

Tabla de Contenido

Conceptos Básicos de Redes.....	2
Hardware.....	2
Comunicación.....	3
Características de los sistemas operativos de red	4
Características de las clases de direcciones.....	5
Netmask (Máscara de Red).....	6
Clases de Red comúnmente usadas.....	7
Modelo OSI.....	8
Diseño de una Red de Área Local.....	9
Dimensionamiento de una red.....	9
Ejemplos.....	9
Interconexión de redes.....	10
Elaboración de cableado de Red.....	11
Tipos de codigos.....	11
Estándares T586A y T586B.....	12
T586B.....	12
T586A.....	12
Implementación, pruebas y mantenimiento de Redes.....	14
Requerimientos de sistemas.....	14
Desastres naturales.....	14
Desastres del entorno	15
Mobiliario especial y equipo adicional.....	17
Corrección de Fallas.....	17
Conceptos básicos de Ruteo de Redes.....	19
Configuración de equipo (APs, Switchs, Routers).....	21
Seguridad de redes Cableadas e Inalámbricas.....	22
Medidas básicas de seguridad	22
Herramientas de medicion y rendimiento para redes	24

Conceptos Básicos de Redes

Hardware

- **Tarjeta de red:** También conocida como NIC (del inglés Network Interface Card), es el elemento que conectaremos al PC para proporcionar el soporte de red. Suele venir en formato ISA o PCI.
- **El cableado:** Si las redes de ordenadores reciben ese nombre es por los cables. Una red puede usar muchos tipos de cables.
- **El hub:** Físicamente todos los hubs son parecidos: pequeñas cajas de forma rectangular parecidos a módems externos grandes, con numerosos conectores para los cables y una serie de indicadores luminosos que muestran el estado de la red, lo que resulta fundamental a la hora de diagnosticar problemas. La mayoría de los hubs pueden unirse unos a otros para ampliar la red, aunque para una red del tamaño que nos interesa merece la pena comprar un único hub que gobierne toda la red. Siempre conviene comprar un hub con un par de puertos más de los que necesitamos, ya que así nos ahorraremos dinero y conflictos si decidimos ampliar la red en el futuro.
- **El Servidor:** es un ordenador de gran potencia y capacidad que actúa de árbitro y juez de la red, la maneja, controla su seguridad y distribuye el acceso a los recursos y los datos.
- **Redes punto a punto:** en las redes punto a punto ningún ordenador está por encima de otro, sino que existe una especie de democracia y los recursos son distribuidos según desee el usuario de cada ordenador.
- **Repetidores:** Estos funcionan en el nivel físico. Envían paquetes desde un sector de red primario (Cable) a otro extremo. No interactúan con los protocolos de más alto nivel.
- **Puentes:** Interconectan dos o más redes, pasando los paquetes entre ellas. Soportan distintos tipos de redes.
- **Routers:** Estos son similares a los puentes.
- **Brouters:** Es una combinación de Puente y Routers.
- **Gateways (Pasarela):** Funcionan en los niveles más altos de la jerarquía de protocolos, permitiendo que puedan interconectarse los sistemas y redes que utilizan protocolos incompatibles.

Comunicación

El software: Una red no es nada más que cuatro cables hasta que no instalamos un software para poder manejarla. El software de red tiene dos partes: el protocolo de red, que es algo así como el idioma que van a usar las tarjetas para comunicarse, y el propio programa de comunicaciones que traduce nuestras órdenes al lenguaje del protocolo de red.

Características de los sistemas operativos de red

Los primeros S. O. de red ofrecían algunas utilidades de gestión de archivos de seguridad simples. Pero la demanda de los usuarios se ha incrementado de forma que los modernos sistemas operativos de red ofrecen amplia variedad de servicios.

Estos son algunos de ellos:

- Adaptadores y cables de red
- Nomenclatura global
- Servicios de archivos y directorios
- Sistema tolerante a fallos
- Disk Caching (Optimización de acceso al disco)
- Sistema de control de transacciones (TTS, Transaction Tracking System)
- Seguridad en la conexión
- Bridges (Puentes) y Routers
- Gateways (Pasarelas)
- Servidores Especiales
- Herramientas software de administración

Características de las clases de direcciones

En los inicios de la Internet, a las organizaciones con redes muy grandes, como la marina de los Estados Unidos o Digital Equipment Corporation, se les concedía rangos de direcciones IP de clase (A). La parte de red de una dirección de clase (A) tiene una longitud de un octeto. Los tres octetos restantes de una dirección IP de clase (A) pertenecen a la parte local y se usan para asignar números a los nodos.

Existen muy pocas direcciones de clase (A) y la mayoría de las organizaciones de gran tamaño han tenido que conformarse con un bloque de direcciones de clase (B) de tamaño medio. La parte de red de una dirección de clase (B) es de dos octetos. Los dos octetos restantes de una dirección de clase (B) pertenecen a la parte local y se usan para asignar números a los nodos.

Las organizaciones pequeñas reciben una o mas direcciones de clase (C). La parte de red de una dirección de clase (C) es de tres octetos. De esta forma sólo queda un octeto para la parte local que se usan para asignar números a los nodos. Es muy sencillo adivinar o identificar la clase de una dirección IP. Basta con mirar el primer numero de la dirección en formato de puntos.

Además de las clases A, B y C, existen dos formatos especiales de direcciones, la clase D y la clase E. Las direcciones de clase D se usan para Multienvío de IP. El Multienvío permite distribuir un mismo mensaje a un grupo de computadoras dispersas por una red. Las direcciones de clase E se han reservado para uso experimental.

Las direcciones de clase D empiezan con un número entre 224 y 239. Las direcciones de clase E empiezan con un número entre 240 y 255.

Netmask (Máscara de Red)

Una máscara de red es una máscara de 32 bits que se usa para dividir una dirección IP en subredes y especifica el número de equipos disponibles.

2 bits son asignados automáticamente. Por ejemplo, en una máscara 255.255.255.0, el "0" es la dirección de red asignada.

Y en 255.255.255.255, "255" es la dirección asignada para broadcast.

El 0 y el 255 siempre son asignados y no se pueden usar.

Ejemplo de máscara de red y su conversión binaria:

Netmask:	255.	255.	255.	255
Binary Conversion:	11111111	11111111	11111111	11111111
Netmask length	8	16	24	32

Contando los números en la conversión binaria nos permite determinar la longitud de la máscara. En el ejemplo anterior, tenemos una dirección de 32 bits.

