Autopista de la información

PROGRAMA:

" SAN LUIS

GESTION PARA LA IMPLEMENTACION DE UNA PROVINCIA DIGITAL

AUTOPISTA DE LA INFORMACION "

PROYECTO :

"POLITICAS DE SEGURIDAD INFORMATICA"

INFORME FINAL

"POLITICAS DE SEGURIDAD INFORMATICA"

- AUTOPISTA DE LA INFORMACION -

Integrantes del Grupo:

Experto: Adolfo Alejandro Silnik

Colaborador: Lorenzo Maximo Vieyra

- Noviembre -

- 2002 -

RESUMEN EJECUTIVO

INFORME FINAL

Como se sabe, el Proyecto de la Autopista de la Información, es uno de los mas grandes existentes en el mundo, permitiendo que miles de usuarios puedan gozar de sus beneficios.

La presente propuesta encara la tarea de elaborar políticas de seguridad aplicables a esta situación, garantizando, tanto la seguridad de los datos provistos al ciudadano, como así también la disponibilidad de los mismos.

Asimismo, propone un esquema (que se funda en el análisis y la evaluación) para elaborar protocolos y políticas, es decir una metodología para poder llevar adelante la inmensa red que abarcará la Autopista de la Información.

Objetivo General:

Por lo dicho anteriormente, el objetivo básico y principal de este trabajo es la Generación de Políticas de Seguridad Informática, considerando la administración, control y mantenimiento de todos los equipos y productos involucrados en la seguridad principal de la Autopista de la Información.

La ejecución del proyecto pretende, con el cumplimiento de la cadena de objetivos específicos establecidos, asegurar la generación y elaboración de propuestas de políticas de seguridad, que se adecuen a este nuevo escenario tecnológico.

Actividades:

- Actividad 1: Esta actividad tiene como objetivo definir la forma de acceder a los recursos compartidos asegurando la integridad de los datos y su disponibilidad para el usuario final. Al concluir esta etapa del Proyecto, se establecieron una serie de pautas y recomendaciones para instalar, configurar y administrar los distintos activos involucrados en la conexión del usuario al corazón de la Autopista, es decir al Data Center, así como también el ingreso físico al mismo.
- Actividad 2: Tanto esta actividad como la siguiente poseen el mismo objetivo en común, la seguridad y la prevención. En particular, esta actividad trata el tema a nivel usuario interno (empleados pertenecientes al Gobierno de la Provincia). Para cumplir con este objetivo, se establecieron una serie de pautas que permiten generar políticas de monitoreo y control del tráfico de datos circulantes por esta red, controlando principalmente a los usuarios pertenecientes al Gobierno de la Provincia.
- Actividad 3: Como se mencionó en el párrafo anterior, el objetivo de esta actividad es también, la seguridad y la prevención. Cabe señalar en este punto que se realizó una distinción entre usuarios internos y externos por una razón de facilidad de rastreo y sanción en caso de intrusiones (accesos no autorizados) por parte de alguna persona. Esta actividad en particular se dedicó mas a la obtención de datos estadísticos (que permiten configurar apropiadamente los equipos, además de proporcionar una visión clara del tráfico de datos sobre la red), es decir que esta actividad complementa a la anterior, garantizando así el cumplimiento del objetivo previsto. Para ello, se

establecieron pautas que permiten generar políticas de monitoreo y control de los datos, pero en esta ocasión haciendo hincapié en los usuarios que se conectan a la red y no pertenecen al Sector Público.

- Actividad 4: Por último, en esta actividad, se establecen las pautas y requisitos necesarios para instalar, configurar y administrar un sistema centralizado de Antivirus, de tal forma que asegure la integridad de los datos contenidos en el Data Center, evitando la circulación de virus por la red, que hoy en día son la principal causa de perdida de datos.

Como se puede apreciar a lo largo de estas actividades, se han establecido las normas o pautas que permiten generar distintas políticas cuyo objetivo es evitar daños a los datos y sistemas, ocasionados por personal del estado o usuarios ajenos al mismo. Además se tratan de impedir o minimizar los inconvenientes ocasionados por la proliferación y propagación de virus informáticos que aparecen cada vez con mas frecuencia.

Para finalizar, se debe aclarar que, si bien la tarea de crear o diseñar las pautas o normas a utilizar para establecer políticas esta concluida, estas tareas, principalmente las tres últimas, son de ejecución continua, es decir, que tanto los monitoreos, las estadísticas y principalmente la detección de virus, se realizan diariamente.

ing. Adolfo Alejandro Silnik

INFORME FINAL

1.- Introducción:

Como se ha observado en los últimos años, las Administraciones Públicas se han relacionado y prestado sus servicios a los ciudadanos y empresas utilizando cada vez mas sistemas y tecnologías de la información y comunicaciones. La eficacia, la agilidad y la calidad de la Administración dependen cada vez más del funcionamiento correcto y seguro de dichos sistemas y tecnologías.

Con esta visión transformadora, el Gobierno Provincial luego de implementar una Intranet de Gobierno, con alcance a todos los empleados públicos y demás interesados, encara un proyecto de mayor magnitud como es el de la Autopista de la Información, convirtiéndose así en un pionero en esta área.

Este proyecto es uno de los mas ambiciosos que lleva adelante el Gobierno Provincial convirtiendo a San Luis en la provincia mas conectada de Latinoamérica, permitiendo así que la población acceda a la información y conocimiento, mediante una serie de iniciativas denominadas "San Luis en línea".

La magnitud de esta situación para el rápido cambio tecnológico que se afronta y el corto plazo disponible, hacen que, cada tema sea tratado de manera específica.

Como la cantidad de usuarios de la Autopista de la Información se verá multiplicada en los próximos meses, se hace necesario aplicar controles de seguridad bien definidos y elaborados.

La presente propuesta encara la tarea de elaborar políticas de seguridad aplicables a esta situación, garantizando, tanto la seguridad de los datos provistos al ciudadano, como así también la disponibilidad de los mismos.

Asimismo, propone un esquema (que se funda en el análisis y la evaluación) para elaborar protocolos y políticas, es decir una metodología para poder llevar adelante la inmensa red que abarcará la Autopista de la Información.

La interconexión de redes y la puesta en marcha de servicios de información compartidos con acceso público, requieren de una administración basada en normas establecidas que especifiquen como han de ser los procedimientos de asignación de recursos, como será su forma de acceso, como se ha de realizar la gestión de encaminamiento y que medidas de seguridad hay que adoptar para garantizar el correcto funcionamiento de la Autopista de la Información y su protección frente a accesos no autorizados, tanto desde dentro de la propia administración pública, como desde fuera.

La ejecución del proyecto pretende, con el cumplimiento de la cadena de objetivos específicos establecidos, asegurar la generación y elaboración de propuestas de políticas de seguridad, que se adecuen a este nuevo escenario tecnológico y así plantear un esquema de trabajo simple y efectivo que permita la detección precoz de fallas en la seguridad.

ACTIVIDAD N° 1

2.- Objetivo:

Elaborar pautas generales y requisitos mínimos necesarios para el manejo, control y administración de accesos.

2.1.- Enunciado de la Actividad:

Generación de pautas generales para la definición de configuración de dispositivos como Firewalls, Routers y Proxys. Protocolos y puertos de acceso autorizados. Acceso físico al Data Center.

2.2.- Desarrollo:

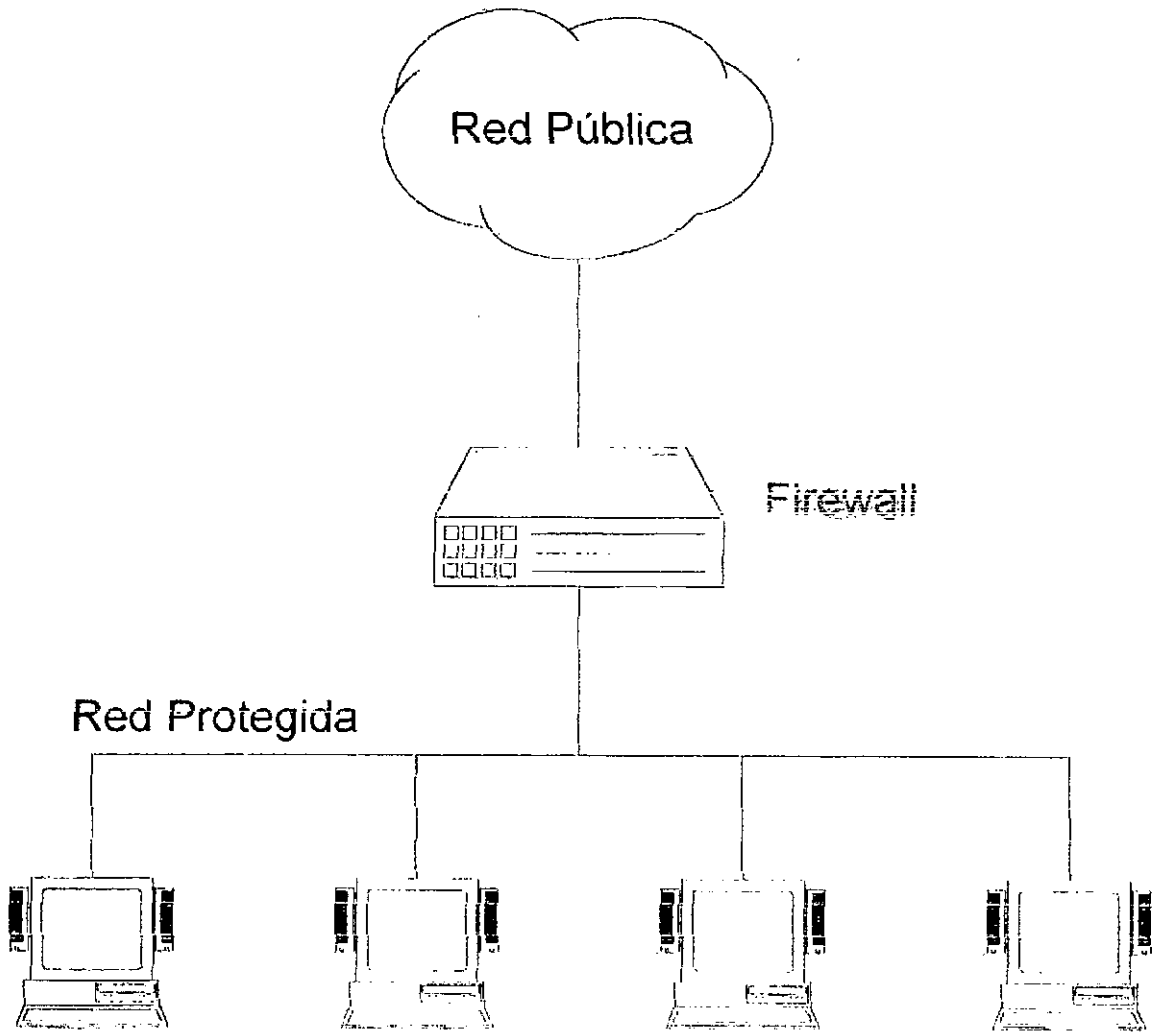
En esta actividad y tal como lo dice el enunciado, se establecerán pautas para configurar los equipos necesarios para acceder, en forma segura, a los datos contenidos en la Autopista de la Información y prevenir además accesos no autorizados a dichos recursos.

Para esto, empezaremos por definir los tres equipos principales a utilizar, que son los Firewalls, los Routers y los Proxys.

2.2.1.- Firewalls:

Estos equipos también llamados en su traducción Cortafuegos, son los encargados principalmente de decir, mediante una serie de reglas previamente configuradas, quién, a qué, y por dónde se acceden a los datos de la red a

proteger. Es decir, que un Firewall actúa a modo de "barrera" entre la zona protegida y la pública.



El funcionamiento de estos equipos se basa en el monitoreo e intercepción de tráfico no permitido de datos, es decir en el "filtrado de paquetes", llevando un registro de dichos movimientos, lo que facilita la detección y seguimiento de estos paquetes.

Esta función de Firewall puede ser llevada a cabo o bien por un hardware dedicado, o bien por un software instalado en un equipo destinado a tal fin. En

rigor, se prefieren los primeros por ser menos vulnerables y mas estables en su funcionamiento que los segundos, pero a su vez poseen un costo muy superior a ellos.

