Capítulo II

Análisis de las Necesidades

En este capítulo se estudian los contenidos disponibles, se denotan las actividades realizadas, se examinan las herramientas necesarias y útiles para el proyecto y se definen los temas a tratar

2.1 Selección de conceptos

Para una mejor y mayor comprensión del concepto de seguridad informática aunados a las crecientes demandas de seguridad por parte de las organizaciones, es pertinente que los estudiantes de Ingeniería en Computación en el módulo de Redes y Seguridad cuenten con los conceptos presentes que deben ser reforzados durante su formación.

2.1.1 Repaso de conceptos básicos de redes de datos

En el presente proyecto fue importante revisar conceptos clave de Redes de Datos necesarios para las prácticas y tareas de este manual:

Revisión de conceptos básicos de redes basados en la bibliografía, apuntes y referencias digitales:

- Topologías físicas: estrella, anillo, bus y sus características
- Medios físicos de transmisión: par de cobre (UTP), fibra óptica, cable coaxial y frecuencias para transmisión inalámbrica
- Topologías lógicas: las topologías lógicas que se pueden implementar con cada medio físico de transmisión.
- Modelo OSI: características y funciones de las 7 capas del modelo
- Modelo TCP/IP: características y funciones de las 4 capas del modelo
- Comparación entre modelos OSI y TCP/IP: diferencias y correspondencia entre capas de cada modelo.
- Protocolos de TCP/IP: (para que sirven y su funcionamiento): IP, TCP, UDP, ICMP, ARP
- Protocolo Ethernet (funcionamiento, direcciones MAC)
- 3-way-handshake en TCP
- Estados de conexión en TCP (RFC 793): LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK,TIME-WAIT, CLOSED.
- Tipos de aplicaciones comunes sobre TCP/IP: FTP, SMTP, POP3, HTTP, SNMP, TELNET, etc.
- Dispositivos de comunicaciones, características y limitaciones: routers, switches, hubs, bridges, access points.
- Conceptos de ruteo (tablas de ruteo, propagación de la información de ruteo, y protocolos de ruteo)
- Redes inalámbricas 802.11a, 802.11b, 802.11g (características y diferencias entre ellas)

2.2 Elección de contenidos

Se hizo una revisión de los temarios de las asignaturas obligatorias contempladas en el módulo de Redes y Seguridad así como en las asignaturas de carácter optativo. Se encontraron coincidencias dentro del plan de estudios de cada asignatura siendo los principales temas:

- Conceptos básicos de redes
- Conocimientos básicos de LINUX (comandos y estructura del sistema operativo).
- Selección de mecanismos y herramientas de protección, para cuidar la seguridad informática en una organización de manera física y lógica.
- Conocimiento de mecanismos y herramientas que permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

- Identificación y análisis de los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que los ocasionan.
- Selección y aplicación de técnicas y métodos que permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.
- Comprensión de la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.
- Ubicar las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías que puedan minimizar estas amenazas.
- Programación en lenguaje C y java.
- Funciones de los sockets y puertos como sus principales características y estándares.
- Diferentes tipos de sockets para difundir información mediante la red de datos.

Dada la diversidad de lenguajes y formas de programación vistos durante la carrera no se llegó a considerar la realización de una práctica que contenga elementos de programación; así mismo se toma como único requisito con carácter obligatorio el haber cursado la asignatura de Redes de Datos, con el fin de que el estudiante pueda manejar la mayoría de las herramientas usadas durante las prácticas.

2.3 Investigación Bibliográfica

Se consultó la bibliografía disponible en materia de seguridad informática que se encuentra disponible en publicaciones científicas, boletines de seguridad informática, libros en las bibliotecas de la Facultad de Ingeniería, material disponible en centros especializados, tales como la Dirección General de Servicios de Cómputo Académico (DGSCA) o en recursos digitales disponibles en la web.

Se revisó y buscaron libros relacionados, tomando aquellos con contenido referente al área de estudio de la seguridad informática, libros relacionados con:

- Seguridad en redes
- Criptografía
- Seguridad en aplicaciones
- Administración de la seguridad
- Hacking
- Biometría

Se buscó material digital relacionado con:

- Redes de telecomunicaciones
- Sistemas operativos Unix o derivados (Linux por ejemplo)
- Auditoría de sistemas
- Simuladores de redes
- Cómputo forense
- Biometría

2.4 Selección de Herramientas

Conscientes de que las herramientas tecnológicas permiten organizar, comunicar, investigar y ayudan a resolver problemas. La tecnología forma parte integral del proceso para resolver problemas de la seguridad en cómputo, por eso es importante adquirir las habilidades para el uso e implementación de nuevas tecnologías que nos permitan desarrollar mejor herramientas asertivas.

