Borrador de manual de PSI en UNICUCES – dic del 2015

MANUAL DE PROCEDIMIENTOS DE SEGURIDAD (PSI) EN UNICUCES

Desarrolle el manual de procedimientos de la UNICUCES. Este manual debe tener el estudio previo que se hizo para establecer la base del sistema de seguridad, el programa de seguridad, el plan de acción, las tablas de grupos de acceso, la valoración de los elementos de la red, los formatos de informes presentados a la gerencia para establecer el sistema de seguridad, los procedimientos escogidos para la red, así como las herramientas, y el desarrollo de cada procedimiento en forma algorítmica (agregue todo lo que considere necesario). Espero que recuerden que el manual de procedimientos es un proceso dinámico, por lo que debe modular todos los contenidos en unidades distintas, para poder modificarlas en caso de que sea necesario.

-- MANUAL DE PROCEDIMIENTOS DE SEGURIDAD (PSI) UNICUCES --

Como ya es de conocimiento de muchas de las personas que trabajan con la rama de sistemas y redes, sé sabe que las tecnologías por sí mismas de poco sirven: es lo que Los usuarios hacen con ellas lo que marca la diferencia. Por tal motivo se ha dedicado tiempo y recursos para la jerarquización del personal que desarrolla funciones informáticas y para la valorización de las áreas responsables de los sistemas de información. En este caso se trata de seguir fomentado la capacitación en materia de Tecnologías Informáticas, a fin de lograr un mayor entendimiento de sus potencialidades, especialmente para lograr ejercer bien las normas y tener una toma de decisiones muy acertada.

Ya en el campo específico que motiva el trabajo que sigue, nadie puede discutir hoy en día que las PSI son un componente necesario de los sistemas de información, en todos los ambientes que se manejan.

Por tal motivo y según lo aceptado administrativamente se ha dispuesto de la adopción de una serie de medidas, con el objetivo de robustecer y fortalecer el área de Informática (PSI).

Este manual se elaboró con la intención de facilitar la tarea de quienes tienen a su cargo la administración de las redes y los sistemas de la empresa y sus sucursales.

Introducción

Como estamos viviendo en la actualidad, las Empresas somos cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de trabajo en la empresa y sucursales.

Cuando no hay medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más

organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior de la Empresa en este caso los trabajadores.

Lo complicado y sus topologías de las redes es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, se han incrementado las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. Estos ataques y violaciones a la seguridad se han estado generando por unos personajes que ya son muy conocidos como son los “Hackers”, “crakers”. Tambien hay otras técnicas y herramientas criptográficas, es importante recalcar que un elemento muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red.

Todo este documento se trata de visualizar prioridades y aprender a conocer el valor de información y si en algún momento hay una pérdida de comunicación o ataques externos. En los temas que se quiere ser enfáticos serian básicamente los siguientes temas:

• El valor de los datos

• Las políticas de seguridad informática

• Los procedimientos para el backup de la información

• Los principales ataques a la información de la Empresa

• Las contraseñas

• Los programas de control y seguimiento de las cuentas de los Usuarios.

Se espera que este manual de procedimiento ayude a fortalecer las normas de seguridad de la empresa y sus sucursales.

1 – Que es seguridad

La seguridad informática ha adquirido una gran importancia, según las condiciones y las nuevas plataformas de sistemas disponibles. La necesidad de

interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la empresa. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas, evitar el uso indebido de la misma. Esto puede ocasionar serios problemas en los bienes y servicios de la empresa.

En este caso, las políticas de seguridad informática (PSI) se implementan como una herramienta para concientizar a cada uno de los trabajadores de la empresa sobre la importancia y la sensibilidad de la información, que favorecen el desarrollo de la empresa y el buen funcionamiento.

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

1.1 - ¿valor de los datos?

El valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Además, las PSI no influyen en la productividad del sistema por lo que las Empresas son renuentes a dedicar recursos a esta problemática que aquejan a muchas empresa por no tener medidas de seguridad así sean básicas.

Cuando se habla del valor de la información nos referimos, por ejemplo, a qué tan peligroso es enviar la información de mi los datos de los administrativos y claves de sus cuenta por error a otra persona o correo que no fuera el de la persona encargada, este tema es complejo.

1.2 - Consultas en la Empresa

Para implementar las PSI en la Empresa hay que realizar unas series de consultas y encuestas con los empleados para ver las posibles fallas de la red, del sistema y el funcionamiento o posibles fallas del trabajador. Porque casi todos ya saben que la implementación de un sistema de seguridad conlleva a incrementar la complejidad en el trabajo diario de la empresa, tanto técnica como administrativa. Por estos motivos los trabajadores al saber que se implementan estas PSI deben de realizar varios procesos para ingresar al sistema o realizar tareas en la red que

antes eran menos complicadas. También se debe de consultar con las Empresas de ISP para aclarar los temas de los tipos de comunicación y la seguridad que ellos prestan y lo que se requiere para un buen funcionamiento al momento de comunicar las sedes.

1.3 - Implementación

Para la implementación de las PSI n la empresa, es un proceso de la parte técnica y la administrativa.

Este es un proceso debe abarcar todos los miembros y usuarios de la empresa, sin exclusión alguna, ha de estar fuertemente debe de tener respaldo de gerencia, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria y se quedara solo en papel.

Hay que tener muy en cuenta la complejidad que suma al trabajo diario de la empresa la implementación de estas medidas. Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Resulta claro que proponer o identificar una PSI requiere de un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente DE LA Empresa.

2 - Políticas generales de seguridad

2.1 - ¿Qué es la (PSI)?

La política de seguridad informática (PSI) es una serie de normas que integra a todas las personas de la empresa. Las PSI establecen las normas con las que los funcionarios deben trabajar y cumplir, en relación con los recursos y servicios informáticos de la empresa.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

Se debe monitorear las PSI del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la empresa.

2.2 - Elementos de la PSI

La PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

• Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la empresa a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

• Objetivos de la política y descripción clara de los elementos involucrados en su definición.

• Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

• Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

• Definición de violaciones y de las consecuencias del no cumplimiento de la política.

• Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la empresa. Debe mantener un lenguaje común libre de tecnicismos y términos

legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios de la empresa:

Ejemplo: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal.

2.3 - Parámetros para establecer PSI

Si bien las características de la PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

- Se debe de realizar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá perfeccionar las PSI de la empresa.

- Se debe de involucrar a las áreas en cargadas de los recursos o servicios, pues ellos poseen la experiencia, conocimiento y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

- Socialice con todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Se debe de tener en cuenta que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área.

- Se debe desarrollar un proceso de monitoreo periódico de las directrices de lo que sede de hacer en la empresa, que permita una actualización oportuna de las mismas.

No se debe dar por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos

entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

2.5 - ¿Por qué las PSI generalmente no consiguen implantarse?

En las empresas y en muchas partes donde se trata de implementar las PSI es un completo conflicto por que ya muchos de los trabajadores saben que es mucho papeleo y requisitos para poder ingresar tanto a la empresa como cuando ya está incorporado.

Convencer a los administrativos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que, llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad. Este es un tema que muy complicado y hay que hacerlo ver a los administrativos como cuando aseguran su vehículo a todo riesgo y lo hacen para no perder su inversión, esto mismo sucede con la seguridad de los datos de la empresa es el tesoro y por qué la empresa funciona y el administrativo debe de aprender o entender que si esta parte falla puede perder mucho dinero y tiempo.

2.8 - Niveles de trabajo (Definiciones Y Conceptos)

- Confidencialidad
- Integridad
- Autenticidad
- Disponibilidad de los recursos y de la información
- Consistencia
- Control de Acceso
- Auditoría

2.8.1 – Confidencialidad

Consiste en proteger la información contra la lectura no autorizada explícitamente.

Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

2.8.2 – Integridad

Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como backups, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software.
- Causadas de forma intencional.
- Causadas de forma accidental
- Problemas eléctricos
- Descuido en las contraseñas
- Contraseñas fáciles e inseguras

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

2.8.3 - Autenticidad

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

2.8.5 - Disponibilidad de los recursos y de la información

De qué sirve la información si se encuentra intacta en los Servidores si los usuarios no pueden acceder a ella. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema, y estar en correcta función con sus entorno y cumpliendo las normas con las cuales fue implementado el sistema.

2.8.6 – Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas. Lo que se espera es que cumpla correctamente con sus funciones para las cuales fue implementado.

2.8.7 - Control de acceso a los recursos

Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hacen. En esta etapa es muy importante los controles a los Usuarios y tener un estricto control en las contraseñas.

2.8.8 – Auditoría

Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

2.9 - Algoritmo

Cuando se quiere establecer una estrategia de seguridad, las primeras inquietudes que surgen serian: ¿en qué baso mi estrategia?. La respuesta a esta pregunta es bien simple. El algoritmo Productor/Consumidor.

En este algoritmo, hay dos grandes entidades: una que es la encargada de producir la información; la otra entidad es el consumidor de esta información y otra, llamada precisamente “otros”. Entre el productor y el consumidor, se define una relación que tiene como objetivo una transferencia de “algo” entre ambos, sin otra cosa

Esta es una definición muy general. De todas maneras, resulta conveniente para nuestra tarea. Podemos mencionar como recurso a cualquier cosa, ya sean bienes específicos o que permitan la subsistencia de la organización como tal.

Debido a ello, es que podemos diferenciar claramente tres tipos de recursos:

- Físicos
- Lógicos
- Servicios.

Los recursos físicos son, por ejemplo, las impresoras, los servidores de archivos, los routers, etc.

Los recursos lógicos son, por ejemplo, las bases de datos de las cuales sacamos la información que permite trabajar en la organización.

Los servicios son, por ejemplo, el servicio de correo electrónico, de página WEB,

etc.

3 - ¿Establecer los niveles de riesgo de los recursos involucrados?

Cuando se crea una PSI, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A

pesar de la cantidad de publicidad sobre intrusos en una red, la pérdida real que proviene de los “miembros internos” es mucho mayor.

El análisis de riesgos implica determinar lo siguiente:

- Qué se necesita proteger
- De quién protegerlo
- Cómo protegerlo

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

El otro problema que nos presentamos, es el de las intromisiones clandestinas.

Aquí, es preciso tener en cuenta el tipo de recurso a proteger. En base a ello, estará dada la política de seguridad.

Daremos, a continuación, algunos ejemplos acerca de a qué nos estamos enfrentando:

- ¿Cómo aseguramos que no están ingresando a nuestro sistema por un puerto desprotegido o mal configurado?
- ¿Cómo nos aseguramos de que no se estén usando programas propios del sistema operativo o aplicaciones para ingresar al sistema en forma clandestina?
- ¿Cómo aseguramos de que, ante un corte de energía eléctrica, el sistema seguirá funcionando?
- ¿Cómo nos aseguramos de que los medios de transmisión de información no son susceptibles de ser monitoreados?
- ¿Cómo actúa la organización frente al alejamiento de uno de sus integrantes?

La respuesta a estos interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando

check-lists para comprobar puntos importantes en la configuración y/o funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones.

Es muy aconsejable que se disponga de una agenda con las tareas que se deben llevar a cabo regularmente, a fin de que el seguimiento de los datos obtenidos sea efectivo y se puedan realizar comparaciones válidas al contar con datos secuenciales.

Esta agenda, podría ser en sí misma un procedimiento.

Damos, a continuación, un ejemplo de procedimiento de chequeo de eventos en el sistema:

Diariamente:

- Extraer un logístico sobre el volumen de correo transportado. Extraer un logístico sobre las conexiones de red levantadas en las últimas 24 horas.
- Semanalmente:
- Extraer un logístico sobre los ingresos desde el exterior a la red interna.
- Extraer un logístico con las conexiones externas realizadas desde nuestra red.
- Obtener un logístico sobre los downloads o descargas de archivos realizados y quién los realizó.
- Obtener gráficos sobre tráfico en la red.
- Obtener logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino).
- Mensualmente:
- Realizar un seguimiento de todos los archivos logísticos a fin de detectar cambios (realizados con los archivos de back-up del mes anterior).

