ADMINISTRACIÓN DE REDES CON ENFOQUE DE INGENIERÍA SOCIAL

José Gpe. Vargas Hernández[1]

Abstract *— Se revisan en esté trabajo, algunos de los métodos con la que los administradores de redes pueden defender sus sistemas de los principales ataques de seguridad existentes. En el presente documento se dan algunos consejos de cómo poder lograrlo. Principalmente esta enfocado a los ataques a la seguridad, denominados: Ingeniería Social, es decir los que se logran con errores y /o exceso de confianza del factor humano. Se realizó parte de la presente investigación con algunas encuestas dirigidas a algunos administradores de redes elegidos al azar, de una base de datos de empresas e instituciones de educación de México. Entre los resultados obtenidos destaca que la un buen porcentaje de nuestros administradores de redes, no tienen respaldado de manera correcta y eficiente sus sistemas.*

Index Terms — Administración de redes, Confidencialidad , Ingeniería social, Seguridad.

INTRODUCIÓN

En este siglo de grandes avances tecnológicos, en donde el uso de la computadoras ha sido generalizado. Las redes de computadoras han tenido un crecimiento sostenido en los últimos años, en donde cada vez un mayor numero de empresas e instituciones educativas, dependen gran numero de sus procesos y operatividad a estas.

Esta creciente expansión de las redes de comunicaciones ha hecho necesario la adopción y el desarrollo de herramientas de seguridad que protejan tanto los datos transmitidos como el acceso a los elementos de la red de los posibles ataques que pueda sufrir.Pero en las empresas e instituciones educativas este crecimiento en muchas ocasiones va mas a allá de la asimilación de la tecnología por sus usuarios y administradores; ya que muchos de los problemas de seguridad que se presentan en una organización esta fuertemente ligada, al facto humano: la famosa ingeniería social. La cual si nos remontamos a los años, en los que se desarrollo la Segunda Guerra Mundial, donde los Alemanes e Italianos tuvieron un mismo grado de confiabilidad al obtener secretos militares, pero uno con sofisticados métodos matemáticos, mientras el otro con el chantaje, robo y el encanto de sus mujeres.

Hoy en día existe la tendencia en el aumento de uso de sistemas Linux, aunque no ha bajado el porcentaje de uso de los sistemas UNIX, contrario a una tendencia a la baja de Novel, y la estabilidad en el uso de Windows es uno de lo aspectos sacados de las encuestas realizadas a administradores de redes, escogidos al azar de los institutos tecnológicos y algunas empresas privadas.

SEGURIDAD

Las normas sobre seguridad empezaron su desarrollo a finales de los años 70, cuando surgió la necesidad de proteger ciertas comunicaciones. Han surgidos diversos organismos que las regulan, como ISO(Organización de estándares Internacionales), ITU (Unión Internacional de Telecomunicaciones) y SC27 (Subcomité 27).

Podemos mencionar de una manera general que mantener un sistema seguro(o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

- **Confidenciabilidad**: Nos indica que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.
- **Integridad**: Significa que los elementos solo pueden ser modificados por elementos autorizados, y de una manera controlada.
- **Disponibilidad**: Indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

Entre las cosas que debemos tener en mente al realizar un diseño de seguridad para establecer las politicas de seguridad de nuestra organización, es que queremos proteger ya sea el Software, el hardware y/o los datos.

Entre los puntos que debemos tener en cuantas como un buen administrador de red, son los tipos de amenazas contra la que necesitamos proteger nuestra información.

- **Interrupción de servicio.** Que por ninguna circunstancia se deje de ofrecer un servicio.
- **Interceptación de datos.** Los datos en un sistema solo podrán tener acceso los usuarios autorizados.
- **Modificación de nuestros datos.** Los datos solo serán modificados por usuarios validos.
- **Fabricación de nuevos datos o suplantación de identidad.** Que no existan formas no autorizadas para tener acceso a los datos, o que no se creen usuarios no autorizados.