Esta parte es la directriz del manual ya que cada herramienta debe cumplir con un fin acorde al conocimiento a ilustrar, y en este sentido cabe destacar que adicionalmente deben ser acorde, a la capacidad de los equipos que se empleen, para que las herramientas no que sobrepasen la capacidad de los equipos disponibles.

2.4.1 Selección de Herramientas de Hardware

Se eligió una configuración común en los equipos utilizados en salas de cómputo como en laboratorios de la Facultad de Ingeniería:

- Procesador de Arquitectura x86 a 1.0 Ghz
- 1GB de memoria RAM DDR
- Disco duro de 80 GB
- Monitor
- Teclado
- Mouse

Asimismo se eligieron dispositivos externos extraíbles que dan apoyo a la realización de las prácticas tales como:

- GPS con interfaz USB compatible con el protocolo Nmea3
- Lector de huella digital externo
- Tarjeta wireless externa de 1 Watt
- Antena de 10 db de ganancia

Los Dispositivos recomendados son:

- *GPS USB GLOBALSAT ND-100 DONGLE*

Dispositivo compacto y portátil, que permite conectar el receptor GPS para el uso en su laptops, netbooks y dispositivos UMPC. No requiere batería adicional.

Especificaciones:

- Adopt SKYTraq Venus 6 chipset con 65-Channel
- Alta sensibilidad (to -160dBm)
- Tiempo de arranque: 29/1 sec.
- Compatible con NMEA 0183, NMEA0183 V3, GGA, GSA, GSV, RMC, AGPS, WAAS / EGNOS
- Conexión USB
- Dimensiones: 68 x 28 x 14mm
- Peso: 25g

- *Adaptador USB Wireless Alfa Network (awus036h) 54Mbps y antena desmontable de 9dBi*

Permite descubrir redes 802.11 b/g a distancia y con más potencia.

Especificaciones

- Chipset Realtek 8187L (RTL8187L)
- Estándar IEEE 802.11g/b
- Interfaz USB rev. 2.0 B-Type to A-Type
- Banda de Frecuencias 2.400GHz ~ 2.484GHz
- Modulación
  - IEEE 802.11g: OFDM(64-QAM, 16-QAM, QPSK, BPSK)
  - IEEE 802.11b: DSSS(CCK/DQPSK/DBPSK)
- Tasas de Transferencia:
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 & 6Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps con auto-rate fall back
- Protocolo de Acceso: CSMA/CA
- Nº de Canales de trabajo:
  - 2.412~2.462GHz (Canadá, FCC) / 11 Canales
  - 2.412~2.484GHz (Japón, TELEC) / 14 Canales
  - 2.412~2.472GHz (Europa, ETSI) / 13 Canales
- Seguridad
  - 64/128bit WEP
  - WPA(TKIP con IEEE 802.1x)
  - WPA2(AES con IEEE 802.1x)
- Potencia de Salida (Típica)
  - 802.11g: hasta 24 ± 1 dBm.
  - 802.11b: hasta 30 ± 1 dBm.
- Sensibilidad
  - 73dBm @ 54 Mbps
  - 85dBm @ 11 Mbps
- Consumo de Energía: Transmisión/ Recepción: 290mA/240mA at 5VDC
- Antena: Una antena desmontable de 5dBi con conector RP-SMA
- Dimensiones (mm.): 95(Largo) x 59(Ancho) x 16(Alto) mm.(antena no incluida)
- Peso: 120g
- Temperatura de Funcionamiento: 0ºC ~ 60ºC Temperatura ambiente
- Humedad 10% ~ 90% (Sin condensación)
- Soporte de controladores: Windows 98SE, ME, 2000, XP 32/64, Vista y Windows 7 32/64 bits, Linux, Wifislax, Backtrack 3

Estas herramientas en conjunto con la paquetería empleada, muestran al estudiante el panorama de lo que es la seguridad informática de manera que sea distinguible el uso específico de cada una de ellas.

2.4.2 Selección de Herramientas de Software

- Microsoft Windows XP

  Es un sistema Operativo que ofrece una interfaz gráfica de usuario amigable, facilitando su uso por usuarios no ambientados. Este sistema operativo de carácter comercial es distribuido bajo una licencia que autoriza sólo el uso del software bajo ciertas condiciones (Microsoft CLUF). Este sistema operativo es actualmente el más popular debido a que muchos de los fabricantes de software en el mundo desarrollan sus productos orientados a esta plataforma.