Sin embargo, esta dirección es una dirección de broadcast y no nos permite ningún equipo host. Una máscara de 24 bits comúnmente usada es la siguiente:

Netmask:	255.	255.	255.	0
Binary Conversion:	11111111	11111111	11111111	00000000
Netmask length	8	16	24	--

Usando una máscara de 24 bits la red sería capaz de 2.097.150 redes o 254 diferentes equipos con un rango IP de 192.0.1.x – 223.255.254.x

Para determinar el monto de redes que una máscara de red soporta se usa una simple fórmula.

Con el entendimiento que la longitud de la máscara es 24, restar 3 de ese número, entonces $24 - 3 = 21$.

Una que este número es determinado, tomar 2 a la potencia de X, donde X es el número recién determinado: $2^{21} - 2 = 2.097.150$. Se sustraen 2 números debido a la asignación de red y su broadcast.

Para determinar el monto de equipos host que una máscara de red es capaz de soportar es similar a lo anterior.

Como se puede observar, se tienen 8 zeros, Este número es similar al 21 que determinamos antes. Entonces, $2^x - 2$. (donde x es el número de ceros en la máscara de red).

$$2^8 - 2 = 254.$$

Una vez más, el 2 es sustraído del resultado derivado de la dirección de red y de broadcast.

Clases de Red comúnmente usadas

Clase	Tamaño de la dirección de red (en octetos)	Longitud de Netmask	Número de Redes	Número de hosts	Netmask
Class A	1	8	126	16,777,214	255.0.0.0
Class B	2	16	16,382	65,534	255.255.0.0
Class C	3	24	2,097,150	254	255.255.255.0

LA PILA OSI

Nivel de Aplicación

Servicios de red a aplicaciones

Nivel de Presentación

Representación de los datos

Nivel de Sesión

Comunicación entre dispositivos de la red

Nivel de Transporte

Conexión extremo-a-extremo y fiabilidad de los datos

Nivel de Red

Determinación de ruta e IP (Direccionamiento lógico)

Nivel de Enlace de Datos

Direccionamiento físico (MAC y LLC)

Nivel Físico

Señal y transmisión binaria

Diseño de una Red de Área Local

Dimensionamiento de una red

Medios de Transmisión

UTP	100 mts
Coaxial Delgado	200 mts
Coaxial Grueso	500 mts
Fibra Multimodo	2 000 mts
Fibra Monomodo	10 000 mts
Inalámbrico 802.11	100-300 mts
Microondas	10 000 mts
Infrarrojo	50-200 mts
Láser	10 Km

Ejemplos

Oficina

- Cableado UTP, HUB o Switch central
- No equipo en cascada ni repetidores o bridges

Edificio de 1 piso

- Cableado UTP, estrella distribuida con varios Hubs y un switch central

Edificio de varios pisos

- Cable “Riser” de piso a piso. Antes se usaba coaxial grueso, hoy se usa UTP o fibra
- Switch, puertos gigabit o ruteador, con diferentes subredes (IP’s) en cada puerto.
- Se puede poner un bridge en cada piso

Varios edificios cercanos

- Fibra para interconectar edificios (mayor distancia, aislante eléctrico, mayor capacidad de datos)
- Anillo (tecnología FDI 80’s) o estrella (switch gigabit).
- Bridges en cada edificio, en muchos casos pueden reemplazarse con switches

Edificios en la misma ciudad

- Microondas, con antenas direccionales. Requieren línea de vista (no obstáculos). Se recibe en un ruteador, para no enviar tráfico innecesario.

Edificios en diferentes ciudades

- Satélite o líneas dedicadas rentadas. Alto costo, optimizar con ruteadores y firewall, administrador de ancho de banda.

Interconexión de redes

¿Porqué es importante la interconectividad de redes?

- Compartir recursos
- Acceso Instantáneo a bases de datos compartidas
- Insensibilidad a la distancia física y a la limitación en el número de nodos
- Administración centralizada de la red
- Da una ventaja estratégica en el mercado competitivo global

¿Cómo se interconectan las redes?

Las redes se conectan mediante equipos de telecomunicaciones conocidos como equipos de interconexión.

Equipos de Interconexión

Dos o más redes separadas están conectadas para intercambiar datos o recursos forman una interred (internetwork). Enlazar LANs en una interred requiere de equipos que realicen ese propósito. Estos dispositivos están diseñados para sobrellevar los obstáculos para la interconexión sin interrumpir el funcionamiento de las redes. A estos dispositivos que realizan esa tarea se les llama equipos de Interconexión.

Existen equipos de Interconexión a nivel de:

- LAN: Hub, switch, repetidor, gateway, puente, access points.
- MAN: Repetidor, switch capa 3, enrutador, multicanalizador, wireless bridges. puente, modem analógico, modem ADSL, modem CABLE, DSU/CSU.
- WAN: Enrutador , multicanalizador, modem analógico, DSU/CSU, modem satelital.

Elaboración de cableado de Red

Tipos de codigos

ANSI

(Instituto Nacional Americano de Normalización)

Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la Organización Internacional para la Normalización.

La RJ-45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

Estándares T586A y T586B

TIA/EIA-568-B es un conjunto de estándares de la Telecommunications Industry Association.

Los estándares cableado comercial de edificios para productos de telecomunicación y servicios.

Los tres estándares son formalmente llamados ANSI/TIA/EIA-568-B.1-2001, -B.2-2001, y -B.3-2001.

Los estándares TIA/EIA-568-B fueron publicados en 2001. Sucedieron a los estándares TIA/EIA-568-A, los cuales ahora son obsoletos.

Los estándares para cableado conductor de par trenzado de 100 Ohms son T568A y T568B.

T586B

Pin	Función	RJ45 Norma 586B	Color
1	Transmite	2	Blanco/Naranja
2	Transmite	2	Naranja
3	Recibe	3	Blanco/Verde
4		1	Azul
5		1	Blanco/Azul
6	Recibe	3	Verde
7		4	Blanco/Café
8		4	Café

T586A

Pin	Función	RJ45 Norma 586A	Color
1	Recibe	3	Blanco/Verde
2	Recibe	3	Verde
3	Transmite	2	Blanco/Naranja
4		1	Azul
5		1	Blanco/Azul
6	Transmite	2	Naranja
7		4	Blanco/Café
8		4	Café

Cable CRUZADO (CROSSOVER)

En un cable cruzado se cambia el orden de los dos pares que transmiten los datos.