A modo meramente informativo, podemos nombrar marcas de equipos dedicados como Cisco, Lucent, entre otras y software como Norton Firewall, Zone Alarm, etc., como aplicaciones dedicados a esta función.

Como se dijo en un párrafo anterior, un Firewall se basa en el filtrado de paquetes, que se realiza en base a reglas que se establecen en la configuración, esto es de suma importancia tenerlo claro, ya que un Firewall funciona, en principio, DENEGANDO cualquier tráfico que se produzca, cerrando todos los puertos de nuestra red y autorizando sólo lo que esté indicado en dichas reglas.

De esta forma, en el momento que un determinado servicio o programa intente acceder a Internet o a nuestra Red nos lo hará saber. Es posible en ese momento aceptar o denegar dicho tráfico, pudiendo asimismo hacer (para no tener que repetir la operación cada vez) "permanente" la respuesta hasta que no cambiemos nuestra política de aceptación o reglas.

El comprender esto último es muy importante, ya que si autorizamos un determinado servicio o programa, el Firewall no va a decirnos que es correcto o incorrecto, o incluso, que siendo correcto los paquetes que están entrando o saliendo, éstos contienen datos perniciosos para nuestro sistema o la Red, por lo que hay que tener especial cuidado en las autorizaciones que otorguemos.

Como ejemplo de esto último podemos poner el Correo Electrónico. Si autorizamos en nuestro Firewall que determinado programa de correo acceda a

Internet, y recibimos un mensaje que contiene datos adjuntos con virus, por ejemplo tipo gusano, el Firewall no nos va a defender de ello, ya que hemos autorizado a que ese programa acceda a la Red. Lo que sucederá es que al ejecutar el adjunto, el gusano intentará acceder a la Red por algún puerto que no esté previamente aceptado por nosotros, lo que evitará su propagación. Ahora bien, si hace uso por ejemplo del mismo cliente de correo, si podrá propagarse, puesto que está autorizado.

La misión del firewall es la de aceptar o denegar el tráfico, pero no el contenido del mismo.

En éste caso la misión de protegernos, además del sentido común de no ejecutar un adjunto, la cumple un software Antivirus.

2.2.2.- Routers:

Un Router o ruteador, como su nombre lo indica, se encarga de direccionar el tráfico de datos hacia las distintas "sub redes" o áreas de una red determinada.

Al igual que el Firewall, funciona en base al filtrado de paquetes y reglas previamente configuradas.

Por lo tanto, valen aquí las mismas consideraciones tomadas en cuenta a la hora de configurar un Firewall, es decir, que se deniega todo el tráfico salvo el que figura explícito en las reglas de permisos.

Otra función que cumple un Router es la función de NAT (Network Address Translation) que permite pasar de una numeración IP a otra sin perder de vista el origen o destino de los datos.

Así por ejemplo, cuando tenemos que transportar determinados paquetes de datos desde una red a otra, podemos configurar un Router para que solamente permita el paso entre dichas redes a esos paquetes. De esta forma se tiene un control de que puede o no circular a través del equipo.

Es válido aclarar que muchos Firewalls y Switches también incorporan la función de Router, por lo que no siempre se encontrarán en equipos separados.

2.2.3.- Proxys:

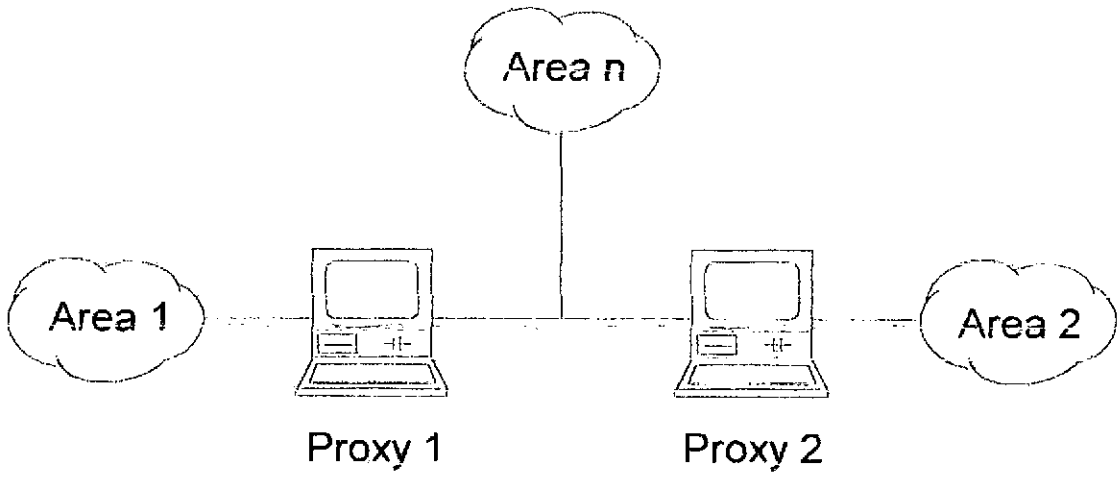
Básicamente los Proxys Servers, son máquinas con un software que permite compartir una conexión determinada con toda una red. Un uso típico, es la conexión a Internet de una "red interna", es decir que se provee a un conjunto de equipos, de un vinculo o puerta de acceso al exterior.

Un Proxy Server cumple tres funciones básicas a saber:

- Cache: Permite agilizar el acceso al exterior, principalmente cuando son reiterados, ya que almacena localmente la información de dichas direcciones (generalmente se usan para accesos a Internet).
- Router: Permite rutear o encaminar todos los pedidos de Internet realizados internamente hacia el vínculo exterior. Esto produce un enmascaramiento de las direcciones internas, ya que a primera vista, sólo se ve la dirección IP del Proxy.
- Firewall: Al poseer reglas configurables relacionadas con el tráfico de paquetes, se puede usar como barrera entre una red insegura y una segura.

Debido a estas funciones, se puede llegar a pensar que solamente colocando un Servidor de este tipo bastaría para proteger a una red, pero esto es sólo válido para un usuario común, ya que alguien con conocimiento, puede llegar a vulnerarlo mas fácilmente que a un Firewall o Router dedicado e implementado por hardware.

Por ejemplo, una aplicación válida será, cuando deseamos conectar varias áreas de un mismo organismo entre si, pero manteniéndolas seguras por separado sin generar grandes gastos, colocar un Proxy Server en cada una asegurando en alguna medida dichas áreas, además de limitar el tráfico entre áreas únicamente a los datos comunes, ya que los datos internos no son ruteados hacia afuera.



2.2.4.- Protocolos y puertos:

Una vez establecidos los servicios que se brindarán a los usuarios, en base a un análisis de los requerimientos de los mismos, se procede a crear las "Reglas" a configurar en los distintos activos involucrados (Firewalls, Routers, Proxys, etc).

Estas reglas indican qué protocolos (http, ftp, pop, smtp, etc.) y que puertos serán permitidos y a quién.

2.2.4.1.- Puertos:

El protocolo TCP/IP identifica los extremos de una conexión por las direcciones IP de los dos nodos implicados (servidor y cliente), pero como sobre este protocolo es posible la ejecución de distintos servicios, la dirección IP no es suficiente, haciendose necesario poder diferenciarlos. La forma de "diferenciarlos" es mediante los puertos.

Por lo tanto, para que la dirección quede completa también se especifica el puerto, así por ejemplo, un Servidor Web escucha las peticiones que le hacen por el puerto 80, un servidor FTP lo hace por el puerto 21, etc.

A modo de ejemplo imaginemos un edificio de oficinas, éste tiene una puerta de entrada al edificio (que en nuestro caso sería la IP) y muchas oficinas que dan servicios (que en nuestro caso serian los puertos). Eso nos lleva a que la dirección completa de una oficina viene dada por la dirección postal y el número de la oficina.

Existen 65536 puertos diferentes, usados para las conexiones de Red. En el Anexo 1 se muestran la relación de puertos y servicios a los que corresponden.

2.2.4.2.- Asegurar puertos:

Una medida básica de seguridad es conocer que puertos tenemos, cuales están abiertos, porque están abiertos y, de estos últimos, los que no utilicemos o que sean fuente de un problema de seguridad.

Antes de cerrar puertos que no utilicemos siempre hay que verificarlos, ya que es evidente que si se cierra un puerto que sí se esta utilizando, ese servicio dejará de funcionar para todos los usuarios de la red.

Tener bien claro que puertos están abiertos, nos puede ayudar a detectar entre otras cosas, Troyanos y otros virus que abran dichas puertas para su propio uso. En el Anexo 2 se muestra una lista de los puertos usados por algunos troyanos conocidos.

Cabe destacar en este momento, que debido al uso popular de Windows, se presenta un problema con el puerto 139, que es el servicio de NETBIOS, el cual es fácilmente reconocido por ser habilitado con el solo hecho de compartir archivos e impresoras. Este puerto es el mas utilizado por los virus para su propagación.

2.2.4.3.- Escaneo de puertos:

Para saber que puertos tenemos abiertos en un momento determinado podemos utilizar cualquier herramienta de las que abundan en Internet, o bien podemos hacer uso de los servicios on-line gratuitos que ofrecen algunos sitios dedicados a la Seguridad Informática.

Cabe destacar, que estas herramientas son un "arma de doble filo", así como nos ayudan a segurizar la red, también ayudan a los intrusos a detectar puertas abiertas.

Por último, una vez que hallamos escaneado e identificado los puertos no utilizados, debemos proceder a cerrarlos de forma inmediata.

2.2.5.- Accesos Físicos:

Cuando nos referimos al acceso físico al Data Center o a cualquier área restringida, estamos hablando principalmente de ejercer un control de quien entra y sale de dicho lugar (físicamente hablando).

Este control se puede llevar a cabo de distintas maneras, que pueden ser personales (personal de seguridad) o remotas (cámaras, accesos electrónicos, identificación de huellas dactilares, etc.).

Para ambos casos se deberá contar, en primer medida, con una nómina del personal autorizado y las acreditaciones correspondientes.

Como en nuestro caso la zona a proteger es el lugar físico donde se hallan los principales equipos de la Autopista de la Información (como estos son el corazón de la Obra, poseen datos de suma importancia y son un equipamiento de elevado costo), no solamente deberemos controlar el acceso en los horarios de trabajo, sino que además deberán existir guardias de seguridad durante las horas no laborales y el edificio obviamente tendrá que poseer un sistema de alarmas acorde a sus dimensiones e importancia.

Hoy en día, existen incontables empresas dedicadas a este rubro, que pueden aportar no sólo los equipamientos necesarios, sino también el personal capacitado para esta tarea, sin contar el aporte de los Entes Oficiales de Seguridad.

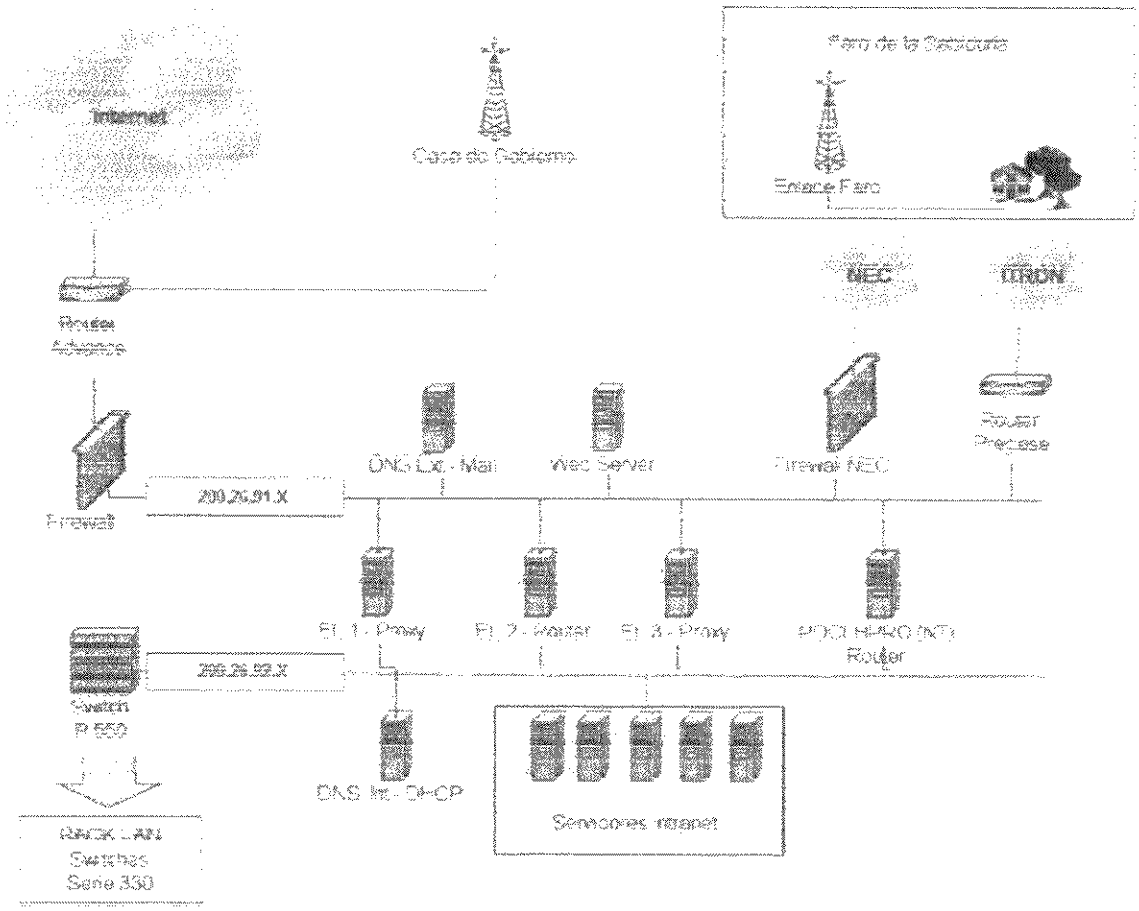
2.3.- Implementación de las pautas:

Para implementar de alguna manera estas pautas, se involucraron tres áreas, Servidores, Redes e Internet.