Cabría resaltar que, en gran parte, este procedimiento puede ser automatizado por medio de programas que realicen las tareas y sólo informen de las desviaciones con respecto a las reglas dadas.

3.2 - Acerca de los procedimientos

Si se piensa certificar ISO, es indispensable tener un manual de procedimientos escrito y llevarlo a cabo al pie de la letra. De esta manera, cabría pensar que un manual de procedimientos es un paso adelante para poder llegar a la certificación ISO.

3.3 - Procedimiento de alta de cuenta de usuario

Cuando un empleado de la empresa requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

- Nombre y Apellido
- Puesto de trabajo
- Jefe inmediato superior que avale el pedido
- Descripción de los trabajos que debe realizar en el sistema
- Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de “buen uso de los recursos” (para lo cual, se le debe dar una copia de tales normas).
- Explicaciones breves, pero claras de cómo elegir su contraseña.

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

- Tipo de cuenta
- Fecha de caducidad
- Fecha de expiración
- Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos)

Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.

3.4 - Procedimiento de baja de cuenta de usuario

Este procedimiento es el que se lleva a cabo cuando un empleado de la empresa deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial.

Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la PSI, debe estar fuertemente apoyado por la parte gerencial de la organización.

Un ejemplo de este circuito, podría ser: ante el alejamiento de un elemento de la organización, la gerencia de personal (o la sección encargada de la administración de los RH), debe informar en un formulario de “Alejamiento de personal”, todos los datos del individuo que ha dejado la organización, así como de la posición que éste ocupaba y el tipo de alejamiento (permanente o no).Una vez llegada la información al departamento encargado de la administración de sistemas, se utiliza para dar de baja o inhabilitar la cuenta del usuario.

La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción. Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia, debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

3.5 - Procedimiento para determinar las buenas contraseñas

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir una contraseña:

Se debe explicitar

- La cantidad de caracteres mínimo que debe tener,
- No tiene que tener relación directa con las características del usuario.
- Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
- Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario).

Una vez que el usuario ha elegido su contraseña, se le debe correr un “programa

crackeador” para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

3.6 - Procedimientos de verificación de accesos

Se debe explicar la forma de realizar las auditorías de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoría y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de “log” con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas para mirar las medidas a tomar.

3.7 - Procedimiento para el chequeo del tráfico de la red

Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma.

El procedimiento debe indicar en los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

3.8 - Procedimiento para el monitoreo de los volúmenes de correo

Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de “mails” en tránsito. Dicho procedimiento se encuentra realizado por programas que llevan las estadísticas, generando reportes con la información pedida. El conocimiento de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está siendo objeto de un “spam”.

Como en los casos anteriores, en el procedimiento debe estar explicitado quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan variaciones.

3.9 - Procedimientos para el monitoreo de conexiones activas

Este procedimiento se efectúa con el objeto de prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios.

Cuando detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un log con el acontecimiento.

3.10 - Procedimiento de modificación de archivos

Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Al igual que en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas.

3.11 - Procedimientos para los backup de seguridad

Este procedimiento debe indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas. También se debe de tener en cuenta que estos backup se deben de realizar en diferentes formas y ubicar el guardado en sitios o lugares diferentes.

3.12 - Procedimientos para la verificación de las máquinas de los usuarios

Este procedimiento permitirá encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quiénes lo llevarán a cabo.

3.13 - Procedimientos para el monitoreo de los puertos en la red

Este procedimiento permite saber qué puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos. El procedimiento deberá

describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

3.14 – Capacitaciones para las nuevas normas de seguridad

Este tipo de procedimiento no siempre es tenido en cuenta. Sin embargo, en una empresa es muy importante conocer las últimas modificaciones realizadas a los procedimientos, de tal manera que nadie pueda poner cómo excusa “que no conocía las modificaciones”. En él, debe describirse la forma de realizar la publicidad de las modificaciones: puede ser mediante un mailing, por exposición en transparencias, por notificación expresa, etc.; quién estará a cargo de la tarea y las atribuciones que tiene.

Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado, proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

4 - Tipos de Ataques y Vulnerabilidades (Conceptos)

4.1 - Negación de servicio (denial of service)

En el presente apartado, se describirán los modos de ataques que podrían ocurrir más frecuentemente en las redes de información. Debido a la pérdida de dinero y de tiempo que estos ataques pueden ocasionar, se presentarán también algunas formas de prevención y de respuesta a los mismos.

4.1.1 - ¿Qué es “Denial of service”?. Descripción de ataques.

Denial of service es un tipo de ataque cuya meta fundamental es la de negar el acceso del atacado a un recurso determinado o a sus propios recursos.

Algunos ejemplos de este tipo de ataque son:

• Tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma;

• Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio;

• Tentativas de evitar que una determinada persona tenga acceso a un servicio;

• Tentativas de interrumpir un servicio específico a un sistema o a un usuario;

Cabría tener en cuenta que, el uso ilegítimo de recursos puede también dar lugar a la negación de un servicio. Por ejemplo, un “hacker” puede utilizar un área del FTP anónimo como lugar para salvar archivos, consumiendo, de esta manera, espacio en el disco y generando tráfico en la red.

Como consecuencia, los ataques de negación de servicio pueden esencialmente dejar inoperativa una computadora o una red. De esta forma, toda una organización puede quedar fuera de Internet durante un tiempo determinado.

4.1.2 - Modos de ataque

Algunos ataques de negación de servicio se pueden ejecutar con recursos muy limitados contra un sitio grande y sofisticado. Este tipo de ataque se denomina “ataque asimétrico”. Por ejemplo, un atacante con una vieja PC y un módem puede poner fuera de combate a máquinas rápidas y sofisticadas. Últimamente, esto es común con ataques de los denominados “nukes” en los cuales caen instalaciones grandes, por ejemplo, de clusters Windows NT.