El cable cruzado se usa, en general, para:

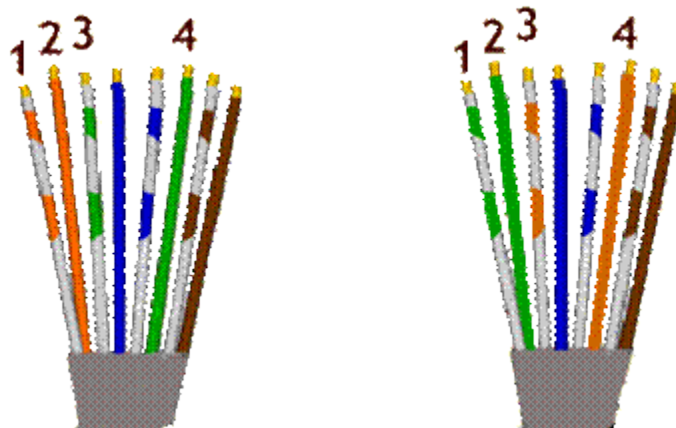
- Conectar un ordenador con otro, que actúa como servidor, sin necesidad de un concentrador.
- Conectar dos estaciones de trabajo aisladas.
- Conectar concentradores entre sí. Este caso se dará cuando nuestro concentrador no disponga de un puerto uplink, o esté desactivada la opción de Enlace ascendente/Normal. O bien si queremos conectar dos concentradores directamente, utilizando cualquier otro puerto.

En redes Ethernet 10/100Base T sólo se utilizan dos pares de cables (Blanco-Naranja/Naranja y Blanco Verde/Verde); así, necesitamos hacer un cable en el que:

Los hilos 1 y 2 de uno de los extremos de un cable estén conectados a los pin 3 y 6 del otro
Los hilos 3 y 6 del primer extremo estén conectados a los pin 1 y 6 del otro.

Para hacer un cable cruzado respetando la norma oficial, en uno de los extremos utilizaremos la norma 586B, que es la que hemos visto para hacer un cable no cruzado; y, en el otro extremo, seguiremos la norma 586A. La disposición quedará de la siguiente manera:

Cable cruzado de dos pares para tecnología 10/100BaseT



Implementación, pruebas y mantenimiento de Redes

El hardware de red está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

Requerimientos de sistemas

Hardware

- Servidores:
RAM, disco duro, ghz, tarjeta de red, RAID, unidades de respaldo, video, audio, etc.
Depende del número de usuarios, numero de procesos, y numero de consulta.
- Switches, hubs, ruteadores:
Puertos de 100 Mbits a las computadoras, 1 Gigabit a otros a switches o a servidores.
Ruteador: Tarjetas a puertos AVI.
- Cableado:
Categoría 6 para Gigabit
Ethernet: Probar con inyectoros de señal.
- Patch Panel, soportes, ductos, conectores:
Buena calidad, probar contactos, usar equipo adecuado (parchador, etc.).
- Estaciones de trabajo:
Algunos sistemas operativos de red requieren más recursos que otros.
- Plan de contingencia

Desastres naturales

En el anterior punto hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su (falta de) prevención.

Terremotos

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o hardware pierde importancia frente a los posibles accidentes - incluso mortales - que puede causar una pieza voluminosa a las personas a las que les cae encima.

Tormentas eléctricas

Una medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad; aunque hablaremos con más detalle de la protección de los backups en el punto de momento podemos adelantar que se han de almacenar lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de nuestros sistemas.

Inundaciones y humedad

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que, como veremos más tarde, puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al hardware y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Desastres del entorno

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo...a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

Ruido eléctrico

Dentro del apartado anterior podríamos haber hablado del ruido eléctrico como un problema más relacionado con la electricidad; sin embargo este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otras máquinas que pueden afectar al funcionamiento de la nuestra. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, especialmente muchos de los instalados en los laboratorios de organizaciones de y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos puede incluso

dañar permanentemente a nuestro hardware si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

Incendios y humo

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el hardware no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero que quedara destrozado por el agua expulsada. Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera, y por otro puede asfixiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un pitido.

Temperaturas extremas

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire, aparato que también influirá positivamente en el rendimiento de los usuarios (las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente). Otra condición básica para el correcto funcionamiento de cualquier equipo que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

Mobiliario especial y equipo adicional

- Rack 1U
- Gabinete (LIU- minigabinte, fibra óptica)
- Soportes (escalerillas)
- Ductos (protección, presentación)
- Switches KVM (keyboard, Videos, Mouse)
- Teclado y monitor VackMount
- Equipo contra incendios
- Equipo de Prueba
- Probador de señal 10, 100, hub a pc.
- Probador de continuidad
- Probador para fibra óptica Atenuación
- Inyectores de señal

Corrección de Fallas

Esta función incluye procesos requeridos para detectar y recuperarse de situaciones anormales, tales como pérdida de respuesta, secuencia inválidas, enlaces cortados o pérdida del carácter del fin de la trama.

Los mecanismos básicos utilizados para recuperación de fallas son:

- Tiempo de expiración (timeout), que consiste en establecer los plazos máximos de tiempo de espera.
- Solicitud de una nueva respuesta, si el plazo ya está vencido.
- Limitación del número de reintentos transcurridos, cuya falla se da por irre recuperable (desde el punto del vista del enlace), comunicándose tal circunstancia al nivel de red para que tome las medidas oportunas. Al no limitar el número de reintentos se corre el peligro de entrar en un ciclo indefinido de solicitudes y respuestas, por ejemplo si un terminal se encuentra fuera de funcionamiento.

Crecimiento de la Red

Hace no muchos años la palabra Internet pertenecía al vocabulario de un selecto grupo de personas que tenían el privilegio de poder acceder a esta red global de información. Estos personajes, normalmente profesionales o estudiantes de informática, disponían de conexiones bastante lentas y una gama de servicios mucho más reducida que la actual, y desde luego muchísimo menos amistosa para el usuario. Internet constituye una fuente de recursos de información y conocimiento compartidos a escala mundial. Es también la vía de comunicación que permite establecer la cooperación y colaboración entre gran número de comunidades y grupos de interés por temas específicos, distribuidos por todo el planeta.

En Internet es posible encontrar toda clase de software para una gran variedad de ordenadores y sistemas operativos. De modo sencillo se puede establecer una conexión con alguno de los miles de ordenadores dedicados a proveer, de forma gratuita, los ficheros que poseen. Así pueden copiarse

programas de uso público, de shareware y aplicaciones comerciales para evaluación, incluidos juegos de ordenador. Los fabricantes de hardware suelen tener servidores donde es posible obtener actualizaciones de los controladores (drivers) de sus productos.