  A continuación se enumeran algunas ventajas de este Sistema Operativo:

  - Windows dispone de una interfaz gráfica que facilita el manejo de los procedimientos.
  - Es el SO más comercial por lo que dispone de más aplicaciones y mantenimiento.
  - La curva de aprendizaje en el sistema Windows es mucho menor.
  - Los Servicios de actualización de software (SUS) de Microsoft ayuda a los administradores a automatizar las actualizaciones del sistema más recientes.
  - Microsoft ha mejorado a lo largo del tiempo en gran cantidad sus productos y así ha aumentado considerablemente su desempeño en ambientes de red.

  Las desventajas de Windows son las siguientes:

  - Software propietario es decir que la empresa es “propietaria” de los códigos fuente del sistema y sólo ella es capaz de modificar al Sistema Operativo, el usuario sólo tiene permitida la instalación del programa en su máquina.
  - El costo de licencias de Windows es muy elevado por lo que en ocasiones resulta más atractivo desde un punto de vista económico

- AudioBlast

  Es un editor de audio de carácter básico, tiene soporte para archivos en formato WAV, y además puede exportarlos a MP3. Emplea operaciones básicas con archivos de sonido: seleccionar, copiar, cortar, pegar, aplicar filtros, efectos sonoros; edición de parámetros como la velocidad, los tonos, ecualizadores. Permite mezclar varios archivos. AudioBlast realiza diversas funciones de edición al alcance del usuario, en un programa accesible, ligero y de uso gratuito

- Fequency Analizer

  Es un programa que emplea la transformada rápida de Fourier para descomponer en funciones senoidales una señal análoga como es la voz humana la versatilidad de este programa y su licencia libre lo hacen una herramienta muy útil.

- WinRAR

  Es un potente programa compresor y descompresor de datos multi-función, también permite el cifrado de datos empleando el algoritmo AES, Winrar usa también una función de hash especialmente lenta para ralentizar al máximo los intentos de descubrir la contraseña mediante ataques de fuerza bruta que son actualmente la única forma de descubrir una contraseña para archivos con cifrado AES.

Esto lo hace especialmente seguro, incluso mucho más que otros compresores que usan claves de 256 bits, por ejemplo, un ataque a un fichero ZIP cifrado con AES-256 es 10 veces más rápido en las mismas condiciones que el mismo ataque a un fichero RAR cifrado con AES-128.

- GPG4WIN

  Es una herramienta de software libre que permite codificar archivos y correos electrónicos mediante el empleo de un sistema de claves públicas y privadas. El algoritmo de codificación que emplea este programa también es libre y se denomina 'GNU Privacy Guard', la alternativa de código abierto a los sistemas de codificación patentados.

- Wireshark

  Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

  Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

  Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

- Uso del Sistema Operativo Linux Fedora

  Es un sistema Operativo que se ha desarrollado bajo la filosofía del software libre, garantizando ciertas libertades a sus usuarios. Aunque su entorno original era altamente especializado (informática y entornos científicos), con el tiempo se ha desarrollado lo suficiente como para llegar a ser una alternativa viable en entornos domésticos o empresariales donde la interfaz gráfica de usuario y facilidad de uso es altamente valorada. Pese a ello, aún hay muchas aplicaciones de uso especializado pero de amplia demanda (tratamiento de audio, imágenes y aplicaciones de gestión, entre otras) que no han sido desarrolladas para Linux o bien, no existe un símil para esta plataforma. GNU/Linux se distribuye bajo la licencia GNU GPL (GNU General Public License), en la mayoría de sus distribuciones.

  A continuación se describen las principales ventajas de este Sistema Operativo:

  - Está inspirado en Unix, por lo que tanto su gestión de recursos del sistema como la orientación cliente/servidor y multitarea/multiusuario hacen de él un sistema robusto, estable y rápido.
  - Se distribuye bajo licencia GNU GPL, lo que garantiza la libre copia y distribución tanto del software en sí como de su código fuente, permitiendo además su modificación bajo ciertas condiciones como respetar la autoría del programa original.
  - Fue desarrollado desde un comienzo en y para un ambiente de red, por lo que los módulos de protocolos de red forman parte del núcleo del sistema, otorgando un excelente desempeño en ambientes de red.

- Existe gran cantidad de documentación acerca de los programas que componen el sistema, tanto en Internet como en el propio sistema.
- Las principales distribuciones de GNU/Linux (Debian, Suze, CentOS, Fedora) incorporan sistemas de descarga de aplicaciones que facilitan la instalación y actualización de software en el sistema en forma semiautomática.
- Existen distribuciones comerciales de Linux, tales como Suze y RHEL que ofrecen soporte al usuario final.
- GNU/Linux ya no está restringido a personas con grandes conocimientos de informática: Los desarrolladores han hecho un gran esfuerzo por dotar a este sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente. Las principales distribuciones de GNU/Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows.

- Cisco Packet Tracer

  Es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y estudiantes de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA. Este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para práctica y aprender por descubrimiento.