Hay tres tipos de ataques básicos de negación de servicios:

a.- Consumo de recursos escasos, limitados, o no renovables

b.- Destrucción o alteración de información de configuración

c.- Destrucción o alteración física de los componentes de la red.

4.1.3 - Consumo de recursos escasos, limitados, o no renovables

Las computadoras y las redes necesitan para funcionar ciertos recursos: ancho de banda de la red, espacio de memoria y disco, tiempo de CPU, estructuras de datos, acceso otras computadoras y redes, entre otros.

Conectividad

Los ataques de Negación de servicio se ejecutan, con frecuencia, contra la conectividad de la red. La meta del hacker es evitar que las computadoras se comuniquen en la red.

Un ejemplo de este tipo de ataque es el “SYN flood”:

En este tipo de ataque, el hacker comienza el proceso de establecer una conexión

TCP a la máquina de la víctima, pero lo hace de manera tal que evita que la conexión se complete. En este tiempo, la máquina del atacado ha reservado uno entre un número limitado de las estructuras de datos requeridas para terminar la conexión inminente. El resultado es que las conexiones legítimas se rechazan mientras que la máquina del atacado se queda esperando para terminar esas falsas conexiones “medio abiertas”.

Debe tenerse en cuenta que este tipo de ataque no depende del ancho de banda que disponga el atacante. En este caso, el hacker está consumiendo las estructuras de datos del kernel, implicadas en establecer una conexión TCP. Un hacker con una simple conexión dial-up puede realizar este ataque contra una poderosa Workstation (este último es un buen ejemplo de un ataque asimétrico).

Aprovechamiento de los recursos del otro

Un hacker también puede utilizar los recursos que usted dispone contra usted mismo, de maneras inesperadas. Por ejemplo, el caso de Negación de servicio UDP. En este ataque, el hacker utiliza los paquetes “falsificados” de UDP para conectar el servicio de generación de eco en una máquina con el servicio de chargen en otra máquina.

El resultado es, que los dos servicios consumen todo el ancho de banda de red entre ellos. Así, la conectividad para todas las máquinas en la misma red desde cualquiera de las máquinas atacadas se ve afectada.

Consumo de ancho de banda

Un hacker puede, también, consumir todo el ancho de banda disponible en su red generando una gran cantidad de paquetes dirigidos a la misma. Típicamente, estos paquetes son de generación de eco de ICMP (ping), pero pueden ser cualquier otra cosa. Además, el hacker no necesita operar desde una sola máquina; él puede poder coordinar varias máquinas en diversas redes para alcanzar el mismo efecto.

Consumo de otros recursos

Además del ancho de banda de la red, los hackers pueden consumir otros recursos que su sistema necesite para funcionar. Por ejemplo, en muchos sistemas, un número limitado de las estructuras de datos en el kernel está disponible para almacenar información de procesos (identificadores, entradas en tablas de procesos, slots, etc.).

Un hacker puede consumir estas estructuras de datos escribiendo un programa o un script que no haga nada pero que cree en varias ocasiones copias de sí mismo.

Muchos sistemas operativos modernos, aunque no la totalidad de ellos, tienen recursos para protegerse contra este problema. Además, aunque las tablas de procesos no se llenen, se consume CPU por la gran cantidad de procesos y conmutación entre los mismos.

Un hacker puede también consumir su espacio en disco de otras maneras, por ejemplo:

- Genera miles de mails (Spam, Bombing. Para ampliar este tema, consultar el próximo).

- Generar intencionalmente errores que deben ser logueados. En este tipo de ataque, podemos citar también la utilización indebida del syslog en unix. Es decir, utilizar el proceso syslog de la víctima para que registre eventos de otra máquina, llenando el espacio en disco con el archivo de syslog.

- Colocar archivos en su disco, utilizando ftp anónimo.

En general, se puede utilizar cualquier cosa que permita que los datos sean escritos en su disco para ejecutar un ataque de negación de servicio si no hay límites en la cantidad de datos que se pueden escribir (quotas).

No obstante, muchos sitios tienen esquemas de “lockout” de cuenta después de un cierto número de logins fallados. Un setup típico bloquea el login después de 3 o 5 tentativas falladas. Un hacker puede utilizar este esquema para evitar que los usuarios legítimos entren. En algunos casos, incluso las cuentas privilegiadas, tales como root o

administrator, pueden ser víctimas de este tipo de ataque.

Recuerde: siempre disponga de un método para acceder ante la emergencia de este tipo de ataques.

Un hacker puede hacer caer su sistema o ponerlo inestable, enviando datos inesperados. Un ejemplo de tal ataque es el “ping flood” o Pings de tamaño

demasiado grande. Si su sistema está experimentando caídas frecuentes sin causa evidente, podría deberse a este tipo de ataque.

Hay otros componentes que pueden ser vulnerables a la negación de servicio y que deben vigilar se. Estos incluyen:

- Impresoras
- Unidades de cinta
- Conexiones de red
- Otros recursos limitados importantes para la operación de su sistema.

4.1.4 - Destrucción o alteración de la información de configuración

Una computadora incorrectamente configurada puede no funcionar bien o directamente no arrancar. Un hacker puede alterar o destruir la información de configuración de su sistema operativo, evitando de esta forma que usted use su computadora o red.

Veamos algunos ejemplos:

Si un hacker puede cambiar la información de ruteo de sus routers, su red puede ser deshabilitada.

Si un hacker puede modificar la registry en una máquina Windows NT, ciertas funciones pueden ser imposibles de utilizar, o directamente el sistema puede no volver a bootear.

4.1.5. - Destrucción o alteración física de los componentes de la red

Es muy importante la seguridad física de la red. Se debe resguardar contra el acceso no autorizado a las computadoras, los routers, los racks de cableado de red, los segmentos del backbone de la red, y cualquier otro componente crítico de la red.