A través de Internet pueden consultarse los catálogos de las bibliotecas más importantes del mundo, acceder a bases de datos con los temas más diversos y transferir copias de los documentos encontrados.

Es posible visualizar y copiar ficheros de imágenes con fotografías de todo tipo o reproducciones de cuadros. Pueden hacerse cosas como conversar a tiempo real. Dos personas, separadas por miles de kilómetros de distancia, pueden comunicarse a través de Internet escribiendo en el ordenador.

No solamente es posible obtener información o utilizar algún tipo de servicio. El usuario también puede ofrecerlos si lo desea. Una de las formas más sencillas es participar de un grupo de noticias o de una lista de correos. Los artículos que allí se envíen serán distribuidos automáticamente entre todos los miembros de la lista, y éstos pueden ser miles repartidos por todo el mundo.

La lista de cosas que pueden hacerse o conseguirse a través de Internet sería interminable. Lo que se busque o se encuentre depende en gran medida de los intereses particulares y de la ocupación de cada uno, resultando imposible dar una imagen de ello en unas cuantas líneas. Lo mejor es que cada uno explore por sí mismo y descubra lo apasionante que puede resultar un viaje a través de las autopistas de la información, un viaje por Internet.

Aunque la Internet es una red global, en muchos aspectos se parece a una pequeña ciudad con servicios similares. Digamos que usted quisiera enviar o recibir correo. La Internet tiene oficinas electrónicas de correo. Hay bibliotecas en línea que puede usar a cualquier hora del día o de la noche, con millones de libros y periódicos para lecturas ilimitadas. Los salones de chat son el equivalente en la Internet a los cafés abiertos las 24 horas, con personas deseosas de charlar en cualquier momento que usted desee. Con el explosivo crecimiento de la Red Mundial es posible ir de compras, ordenar pizza, ver los cortes de una película y escuchar estaciones de radio de todo el mundo. Todas estas son diferentes maneras de usar la Internet.

En el mundo real usted puede viajar a lugares diferentes en la misma red de carreteras, pero usando diferentes medios de transporte. Puede usar un coche para un propósito y un camión para otro diferente. Desplazarse en la Internet funciona de manera muy similar.

Para entender la Internet, es bueno tener en cuenta que se dan muchos tipos de comunicaciones al mismo tiempo. Se usan diferentes programas para realizar diferentes tareas: por ejemplo, un navegador Web para acceder a los sitios de compras y un programa de correo electrónico para enviar y recibir mensajes.

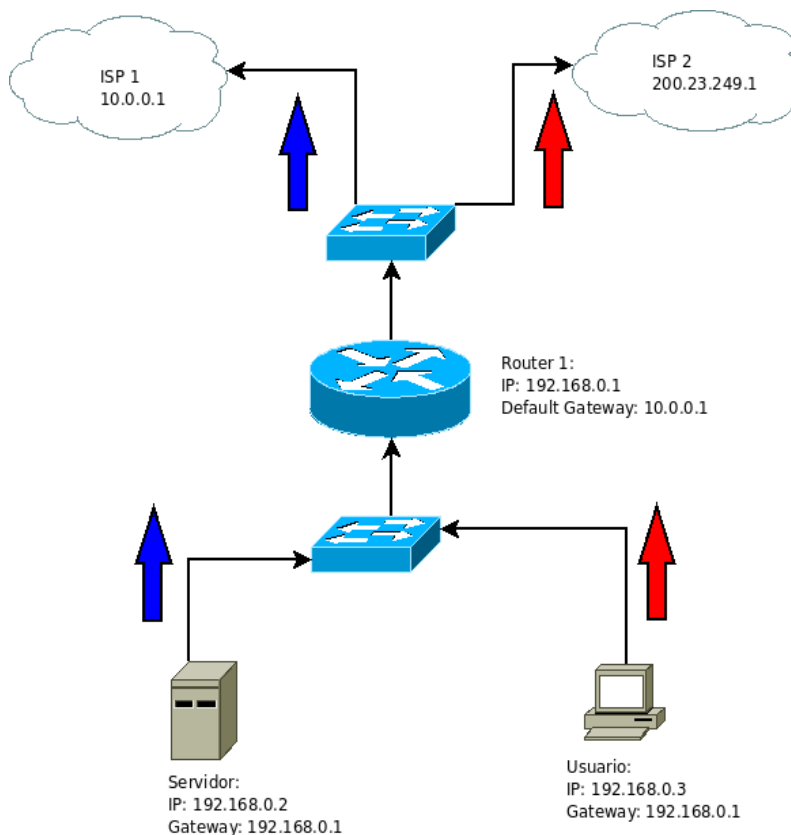
Conceptos básicos de Ruteo de Redes

Un conmutador o **switch** es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

El encaminador (calco del inglés **router**), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Host: Computadora o equipo (Nodo) dentro de una red.

Gateway: Host con capacidades de Interactuar con otras redes que usan protocolos diferentes.



Tipos de enrutamiento:

Routing Information Protocol (RIP). RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico.

Open Short Path First (OSPF). OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes.

Interior Gateway Protocol (IGRP). IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco.

Enhanced IGRP - EIGRP. Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace.

Border Gateway Protocol (BGP). Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos.

Configuración de equipo (APs, Switchs, Routers)

- Instalación de un Ruteador Basado en GNU/Linux (SmoothWall Express)
- Configuración de un AP

Seguridad de redes Cableadas e Inalámbricas.

Medidas básicas de seguridad

Física

El hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización, especialmente en las dedicadas a universidades, centros de investigación, institutos tecnológicos...suelen poseer entre sus equipos máquinas muy caras, desde servidores con una gran potencia de cálculo hasta routers de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.

Son muchas las amenazas al hardware de una instalación informática; aquí se van a presentar algunas de ellas, sus posibles efectos y algunas soluciones, si no para evitar los problemas sí al menos para minimizar sus efectos.

Protección eléctrica

Todos los dispositivos de una red necesitan corriente eléctrica para su funcionamiento. Los ordenadores son dispositivos especialmente sensibles a perturbaciones en la corriente eléctrica. Cualquier estación de trabajo puede sufrir estas perturbaciones, aunque esta contrariedad perjudique exclusivamente a un único usuario. Sin embargo, si el problema se produce en un servidor, el daño es mucho mayor, ya que esta en juego el trabajo de toda o gran parte de una organización. Por tanto, los servidores deberán estar especialmente protegidos.