Los resultados obtenidos para cada pauta planteada (Anexo 3) son los siguientes:

Contar con un diagrama esquemático de las redes a proteger y sus características.

El diagrama esquemático de la red es el siguiente:



Calcular de la manera mas exacta posible la cantidad de usuarios, para poder dimensionar el hardware.

Con los datos obtenidos de muestreos de las conexiones, se pudo verificar que, si bien la cantidad de usuarios es importante, genera un trafico en la intranet que apenas llega al 10% del ancho de banda disponible.

El cuello de botella es el servicio de Internet el cual tiene aproximadamente 1200 usuarios (datos entregados por el área de Internet) de los cuales podemos suponer que alrededor de 20% se conectan simultáneamente.

Definir previamente, de forma clara, los servicios que se quieren prestar y a que usuarios..

Examinar y definir que puertos y protocolos se van a utilizar, es decir, definir las reglas de cada equipo.

Cerrar o deshabilitar todos los puertos no usados (se pueden verificar usando un scanner de puertos).

Con los datos obtenidos del muestreo de usuarios, y el poco ancho de banda disponible (la Empresa encargada de poner en marcha la Autopista de la Información esta gestionando mas ancho de banda) se vio la necesidad de restringir, por un tiempo, los servicios de Internet hasta dejar solo los indispensables (correo, http y en algunas excepciones ftp), por lo tanto únicamente se dejaron abiertos los puertos correspondientes a estos servicios cerrando todos los demás.

En lo que se refiere a la Intranet y al servicio de correo, estos no sufren problemas ya que, al ser internos, no necesitan vínculos con Internet.

Elegir hardware y/o software en base a la seguridad, confiabilidad, velocidad y costos.

Por una razón de seguridad se prefirió un Firewall por hardware antes que uno por soft. Se dejó a cargo de una aplicación el control de ancho de banda y la

función de Proxy, ya que al estar por detrás del Firewall, la seguridad no fue tan crítica como los costos.

Proceder a la configuración de los equipos.

Con todo lo anterior, se procedió a configurar o reconfigurar los equipos. Realizada esta configuración se logró prestar el servicio de Internet en una forma continua, aunque lenta debido al poco ancho de banda disponible para los usuarios.

Colocar un Firewall cuando se desee proteger algún dato vital, un Router cuando se necesite vincular dos o mas redes con distintas características y finalmente un Proxy cuando se trate de una conexión compartida a Internet.

Como se aprecia en el diagrama de la red, se utilizaron los tres equipos en sus respectivas funciones.

Configurar los anchos de banda permitidos para las conexiones teniendo en cuenta la cantidad de usuarios.

Para calcular el ancho de banda asignado a cada usuario utilizamos la siguiente ecuación:

ancho de banda >= cant. usuarios * 0.20 * veloc. permitida para c/u

Una velocidad razonable seria 10Kb/seg, pero en nuestro caso debimos bajarla a 6Kb/seg ya que el número de usuarios es demasiado elevado para la conexión disponible.

Contar con una estadística del tráfico de datos hacia y desde Internet para configurar correctamente el servicio de cache.

En este punto se presentó otro problema, según las estadísticas los sitios mas visitados son los de Webmail (Hotmail, Yahoo), Noticias (Clarín, Radio Mitre, Ole) y los buscadores (Google). Esto hace que, al ser sitios que cambian continuamente, el cache no pueda almacenar las páginas por mucho tiempo, por lo que no se priorizó, es decir, se dejó la configuración por defecto que es un término medio para la mayoría de las conexiones.

Probar con las herramientas adecuadas la correcta configuración de los equipos.

Por último, se probó todo lo anteriormente mencionado con un portscan local (aplicación para linux nmap o xnmap) y uno remoto http://seguridad.internautas.org/scan-puertos.php, verificándose la correcta configuración de los equipos.

Nota: Por razones de seguridad y al ser este un documento público, no consideramos oportuno nombrar marcas de equipos ni software utilizados ya que se facilitaría el camino a cualquier persona que intente vulnerar la red.

2.4.- Conclusión:

En esta actividad se han tratado de establecer algunas pautas para lograr asegurar, en alguna medida, un área privada de una red pública. El tema es muy extenso y dinámico (todos los días aparece algo nuevo), da para escribir varios libros.

Como se ha visto a lo largo de esta actividad, la forma mas eficiente de protegerse es tener bien claro lo que se quiere y se tiene. Además el personal que se dedica a este tema, deberá estar actualizado al máximo, ya que la velocidad de aparición de nuevas tecnologías, hace que los equipos que hoy están seguros, mañana no lo estén tanto.

Es por esto que siempre deberemos tener como premisa que alguien va a vulnerar nuestro sistema en algún momento, por lo tanto deberemos estar un paso adelante, para que cuando esto suceda no pase mas allá de la primer capa de seguridad.

ACTIVIDAD N°2

3.- Objetivo:

Elaborar manuales, procedimientos, políticas de seguridad y pautas generales para prevenir y asegurar los servidores del Data Center.

3.1.- Enunciado de la Actividad:

Generación de pautas generales para la definición e implantación de políticas de monitoreo del tráfico de datos internos (personal con acceso a sistemas dentro de la administración pública).

3.2.- Desarrollo:

En esta actividad lo que se busca es asegurar los datos contenidos en los servidores del Data Center de posibles alteraciones por parte del personal de la administración pública.

Se ha comprobado a nivel mundial que las redes, tanto de gran envergadura como de pequeñas, sufren mas ataques internos que externos; esto se debe principalmente a una falsa creencia de pensar que sólo se pueden recibir ataques a los datos desde fuera de nuestra red y al momento de conectarnos públicamente, descuidando de esta manera al propio personal.

En este punto podemos mencionar que en la Intranet de Gobierno, se detectaron algunos intentos de accesos no autorizados, todos desde dentro de la misma Intranet, procediéndose a tomar las medidas necesarias.

3.2.1.- Monitoreo de datos:

Para lograr el objetivo buscado en esta actividad, la medida mas apropiada es siempre la prevención. Para ello, es necesario contar con un buen esquema de monitoreo de datos, sin entrar en lo que sería una violación de la privacidad.

De este modo sólo se tendrían en cuenta las actividades extrañas o sospechosas, que pueden ser el resultado de un posible ataque a los datos, ya sea por un usuario o por un virus, o bien simples pruebas de software realizadas por personal autorizado, como es el caso de algunas de las herramientas probadas en esta etapa.

Básicamente, monitorear el tráfico de datos implica estar observando en forma continua los datos circulantes por una red, recolectando por medio de filtros los datos o sucesos que nos interesen.

3.2.2.- Herramientas de monitoreo:

Las herramientas utilizadas para esta tarea pueden ser implementadas con un equipo (hardware) como es el caso de los Analizadores de Protocolos, o bien lo que es mas común y económico utilizar una aplicación destinada a tal fin. En nuestro caso, contamos con ambos tipos de herramientas, que al complementarse nos permiten obtener un abanico de datos bastante amplio.

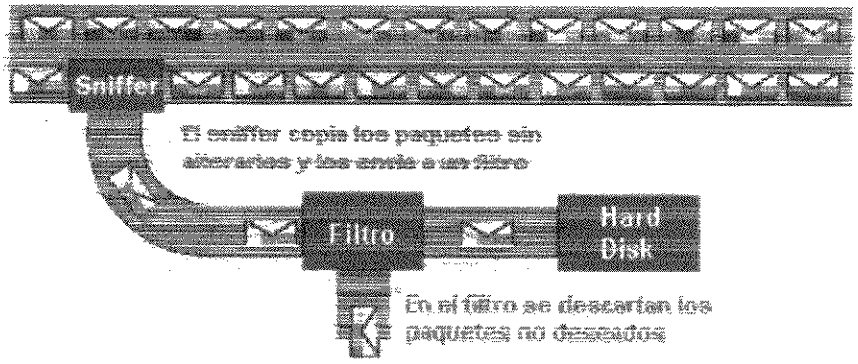
La diferencia principal entre una herramienta implementada por hardware y una por software es la velocidad de muestreo de la primera, ya que se realiza en tiempo real. En cambio, cuando se utilizan aplicaciones, se capturan paquetes que luego son analizados, la velocidad de captura de los mismos depende de la velocidad del equipo que se este usando y nunca llega a un 100% del total.

Entre estas herramientas podemos distinguir tres grandes grupos:

- Sniffer o Monitores de tráfico
- Sistemas de Detección de intrusos
- Analizadores de Logs

3.2.3.- Monitores de tráfico:

Estas herramientas, conocidas también como Sniffers, son utilizadas para analizar los paquetes de datos que circulan por una red, su funcionamiento se puede apreciar en la siguiente figura:



En el filtro se configuran las reglas que nos permitirán obtener los datos buscados "limpiando" de alguna manera toda la información capturada.

Debido a su forma de trabajar, estas aplicaciones nos permiten desde obtener estadísticas de accesos, hasta detectar problemas lógicos o de configuración de la red. En contrapartida y por este mismo motivo, también permite capturar paquetes con datos importantes como lo son usuarios y contraseñas que viajen por la red en forma abierta y sin encriptar.

En nuestro caso, estamos utilizando un Analizador de Protocolos (otro nombre para un sniffer) por hard y algunas aplicaciones como ser Commview y

Observer, ambas en sus versiones con soporte para sondas, es decir que se instalan pequeños clientes en los distintos segmentos de la red y se monitorean en forma centralizada.

Estas dos aplicaciones además de mostrarnos el estado del tráfico en la red (ancho de banda, porcentaje de utilización), nos permiten buscar paquetes que cumplan con alguna determinada condición (ips, Macaddress, protocolos, puertos), realizar estadisticas (ips o urls mas accedidas), mostrar protocolos utilizados, y algo muy importante como es permitir ver un detalle de cada paquete capturado.

Entre otras herramientas que hemos testeado (algunas especificas y poco configurables, que se utilizan para buscar recursos compartidos, obtener usernames y paswords, scanear puertos, o realizar cualquier tipos de ataque), podemos nombrar Ipsearch, Netscan, SnifferPro, SpyNet, Legión, etc.

Dichas aplicaciones se encuentran publicadas en Internet en forma libre y gratuita, por lo que son de fácil adquisición para el público en general; sólo hay que saber buscar un poco.

Hay que destacar que normalmente hablamos de software muy "liviano", es decir que es fácil de transportar ya que entran en un disquete y casi no consumen recursos, por lo que se pueden ejecutar prácticamente en cualquier máquina con el riesgo que ello trae aparejado.

Por otra parte, observamos que las aplicaciones mas versátiles y con mejores características son las desarrolladas para el sistema operativo Linux, por lo que podemos decir con seguridad que para lograr un buen monitoreo deberemos

contar con distintos sistemas, principalmente Linux y Windows 2000 o NT, por nombrar algunos.

