1. ANTECEDENTES Y OBJETIVOS

INTRODUCCIÓN

1.1 Motivación del Proyecto

1. Profundizar en GNU/Linux

La idea principal de este proyecto fin de carrera surge ante el interés del alumno en profundizar en el estudio de sistemas basados en software libre tal como **GNU/Linux** y las herramientas existentes para realizar determinadas funciones de red en este sistema operativo.

A día de hoy, el software libre se encuentra en un proceso de extensión bastante significativo. Algunos pensadores incluso lo califican como un proceso de la magnitud de la revolución industrial. Cada vez son más las empresas que migran sus sistemas a entornos basados en software libre.

Una de las ventajas fundamentales del uso del software libre es el ahorro del coste de las licencias, que aunque para grandes empresas puede ser un coste insignificante del total, para pequeñas y muchas medianas empresas puede significar un ahorro considerable.

Otro aspecto importante es que utilizando software libre no nos vemos atado a un solo proveedor, ya que al estar disponibles las especificaciones y el código cualquiera puede implementar sus herramientas. Esto evita tener la preocupación e inseguridad de usar software privativo. Con el software privativo no es la oferta y demanda la que rige el mercado, no son los clientes quienes deciden qué usar y qué comprar. En el software libre si una empresa desea abandonar su producto, al estar el código disponible cualquier otra empresa, asociación, gobierno o personas pueden continuarla por su cuenta.

Hay varias empresas que comercializan soluciones basadas en Linux: IBM, Novell, Red Hat, así como miles de PYMES que ofrecen productos o servicios basados en esta tecnología. La consideración de esta tecnología como un servicio supone un cambio importante respecto al modelo de negocio de venta de un software como producto, significa la personalización de la tecnología a las necesidades del usuario: por ejemplo, vender una garantía de mantenimiento, formación sobre su uso, certificación para diversas tareas y la adaptación a las necesidades del cliente. La importancia en este caso se traslada al conocimiento sobre los programas y tecnologías, que es lo que los productores de software libre tienen que rentabilizar.

Desde el punto de vista técnico, además el sistema operativo Linux está diseñado para trabajar con protocolos de red, TCP/IP, lo cual lo hace muy eficiente y seguro al utilizarlo en dispositivos de comunicaciones.

2. Profundizar en la administración y seguridad de redes de ordenadores

Por otro lado, como alumno de telemática interesado en el ***Networking***, con este proyecto se pretende ampliar conocimientos tanto teóricos como prácticos acerca del funcionamiento y fundamento de las redes de ordenadores, especialmente en tareas de diseño, creación, administración y sobre todo **seguridad informática**.

La seguridad es una de las preocupaciones principales del administrador de red. Hay muchas páginas inseguras en Internet y la mayor parte de nosotros desconoce lo que realmente pasa durante la transmisión de los datos, o si éstos pueden venir acompañados de virus o intrusos. Así pues, es necesario desarrollar un sistema que proteja a la red interna de la otra red, la Internet, mediante el uso de filtros equipados para evitar automáticamente que un usuario no-autorizado ataque al equipo.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos "crackers" aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

3. Hacer un buen uso del Hardware

Por último, otra motivación para la realización de este Proyecto Fin de Carrera, surge ante la necesidad de hacer un **buen uso del hardware** de aquel primer o segundo ordenador que compramos hace unos años y que ahora está apilado en algún rincón de la casa. En nuestro proyecto utilizaremos dicho hardware para la instalación del sistema operativo y simulación de escenarios reales, pudiendo comprobar que es suficientemente potente para realizar las funciones que buscamos.

Siguiendo esta filosofía, podría aplicarse este diseño de dispositivo de red a muchas empresas que tiran cada año PCs medianamente antiguos por quedarse obsoletos sin darle ninguna utilidad práctica.

Cada año se acumulan millones de toneladas de chatarra informática. Una cantidad que va creciendo geométricamente año tras año, en parte por la rápida renovación del hardware y los componentes que integran nuestros equipos informáticos. Todas estas máquinas y dispositivos han sido relevados de su uso simplemente por no disponer de la potencia necesaria para ejecutar el último programa, aplicación o juego que hipnotiza a sus propietarios. Sin embargo, no todos terminan en los contenedores de los puntos limpios dedicados a recogerlos, o por lo menos no deberían. Muchas veces, incluso el hardware que pensamos que está más obsoleto es perfecto para llevar a cabo toda una amplia gama de tareas especializadas. Esto nos permitirá ahorrar dinero, al no tener que comprar sistemas nuevos, y de paso dar un uso a ese «viejo trasto» que tenemos guardado.

1.2 Introducción al Proyecto: Seguridad en GNU/Linux

Como hemos comentado previamente, el tema principal de nuestro proyecto es la **seguridad**, veremos cómo implementar sistemas de seguridad de redes IP basados en el sistema operativo GNU/Linux Debian.