4.1.6 - Prevención y respuesta

Tal como se ha expresado anteriormente, los ataques de Negación de servicio pueden dar lugar a pérdidas significativas de tiempo y dinero para muchas organizaciones, por lo que se recomiendan una serie de medidas:

- Coloque access lists en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio

- Instale patches a su sistema operativo contra flooding de TCP SYN. Esta acción permitirá reducir sustancialmente su exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva.

- Invalide cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio. Por ejemplo: chargen, Echo, etc.

- Si su sistema operativo lo permite, implemente sistemas de cuotas. Por ejemplo, si su sistema operativo soporta “disk Quotas” impleméntelo para todos los logins. Si su sistema operativo soporta partición o volúmenes, separe lo crítico de lo que no lo es.

- Observe el funcionamiento del sistema y establezca valores base para la actividad ordinaria. Utilice estos valores para calibrar niveles inusuales de la actividad del disco, del uso de la CPU, o del tráfico de red.

- Incluya como parte de su rutina, el examen de su seguridad física. Considere, entre otras cosas, los servidores, routers, terminales desatendidas, ports de acceso de red y los gabinetes de cableado.

- Utilice Tripwire o una herramienta similar para detectar cambios en la información de configuración u otros archivos.

- Trate de utilizar configuraciones de red redundantes y fault-tolerant.

4.2 - Cracking de contraseñas

En este apartado, se presentarán una serie de consideraciones referidas al

“cracking de contraseñas” basadas en UNIX1.

El objetivo inicial consiste en entrar al server. Para ello, se procede como si se tratase de una máquina remota (telnet). Pero, debido a que se permite el acceso a múltiples usuarios, los sistemas UNIX nos solicitarán un nombre de identificación

acompañado de una clave. Dicho nombre darse de alta en el sistema para que se pueda acceder.

Cuando un usuario desea entrar en una máquina, el sistema solicitará:

Un login de acceso o nombre de usuario. Si el login es incorrecto, el sistema no lo notificará para impedirle conocer qué accesos se encuentran dados de alta.

Una contraseña o palabra clave. Si la contraseña coincide con la que tiene asignada el login que se emplea, el sistema permitirá el acceso.

4.2.1 - El archivo “/etc/contraseña”: descripción

Los usuarios que se encuentran dados de alta en el sistema, así como las contraseñas que emplean, se hallan localizados en el archivo: /etc/contraseña (para la mayoría de los sistemas operativos basados en UNIX).

Lamentablemente para algunos, y afortunadamente para otros, este archivo es el punto más débil del sistema. Está compuesto de líneas o registros en las cuales cada línea se divide en siete campos con dos puntos (:).

4.2.2 - Descubrir una contraseña

Una vez encriptada una contraseña, no se puede desencriptar. Sin embargo, esto no garantiza la seguridad de la contraseña, puesto que no significa que la contraseña no se pueda averiguar.

El mecanismo que se utiliza para descubrir (no desencriptar) las contraseñas consiste en efectuar encriptaciones de palabras (posibles contraseñas) y comparar estas encriptaciones con el original.

¿De qué depende el éxito?

El éxito depende de la calidad del diccionario (archivo que contiene un conjunto de posibles contraseñas), del programa que se utilice, del CPU y, por supuesto, de nuestra paciencia.

Los programas buscadores de contraseñas son fácilmente diseñables.

Si mediante un “bug” se obtiene el archivo /etc/passwd, se puede iniciar un ataque de diccionario contra el mismo obteniéndose, de este modo, las contraseñas.

Otro tipo de ataque es el de “fuerza bruta”, que consiste simplemente en realizar todas las combinaciones posibles de caracteres hasta hallar la contraseña.

En el siguiente cuadro podemos ver el tiempo de búsqueda de una contraseña de acuerdo a la longitud y tipo de caracteres utilizados. Se supone una velocidad de búsqueda de 100.000 contraseñas por segundo.

Como puede apreciarse, resulta importante utilizar más de 8 caracteres y cuantos más símbolos intervengan, menos probabilidades habrán de encontrar la contraseña.

4.3 - E-mail bombing y spamming

En este apartado, se presentarán algunas de las dificultades que pueden surgir como consecuencia de la utilización de los servicios de mail. Se brindarán, por otro lado, algunas respuestas a dichos obstáculos.

4.3.1 - Descripción

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario.

El spamming,, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés. El Spamming puede resultar aún más perjudicial si los destinatarios contestan el mail, haciendo que todos reciban la respuesta.

Puede, además, ocurrir inocentemente como resultado de enviar un mensaje a la lista y no darse cuenta de que la lista lo distribuye a millares de usuarios, o como resultado de mala configuración de un autorespondedor, por ejemplo el “vacation”.

El e-mail bombing/spamming se puede combinar con el e-mail spoofing – que altera la identidad de la cuenta que envía el mail -, logrando que sea más difícil determinar quién está enviando realmente el mail.

4.3.2 - Detalles técnicos

Cuando se proveen los servicios de e-mail los usuarios son, lógicamente, vulnerables al e-mail bombing y spamming.

En efecto, el e-mail spamming es casi imposible de prevenir. Un usuario con una dirección válida de mail puede realizar " Spam " a cualquier otra dirección de mail,

newsgroup, o sistema de BBS.

Cuando gran cantidad de mails son dirigidos a un solo sitio, éste puede sufrir

“denial of service” por pérdida de conectividad, caerse el sistema o producirse fallas en el servicio debido a:

- Sobrecarga de conexiones de red;
- Utilización de todos los recursos de sistema disponibles;
- llenado del disco como resultado de postings múltiples y de entradas en el “syslog”.

4.3.3. - ¿Cómo proceder?

Detección

Si un sistema aparece repentinamente lento (el e-mail es lento o no parece ser enviado o recibido), la razón puede ser que su mailer está intentando procesar una excesiva cantidad de mensajes. Esto puede comprobarse a través del “log” de sistema.