Cuando se recibe alguno de los ataques anteriores, se pudieron realizar de cualquiera de las dos formas siguientes:

[1] José Gpe. Vargas Hernández. Centro Universitario del Sur, Universidad de Guadalajara, Prol. Colón SN, Cd. Guzmán, Jalisco, 49000, México. Telefax: +52 34141 25189, jvargas@cusur.udg.mx

- **Activos**: Ataques que se hacen de forma directa a los datos y/o equipos.
- **Pasivos**: Ataques que se realizan de forma indirecta a los datos y/o equipos.

El lograr tener una buena política de seguridad, se logra manteniendo mecanismos de seguridad fiables como por ejemplo :

- **Prevención.** Verificando con anterioridad posibles problemas de seguridad.
- **Detección**. Realizando una chequeo en línea de los ataques a la seguridad.
- **Recuperación.** Después de un problema recuperar las fallas ocurridas.

Para este ultimo podemos mencionar que las copias de seguridad del sistema son con frecuencia el único mecanismo de recuperación que poseen los administradores para restaurar una máquina que por cualquier motivo (no siempre se ha de tratar de un pirata que borra los discos), ha perdido los datos. Asociado a las copias de seguridad suelen existir unos problemas de seguridad típicos, p.e. la no verificación del contenido. Otro problema clásico de las copias de seguridad es la política de etiquetado, etc.

Para prevenir la entrada de usuario no validos se han establecido métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad:

- **Algo que el usuario sabe**
- **Algo que éste posee**
- **una característica física del usuario o un acto involuntario del mismo.**

Esta última categoría se conoce con el nombre de autenticación biomética.

Pero podrán existir los mejores métodos, el equipo mas sofisticado, pero si los usuarios y/o administradores no llevan orden, y son descuidados con las políticas de seguridad establecidas. Se tendrá un sistema inseguro. En encuestas realizadas a un grupo elegido al azar de administradores de redes de las principales empresas e instituciones de educación superior de México.

Podemos establecer que uno de los ataques mas peligrosos y que dan origen a mayores riesgos son los denominados de ingeniería social, es decir los ocasionados por el factor humano. Ya sea por un descuido del administrador, por que el usuario sea malintencionado, o por descuido del usuario se obtenga, pierda o cambie información.

Por otro lado ocasionado por el factor humano es la resistencia al cambio por parte de miembros de nuestra organización, como lo descuido ocasionado por ello.

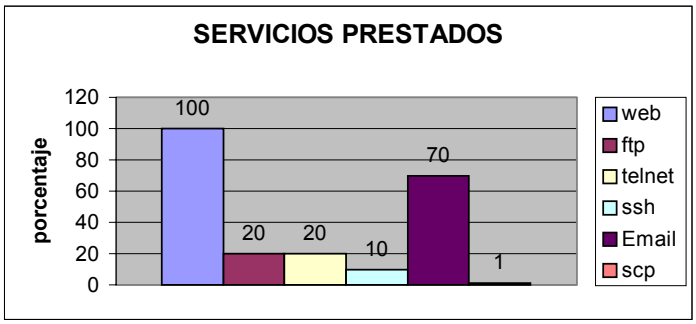

FIGURA. 1
SERVICIOS PRESTADOS

El 100% de los encuestados dan en cierta medida, acceso a Internet a sus usuarios, convirtiéndose esto en un problema de seguridad, ya que la mayoría de sus usuarios, utiliza servicio de Internet inseguros, como es el ftp, telnet, y www.

En la gran mayoría de las empresas e instituciones de educación no existen políticas, bien definidas de autoridad, y canales de mando en muchas de estas organización, en gran porcentaje de ellas el único que conoce las claves de administración, es el encargado. Esto mientras no exista mucha rotación de personal, es adecuado. ¿ Pero que pasaría si el encargado de la red, cambia de empresa?

Entonces podemos visualizar que lo anterior es uno de los principales problemas que se puede enfrentar, los administradores de la empresa. Y por lo que se debe tener un buen control del personal, capacitación al mismo y que estos quieran a la empresa, así como "amor a camiseta".