Esto no significa de ninguna manera que sea necesario colocar un equipo para cada sistema, ya que estos se pueden instalar dentro de un mismo equipo, el cual debe cumplir con los requerimientos mínimos exigidos para cada sistema operativo.

Este grupo cuenta en la actualidad con equipos trabajando bajo Windows 98, Windows 2000 y Linux en los cuales se ejecutan estas herramientas.

3.2.3.1.- Encriptación de Datos:

Una forma de evitar el ataque con sniffers es encriptar o codificar la información que se transmite.

La encriptación usa una técnica (criptografía) que modifica un mensaje original mediante una o varias claves, de manera que resulte totalmente ilegible para cualquier persona, y solamente lo pueda leer quien posea la clave correspondiente para descifrar el mensaje. Junto con la firma digital y las marcas de aguas digitales, la encriptación es una de las posibles soluciones para proteger datos cuando son enviados a través de una red.

Para realizar esto existen diversas herramientas, pero ninguna brinda una seguridad total.

En la implementación de la Autopista de la Información, esta contemplada la encriptación de los datos críticos como ser usernames y passwords.

3.2.4.- Sistemas de Detección de Intrusos:

Este tipo de sistemas se encargan principalmente de advertir a los administradores de posibles intrusiones o ataques a la red que se quiere proteger, además pueden evitar alguno de dichos ataques.

Entre este tipo de herramientas podemos encontrar aplicaciones como Norton Personal Firewall y Zone Alarm, que básicamente son firewall personales y permiten proteger un determinado equipo.

Los antivirus como Kaspersky y Norton, también sirven para detectar la presencia de intrusos en un equipo, ya que al realizar actividades no autorizadas, se comportan como si un virus estuviera tratando de infectar el equipo.

Otras aplicaciones como Ad Aware, permiten eliminar los denominados Spywares, que son programas que envían información desde nuestro equipo a otro remoto.

Todas estas aplicaciones cumplen con la función de alertar en caso que exista un movimiento no permitido de datos y han sido probadas y son utilizadas por este grupo de trabajo.

En cuanto a los productos conocidos como "Sistemas de Detección de Intrusos" o IDS, van mas allá de los nombrados anteriormente, son especializados y generalmente constan de dos módulos: sondas o monitores y una estación centralizada de administración. Además, trabajan en forma pasiva, lo que les permite efectuar su tarea sin alertar a los intrusos de su presencia. Otro punto a favor de estas aplicaciones es que permiten agregar rutinas para detectar ataques específicos.

En nuestro caso, la empresa encargada de poner en funcionamiento el Data Center ofreció un sistema de este tipo.

3.2.5.- Analizadores de Logs:

Estas aplicaciones son muy utilizadas a la hora de reportar no solo intrusiones o intentos de realizarlas, sino también nos sirven para detectar cualquier tipo de problema en los equipos.

Trabajan analizando y entregando datos extraídos de los log o registros que generan las distintas aplicaciones o sistemas operativos.

Normalmente cualquier sistema operativo trae alguna herramienta de este tipo, pero si estas no alcanzan para cumplir con nuestras necesidades, se pueden bajar desde Internet, ya que normalmente son de libre distribución.

En particular, todos los servidores en funcionamiento dentro de la Autopista de la Información tienen los registros de eventos activos y con las alertas configuradas.

3.2.6.- Ingeniería Social:

Este es un punto importante a tener en cuenta a la hora de protegernos contra ataques internos ya que para una red de este tamaño y de carácter público, se convierte en un problema puesto que cualquier persona puede simular ser personal de la Autopista de la Información (ya que son muy pocos los usuarios que exigen una acreditación a dicho personal), y así obtener datos personales de los usuarios que permitan encontrar, directa o indirectamente, los tan

buscados "usèrname" y "password" autorizados logrando así entrar (loguearse) a la Autopista en forma válida.

Cuando se usa esta técnica para acceder a un sistema o red, la detección se dificulta puesto que los datos del usuario son válidos. Por lo tanto la única forma de detenerlo es la prevención y la concientización del personal.

3.3.- Conclusión:

De lo comentado anteriormente y lo experimentado a lo largo de esta actividad podemos decir que, atender de manera eficiente la seguridad de una red se hace cada vez más difícil, por lo que un buen monitoreo puede prevenirnos de futuros problemas.

Además, a pesar que las herramientas se mejoran día a día, los Hackers también aumentan su nivel de conocimientos técnicos y de sofisticación por lo que el personal dedicado a la seguridad también debe estar en constante aprendizaje.

Otro punto que dificultad la tarea de asegurar una red es la proliferación de sitios en Internet dedicados al tema, que ofrecen sin cargo distintas herramientas que "tientan" al usuario a probarlas.

ACTIVIDAD N°3

4.- Objetivo:

Elaborar manuales, procedimientos, políticas de seguridad y pautas generales para prevenir y asegurar los servidores del Data Center.

4.1.- Enunciado de la Actividad:

Generación de pautas generales para la definición e implantación de políticas de monitoreo del tráfico de datos externos (personas que acceden desde fuera de la ubicación física del Data Center).

4.2.- Desarrollo:

Al igual que en la actividad anterior, en esta también se busca resguardar la integridad de los datos contenidos en el Data Center.

De la misma manera en que se controlan los accesos desde dentro de la administración pública, deberemos hacerlo con los usuarios que acceden desde fuera de nuestra red.

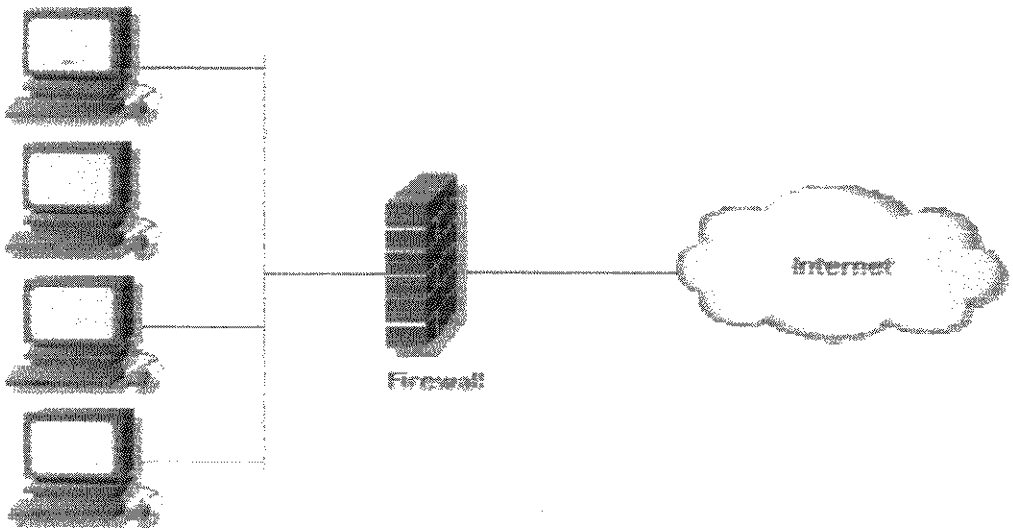
Esta distinción entre usuarios internos (insiders) y externos (outsiders) no es arbitraria ya que, como se menciono anteriormente, es mayor la posibilidad de intrusiones del propio personal, que la de personas ajenas al Gobierno de la Provincia.

Esto se debe principalmente a una premisa existente entre hackers que dice "El gobierno puede gastar dinero buscando al intruso".

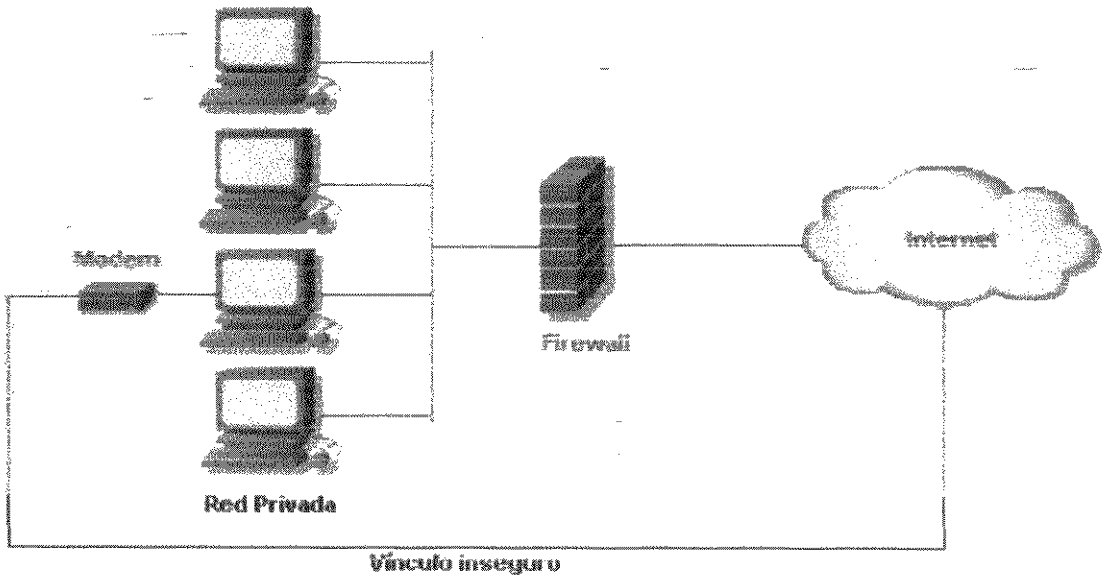
Por otra parte, y como sucede en nuestra institución, el vínculo externo está más protegido que el interno, ya que el empleado público necesita utilizar servicios que no son accesibles desde fuera de la intranet.

4.2.1.- Vínculos a redes públicas:

En cualquier red privada (en este caso la Intranet de Gobierno) conectada a una red pública (léase Internet), se persigue como objetivo poseer un solo vínculo entre ambas, para así garantizar un cierto nivel de seguridad y la privacidad de la red en cuestión.



En redes corporativas de gran tamaño, como es nuestro caso, esto se torna un poco mas complicado puesto que existen usuarios que se conectan vía modem (es decir telefónicamente), provocando problemas de seguridad en la red, principalmente en lo que se refiere a propagación de virus.



Como se observa en las figuras, en el primer caso y al tener un solo vínculo físico con la red pública, se puede controlar el tráfico circulante de manera eficaz.

En el segundo caso, este control sirve, pero sólo cuando no se utiliza el vínculo "alternativo", que puede ocasionar el colapso total de la red, debido a la posibilidad de intrusiones tanto de hackers como de virus, y afines.

Por este motivo es importante que, al generar cualquier política relacionada con tráfico de datos, se tenga en cuenta la posibilidad de existencia de este tipo de conexión, para así poder eliminarlas.

4.2.2.- Monitoreo de tráfico de datos:

Como se mencionó en la actividad anterior, el monitoreo de los datos circulantes a través de una red, nos posibilita no sólo conocer el movimiento de dicha red, sino también detectar condiciones anómalas y realizar estadísticas.

Una vez controlada la cantidad de vínculos con la red pública, (en lo posible mantener sólo uno ya que disminuye enormemente la posibilidad de

intrusiones), se procede a monitorear el tráfico a través de ellos. Cabe señalar en este punto que la Autopista de la Información cuenta con un vínculo único, mientras que en la Red de Gobierno y por razones operativas se han autorizado algunas conexiones dial-up (telefónicas) controladas y a sitios seguros.

Entonces, considerando que sólo existe un vinculo a la red pública, el monitoreo de tráfico de datos externos se realizará en este punto.

Las herramientas empleadas para esta tarea, básicamente son las mismas que para el monitoreo interno, pero con ciertas restricciones.

Cabe destacar que al contar con un sistema de firewall, este se encarga de detectar cierto tipo de trafico no permitido y comunicarlo al responsable del área, por lo tanto, las aplicaciones de monitoreo cumplen una función mas estadística que de control.

4.2.3.- Herramientas de monitoreo y estadísticas:

Para monitorear el tráfico externo, es decir, los datos que circulan desde y hacia Internet, se utilizan las mismas herramientas usadas en la actividad anterior, tales como sniffer, detectores de intrusos, analizadores de logs, etc., siempre con preferencia a las implementadas por hardware.