Reacción

Es importante:

- Identificar la fuente del e-mail bomb/spam y configure su router para evitar el acceso de los paquetes entrantes de esa dirección. Puede colocar un “Access list” en el port 25 (SMTP) del tipo “established” para esa dirección.
- Observar los “headers” del e-mail para determinar su origen verdadero.
- Ponerse en contacto con el sitio que usted identificó en su revisión con el propósito de alertarlos de la actividad del spammer.
- Asegurarse de tener la versión más actualizada del “daemon” de mail (por ejemplo sendmail) y aumente el grado de “debug” o “log” que posea el proceso, para detectar o alertar estas actividades. Tenga la precaución de vigilar el tamaño del archivo de log, que puede crecer considerablemente, si se está bajo un e-mail-bombing.

- Prevención

Desafortunadamente, hasta el momento, no hay manera de prevenir el bombardeo de e-mail o spamming y es imposible predecir el origen del ataque siguiente. Es trivial obtener acceso a listas de interés o acceder a información que contenga grandes volúmenes de direcciones de e-mail, las que proporcionan al atacante direcciones de destino para el spam.

Pueden desarrollarse herramientas internas, que pueden ayudar a reconocer y a responder al e-mail bombing/spamming reduciendo, de esta manera, el impacto de tal actividad. Tales herramientas deben aumentar las capacidades de log y alertar de mensajes que vienen de un mismo lugar en un corto período de tiempo. Asimismo, deberían ser capaces de rechazar esos mensajes, o descartarlos.

Si un sitio utiliza un número pequeño de servidores de e-mail, podría configurarse un “firewall” para asegurarse de que las conexiones de “smtp” fuera de su firewall puedan hacerse solamente a sus “hubs” de mail y a ninguno de los otros equipos.

Aunque esta operación no prevendrá un ataque, reduce al mínimo el número de las máquinas disponibles para un ataque basado en SMTP. De este modo, se puede controlar el tráfico entrante SMTP y filtrarlo de manera acorde.

Recuerde: no conteste y/o haga un forward de los Spams. De este modo evitará que el problema se propague.

4.4 - Problemas de seguridad en el FTP

4.4.1 - El comando PORT

En los últimos años, se ha incrementado el debate en torno a los problemas relacionados con el comando PORT del protocolo del FTP. Estos problemas se basan el uso erróneo de dicho comando.

4.4.2. - El Protocolo FTP

Para entender estos ataques, es necesario tener una comprensión básica del protocolo FTP.

Un cliente abre una conexión al port de control de ftp (21) de un FTP SERVER. De este modo, para que el servidor sea capaz luego de enviar datos de nuevo a la

máquina del cliente, una segunda conexión (de datos) debe abrirse entre el servidor y el cliente.

Para hacer esta segunda conexión, el cliente envía un comando PORT al servidor.

Este comando incluye parámetros que indican al servidor cuál IP ADDRESS conectar y qué port abrir en aquella dirección.

El servidor luego abre aquella conexión, siendo la fuente de la conexión el port 20 del servidor y el destino el port identificado en los parámetros del comando PORT.

El comando PORT se utiliza generalmente sólo en el " modo activo " del ftp (por default). No se suele utilizar en modo pasivo (PASV). Debe notarse que los servidores de ftp generalmente implementan ambos modos en ejecución, y el cliente especifica qué método utilizar.

4.4.3. - El ataque “Ftp bounce”

Conforme con el protocolo FTP, el comando PORT hace que la máquina que lo origina especifique una máquina de destino y un port arbitrarios para la conexión de datos. Sin embargo, esto también significa que un hacker puede abrir una conexión a un port del hacker eligiendo una máquina que puede no ser el cliente original.

Hacer esta conexión a una máquina arbitraria es hacer un ataque “ftp bounce”. Con fines ilustrativos, se presentan seguidamente varios ejemplos de cómo los hackers pueden utilizar el “ftp bounce”.

“Scanning” de ports

Un hacker que desea realizar una port scan contra un sitio puede hacerlo de un server FTP de un tercero , que actúa como un “puente” para el scan. El sitio de la víctima ve la exploración como procedente del server FTP más que de la fuente verdadera (el cliente FTP).

Bajo algunas circunstancias, esta técnica ofrece al hacker más ventajas que ocultar la fuente verdadera de la prueba. Cuando el sitio previsto de la víctima está en la misma subnet que el server FTP server, o cuando no filtra tráfico del server FTP , el hacker puede utilizar la máquina del servidor como la fuente del port scan más que la máquina del cliente, desviando de esta manera los controles de acceso que de otra manera se aplicarían.

“Bypass” de dispositivos básicos de filtrado de paquetes.

Un hacker puede realizar un “bypass” de un firewall en ciertas configuraciones de red.

Por ejemplo, supongamos que un sitio tiene su servidor de FTP anónimo detrás

del firewall. Usando la técnica de port scan, un hacker determina que un web server interno en ese sitio está disponible en el acceso 8080, un port normalmente bloqueado por un firewall.

Conectándose al server FTP público del sitio, el hacker inicia otra conexión entre el server FTP y un port arbitrario, en una máquina no pública del sitio (por ejemplo el web server interno en el port 8080). Como resultado, el hacker establece una conexión a una máquina que sería protegida de otra manera por el firewall.

4.4.4 - Bypass de dispositivos de filtrado dinámicos

Otro problema se refiere a los sitios que tienen firewalls que utilizan filtros dinámicos para protegerse. Los sitios están abiertos al ataque porque el firewall confía en la información que recibe.

En este ejemplo, el sitio de la víctima contiene todos sus sistemas detrás de un firewall que utiliza los filtros dinámicos. Una persona en el sitio de la víctima hojea las páginas de la Web y baja un Java applet construido por el hacker. Sin el conocimiento de esa persona, el Java applet abre una conexión de salida de ftp a la máquina del hacker. El applet entonces publica un comando PORT de ftp, ordenando a la máquina del servidor abrir una conexión a, por ejemplo, el port telnet que de otra manera se encontraba protegido detrás del firewall.