Algunos factores eléctricos que influyen en el funcionamiento del sistema de red son los siguientes:

- La potencia eléctrica en cada nodo, especialmente en los servidores, que son los que soportan más dispositivos: por ejemplo, discos. A un servidor que posea una fuente de alimentación de 200 vatios no le podemos conectar discos y tarjetas que superen este consumo o que estén en el límite. Hay que guardar un cierto margen de seguridad si no queremos que cualquier pequeña fluctuación de corriente afecte el sistema.
- La corriente eléctrica debe ser estable. Si la instalación eléctrica es defectuosa, debemos instalar unos estabilizadores de corriente que aseguren los parámetros básicos de la entrada de corriente en las fuentes de alimentación de los equipos. Por ejemplo, garantizando tensiones de 220 voltios y 50 Hz de frecuencia. El estabilizador evita los picos de corriente, especialmente los producidos en los arranques de la maquinaria.
- La correcta distribución del fluido eléctrico y equilibrio entre las fase de corriente. En primer lugar, no podemos conectar a un enchufe de corriente más equipos de los que pueden soportar. Encadenar ladrones de corriente en cascada no es una buena solución. Además, las tomas de tierra – referencia común en toda comunicación- deben ser los mejores posibles. Si la instalación es mediana o grande, deben instalarse picas de tierra en varios lugares y asegurarse de que todas las tierras de la instalación tienen valores similares. Una toma de tierra defectuosa es una gran fuente de problemas intermitentes para toda la red, además de un importante riesgo para los equipos.
- La continuidad de la corriente. Esto se consigue con un SAI (Sistema de Alimentación

Ininterrumpida) o UPS.

Normalmente, los sistemas de alimentación ininterrumpida corrigen todas las deficiencias de la corriente eléctrica: es decir, actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etc.

- Señales Biométricas . La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital. En el caso de la huella digital, el dispositivo capta la muestra y el software biométrico transforma los puntos característicos de esta muestra en una secuencia numérica a través de un algoritmo matemático que no tiene inversa.

Seguridad del software

- Uso de passwords

A continuación se enumeran cinco características que un buen password debe tener.

- a. Tiene ocho o más caracteres
- b. Mezcla minúsculas y mayúsculas
- c. Mezcla letras con números, signos de puntuación y símbolos especiales como \$ % & "
- d. Se puede digitar rápidamente
- e. Es fácil de recordar

- Se debe cambiar a menudo
- No se deja a la vista pues puede verlo cualquiera
- Cuanto más grande más protege
- Es de uso personal y no se comparte ni con el mejor amigo

- Criptografía

La técnica de transformar un mensaje inteligible, denominado texto en claro, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos criptograma o texto cifrado. El método o sistema empleado para encriptar el texto en claro se denomina algoritmo de encriptación.

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

La base de las Criptografía suele ser la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose criptosistema o sistema de cifrado a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

- Comunicación cifrada

Herramientas de medicion y rendimiento para redes

Lista de las 25 primeras herramientas más populares en <http://insecure.org/tools/tools-es.html> (ver link para las 75 aplicaciones en la lista).

Nessus: Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plugin(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

Ethereal: Oliendo el pegamento que mantiene a Internet unida.

Ethereal es un analizador de protocolos de red para Unix y Windows, y es libre {free}. Nos permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que querramos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.

Snort: Un sistema de detección de intrusiones (IDS) libre para las masas.

Snort es una sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos {"stealth port scans"}, ataques a CGI, pruebas de SMB {"SMB Probes"}, intentos de reconocimientos de sistema operativos {"OS fingerprinting"} y mucho más. Snort utilizar un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. Mucha gente también sugirió que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort.

Netcat: La navaja multiuso para redes.

Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad del tipo "back-end" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta rica en características, útil para depurar {debug} y explorar, ya que puede crear casi cualquier tipo de conexión que podamos necesitar y tiene muchas habilidades incluidas.

TCPDump / WinDump: El sniffer clásico para monitoreo de redes y adquisición de información.

Tcpdump es un conocido y querido analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red {"network interface"} que concuerden con cierta expresión de búsqueda. Podemos utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión {port} para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades. Hay que tener en cuenta que muchos usuarios prefieren el sniffer más nuevo Ethereal.

Hping2: Una utilidad de observación {probe} para redes similar a ping pero con esteroides. hping2 ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado. También tiene un modo traceroute bastante útil y soporta fragmentación de IP. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

DSniff: Un juego de poderosas herramientas de auditoría y pruebas de penetración de redes. Este popular y bien diseñado set hecho por Dug Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspay monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la interceptación de tráfico en la red normalmente no disponible para un atacante -- por ej. debido al uso de switches {"layer-2 switches"}. sshmitm y webmitm implementan ataques del tipo monkey-in-the-middle activos hacia sesiones redirigidas de SSH y HTTPS abusando de relaciones {"bindings"} débiles en sistemas con una infraestructura de llaves públicas {PKI} improvisados. Una versión para Windows mantenida por separado está disponible acá.

GFI LANguard: Un escáner de red no-libre para Windows. LANguard escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches {patches} de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro {"key registry entries"}, passwords débiles, usuarios y grupos; y más. Los resultados del escaneo se muestran en un reporte en formato HTML, que puede ser modificado a gusto propio o consultado. Aparentemente, una versión gratuita está disponible para prueba y usos no comerciales.

Ettercap: Por si acaso todavía pensemos que usar switches en las LANs nos da mucha seguridad extra.

Ettercap es un interceptor/sniffer/registrator para LANs con ethernet basado en terminales {terminal-based}. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También es posible la inyección de datos en una conexión establecida y filtrado al vuelo {"on the fly"} y aun manteniendo la conexión sincronizada. Muchos modos de sniffing fueron implementados para darnos un set poderoso y completo de sniffing. También soporta plugins. Tiene la habilidad para comprobar si estamos en una LAN con switches o no, y de identificar huellas de sistemas operativos {OS fingerprints} para dejarnos conocer la geometría de la LAN.

Whisker/Libwhisker: El escáner y la biblioteca de vulnerabilidades de CGI de Rain.Forest.Puppy.

Whisker es un escáner que nos permite poner a prueba servidores de HTTP con respecto a varios agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts/programas que utilicen CGI. Libwhisker es una biblioteca para perl (utilizada por Whisker) que nos permite crear escáneres de HTTP a medida. Si lo que se desea es auditar más que sólo servidores de web, podemos darle una mirada a Nessus.

John the Ripper: Un extraordinariamente poderoso, flexible y rápido cracker de hashes de passwords multi-plataforma.

