas de red (NIDS) para centrarnos en estos últimos.

   Los sistemas NIDS son una evolución de los primitivos firewalls que únicamente filtraban el tráfico de red existente entre Internet y la red LAN. Entre sus nuevas capacidades añaden la de analizar el tráfico existente en toda la red local en búsqueda de anomalías o comportamientos sospechosos.

   Analizaremos también sus protocolos de comunicación, sus posibles ubicaciones y arquitecturas así como las limitaciones que pueden presentar. También se introducirán los conceptos de falsos positivos y falsos negativos que hacen referencia a las detecciones erróneas que a veces producen estos sistemas o a la no detección de un comportamiento extraño por el IDS.

   Finalmente se describirá de forma minuciosa el "ataque Mitnick" perpetrado por uno de los *hackers* más famosos del mundo Kevin Mitnick y que le costó varios años de cárcel. En la actualidad este ataque clásico se considera el umbral mínimo de detección para un sistema IDS.

4. **Honeypots y Honeynets**: En el último capítulo de la parte de investigación se describirá el nuevo escenario que se está produciendo como consecuencia de la evolución de las comunicaciones en Internet.

   El abaratamiento de los costes de conexión y el aumento del ancho de banda disponible modifican los escenarios típicos de ataques. Consecuentemente la comunidad investigadora propone una nueva herramienta de seguridad: los Honeypot (potes de miel textualmente o ratoneras).

   Los Honeypots son sistemas pasivos cuyo funcionamiento se basa en estar diseñados para ser atacados e incluso comprometidos por cualquier atacante. El objetivo de tener un sistema destinado a ser atacado es doble:

Por un lado permitir el estudio de los comportamientos y técnicas reales que utilizan los *hackers* en un entorno "real". Este entorno puede ser configurado de forma que incluso pueda ser capaz de proporcionar información falsa a eventuales atacantes.

Por otro lado, la existencia de un sistema con estas características nos permite desviar la atención sobre nuestros sistemas reales y prepararlos para los ataques registrados en el Honeypot.

Las Honeynets son un tipo concreto de Honeypots. El objetivo es la existencia de diferentes Honeypots agrupadas en una red "aislada" de la red de producción con el objetivo de crear un entorno más verosímil para los posibles atacantes.

Comentaremos las dos generaciones (GEN I y GEN II) de Honeynets existentes así como sus características y arquitecturas principales. También introduciremos los conceptos de Honeynets virtuales y distribuidas que permiten la minimización de los recursos necesarios para la implementación de estas técnicas.

5. **Análisis de un sistema conectado a Internet**: En el quinto capítulo realizamos la parte experimental de este trabajo. Nuestro objetivo es el de monitorizar durante siete días un sistema conectado permanentemente a Internet.

   Analizaremos los distintos objetivos que plantea la tarea exigida y expondremos los distintos requerimientos del experimento. Se propondrá una arquitectura de red que cumpla nuestros requisitos y se escogerán las distintas herramientas (software y hardware) que nos permitirán evaluar nuestro experimento.

   La presentación de los datos se realizará mediante un informe diario pormenorizado con los datos del tráfico de red obtenidos (distintas peticiones y ataques recibidos) que se desglosará en tráfico registrado por tipo de servicio (SSH, WWW…) y por tipo de protocolo al que hace referencia.

Finalmente también se presentará un informe semanal que contendrá los aspectos más relevantes registrados durante los siete días analizados así como las conclusiones obtenidas del experimento.

En la parte final de este trabajo se presentarán las conclusiones obtenidas durante la realización de este informe así como las futuras líneas de continuación que podrían llevarse a cabo.