Como el firewall de filtros dinámicos examina los paquetes de salida para determinar si alguna acción se requiere de su parte, observa el comando PORT y permite una conexión entrante del server web remoto al port del telnet en la máquina de la víctima. Esta conexión normalmente no es permitida por el firewall; fue permitida en este caso porque el comando PORT fue realizado por el cliente.

4.4.5 - Soluciones

Los ataques de los ejemplos demuestran el componente base de la vulnerabilidad: los contenidos del comando PORT del ftp no son tan dignos de confianza mientras están bajo control de un potencial atacante. El ejemplo del “ftp bounce” demuestra

qué sucede cuando un servidor confía en la información. El ejemplo del filtro dinámico demuestra qué sucede cuando un firewall confía en la información.

Software del Ftp server

La mejor solución al problema del “ftp bounce” desde la perspectiva de la seguridad es asegurarse de que el software del server FTP no puede establecer conexiones a máquinas arbitrarias. Sin embargo, los sitios que confían en el comportamiento “RFC-compliant” pueden encontrar que el implementar esta solución afectará las aplicaciones que ellos utilizan.Por lo tanto, muchos vendedores ofrecen soluciones que permiten al sitio dar servicio de ftp adaptado a las necesidades del cliente. Las implementaciones del vendedor caen en tres grupos:

1) conformidad estricta con funciones del RFC: el comando PORT se puede utilizar para conectar directamente con una máquina de una tercera persona, y ésta es la única funcionalidad permitida. Algunos vendedores que eligen mantener conformidad estricta, han tratado este problema modificando el resto de los servicios de red para rechazar las conexiones que se originaban en el port de datos del ftp (port 20).

2) supresión estricta del comando PORT: el comando PORT puede ser utilizado para conectar con el cliente de origen, y ésta es la única funcionalidad permitida.

3) comportamiento variable del comando PORT: el comando PORT se puede utilizar en las dos formas descriptas, siendo una la forma por default. El cambiar entre ellas se logra generalmente con un parámetro en la línea de comando. Se debe tener cuidado de verificar cuál es el valor por default.

Asimismo, se debe tener conciencia sobre la categoría en que se halla el software del server. La recomendación es utilizar la opción 2, o la opción 3 con la supresión habilitada.

Configuración del Ftp server

Algunos de los ataques “ftp bounce” descriptos confían en unas o más máquinas del servidor (dependiendo del ataque) permitiendo el upload de archivos vía ftp (generalmente FTP anónimo).

Su sitio debe ofrecer recursos anónimos de upload solo si es absolutamente necesario. Incluso luego, usted debe configurar cuidadosamente el área entrante.

Configuración de Red

Hay algunas cosas a tener presente al configurar las “fronteras” de la red, esto es, los routers con access-lists y los firewalls.

Los sitios deben asegurarse de que se diseñe cuidadosamente la topología de red de modo que los límites eficaces del tráfico existan entre los sistemas que ofrecen niveles distintos del servicio. Por ejemplo, un sitio tiene típicamente un servicio de FTP

Anonymous, servicio del Web, y un hub entrante de correo electrónico. Una buena práctica de seguridad consiste en separar las máquinas que proporcionan estos servicios externos de las que realizan servicios internos. Es importante tener límites

“fuertes” en la red, preferiblemente firewalls, entre estos dos conjuntos de máquinas.

Por ejemplo, los sitios que tienen un server FTP que permite el comando PORT para establecer conexiones a las máquinas de un tercero deben bloquear el tráfico entre el server FTP y las máquinas que ofrecen servicios que confían en el hostname o la dirección IP para la autenticación. Los ejemplos de tales servicios son rlogin, rsh y

NFS. Mientras que un firewall o un filtering router debe prevenir siempre el acceso externo directo a tales servicios, debe también filtrar el tráfico de un server FTP interno que se comporte de esta manera. Esto advierte al server FTP que está siendo utilizado como una máquina de relay para atacar protocolos con mecanismos débiles de autenticación basados en el hostname o la dirección IP.

Los sitios que usan firewall de filtrado dinámico de paquetes dinámico necesitan tomar medidas adicionales para asegurarse de que los comandos PORT de terceros sean bloqueados por el firewall.

4.5 - Seguridad en WWW

En este apartado se verán las vulnerabilidades más comunes encontradas en los servidores de Web. Vía WWW, el demonio httpd se ha convertido rápidamente en una de las primeras "puntas de ataque" de los hackers. Es común ver reportes de los CERT que informan vulnerabilidades tales como el PHF (servicio de directorio “White pages”) en muchos servers, y las hay menos conocidas, como los scripts "query", y "prueba-cgi

".

Existen dos caras de seguridad del webserver, una es proteger el sistema operativo en sí mismo de ser atacado vía WWW, la otra es proteger un Website en sí mismo de acceso no autorizado.

Atacar el sistema operativo vía WWW implica generalmente “trampear” un cgi script o lograr que el webserver haga algo que no fue pensado que haga, como por ejemplo dar al hacker acceso al shell del host, que ese hacker ejecute comandos arbitrarios en él , o le provea información útil para lograr esos objetivos.

4.5.1 - Conclusión

Se han descripto ataques comunes al WEB server, algunos antiguos y para los cuales se dispone de patches, pero estos ataques están en continua evolución, explotando bugs de los web servers, o descuidos de los administradores. Como recomendación general, además de ser cuidadoso en, particularmente, los scripts cgi, hay que revisar las configuraciones de acceso en el web server , los permisos con los que el mismo se ejecuta, y los directorios de datos expuestos.

Otros tipos de ataques no han comprometido los datos del sistema, pero han hecho caer al web server: uno muy común explotaba un bug del Internet Information

Server de Microsoft, disponible con el Windows NT, que no soportaba URL’s mayores de

64 Kb.

4.6 - TFTP

El Trivial File Transport Protocol (TFTP) es un mecanismo sencillo de file transfer basado en UDP. Este protocolo no tiene autenticación, constituyendo un potencial problema de seguridad. Es usado frecuentemente para bootear estaciones de trabajo

X11, o para bootear routers desde sistemas unix.