Como se mencionó en párrafos anteriores, para usar algunas herramientas, mas precisamente sniffers, hay que aplicar restricciones ya que no podemos correr una aplicación de este tipo sobre la red pública puesto que se vería como un intento de obtener alguna información, es decir, estaríamos usando

esta herramienta para usos no demasiados claros y seríamos considerados "hackers".

En particular, nuestro grupo ha dejado la tarea de detección de intrusos y monitoreo de intentos de ingresos ilegales, al Firewall, que ante cualquier tráfico extraño, envía un aviso de alarma al responsable del área y la tarea de detección de virus al antivirus corporativo (actividad 4).

Debemos hacer notar en este punto, que si bien las intrusiones realizadas por outsiders, son mucho menos frecuentes que las realizadas por insiders (de hecho, en el último año no se han registrado intentos de hackeo desde fuera, pero si desde dentro), hay que tenerlas presentes ya que son difíciles de rastrear y por lo tanto de sancionar, cosa que no ocurre con el personal de la Administración Pública.

Por lo dicho anteriormente, las aplicaciones que se probaron en esta actividad estaban destinadas principalmente a recabar información del tráfico de datos para realizar estadísticas, eligiendo como herramienta principal a "Webtrend Firewall Suite".

4.2.3.1.- <u>Webtrend Firewall Suite:</u>

Esta aplicación realizada por la empresa NetIQ, básicamente es una herramienta que permite obtener todo tipo de reportes, no solamente de un Firewall como indica su nombre, sino que además permite obtener datos desde routers, proxys, etc.

Esta herramienta fue seleccionada por nuestro grupo ya que entre sus funciones encontramos:

- Uso de ancho de banda y predicción por semana, día u hora: esto nos facilitó la tarea de detectar cuales son los momentos de mayor uso de Internet, para así aplicar restricciones según el horario (recordar que la conexión a Internet es el cuello de botella de nuestra Red).
- Categorización de las URLs: Nos permite conocer a grandes rasgos cuales son los usos principales que se le da a Internet. Con ello pudimos determinar que el uso principal que se le da es el Web-mail y la mensajería instantánea (Messenger, ICQ).
- Utilización de los cache: Nos proporciona información acerca del comportamiento de los caches en los proxys. En nuestro caso nos informó de un uso de un 30%, es decir que 30 pedidos de 100, se resuelven internamente y sin usar el vinculo hacia Internet; este porcentaje (bajo respecto de lo deseado, 45% a 50%) se debe principalmente al acceso a páginas demasiado dinámicas, como lo son los web-mails.
- Usuarios mas activos: Este reporte nos permite saber que usuarios están abusando del recurso, para actuar en consecuencia, ya sea restringiéndolo o cortándole el servicio.
- Cantidad de visitas a nuestro Site: Nos permite tener una estadística sobre los accesos al Portal de la Provincia (cantidad, duración, etc.).
- Alarmas: En conjunto con el Firewall nos permite llevar una estadística de las distintas alarmas generadas por este (accesos fallidos, intentos de intrusión, fallas de conexión, etc.).

- Envío de reportes por e-mail: Esta es una característica fundamental a la hora de generar reportes, puesto que se pueden enviar a todos los involucrados, aun cuando no se encuentren junto a los equipos.

De los datos observados, vemos que el tráfico desde fuera de nuestra red no es demasiado peligroso en lo que a seguridad se refiere, ya que al pasar por varias capas de seguridad se va depurando.

El problema principal lo constituyen los e-mail con virus, que como se puede ver en la actividad 4, se controlan mediante un antivirus estratégicamente instalado y correctamente configurado, pero que lamentablemente todavía no se ha implementado en forma masiva por una razón de licenciamiento.

Además se realizan filtrados de paquetes en firewall, router y switches, lo que nos da una mayor seguridad.

4.2.4.- Herramientas On-line:

Navegando por Internet, se han encontrado sitios "serios" y gratuitos que ofrecen servicios de estadísticas de los vínculos hacia Internet. Además algunos de ellos proporcionan soporte técnico a través de foros para mejorar o solucionar los problemas con las conexiones.

Entre estos sitios podemos citar:

- www.bandwidthplace.com : que nos proporciona una medición de la velocidad de nuestra conexión.
- http://seguridad.internautas.org: que nos ofrece distintos servicios para probar la seguridad de nuestra red.
- www.cotse.com: ofrece soporte técnico y herramientas gratuitas.

- www.arcert.gov.ar: Sitio argentino de Coordinación de Emergencias en Redes Teleinformáticas, nos proporciona información sobre vulnerabilidades, soporte técnico y herramientas.

4.2.5.- Encriptación de datos:

En este punto se toman las mismas consideraciones que las referidas al tráfico interno, es decir que a la hora de enviar información importante a través de Internet, como es una red totalmente pública, es conveniente aplicar alguna técnica de encriptación y, si es necesario asegurar aun mas el vínculo, se deberá utilizar una red privada virtual (VPN).

4.3 Conclusión:

Como se pudo observar en esta actividad, un buen monitoreo de los datos circulantes hacia y desde Internet, nos puede ahorrar el tener que lidiar con problemas serios que afecten la seguridad e integridad de nuestros datos.

Por otra parte, tener los datos estadísticos del tráfico existente en todo momento nos posibilita ir realizando un "ajuste fino" de las configuraciones de los diferentes equipos.

Por último, siempre debemos tener en cuenta que estamos trabajando con una red pública, a la cual tienen acceso millones de usuarios, por lo que asegurar nuestros datos se torna de máxima importancia.

ACTIVIDAD N°4

5.- Objetivo:

Elaborar los procedimientos, políticas de seguridad y pautas generales para prevenir la difusión y los ataques de virus al Data Center.

5.1.- Enunciado de la Actividad:

Elaboración de requisitos mínimos para la instalación, control y mantenimiento de antivirus corporativos, servidores de antivirus, filtrado de paquetes en Firewalls y Routers. Monitoreo de tráfico.

5.2.- Desarrollo:

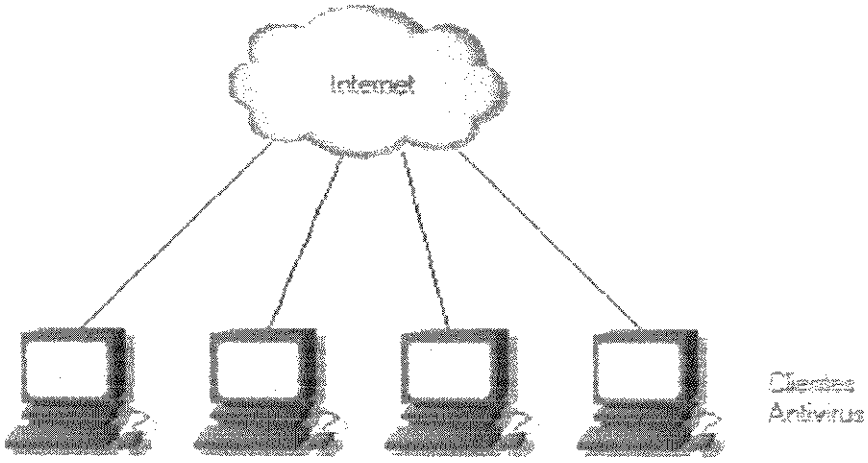
Esta es una de las actividades más importantes del proyecto, dada la rápida proliferación de virus informáticos, que afectan no sólo a los datos, sino a los sistemas operativos .

Esta difusión masiva de virus, principalmente vía Correo Electrónico (e-mail), puede hacer colapsar una red en pocos segundos, por esto se hace necesario contar con un sistema eficaz que detenga los virus, o paquetes sospechosos de contenerlos, además de prevenir la entrada por otros medios que no sean la red, por ejemplo disquetes.

A raíz de esta necesidad surgen dos grandes clases de software antivirus, los personales y los corporativos.

5.2.1.- Antivirus Personales:

Un antivirus personal es aquel que se instala en un equipo y es administrado en forma local, es decir, el usuario debe encargarse de actualizar periódicamente las bases de datos que contienen las definiciones de los virus existentes, y realizar los scaneos correspondientes.



Entre los productos existentes en el mercado podemos destacar Norton Antivirus, Kaspersky Personal Antivirus, Panda Antivirus, McAfee VirusScan, PC-Cillin todos funcionando sobre Windows y F-Prot para plataforma DOS.

Luego de realizar distintas pruebas con estos productos, observamos que, a nivel personal, Kaspersky Antivirus si bien no es uno de los mas utilizados en el ámbito informático de la Provincia, es el que mejor porcentaje de virus detectó, además, al generar discos de rescate en GNU/Linux, permite realizar tareas de limpieza en forma mucho mas eficiente que otros antivirus.

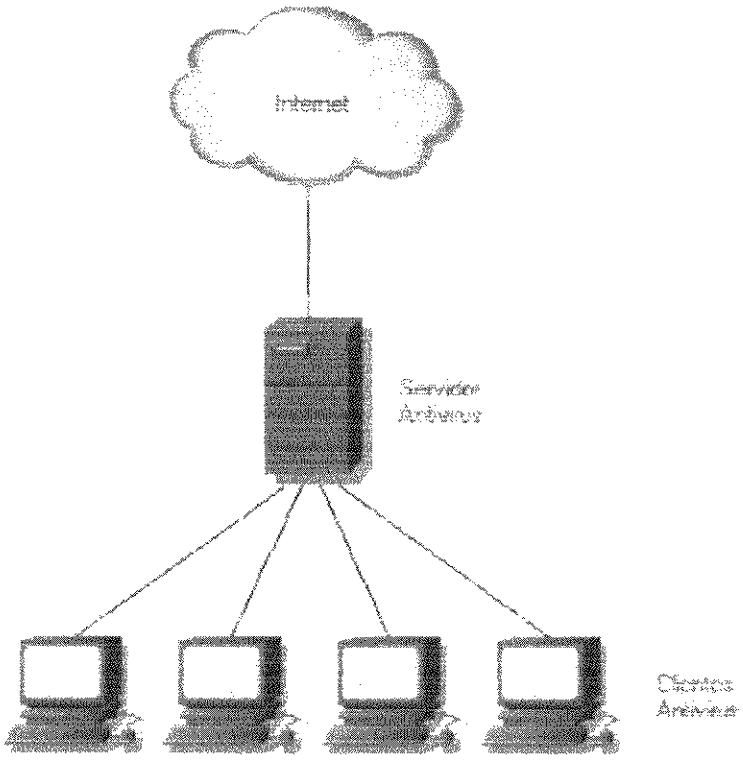
Lo anteriormente dicho hace que a la hora de recomendar un producto personal, este grupo se incline hacia la herramienta rusa Kaspersky Personal Antivirus.

Ahora bien, en el caso de la Autopista de la Información, y debido a que deseamos proteger datos críticos y la cantidad de usuarios es elevada, preferimos realizar una administración centralizada de los antivirus.

5.2.2.- Antivirus Corporativos:

A diferencia de los antivirus personales, los productos corporativos son administrados desde un único punto, es decir que se realiza una administración centralizada del producto, lo que hace que sea transparente al usuario.

Este tipo de administración permite tener un control sobre las actualizaciones de los clientes, y en caso de sospechar de algún equipo, ejecutar scaneos remotos, mantener archivos en cuarentena en un solo sitio y no distribuidos, etc.



En el mercado existen varias soluciones corporativas entre las que destacamos Norton Corporativo y Kaspersky.

La solución de sistema antivirus escogida para la Autopista de la información es "Norton Antivirus Edición Corporativa". Este software se eligió por ser uno de los más eficaces del mercado a nivel corporativo, y por el soporte técnico existente en la República Argentina.

Al momento de redactar este informe, ya se ha instalado y puesto en funcionamiento un Servidor de Antivirus dedicado a toda la Secretaria de Tecnologías de la Información, no extendiéndose mas por una cuestión de licenciamiento.

Además, la empresa contratada para llevar a cabo el proyecto de la Autopista de la Información, también ha instalado y puesto en funcionamiento un sistema similar en el Data Center.

5.2.3.- Filtrado de paquetes:

Esta técnica funciona en base a un monitoreo del tráfico de datos circulante, estableciendo una serie de reglas para decidir si un paquete de datos pasa o no a través del "filtro".

En cuanto al monitoreo de tráfico, podemos decir que viene de la mano de las actividades 2 y 3, pero como aquí es algo bien específico, las herramientas utilizadas son mas simples.