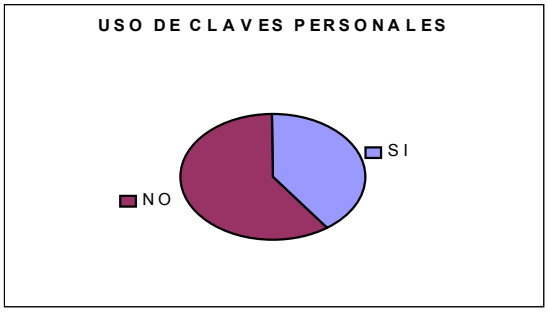

FIGURA. 2
USO DE CLAVES PERSONALES

Uno de los problemas mas graves que enfrenta un administrador de redes, es el descuido de sus usuarios al asignar sus contraseñas. Ya que muchas veces la clave que le asigna son muy sencillas. Así como del descuido de los mismos al no darle la seriedad que se merece al uso de las contraseñas, ya que piensa "..No tengo nada importante...", pero lo que no sabe es que puede usar su cuenta o equipo de pasarela, para atacar otros equipos que tengan información valiosa, aunque no este en la misma red. Aquí el inconveniente es que el prestigio de la institución a la

pertenece o donde fue dirigido el ataque, es el que queda en entredicho.

Al no darle la importancia debida, y pensando que no existe nada que una persona curiosa quiera, se dejan muchos sistemas, completamente sin restricciones para un usuario curioso o con iniciativa. Con esto no se le da el valor que se debe al prestigio de la organización, y existen comentarios como: "... ellos siempre tienen virus..", "... hasta mi hermano de secundaria ha entrado a ese sistema...", etc

Ya que es posible que no se pierda información en ese punto, pero prestigió SI. En este punto un vandalo informatico, puede suplantar la identidad de alguien, y mandar por ejemplo un correo a un usuario pensando que lo manda un tercero.

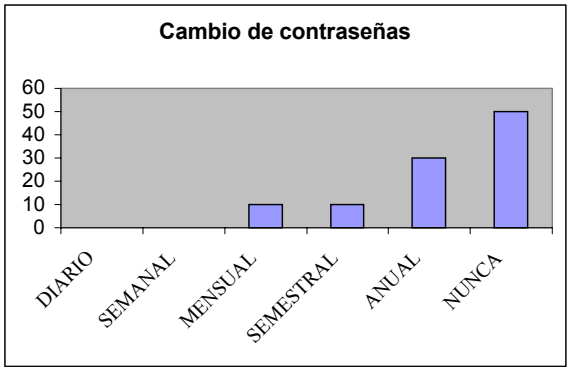

FIGURE 3
FRECUENCIA EN EL CAMBIO DE CONTRASEÑA

CONCLUSIONES

Cuando queremos proteger la información de nuestra organización, y por tanto tener nuestros sistemas confiables y seguros. No requerimos en la mayoría de los casos, conocer todos los huecos o fallas de seguridad de un sistema operativo, y demás programas que se requieren en una organización. Se necesita mas que nada la construcción de sistemas de autenticación fiables y baratos y/o el diseño de nuevos criptosistemas seguros.

Pero es preferible utilizar los existentes como DES, RSA o Kerberos que no tener ninguno como protección en la distribución y autentificación de claves. Otros de los puntos que podemos concluir es que existen en las diversas redes de nuestro país un uso generalizado de mas de dos sistemas operativos, conviviendo por recursos. Siendo este un punto débil en la seguridad de los sistemas, ya que por lo regular es un punto de "quiebra" de la seguridad, si no se tienen los conocimientos del funcionamiento de ambos a nivel de seguridad..

Eso aunado que en muchas instituciones de educación, por falta de recursos humanos, tienen a sus alumnos a cargo de muchos de los procesos informáticos dentro de ella, principalmente de telecomunicaciones.

Actualmente, casi cualquier sistema en Internet es vulnerable, y los problemas de seguridad causan grandes inquietudes en las industrias de ordenadores de comunicaciones. Las preocupaciones sobre los problemas de seguridad incluso han empezado a enfriar las sobrecalentadas esperanzas acerca de la capacidad de Internet para servir de soporte para las actividades comerciales.