John the Ripper es un cracker de passwords rápido, actualmente disponible para muchos sabores de Unix (11 son oficialmente soportados, sin contar arquitecturas diferentes), DOS, Win32, BeOs, y OpenVMS. Su propósito principal es detectar passwords de Unix débiles. Soporta varios tipos de hashes de password de crypt(3) que son comúnmente encontrados en varios sabores de Unix, así como

también AFS de Kerberos y las "LM hashes" de Windows NT/2000/XP. Otros varios tipos de hashes se pueden agregar con algunos parches que contribuyen algunos desarrolladores.

OpenSSH / SSH: Una manera segura de acceder a computadoras remotas.

Un reemplazo seguro para rlogin/rsh/rcp. OpenSSH deriva de la versión de ssh de OpenBSD, que a su vez deriva del código de ssh pero de tiempos anteriores a que la licencia de ssh se cambiara por una no libre. ssh (secure shell) es un programa para loggarse en una máquina remota y para ejecutar comandos en una máquina remota. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables {"untrusted hosts"} sobre una red insegura. También se pueden redirigir conexiones de X11 y puertos arbitrarios de TCP/IP sobre este canal seguro. La intención de esta herramienta es la de reemplazar a `rlogin`, `rsh` y `rcp`, y puede ser usada para proveer de `rdist`, y `rsync` sobre una canal de comunicación seguro. Hay que notar que la versión del siguiente link a SSH.com cuesta dinero para algunos usos, mientras que OpenSSH es siempre de uso libre. Los usuarios de Windows quizás quieran el cliente de SSH libre PuTTY o la linda versión para terminal {"terminal-based port"} de OpenSSH que viene con Cygwin.

Sam Spade: Herramienta de consulta de redes de distribución gratuita.

SamSpade nos provee de una interfaz de usuario gráfica (GUI) consistente y de una implementación de varias tareas de investigación de red útiles. Fue diseñada con la idea de rastrear spammers en mente, pero puede ser útil para muchas otras tareas de exploración, administración y seguridad. Incluye herramientas como ping, nslookup, whois, dig, traceroute, finger, explorador de web crudo, transferencia de zona de DNS {"DNS zone transfer"}, comprobación de "relay" de SMTP, búsqueda en sitios web, y más. Los que no son usuarios de Windows pueden disfrutar de las versiones online de muchas de sus herramientas.

ISS Internet Scanner: Evaluación de vulnerabilidades a nivel de Aplicación.

Internet Scanner comenzó en el '92 como un pequeño escáner "Open Source" escrito por Christopher Klaus. ISS creció hasta ser una enorme empresa con una amplia gama de productos de seguridad. El escáner de Internet de ISS es bastante bueno, ¡pero no es barato! Las empresas con presupuestos ajustados quizás quieran darle una mirada a Nessus. Una revisión de 5 herramientas de análisis de vulnerabilidades {"VA tools"} en la revista "Information Security" de marzo del 2003 está disponible acá.

Tripwire: El abuelo de las herramientas de comprobación de integridad de archivos.

Un comprobador de integridad de archivos y directorios. Tripwire es una herramienta que ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema (por ej. diariamente), Tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo. Una version "Open Source" para Linux está disponible de manera gratuita en Tripwire.Org.

Nikto: Un escáner de web de mayor amplitud.

Nikto es un escáner de servidores de web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de 200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker.

Kismet: Un poderoso sniffer para redes inalámbricas.

Kismet es un sniffer y disecador de redes 802.11b. Es capaz de "sniffear" utilizando la mayoría de las placas inalámbricas; de detectar bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP; listar equipos de Cisco por medio del "Cisco Discovery Protocol"; registrar paquetes criptográficamente débiles y de generar archivos de registro compatibles con los de ethereal y tcpdump. También incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes. La versión para Windows está todavía en etapas preliminares. Es por eso que quien lo necesite quizás quiera darle una mirada a Netstumbler si tiene algún problema..

SuperScan: El escáner de TCP para Windows de Foundstone.

Un escáner de puertos de TCP, pinger y resolvidor de nombres {"hostname resolver"} basado en connect(). Viene sin el código fuente. Puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP especificados. También puede conectarse a cualquier puerto abierto descubierto utilizando aplicaciones "ayudantes" especificadas por el usuario (e.g. Telnet, Explorador de Web, FTP).

L0phtCrack 4: Aplicación de recuperación y auditoría de passwords para Windows.

L0phtCrack intenta crackear los passwords de Windows a partir de las hashes que puede obtener (por medio de acceso apropiado) de máquinas con Windows NT/2000 independientes, servidores en red, controladores primarios de red {"primary domain controllers"}, o Active Directory. En algunos casos, puede olfatear {sniff} las hashes directamente desde el cable. También tiene numerosos métodos de generar suposiciones de passwords (diccionario, fuerza bruta, etc.). L0phtCrack cuesta actualmente US\$ 350 por máquina y no incluye el código fuente. Las empresas con presupuesto ajustados, pueden darle una mirada a John the Ripper, Cain & Abel, y a pwdump3.

Retina: Escáner para la evaluación de vulnerabilidades no-libre hecho por eEye.

Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada. Una revisión de 5 herramientas de análisis de vulnerabilidades {"VA tools"} en la revista "Information Security" de marzo del 2003 está disponible acá.

Netfilter: El filtro/firewall de paquetes del kernel Linux actual.

Netfilter es un poderoso filtro de paquetes el cual es implementado en el kernel Linux estándar. La herramienta iptables es utilizada para la configuración. Actualmente soporta filtrado de paquetes stateless o statefull, y todos los diferentes tipos de NAT (Network Address Translation) y modificación de paquetes {"packet mangling"}. Para plataformas no Linux, podemos ver pf (OpenBSD), ipfilter (muchas otras variantes de UNIX), o incluso el firewall personal Zone Alarm (Windows).

tracert/route/ping/telnet/whois: Lo básico.

Aunque hay muchas asombrosas herramientas de alta tecnología dando vueltas para ayudar en la auditoría de seguridad, ¡no hay que olvidar lo básico!. Todos deberían estar muy familiarizados con estas herramientas ya que están presentes en la mayoría de los sistemas operativos (a excepción de Windows, que omite whois y utiliza el nombre tracert). Pueden ser muy útiles, aunque para usos más avanzados quizás sea mejor utilizar Hping2 y Netcat.

Fport: El netstat mejorado de Foundstone.

fport reporta todos los puertos, TCP/IP y UDP abiertos en la máquina en la que es ejecutado y muestra qué aplicación abrió cada puerto y sus aplicaciones asociados. Sólo funciona bajo Windows, pero muchos sistemas UNIX nos proveen de esta información a través de netstat (prueben con 'netstat -pan' en Linux). Aquí hay un artículo de SANS referido al uso de fport y el análisis de sus resultados.