Es por esto que la mayoría de Firewall y Routers poseen alguna forma de monitorear los paquetes de datos que por ellos circulan y así poder filtrarlos en caso de estar con virus.

Estos filtros si bien son muy efectivos, si no se configuran en forma apropiada, pueden llegar a molestar mas de lo que ayudan, así por ejemplo, se pueden llegar a eliminar todos los archivos adjuntos a un e-mail sin que estos necesariamente traigan virus (esto es un caso real de una empresa que no viene al caso nombrar).

Otra desventaja que tiene el filtrado de paquetes es que si bien es rápido, ya que lo realiza un hardware y no un software, si esta mal configurado puede ocasionar una demora en el tráfico de datos a través de dichos equipos.

5.2.4.- Selección del antivirus:

Seleccionar un Sistema de Antivirus, no es una tarea sencilla, ya que los productos, en general, se comportan de forma similar.

Al elegir un Sistema de Antivirus, primero debemos decidir si es corporativo o personal, para ello necesitamos saber la cantidad de usuarios a los que se desea proteger.

De esta forma, si solo se protegen 1 o 2, no se justifica el gasto de un antivirus corporativo, en cambio si el caso es como en la Autopista de la Información (mas de 3000), se justifica plenamente invertir en un antivirus corporativo ya que ante tal cantidad de usuarios se torna imposible la tarea de administrar a cada uno por separado.

Una vez que se optó por uno personal o uno corporativo, debemos ver cuales son las plataformas a proteger, así en nuestro caso nos encontramos con Microsoft Windows en todas sus versiones.

Otro punto a tener muy en cuenta al elegir un producto de este tipo, es el soporte técnico y la facilidad de actualización.

Como se puede apreciar en este ítem de la actividad, se hace referencia a soluciones implementadas por software y no por hardware. Esto se debe a que muchas veces se opta por un buen sistema de antivirus por software antes que un filtrado de paquetes por hardware puesto que este último presenta complicaciones a la hora de actualizarse y generalmente el soporte queda a cargo del personal encargado de su mantenimiento.

5.2.5.- Actualización y Mantenimiento:

Uno de los motivos que lleva a seleccionar un antivirus corporativo es la falta de concientización de los usuarios, que no actualizan y mantienen periódicamente sus herramientas antivirus.

Al instalar un servidor de antivirus, los clientes quedan conectados a él y se actualizan cuando este distribuye las nuevas definiciones de virus.

Nosotros hemos programado el LiveUpdate (herramienta de actualización) de Norton Antivirus Corporativo para que actualice en forma diaria y envíe los datos en forma inmediata.

Pese a esto, hemos comprobado que las empresas fabricantes de las herramientas antivirus actualizan sus datos aproximadamente una vez por semana, salvo que se desate una "epidemia" como sucedió con el virus Tanatos o Bugbear.

Un punto importante a tener en cuenta con estos productos es el mantenimiento, cuando se actualizan algunos componentes del Sistema

Operativo ó del propio Antivirus, debemos cercioramos que sigan en correcto funcionamiento, ya que pueden presentarse incompatibilidades entre los distintos componentes.

5.2.6.- Requisitos para la Instalación:

Los requisitos mínimos para instalar, administrar y mantener este tipo de software, son definidos por el propio fabricante del producto, pero existen algunas pautas a tener en cuenta, tales como la cantidad de clientes conectados en forma simultanea, la periodicidad de las actualizaciones en base a la circulación de nuevos virus, etc.

5.3.- Conclusión:

Por último y para finalizar esta actividad, debemos decir que: " PARA QUE UN SISTEMA DE ANTIVIRUS FUNCIONE, HAY QUE UTILIZARLO Y ACTUALIZARLO PERIODICAMENTE ", por lo que siempre se debe tratar de concientizar al usuario para que cumpla con esta premisa.

Este es el motivo principal por el cual se opta por un sistema centralizado, ya que es mas fácil de actualizar y mantener un solo servidor que miles de clientes.

Además, al poseer una administración centralizada, el funcionamiento de los clientes es transparente al usuario, lo que evita en gran medida la proliferación de virus informáticos reduciendo así la posibilidad de pérdida de datos.

Ing. Adolfo Alejandro Siinik

Anexos

6.- Anexo 1:

Números de puertos para los servicios más conocidos tal y como están definidos por la RFC 1700 (Assigned Numbers).

Servicio	Puerto / Protocolo	Alias	Comentario
echo	7/tcp		
echo	7/udp		
discard	9/tcp	sink null	
discard	9/udp	sink null	
systat	11/tcp	users	Usuarios activos
systat	11/tcp	users	Usuarios activos
daytime	13/tcp		
daytime	13/udp		
qotd	17/tcp	quote	Cuota del día
qotd	17/udp	quote	Cuota del día
chargen	19/tcp	ttytst source	Generador del carácter
chargen	19/udp	ttytst source	Generador del carácter
ftp-data	20/tcp		FTP, datos
ftp	21/tcp		FTP, control
telnet	23/tcp		
smtp	25/tcp	mail	Protocolo simple de transferencia de correo (SMTP)
time	37/tcp	timserver	
time	37/udp	timserver	
rlp	39/udp	resource	Protocolo de ubicación del recurso
nameserver	42/tcp	name	Servidor del nombre host
nameserver	42/udp	name	Servidor del nombre host
nicname	43/tcp	whois	
domain	53/tcp		Servidor de nombre-dominio
domain	53/udp		Servidor de nombre-dominio
bootps	67/udp	dhcps	Servidor del protocolo de inicio del sistema
bootpc	68/udp	dhcpc	Servidor del protocolo de inicio del sistema
tftp	69/udp		Transferencia de archivos trivial
gopher	70/tcp		
finger	79/tcp		
http	80/tcp	www http	World Wide Web
kerberos-sec	88/tcp	krb5	Kerberos
kerberos-sec	88/udp	krb5	Kerberos

Servicio	Puerto / Protocolo	Alias	Comentario
hostname	101/tcp	hostnames	Servidor del nombre host NIC
iso-tsap	102/tcp		ISO-TSAP Clase 0
rtelnet	107/tcp		Servicio Telnet remoto
pop2	109/tcp	postoffice	Protocolo de oficina de correos: versión 2
pop3	110/tcp		Protocolo de oficina de correos: versión 3
sunrpc	111/tcp	rpcbind portmap	Llamada de procedimiento remoto SUN
sunrpc	111/udp	rpcbind portmap	Llamada de procedimiento remoto SUN
auth	113/tcp	ident tap	Protocolo de identificación
uucp-path	117/tcp		
nntp	119/tcp	usenet	Protocolo de transferencia de noticias a través de la red
ntp	123/udp		Protocolo de tiempo de red
epmap	135/tcp	loc-srv	Resolución del extremo DCE
epmap	135/udp	loc-srv	Resolución del extremo DCE
netbios-ns	137/tcp	nbname	Servicio de nombre NETBIOS
netbios-ns	137/udp	nbname	Servicio de nombre NETBIOS
netbios-dgm	138/udp	nbdatagram	Servicio de datagramas NETBIOS
netbios-ssn	139/tcp	nbsession	Servicio de sesión NETBIOS
imap	143/tcp	imap4	Protocolo de acceso de mensajes de Internet
pcmail-srv	158/tcp		Servidor PCMail
snmp	161/udp		SNMP
snmptrap	162/udp	snmp-trap	Captura SNMP
print-srv	170/tcp		Red PostScript
bgp	179/tcp		Protocolo de puerta de enlace de borde
irc	194/tcp		Protocolo IRC (Internet Relay Chat)
ipx	213/udp		IPX para IP
ldap	389/tcp		Protocolo de acceso al directorio de peso ligero
https	443/tcp		MCom
https	443/udp		MCom
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
#? kpasswd	464/tcp		Kerberos (v5)
#? kpasswd	464/udp		Kerberos (v5)
isakmp	500/udp	ike	Intercambio de claves de Internet
exec	512/tcp		Ejecución del proceso remoto
biff	512/udp	comsat	

Servicio	Puerto / Protocolo	Alias	Comentario
login	513/tcp		Inicio de sesión remoto
who	513/udp	whod	
cmd	514/tcp	shell	
syslog	514/udp		
printer	515/tcp	spooler	
talk	517/udp		
ntalk	518/udp		
efs	520/tcp		Servidor de nombres de archivos extendido
router	520/udp	route routed	
timed	525/udp	timeserver	
tempo	526/tcp	newdate	
courier	530/tcp	rpc	
conference	531/tcp	chat	
netnews	532/tcp	readnews	
netwall	533/udp		Para emisiones de emergencia
uucp	540/tcp	uucpd	
klogin	543/tcp		Kerberos
kshell	544/tcp	krcmd	Kerberos shell remoto
new-rwho	550/udp	new-who	
remotefs	556/tcp	rfs rfs_server	
rmonitor	560/udp	rmonitord	
monitor	561/udp		
ldaps	636/tcp	sldap	LDAP para TLS/SSL
doom	666/tcp		Software del Id. Doom
doom	666/udp		Software del Id. Doom
kerberos-adm	749/tcp		Administración Kerberos
kerberos-adm	749/udp		Administración Kerberos
kpop	1109/tcp		Kerberos POP
phone	1167/udp		Llamada de conferencia
ms-sql-s	1433/tcp		Microsoft-SQL-Server
ms-sql-s	1433/udp		Microsoft-SQL-Server
ms-sql-m	1434/tcp		Microsoft-SQL-Monitor
ms-sql-m	1434/udp		Microsoft-SQL-Monitor
wins	1512/tcp		Servicios de nombres Internet de Microsoft Windows (WINS)
wins	1512/udp		Servicios de nombres Internet de Microsoft Windows (WINS)
ingreslock	1524/tcp	ingres	
l2tp	1701/udp		Protocolo de túnel capa 2
pptp	1723/tcp		Protocolo de túnel punto a punto
radius	1812/udp		Protocolo de autenticación RADIUS
radacct	1813/udp		Protocolo de gestión de cuentas RADIUS
nfsd	2049/udp	nfs	Servidor NFS

Servicio	Puerto / Protocolo	Alias	Comentario
knetd	2053/tcp		Desmultiplexor Kerberos
ttcp	5001/tcp		TTCP
ttcp	5001/udp		TTCP
man	9535/tcp		Servidor remoto MAN

7.- Anexo 2:

Listado de puertos usados por algunos troyanos

Pueto	Protocolos	Nombre del Troyano
0	ICMP	Click attack
8	ICMP	Ping Attack
9	UDP	Chargen
19	UDP	Chargen
21	TCP	Dolly Trojan
23	TCP	TELNET Service
25	TCP	SMTP AntiGen
31	TCP	Agent 31 Hacker's Paradise
41	TCP	Deep Throat
53	TCP	DNS
58	TCP	DM Setup
79	TCP	Firehotcker
80	TCP	Executor
90	TCP	Hidden Port 2.o
110	TCP	ProMail Trojan
113	TCP	Kazimas
119	TCP	Happy99
121	TCP	Jammer Killah
129	TCP	Password Generator Protocol
135	TCP UDP	Netbios Remote procedure call
137	TCP UDP	Netbios name (DoS attacks)
138	TCP UDP	Netbios datagram
139	TCP UDP	Netbios session (DoS attacks)
146	TCP	Infector 1.3
421	TCP	Tcp Wrappers
456	TCP	Hacker's Paradise
531	TCP	Rasmin
555	TCP	Stealth Spy Phaze
666	TCP	Attack FTP
777	TCP	AIM Spy Application
911	TCP	Dark Shadow
999	TCP	DeepThroat
9400	TCP	InCommand
9999	TCP	The prayer 1.2 -1.3
1000	TCP	Der Spaeher