  Packet Tracer 5.3.1 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental si el estudiante está cursando CCNA o se dedica al networking.

- VMware. (VM de *Virtual Machine*)

  Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un ordenador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

  Un virtualizador por software permite ejecutar (simular) varios ordenadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. No obstante, y al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

  VMware es similar a su homólogo Virtual PC, aunque existen diferencias entre ambos que afectan a la forma en la que el software interactúa con el sistema físico. El rendimiento del sistema virtual varía dependiendo de las características del sistema físico en el que se ejecute, y de los recursos virtuales como CPUy RAM, asignados al sistema virtual.

- Zenmap
  Es una herramienta de escaneos de redes muy profunda como la conocida nmap, pero con una agradable interfaz gráfica. Este programa utiliza protocolos como el UDP y TCP. Nmap es una herramienta para escanear redes, ya sea escanear puertos a través de un dominio web o una direccíon IP.

- Nessus
  Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

- Hamachi
  Es una aplicación gratuita (freeware) configuradora de redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin requerir reconfiguración alguna (en la mayoría de los casos). En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por ordenadores remotos. Actualmente está disponible la versión para Microsoft Windows y la versión beta para Mac OS X y Linux.

  Hamachi es un sistema VPN de administración redondeada que consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

- Dropbpox
  Se trata de un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre computadoras y compartir archivos y carpetas con otros. Existen versiones gratuitas y de pago, cada una de las cuales con opciones variadas.

- NetStumbler
  Es un programa para Windows que permite detectar redes inalámbricas (WLAN) usando estándares 802.11a, 802.11b y 802.11g. No sólo se reduce a detectarlas, sino que nos muestra una gran cantidad de información al respecto como el SSID (nombre de la red), el canal por el que emite, la velocidad, el tipo de encriptación e incluso la MAC del punto de acceso y el fabricante.

  La utilidad es máxima, sobre todo para personas que trabajen a menudo con redes inalámbricas y está orientado a la resolución de problemas, localización de interferencias incluso la intrusión de puntos de acceso no autorizados en nuestro rango.

- EarthStumbler
  Es un programa para importar la información marcada con GPS del Netstumbler y visualizarla gráficamente en Google Earth.

- Google Earth
  Es un programa informático similar a un Sistema de Información Geográfica (SIG), que permite visualizar imágenes en 3D del planeta, combinando imágenes de satélite, mapas y el motor de búsqueda de Google que permite ver imágenes a escala de un lugar específico del planeta.

2.4.3 Otras Herramientas

Internet
Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. El uso de este recurso se basa principalmente en la disponibilidad y difusión que permite indistintamente a cualquier usuario compartir información a nivel mundial.

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como:

- CERT/CC (Computer Emergency Response Team Coordination Center) del SEI (Software Engineering Institute) de la Carnegie Mellon University.
  El cual es un prestigioso organismo dependiente de la Universidad Carnegie Mellon de referencia obligada en el terreno de publicación de vulnerabilidades e incidencias en el terreno de la seguridad informática, centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.
  http://www.cert.org/

- Common Criteria
  Es, a pesar de lo polémico y discutido de la certificación obtenida por Windows 2000 en el año 2002, uno de los organismos más prestigiosos en lo tocante a certificaciones de seguridad.
  http://www.commoncriteria.org/

- SANS Institute [SANS (SysAdmin, Audit, Network, Security)]
  Fue fundado en 1989 como un órgano educativo e investigador. Desde entonces hasta nuestros días se ha convertido en el principal punto de referencia dentro de la Seguridad Informática.
  http://www.sans.org/

- CIS, (The Center for Internet Security)
  Organismo dedicado a proporcionar herramientas y métodos para mejorar la seguridad y las prácticas encaminadas a conseguirla.
  http://www.cisecurity.org/

- Security Focus
  Otro de los más prestigiosos organismos dedicados a la seguridad. Particularmente famosa (y útil) es Bugtraq, una lista de correo sobre vulnerabilidades. En agosto de 2002 se anunció su compra por parte de Symantec. Esperemos que no haga cambiar la eficacia de la empresa ni la independencia de sus informes.
  http://www.securityfocus.com/

- Open Source Vulnerability Database
  Base de datos dedicada en exclusiva a la recopilación e información de incidencias de seguridad en código de fuente abierta.
  http://www.osvdb.org/

- ESCERT
  Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas de la Universidad Politécnica de Cataluña.
  http://escert.upc.es/

En México

- UNAM-CERT(Equipo de Respuesta a Incidentes de Seguridad en Cómputo)
  Es un equipo de profesionales en seguridad en cómputo. Está localizado en la Subdirección de Seguridad de la Información (SSI) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, de la UNAM.

  El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.
  http://www.cert.org.mx/index.html