SAINT: Security Administrator's Integrated Network Tool (Herramienta de red integrada para el Administrador de Seguridad).

Saint es otra herramienta no-libre de evaluación de seguridad (al igual que ISS Internet Scanner o Retina de eEye). A diferencia de esas herramientas basadas exclusivamente en Windows, SAINT corre exclusivamente sobre UNIX. Saint solía ser gratuito y "open source" pero ahora es un producto no-libre.

Network Stumbler: Sniffer gratuito de 802.11 para Windows.

Netstumbler es la más conocida herramienta para Windows utilizada para encontrar "access points" inalámbricos abiertos ("wardriving"). También distribuyen una versión para WinCE para PDAs y similares llamada Ministumbler. Esta herramienta es actualmente gratis pero sólo para Windows y no incluye el código fuente. Se hace notar que "El autor se reserva el derecho de cambiar este acuerdo de licencia a gusto, sin previo aviso." Los usuarios de UNIX (y usuarios de Windows avanzados) quizás quieran darle una mirada a Kismet.

SARA: Asistente de Investigación para el Auditor de Seguridad (Security Auditor's Research Assistant).

SARA es una herramienta de evaluación de vulnerabilidades derivada del infame escáner SATAN. Tratan de publicar actualizaciones dos veces al mes y de fomentar cualquier otro software creado por la comunidad de código abierto (como Nmap y Samba).

N-Stealth: Escáner de Servidores de Web.

N-Stealth es un escáner de seguridad de servidores de web no-libre. Es generalmente, actualizado más frecuentemente que los escáneres de web libres tales como whisker y nikto, pero exageran en su sitio web. Alegan "20.000 vulnerabilidades y exploits" y que "Docenas de comprobaciones de vulnerabilidades son agregadas cada día" y esto es altamente cuestionable. También, cabe notar que básicamente, todas las herramientas generales análisis de vulnerabilidades {"VA tools"} tales como nessus, ISS, Retina, SAINT, y SARA incluyen componentes para escaneo de web. Quizás no estén tan actualizados, o sean lo suficientemente flexibles. n-stealth es sólo para Windows y no se incluye el código fuente.

AirSnort: Herramienta de crackeo del cifrado WEP de 802.11.

AirSnort es una herramienta para LANs inalámbricas (WLAN) que recupera las llaves de cifrado. Fue desarrollada por el Shmoo Group y opera monitoreando pasivamente las transmisiones, cocomputando la llave de cifrado cuando suficientes paquetes han sido recolectados. La versión para Windows es todavía demasiado preliminar.

NBTScan: Recolecta información de NetBIOS de redes de Windows.

NBTscan es un programa que escanea redes IP en busca de información de nombres de NetBIOS. Envía pedidos de "status" de NetBIOS a cada dirección en un rango provisto por el usuario y lista la información recibida de manera humanamente legible. Por cada host que responde, se lista su dirección, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina {"logged in"}, y dirección de MAC.

GnuPG / PGP: Protejamos nuestros archivos y comunicaciones con cifrado avanzado.

PGP es el famoso programa de encriptación diseñado por Phil Zimmerman que ayuda a proteger nuestra información de curiosos y otros riesgos. GnuPG es una muy respetada implementación del estándar PGP (el nombre del ejecutable es, en realidad, gpg). Mientras GnuPG es software libre, PGP puede costar algo de dinero para algunas aplicaciones.

Firewalk: traceroute avanzado.

Firewalk emplea técnicas similares a las de traceroute para analizar las respuestas a paquetes de IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways. Esta herramienta clásica fue reescrita desde cero en octubre del 2002. Hay que notar que mucha de su funcionalidad (si no toda) también puede ser realizada por la opción --traceroute de Hping2.

Cain & Abel: El L0phtcrak para el pobre.

Cain & Abel es una herramienta de recuperación de passwords gratuita para los sistemas operativos de Microsoft. Permite una fácil recuperación de varias clases de password, escuchando {sniffing} la red, crackeando los passwords cifrados utilizando ataques por diccionario y Fuerza Bruta, decodificando passwords codificados {scrambled}, revelando cuadros de diálogo del tipo password, develando passwords en cachés y analizando protocolos de enrutamiento {routing}. El código fuente no viene incluido.

XProbe2: herramienta de identificación de sistemas operativos {"OS fingerprinting"} activa.

XProbe es una herramienta que sirve para determinar el sistema operativo de un host remoto. Logran esto utilizando algunas de las mismas técnicas que Nmap al igual que muchas ideas diferentes. Xprobe siempre ha enfatizado el protocolo ICMP en su enfoque de identificación {fingerprinting}.

SolarWinds Toolsets: Abundancia de herramientas de descubrimiento/monitoreo/ataque para redes.

SolarWinds ha creado y vende docenas de herramientas de propósito especial orientadas a administradores de sistemas. Las herramientas referidas a la seguridad incluyen varios escáneres de descubrimiento para redes y un cracker por fuerza bruta de SNMP. Estas herramientas son para Windows solamente, cuestan plata, y no incluyen el código fuente.

NGrep: Muestra y busca paquetes.

ngrep se esfuerza por proveer de la mayoría de características comunes del "grep" de GNU, aplicándolas a la capa de network ({"network layer"} del modelo de referencia OSI). ngrep es consciente de la presencia de pcap y permite usar expresiones regulares que concuerden con el "payload" (o sea la carga, el cuerpo y _no_ los encabezados) de los paquetes. Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interfaces nulas {"null interfaces"}, y comprende la lógica de un filtro "bpf" de la misma manera que herramientas más comunes de sniffing como tcpdump y snoop.

Perl / Python: Lenguajes de scripting de propósito general para múltiples plataformas {portables}.

Aunque en esta página hay disponibles varias herramientas de seguridad enlatadas, es importante tener la habilidad de escribir las nuestras(o modificar las existentes) cuando necesitemos algo más a medida. Perl y Python hacen que sea muy fácil escribir scripts rápidos y portables para comprobar, abusar {exploit}, o incluso ;arreglar sistemas! Archivos como CPAN están llenos de modulos tales como Net::RawIP e implementaciones de protocolos para facilitar nuestras tareas.

THC-Amap: Un escáner de identificación de aplicaciones {"application fingerprinting"}. Amap (escrito por THC) es un escáner nuevo pero poderoso que prueba cada puerto buscando identificar aplicaciones y servicios en lugar de confiar en un mapeo de puertos estático.