Pueto	Protocolos	Nombre del Troyano
1001	TCP	Silencer WebEx
1011	TCP	Doly Trojan
1012	TCP	Doly Trojan
1015	TCP	Doly Trojan
1024	TCP	NetSpy
1025	UDP	Maverick's Matrix 1.2 - 2.0
1027	TCP	ICQ
1029	TCP	ICQ
1032	TCP	ICQ
1033	TCP	NetSpy
1042	TCP	Bla
1045	TCP	Rasmin
1080	TCP	Socks/Wingate
1090	TCP	Xtreme
1170	TCP	Voice Streaming Audio
1207	TCP	SoftWar
1234	TCP	Ultors Trojan
1243	TCP	Sub Seven
1245	TCP	VooDoo Doll
1269	TCP	Maverick's Matrix
12631	TCP	WhackJob
1349	UDP	BackOrifice DLL Comm
1394	TCP	GoFriller Backdoor G-1
1492	TCP	FTP99CMP
1505	TCP UDP	FunkProxy
1509	TCP	Psyber Streaming server
1600	TCP	Shivka-Burka
1604	TCP UDP	ICA Browser
1807	TCP	SpySender
1981	TCP	Shockrave
1999	TCP	BackDoor
2000	TCP	Remote Explorer
2001	TCP	Trojan Cow
2002	TCP	TransScout
2003	TCP	TransScout
2004	TCP	TransScout
2005	TCP	TransScout
2023	TCP	Ripper
2115	TCP	Bugs
2140	TCP	Deep Throat
2140	UDP	Deep Throat
2155	TCP	Illusion Mailer
2283	TCP	HLV Rat5
2565	TCP	Striker
2583	TCP	WinCrash
2716	TCP	The Prayer 1.2 -1.3

Pueto	Protocolos	Nombre del Troyano
2721	TCP	Phase Zero
2801	TCP	Phineas Phucker
2989	UDP	Rat
3024	TCP	WinCrash
3028	TCP	Ring Zero
3129	TCP	Master's Paradise
3150	TCP	Deep Throat
3150	UDP	Deep Throat
3332	TCP	Q0 BackDoor
3459	TCP	Eclipse 2000
3700	TCP	Portal of Doom
3791	TCP	Eclypse
3801	UDP	Eclypse
4100	TCP	Watchguard Firebox admin DoS Expl
4092	TCP	WinCrash
4567	TCP	File Nail
4590	TCP	ICQ Trojan
5000	TCP	Sokets de Trois v1.
5001	TCP	Sokets de Trois v1.
5011	TCP	OotIt
5031	TCP	Net Metropolitan 1.0
5032	TCP	Net Metropolitan 1.04
5321	TCP	Firehotcker
5400	TCP	Blade Runner
5401	TCP	Blade Runner
5402	TCP	Blade Runner
5521	TCP	Illusion Mailer
5550	TCP	Xtcp
5512	TCP	Xtcp
5555	TCP	ServeMe
5556	TCP	BO Facil
5557	TCP	BO Facil
5569	TCP	Robo-Hack
5637	TCP	PC Crasher
5638	TCP	PC Crasher
5714	TCP	WinCrash
5741	TCP	WinCrash
5742	TCP	WinCrash
6000	TCP	The Thing 1.6
6346	TCP	Gnutella clone (not a trojan) see info
6400	TCP	The Thing
6667	TCP	Sub-7 Trojan (new icq notification)
6669	TCP	Vampyre
6670	TCP	Deep Throat
6671	TCP	Deep Throat
6711	TCP	Sub Seven

Pueto	Protocolos	Nombre del Troyano
6712	TCP	Sub Seven
6713	TCP	Sub Seven
6723	TCP	Mstream attack-handler
6771	TCP	Deep Throat
6776	TCP	Sub Seven
6838	UDP	Mstream Agent-handler
6912	TCP	Sh*t Heap
6939	TCP	Indoctrination
6969	TCP	Gate Crasher Priority
6970	TCP	Gate Crasher
7000	TCP	Remote Grab
7028	TCP	Unknown Trojan
7028	UDP	Unknown Trojan
7300	TCP	Net Monitor
7301	TCP	Net Monitor
7306	TCP	Net Monitor
7307	TCP	Net Monitor
7308	TCP	Net Monitor
7597	TCP	QaZ (Remote Access Trojan)
7789	TCP	ICKiller
7983	UDP	MStream handler-agent
8080	TCP	Ring Zero
8787	TCP UDP	BackOrifice 2000
8879	TCP UDP	BackOrifice 2000
9325	UDP	MStream Agent-handler
9872	TCP	Portal of Doom
9873	TCP	Portal of Doom
9874	TCP	Portal of Doom
9875	TCP	Portal of Doom
9876	TCP	Cyber Attacker
9878	TCP	Trans Scout
9989	TCP	iNi-Killer
10008	TCP	Cheese worm
10067	TCP	Portal of Doom
10067	UDP	Portal of Doom
10167	TCP	Portal of Doom
10167	UDP	Portal of Doom
10498	UDP	Mstream handler-agent
10520	TCP	Acid Shivers
10607	TCP	Coma
10666	TCP	Ambush
11000	TCP	Senna Spy
11050	TCP	Host Control
11223	TCP	Progenic Trojan
11831	TCP	Latinus Server
12076	TCP	Gjamer

Pueto	Protocolos	Nombre del Troyano
12223	TCP	Hack'99 KeyLogger
12345	TCP	Netbus Ultor's Trojan
12346	TCP	Netbus
12456	TCP	NetBus
12361	TCP	Whack-a-Mole
12362	TCP	Whack-a-Mole
12631	TCP	Whack Job
12701	TCP	Eclypse 2000
12754	TCP	Mstream attack-handler
13000	TCP	Senna Spy
13700	TCP	Kuang2 the Virus
15104	TCP	Mstream attack-handler
16484	TCP	Mosucker
16959	TCP	SubSeven DEFCON8 2.1 Backdoor
16969	TCP	Priority
17300	TCP	Kuang2 The Virus
18753	UDP	Shaft handler to Agent
20000	TCP	Millennium
20001	TCP	Millennium
20034	TCP	NetBus 2 Pro
20203	TCP	Logged!
20331	TCP	Bla Trojan
20432	TCP	Shaft Client to handlers
20433	TCP	Shaft Agent to handlers
21554	TCP UDP	GirlFriend
22222	TCP	Prosiak
23456	TCP	EvilFTP UglyFTP
23476	TCP	Donald Dick
23477	TCP	Donald Dick
26274	TCP	Delta Source
26274	UDP	Delta Source
27374	UDP	Sub-7 2.1
27444	UDP	Trin00/TFN2K
27573	UDP	Sub-7 2.1
27573	TCP	Sub-7 2.1
27665	TCP	Trin00 DoS Attack
29559	TCP	Latinus Server
29891	TCP	The Unexplained
30029	TCP	AOL Trojan
30100	TCP	NetSphere
30101	TCP	NetSphere
30102	TCP	NetSphere
30133	TCP	NetSphere Final
30303	TCP	Sockets de Troie
30999	TCP	Kuang2
31335	UDP	Trin00 DoS Attack

Pueto	Protocolos	Nombre del Troyano
31336	TCP	BO-Whack
31337	UDP	Backorifice (BO)
31337	TCP	Netpatch
31338	TCP	NetSpy DK
31338	UDP	Deep BO
31339	TCP	NetSpy DK
31666	TCP	BOWhack
31785	TCP	Hack'a'Tack
31787	UDP	Hack`a'Tack
31789	UDP	Hack'a'Tack
31790	UDP	Hack`a'Tack
31791	UDP	Hack'a'Tack
32418	TCP	Acid Battery
33270	TCP	Trinity Trojan
33333	TCP	Prosiak
33390	UDP	Unknown trojan
33911	TCP	Spirit 2001
34324	TCP	BigGluck TN
37651	TCP	Yet Another Trojan
40421	TCP	Master's Paradise
40412	TCP	The Spy
40421	TCP	Agent Master's of Paradise
40422	TCP	Master's Paradise
40423	TCP	Master's Paradise
40425	TCP	Master's Paradise
40426	TCP	Master's Paradise
43210	TCP	Master's Paradise
47252	TCP	Delta Source
47262	UDP	Delta Source
49301	UDP	OnLine keyLogger
50505	TCP	Sokets de Trois v2.
50776	TCP	Fore
53001	TCP	Remote Windows Shutdown
54320	TCP	Back Orifice 2000
54320	UDP	Back Orifice
54321	TCP	School Bus/Back Orifice
54321	UDP	Back Orifice 2000
57341	UDP	NetRaider Trojan
57341	TCP	NetRaider Trojan
60000	TCP	Deep Throat
61466	TCP	Telecommando
61348	TCP	Bunker-Hill Trojan
61603	TCP	Bunker-Hill Trojan
63485	TCP	Bunker-Hill Trojan
65000	TCP	Stacheldraht Devil

8.- Anexo 3:

Pautas a tener en cuenta para configurar Firewalls, Routers y Proxys:

- Contar con un diagrama esquemático de las redes a proteger y sus características.
- Calcular de la manera mas exacta posible la cantidad de usuarios, para poder dimensionar el hardware.
- Definir previamente, de forma clara, los servicios que se quieren prestar y a que usuarios.
- Hecho esto, examinar y definir que puertos y protocolos se van a utilizar, es decir, definir las reglas de cada equipo.
- Cerrar o deshabilitar todos los puertos no usados (se pueden verificar usando un scanner de puertos).
- Activar las alarmas que se consideren necesarias y si el equipo lo permite, la notificación vía e-mail a los responsables del área.
- Elegir hardware y/o software en base a la seguridad, confiabilidad, velocidad y costos.
- Con todo lo anterior, proceder a la configuración de los equipos.
- Colocar un Firewall cuando se desee proteger algún dato vital, un Router cuando se necesite vincular dos o mas redes con distintas características y finalmente un Proxy cuando se trate de una conexión compartida a Internet.
- Configurar los anchos de banda permitidos para las conexiones teniendo en cuenta la cantidad de usuarios.
- Contar con una estadística del tráfico de datos hacia y desde Internet para configurar correctamente el servicio de cache.

- En el caso de los Proxys, una buena cantidad de cache puede resultar beneficiosa, pero en contrapartida se necesitará mas hardware.
- Probar con las herramientas adecuadas la correcta configuración de los equipos.
- En cuanto a la instalación física del hardware, seguir las pautas establecidas por el fabricante del equipo.

9.- Anexo 4:

Tipos de ataque a una red:

PACKET SNIFFING: Muchas redes son vulnerables al packet sniffing, o la pasiva intercepción (sin modificación) del tráfico de red. Esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red. Puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso. Es un método muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan sin encriptar, números de tarjetas de crédito y direcciones de e-mail entrantes y salientes.

SNOOPING Y DOWNLOADING: Tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información

a su propia computadora. El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

DATA DIDDLING: Es la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor. La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus.

SPOOFING: Esta técnica es utilizada para actuar en nombre de otros usuarios, generalmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego usa este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. El envio de falsos e-mails es otra forma de spoofing permitida

por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos.

JAMMING o FLOODING: Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

CABALLOS DE TROYA: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

BOMBAS LOGICAS: Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificará la información o provocará el cuelgue del sistema.

INGENIERA SOCIAL: Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Cómputos los administradores son amigos o conocidos.

10.- Anexo 5:

Pautas para generar políticas de monitoreo de datos (internos):

- Conocer datos sobre usuarios y accesos.

- Establecer que datos se desean muestrear.
- Seleccionar herramientas que no influyan en el tráfico normal y sean de difícil detección.
- Configurar un cronograma de monitoreos (preferentemente constante).
- Clasificar, analizar y controlar los datos entregados por los monitores.
- Activar las alarmas necesarias en caso de detectar un intruso.
- En caso de alarma notificar a los responsables del área.
- Documentar los registros entregados por los sistemas de detección.