Lo primero que debemos asimilar sobre la seguridad informática es que ningún sistema es completamente seguro. El único seguro es aquel que no está conectado a la red, apagado y encerrado bajo llave. Una vez comprendido esto, partiremos de que nuestra misión consisitirá en dificultar lo máximo posible que alguien pueda comprometer nuestros sistemas. Cabe destacar que un atacante experimentado con el tiempo suficiente se hará con nuestro sistema sin ninguna duda. Pero como hemos visto, nuestra tarea será dificultarle lo máximo posible esta misión, alejando de esta forma a la gran mayoría de atacantes, que por lo general serán mucho menos peligrosos.

Hemos de tener en cuenta que existe una relación inversa entre seguridad y funcionalidad. Para cada situación tendremos que decidir dónde se encuentra el equilibrio entre la facilidad de uso de nuestro sistema y su seguridad. Por ejemplo, quizá no sea interesante (o posible) dehacernos del acceso a internet de la empresa para protegerla de posibles ataques del exterior. De la misma forma, sería frustrante para un usuario de la máquina tener que identificarse cinco veces ante el sistema para poder hacer uso de él.

En todos los entornos no existen las mismas necesidades de seguridad, ni los mismos aspectos de ésta a cubrir. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de la información sobre su disponibilidad (seguramente sea preferible que en un momento determinado esa información no esté disponible para los usuarios autorizados, a que un intruso pueda leerla). En un sistema bancario, lo más importante sería asegurar la integridad de los datos (es más grave que un usuario pueda modificar el saldo

de una cuenta a que pueda leerlo).

Otro caso sería el de un usuario doméstico: éste, sin grandes requisitos de seguridad como los casos anteriores, ha de mantener sus sistemas con unas barreras básicas de seguridad, para asegurar la fiabilidad de su trabajo, y que sus operaciones por Internet sean medianamente seguras (aunque no se trate de una entidad militar, o un negocio a escala mundial, a ningún usuario le gustaría que alguien pueda tener acceso a todos los emails que escriba a diario, o registre sus números de cuenta y claves cuando acceda a su banco a través de Internet).

Con la generalización de las conexiones a Internet y el rápido desarrollo del software, la seguridad se está conviritiendo en una cuestión cada vez más importante. Ahora, la seguridad es un requisito básico, ya que la red global es insegura por definición. Mientras sus datos vayan desde un sistema a otro, pueden pasar por ciertos puntos proporcionando a otros usuarios la posibilidad de interceptarlos e incluso alterar la información contenida.

Incluso algún usuario del sistema puede modificar datos de forma maliciosa para hacer algo que nos pueda resultar perjudicial. En este sentido, el acceso masivo y barato a Internet ha reducido notablemente los costes de un atacante para asaltar un sistema en red, a la vez que ha aumentado paralelamente el número de potenciales atacantes.

El campo de la seguridad informática crece por instantes. Esto viene motivado porque a diario aparecen nuevas vulnerabilidades de software, nuevos métodos para conseguir accesos indebidos o comprometer el funcionamiento de la red, nuevas aplicaciones que exploten vulnerabilidades existentes, etc. Esto nos obliga a estar actualizados permanentemente para no ser sorprendidos ante un nuevo problema detectado.

Las fuentes del núcleo de Linux son abiertas. Cualquiera puede obtenerlas, analizarlas y modificarlas. Este modelo de desarrollo abierto, que siguen tanto Linux como la mayoría de las aplicaciones que se ejecutan sobre él, conduce a altos niveles de seguridad. Es cierto que cualquiera puede acceder al código fiente para encontrar debilidades, pero no es menos cierto que el tiempo que tarda en aparecer la solución para cualquier debilidad se mide más fácilmente en horas que en días.

Gracias a esto, Linux es conocido por su alto nivel de estabilidad que parte del propio núcleo del sistema operativo. En numerosas ocasiones aparecen hilos de discusión sobre el número de fallos de seguridad que aparecen en cada uno de los sistemas operativos, arreglándose en muchos de ellos que aparecen muchas más vulnerabilidades en los sistemas Linux (y otros sistemas de código abierto, como FreeBSD) que en otros propietarios, como los sistemas Windows de Microsoft. En estas afirmaciones no se suelen tener en cuenta generalmente dos aspectos: el primero sería que muchos de estos fallos de seguridad que afectan a sistemas Linux no son propiamente fallos de Linux (no es frecuente que aparezcan fallos de seguridad en el núcleo), sino de aplicaciones que acompañan a la distribución. Difícilmente podrá aparecer un fallo de seguridad de un sistema gestor de bases de datos en algunos sistemas Windows, ya que el sistema operativo no acompaña ninguno, mientras que muchas distribuciones incluyen alguno por defecto. Podemos hablar si es necesario dar seguridad física y lógica en nuestros sistemas Linux pero nos centraremos en la seguridad de las redes.