OpenSSL: La más célebre biblioteca de cifrado para SSL/TLS.

El proyecto OpenSSL es un esfuerzo de cooperación para desarrollar un set de herramientas robusto, de nivel comercial, completo en características, y "Open Source" implementando los protocolos "Capa de sockets seguros" {"Secure Sockets Layer"} (SSL v2/v3) y "Seguridad en la Capa de Transporte" {"Transport Layer Security"} (TLS v1) así como también una biblioteca de cifrado de propósito general potente. El proyecto es administrado por una comunidad de voluntarios a lo ancho del mundo que utilizan Internet para comunicarse, planear, y desarrollar el set de herramientas OpenSSL y su documentación relacionada.

NTop: Un monitor de uso de tráfico de red.

Ntop muestra el uso de la red en una manera similar a lo que hace top por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

Nemesis: Inyección de paquetes simplificada.

El Proyecto Nemesis está diseñado para ser una pila de IP ("IP stack") humana, portable y basada en línea de comandos para UNIX/Linux. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell. Si Nemesis es de nuestro agrado, quizás querramos mirar hping2. Se complementan mutuamente bastante bien.

LSOF: LiSt Open Files (Listar archivos abiertos).

Esta herramienta forense y de diagnóstico específica de Unix lista información acerca de cualquiera archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.

Hunt: Un "packet sniffer" y un intruso en conexiones {"connection intrusion"} avanzado para Linux.

Hunt puede observar varias conexiones de TCP, entrometerse en ellas, o resetearlas. Hunt fue hecho para ser usado sobre ethernet, y tiene mecanismos activos para olfatear {sniff} conexiones en redes con switches. Las características avanzadas incluyen "ARP relaying" selectivo y sincronización de conexión luego de ataques. Si Hunt es de nuestro agrado, también podemos darle una mirada a Ettercap y a Dsniff.

Honeyd: Nuestra honeynetpersonal.

Honeyd es un pequeño daemon que crea hosts virtuales en una red. Los hosts pueden ser configurados para ejecutar servicios arbitrarios, y su personalidad de TCP puede ser adaptada para que parezcan estar ejecutando ciertas versiones de sistemas operativos. Honeyd permite que un host alegue tener múltiples direcciones en una LAN para simulación de red. Es posible hacer ping o traceroute a las máquinas virtuales. Cualquier tipo de servicio en la máquina virtual puede ser simulado de acuerdo a un archivo de configuración simple. También es posible ser proxy de servicios para otras máquinas en lugar de simularlos. La página en la Web está fuera de servicio actualmente por motivos legales, pero el archivo tar de la V. 0.5 está aún disponible acá.

Achilles (sitio no oficial): Un proxy de ataques por web para Windows.

Achilles es una herramienta designada para comprobar la seguridad de aplicaciones web. Achilles es un servidor proxy, que actúa como una persona-en-el-medio {man-in-the-middle} durante una sesión de HTTP. Un proxy de HTTP típico pasa paquetes hacia y desde el explorador de web cliente y un servidor de web. Achilles intercepta los datos en una sesión de HTTP en cualquier dirección y le da al usuario la habilidad de alterar los datos antes de ser transmitidos. Por ejemplo, durante una conexión de HTTP SSL normal, un proxy típico pasa la sesión entre el servidor y el cliente y permite a ambos nodos negociar SSL. En contraste, cuando Achilles está en modo de interceptación, Achilles simula ser el servidor y negocia dos sesiones de SSL, una con el explorador de web cliente y otra con el servidor de web. Mientras la información se transmite entre ambos nodos, Achilles descifra los datos y le da al usuario la habilidad de alterar y/o registrar los datos en texto claro antes de su transmisión.

Brutus: Un cracker de autenticación de fuerza bruta para redes.

Este cracker sólo para Windows se lanza sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más. El código fuente no está disponible. Los usuarios de UNIX deberían darle una mirada a THC-Hydra.

Stunnel: Una envoltura criptográfica SSL de propósito general.

stunnel está diseñado para trabajar como una envoltura de cifrado SSL entre un cliente remoto y un servidor local (ejecutable por inetd) o remoto. Puede ser utilizado para agregarle funcionalidad SSL a daemons utilizados comúnmente como POP2, POP3, y servidores de IMAP sin cambios en el código del programa. Negocia una conexión SSL utilizando la biblioteca de OpenSSL o la SSLeay.

Paketto Keiretsu: TCP/IP extremo.

Paketto Keiretsu es una colección de herramientas que utilizan nuevas e inusuales estrategias para manipular redes con TCP/IP. Modifican la funcionalidad dentro de una infraestructura existente y expanden los protocolos más de lo esperado por su diseño. Incluye Scanran, una sistema de descubrimiento de servicios de red y topología inusualmente rápido, Minewt, un router NAT/MAT para espacio de usuario {"user space"}, linkcat, que presenta un enlace Ethernet a la entrada/sálida estándar. {stdio}, Paratrace, que rastrea los caminos de red sin realizar nuevas conexiones, y Phentropy, que utiliza OpenQVIS para graficar cantidades arbitrarias de entropía de fuentes de datos en un espacio de tres dimensiones. ¿Se entendió algo? :).

Fragroute: La peor pesadilla de los IDS.

Fragroute intercepta, modifica, y reescribe el tráfico de salida, implementando la mayoría de los ataques descritos en el "IDS Evasion paper" de Secure Networks. Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar, superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operaciones más en todos los paquetes salientes destinados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico. Esta herramienta fue escrita de buena fe para ayudar en el ensayo de sistemas de detección de intrusión, firewalls, y comportamiento básico de implementaciones de TCP/IP. Al igual que Dsniff y Libdnet, esta excelente herramienta fue escrita por Dug Song.

SPIKE Proxy: Cracking de HTTP.

Spike Proxy es un proxy de HTTP "open source" que sirve para encontrar fallas de seguridad en sitios web. Es parte del Spike Application Testing Suite y soporta detección de inyección de SQL automatizada, crawling *** de sitios web, uso de fuerza bruta en formularios de entrada, detección de overflow, y detección de acceso a directorios que debieran estar fuera de los límites del sitio de web {"directory traversal"}.

THC-Hydra: Cracker de autenticación de red paralelizado.

Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada {login} por red, incluyendo FTP, POP3, IMAP, Netbios, Telnet, HTTP Auth, LDAP, NNTP, VNC, ICQ, Socks5, PCNFS, y más. Incluye soporte para SSL y aparentemente es ahora parte de Nessus. Al igual que Amap, esta versión es de la gente de THC.