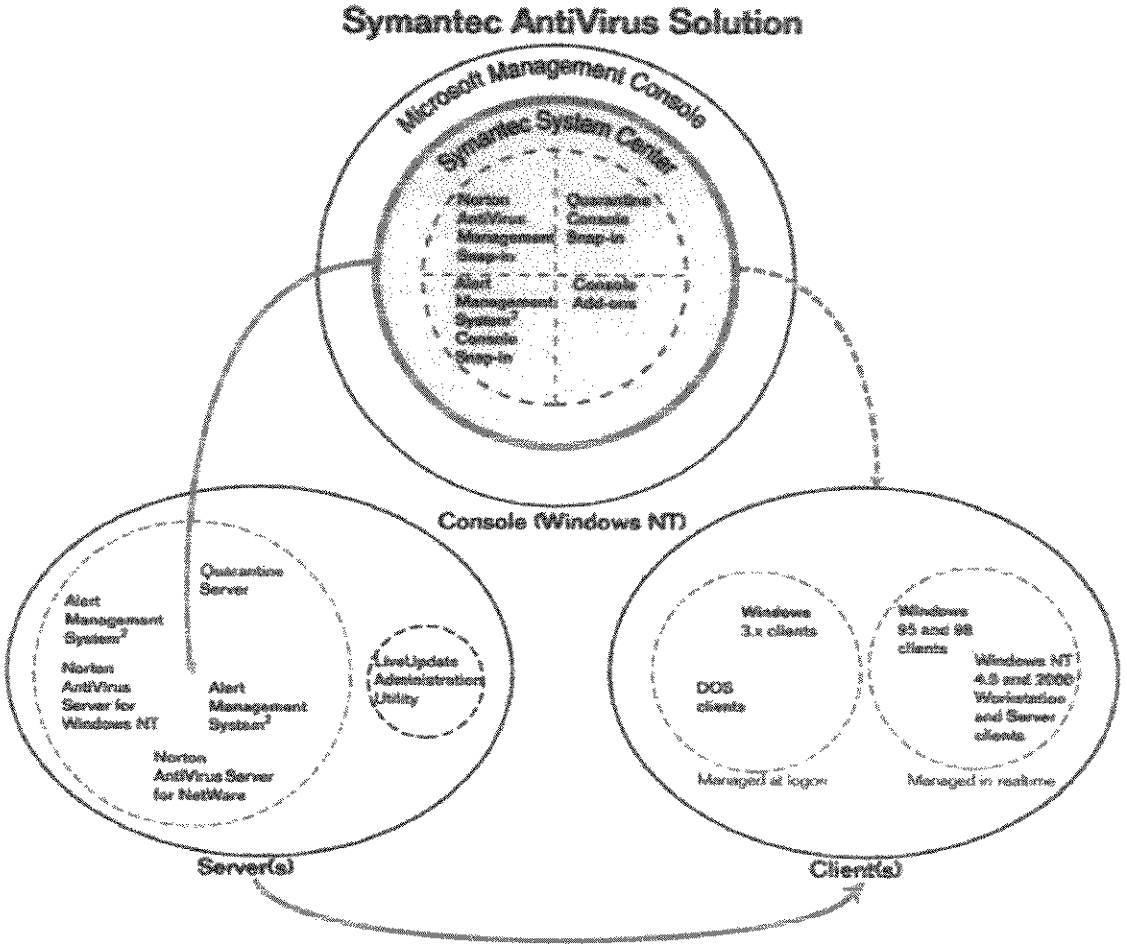
11.- Anexo 6:

Pautas para generar políticas de monitoreo de datos (externos):

- Conocer datos sobre usuarios, accesos y anchos de banda requeridos.
- Establecer que datos se desean muestrear.
- Seleccionar herramientas que no influyan en el tráfico normal y cumplan con el punto anterior.
- Configurar un cronograma de monitoreos (en tiempo real y permanente para seguridad y a intervalos regulares para estadísticas).
- Clasificar, analizar y controlar los datos entregados por los monitores.
- Activar las alarmas necesarias en caso de detectar un intruso.
- En caso de alarma notificar a los responsables del área.
- Documentar los registros entregados por los sistemas de detección.
- Ajustar la configuración de los equipos.

12.- Anexo 7:

Funcionamiento de Norton Antivirus Corporativo



13.- Anexo 8:

Instalación de Norton Antivirus Corporativo:

1) Instale Microsoft Management Console, Symantec System Center y Alert Management System para centralizar la administración y las alertas de los productos Symantec.

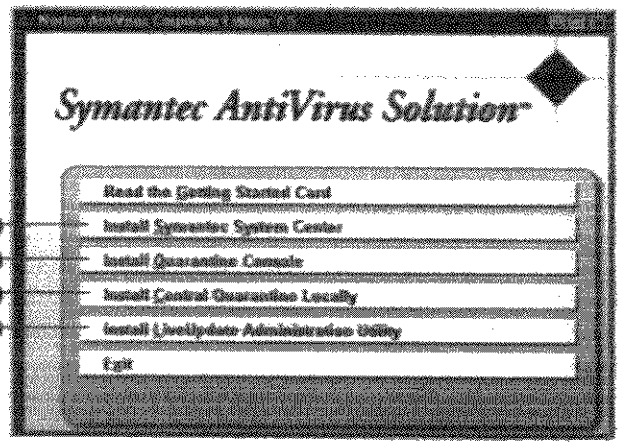
2) Instale Norton Antivirus snap-in para administrar NAVCE en servidores y clientes en todos los equipos con Symantec System Center.

3) (Opcional) Instale las herramientas de Symantec System Center.

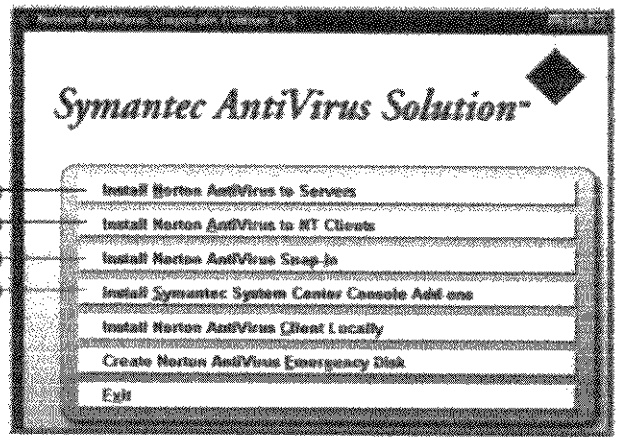
4) (Opcional) Instale Central LiveUpdate, un segundo método alternativo de distribución de archivos de definición de virus.

5) Instale Quarantine Consola usado para administrar cuarentenas desde Symantec Center Console.

Disk 1



Disk 2



6) Instale Quarantine Server para aislar archivos infectados en un lugar centralizado.

7) Instale NAVCE Server en el servidor especificado.

8) Instale remotamente NAVCE Client en los clientes NT/2000

14.- Anexo 9:

Tipos de virus:

Virus de Booteo: Se instalan en el Sector Maestro de Booteo (MBR) lo que permite que se ejecuten antes que el sistema operativo se cargue. No necesita de un archivo para ejecutarse y se mantiene en memoria desde el encendido hasta el apagado del equipo.

Virus de Archivos: denominados así por que son capaces de copiarse dentro del cuerpo de ciertos tipos de archivos (ejecutables) y activarse cuando estos lo hacen.

Macro virus: Hacen uso de la posibilidad de incluir código ejecutable en los distintos documentos generados por las aplicaciones de Microsoft, como Word, Excel, Power Point, Access, etc.

Gusanos o Worms: Se les da esta denominación porque su funcionamiento se basa en aprovechar vulnerabilidades en los distintos servicios de los equipos para poder propagarse; un ejemplo son los que utilizan el correo electrónico.

Troyanos: Son programas maliciosos que no se comportan como virus, ya que no infectan otros archivos. Ingresan a los sistemas en forma encubierta haciendo pensar al usuario que son inofensivos para que este los ejecute.

Backdoors: Son un derivado de los troyanos; reciben esta denominación ya que abren una "puerta trasera" instalando un servicio que permita el acceso remoto al equipo en cuestión.

15.- Anexo 10:

Pautas a tener en cuenta para la instalación, mantenimiento y actualización de un Sistema Antivirus:

- Conocer el número de usuarios a proteger (es indispensable por las licencias del producto).
- En base a este número, seleccionar el tipo de aplicación, Personal o Corporativa.
- Si se opta por la Corporativa, instalar el Servidor de Antivirus tal como lo indique el fabricante.
- Instalar los clientes, ya sean personales o corporativos.
- Configurar las acciones a tomar en caso de detectar virus (desinfectar, mandar a cuarentena o borrar). Siempre impedir el acceso al archivo infectado.
- Configurar la periodicidad de las actualizaciones, no menos de una vez por semana.
- Configurar que se va a actualizar (productos, definiciones, etc).
- Controlar periódicamente el correcto funcionamiento del Sistema Antivirus.
- Chequear en el fabricante por nuevos agregados o parches del producto, así como también la información sobre nuevos virus.

GLOSARIO

Ancho de banda: Medida que indica la máxima velocidad disponible para un determinado vinculo, se expresa en Kbits/s.

Antivirus: Aplicación destinada a prevenir el ingreso de virus informáticos a un determinado equipo.

Cache: Servicio de memoria intermedia usado para acelerar un proceso, en nuestro caso los accesos a Internet.

Cortafuegos: Ver Firewall.

Data Center: Centro de Datos. Lugar físico donde se encuentra el corazón de una red.

Dial-Up: Conexión tipo telefónica.

Download: Descarga de información a la máquina local.

Filtrado de paquetes: Técnica usada para seleccionar que información circula por una red y cual no.

Firewall: Equipo destinado a separar en forma segura una red pública de una privada.

Hacker: Persona que vulnera un sistema de seguridad por el solo hecho de vulnerarlo en pos de la libre información.

Hardware: Todo lo relacionado al equipamiento físico.

Insiders: Personas que pertenecen a la entidad que se desea asegurar.

Ip: Dirección (de la forma xxx.xxx.xxx.xxx) establecida para identificar un equipo bajo el protocolo TCP/IP.

Log: Registro de actividades generado por alguna aplicación o el sistema operativo.

Mensajería instantánea: Servicio de envío de mensajes en tiempo real a usuarios que se encuentren conectados a la red.

MODEM: MODulador / DEModulador, es el hardware encargado de establecer una conexión via telefónica.

NAT: Network Address Translation. Servicio de traducción de direcciones de red.

NetBios: Servicio de identificación por nombres de Microsoft Windows.

On-Line: Indicador que muestra el estado de un servicio. También indica que el servicio esta disponible solo con conexión.

Outsiders: Personas ajenas a la entidad a proteger.

Password: Palabra clave utilizada en conjunto con el username para conseguir un determinado permiso.

Protocolos: Conjunto de reglas y métodos establecidas para poder realizar una comunicación eficiente.

Proxy: Generalmente una aplicación usada para compartir un vínculo único a toda una red.

Puertos: Puertas de acceso requeridos por los distintos servicios.

Router: Equipo usado para direccionar los datos de una red hacia otra.

Servidor: Equipo destinado a brindar uno o varios servicios a los usuarios conectados.

Sniffer: Aplicación destinada al monitoreo del tráfico circulante por una red.

Software: Es todo lo relacionado a las aplicaciones que se ejecutan en un equipo.

Sub-Redes: Redes de equipos menores conectadas a una red de mayor tamaño.

Switch: Dispositivo destinado a conectar varios equipos o sub-redes entre si.

Troyanos: Programa malicioso cuyo comportamiento se asocia al famoso Caballo de Troya.

URL: Dirección de un determinado sitio de Internet.

Username: Nombre de usuario solicitado en conjunto con un password para obtener permiso de uso de uno o varios servicios en una red.

Vínculo: Canal de comunicación por el cual se transmiten datos, voz o ambos.

Virus: Programas realizados con fines generalmente dañinos, capaces de autopropagarce por las redes.

Web-Mail: Servicio de correo electrónico basado en Web, por ejemplo Hotmail, Yahoo.

VPN: Virtual Private Network (Red Privada Virtual), método de transportar datos seguros sobre una red pública.

BIBLIOGRAFIA

- Curriculum On Line - Cisco Networking Academies
- Packet Magazine - Cisco System
- Manual de Symantec Norton Antivirus Corporate Edition
- Manual de Kaspersky Personal Antivirus
- Manual de Webtrends Firewall Suite
- Sites oficiales de distintas empresas dedicadas a soluciones Antivirus
- Manual de protocolos – RAD Data Communication
- TCP / IP – Osborne McGraw-Hill
- Network and Internetwork Security 2da. Edición – Prentice Hall
- La caza de Hackers - Freeware Literario
- Publicaciones varias de ArCert
- Articulos sobre Seguridad en Redes (Asociacion de Internautas)
- Publicaciones extraidas de Cotse (The computer Professional Reference)
- Publicaciones varias sobre escaneos de puertos.
- Publicaciones underground sobre Hacking, Cracking, Virus
- Foros y News varios sobre Hacking, Cracking, etc
- RFC Document Series

INDICE

Ing. Adolfo Alejandro Silnik

Lic. [illegible] Acuña
GERENTE DE
CONCIENTIZACION COMUNITARIA
SECRETARÍA DE TECNOLOGÍA DE LA INFORMACION

Secretaría de Estado de Tecnologías de la Información
San Luis