Los sistemas Linux han sobresalido especialmente en entornos de red. Así pues, numerosos premios entregados por publicaciones especializadas, han reconocido a Linux como el mejor sistema operativo de red del momento.

1.3 Objetivos

En nuestro caso, aprovecharemos esa eficiencia del sistema operativo GNU/Linux para construir un dispositivo “mínimo”, es decir, instalando únicamente los paquetes necesarios, sin utilizar entorno gráfico y optimizando al máximo los recursos de la máquina, y “estable”, utilizando software robusto, bastante probado y con apenas fallos. Parte importante de nuestro estudio será la instalación del sistema operativo Debian GNU/Linux, así como las aplicaciones exclusivamente necesarias que nos permitan realizar las siguientes tareas:

- Control de acceso a la red interna a proteger (control de acceso en redes WiFi, 802.1x, Servidor RADIUS, etc.):

  Esta funcionalidad permite que nuestro dispositivo pueda discriminar qué equipos tendrán acceso a los recursos de la red y cuáles no. Mediante el protocolo 802.1x, veremos cómo se pueden establecer políticas de autenticación, así como encriptación de conexiones inalámbricas de manera que sólo los usuarios que estén dados de alta en el sistema puedan tener acceso al resto de recursos de red así como salida a Internet. El control de los usuarios se llevará a cabo utilizando un servidor Radius (Remote Authentication Dial-In User Server).

- Servicios de autoconfiguración de parámetros de red (BOOTP, DHCP, etc.):

  Servicio que nos permitirá establecer automáticamente las direcciones IP de los equipos que se conecten a nuestra red interna.

- Enrutamiento de paquetes IP:

  Configuraremos nuestro dispositivo para que actúe de **encaminador o router,** o lo que es lo mismo, un dispositivo de red que funcione en la capa 3 de OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red y determinan la mejor ruta para la transmisión de datos a través de las redes conectadas.

  Los accesos de alta velocidad a Internet, como el cable módem y los servicios ADSL, están disponibles tanto para el hogar como para la pequeña oficina, lo que ha provocado un incremento de la demanda para dar soporte a los servicios. No satisfecho aún con una sola computadora conectada a Internet, el consumidor necesita las herramientas necesarias para compartir la conexión. Internet es la red de datos más grande del mundo. Internet consiste en multitud de redes, grandes y pequeñas, interconectadas. En el borde de esta red gigante se encuentra la computadora del consumidor individual.

- Filtrado de tráfico a distintos niveles: MAC, IP, etc:

  Además, nos interesa que dicho sistema sea seguro, esto es, que evite las intrusiones desde el exterior y los posibles ataques que se puedan realizar. Por tanto, utilizaremos un sistema de **cortafuegos** ó firewalling y filtrado de paquetes.

  Un cortafuegos consiste en filtrar el tráfico TCP/IP, generalmente en el punto donde la red se conecta a otra que puede ser no fiable (en el caso de Internet) o quizás incluso fiable. Al igual que los cortafuegos de los grandes edificios, un cortafuegos de red puede evitar e incluso bloquear la extensión del ataque si un segmento se ve comprometido con éxito, al igual que su homónimo cortafuegos puede evitar que la red se siga viendo comprometida.

- Realización de NAT (estático y dinámico):

  NAT (Network Address Translation) es un proceso de reemplazo de una dirección IP por otra en la cabecera de un paquete IP. NAT se diseñó para aprovechar las direcciones IP públicas y permitir en las redes locales utilizar direcciones privadas. Mediante NAT esas direcciones privadas internas son traducidas a direcciones públicas ruteables.
  Analizaremos los diferentes métodos de traducciones que existen y configuraremos NAT en nuestro dispositivo Debian para compartir una única dirección pública para todos los equipos conectados en la interfaz LAN de nuestro dispositivo.

- Realización de conexiones seguras: VPN IP:

  Las VPN (Virtual Private Network) o redes privadas virtuales son una tecnología de red que permite la extensión de la red local sobre una red pública o no controlada. El objetivo en nuestro proyecto es estudiar qué protocolos son los más habituales y cómo se implementan en GNU/Linux; para ello, plantearemos dos escenarios: en primer lugar crearemos un túnel extremo a extremo entre dos dispositivos Linux con el objetivo de dar conectividad entre las dos redes de área local que están detrás de dichos dispositivos.

En segundo lugar crearemos un túnel entre un cliente y nuestro servidor Linux que dará acceso a una red local.

- Estudio de sistemas de detección/protección de intrusiones:

  Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos desautorizados a un ordenador o a una red. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas. Veremos qué herramientas existen en Linux para detección de intrusiones.

- Estudio y utilización de los servicios Secure Shell para lograr comunicaciones seguras:

  Utilizaremos SSH (Secure Shell) para acceder a nuestra máquina remotamente. Nos permitirá manejar por completo el ordenador mediante un intérprete de comandos.