Se recomienda NO HABILITAR el tftp a menos que sea estrictamente necesario. Si se lo hace, verificar que este correctamente configurado, para enviar solo los archivos correctos a solo los clientes autorizados.

4.7 - TELNET

TELNET provee acceso de terminal a un sistema. El protocolo incluye previsiones para soportar varios seteos de terminal como ser raw mode, eco de caracteres, etc.

Generalmente, el demonio de telnet llama al programa login para autenticar al usuario e iniciar la sesión. El mismo provee un nombre de cuenta y una contraseña para el login.

Una sesión de telnet puede ocurrir entre dos máquinas de la misma organización o confiables, en ese caso se puede utilizar un secure telnet para encriptar la sesión completa, protegiendo la contraseña y la sesión completa.

Pero en la mayoría de los casos, la mayoría de las sesiones de telnet vienen de sistemas no confiables. Es decir, no podemos confiar ni en el sistema operativo que hace telnet al nuestro, ni en las redes que intervienen en el proceso. La contraseña y la sesión entera son fácilmente visibles para los ojos de un espía, típicamente usando

sniffers.

Una técnica común de hackeo es “pinchar” el programa cliente de telnet, logrando que registre los nombres de usuario y contraseña, e inclusive la sesión entera. De todas formas, si la red está bajo “sniffing”, es extremadamente sencillo obtener las contraseñas que circulan por sesiones de telnet. La mejor defensa para este tipo de ataque es el esquema de contraseña de única vez.

Una de las implementaciones de este esquema consiste en que el usuario disponga de un dispositivo programado mediante una clave secreta. El sistema que acepta el login envía un “challenge”, que el usuario digita en su dispositivo. Esto le devuelve la contraseña adecuada para el código “challenge” enviado. Pero esa pasword que circulo por la red es válida solo para esa sesión, el hacker, si observo la sesión, deberá descifrar cual es el algoritmo utilizado para que en base al “challenge” variable y una clave secreta que no circulo por la red se obtenga la contraseña de única vez.

4.8 - Los comandos “r”

Los comandos “r” provienen del sistema de autenticación del UNIX BSD. Un usuario puede realizar un rlogin a una máquina remota sin ingresar contraseña si el criterio de autenticación es el correcto. Estos criterios consisten en:

• La conexión debe originarse desde un port TCP privilegiado. En sistemas como PC's con Win95, por ejemplo, estas restricciones no existen con lo cual no tienen mucho sentido. Como corolario, rlogin y rsh deben ser permitidos sólo desde máquinas donde esta restriccion exista.

• El usuario y la máquina cliente deben estar listados en la máquina server como socios autenticados. (Típicamente /etc/hosts.equiv o en el directorio home del usuario, en el archivo .rhosts)

• La máquina cliente y su dirección IP deben coincidir, estando listadas en el server.

Desde el punto de vista del usuario, este esquema es muy interesante. El usuario no es molestado con prompts de contraseñas en logins que utilza frecuentemente. Pero desde el punto de vista del hacker, los comandos "r" ofrecen dos ventajas: una manera de entrar a un sistema, y una vez dentro, una forma de ganar acceso a máquinas de confianza de la primera máquina hackeada.

El principal objetivo del hacker es colocar una entrada apropiada en

/etc/hosts.equiv o .rhosts. Para ello utilizan FTP, UUCP, TFTP u otros medios. Por ejemplo, pueden utilizar FTP para dejar .rhosts en /usr/ftp . o UUCP, para dejarlo en

/usr/spool/uucppublic. Obviamente, uno debe verificar la estructura de permisos de la máquina server para prohibir eso.

Una vez adquirido el acceso no autorizado, muchas otras computadoras son accesibles. El hacker accede a /etc/hosts.equiv de la máquina atacada, y de ahí puede seguir su cadena de accesos, obteniendo más archivos /etc/passwd.

Notemos que la implementacion de comandos "r" presenta un problema adicional:

Parte de la seguridad del sistema puede residir en decisiones del usuario y no del administrador. En efecto, el usuario puede hacer que su archivo .rhosts sea de lectura y escritura para todos los otros usuarios. Algunas implementaciones de rlogin y rsh solucionan esto: si el usuario no lo hace, un cron se ocupa que los archivos .rhosts

esten con sus permisos en orden.

Dado las debilidades del sistema de autenticación de los comandos "r" que hemos visto, no se recomienda que estos servicios estén disponibles en sistemas accesibles directamente en internet.

Aquí hay un punto delicado. La alternativa usual a emplear rlogin es usar telnet, que como hemos visto transmite por la red una contraseña, mientras que rlogin no lo hace. Las alternativas y los riesgos deben ser cuidadosamente evaluados.

5 - Descripción de algunas herramientas de control y seguimiento de accesos (conceptos basicos)

Se enumeraran algunas herramientas que nos permitirán tener una información mediante archivos de trazas o logísticos de todos los intentos de conexión que se han producido sobre nuestro sistema o sobre otro que nosotros hayamos señalado, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP (herramientas de tipo SATAN).

5.1 - tcp-wrappers

El tcp-wrappers es un software de domino público desarrollado por Wietse

Venema (Universidad de Eindhoven, Holanda). Su función principal es: proteger a los sistemas de conexiones no deseadas a determinados servicios de red, permitiendo a su vez ejecutar determinados comandos ante determinadas acciones de forma automática.

5.2. - Netlog

Este software de dominio público diseñado por la Universidad de Texas, es una herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red (los programas pueden ejecutarse en modo promiscuo) que pudiera ser "sospechoso" y que indicara un posible ataque a una máquina (por la naturaleza de ese tráfico).

El paquete está formado por el siguiente conjunto de programas:

5.2.1. - Tcplogger

Este programa escucha todos los servicios sobre TCP, dejando una traza de cada

servicio en un archivo de trazas, indicando la hora, la máquina origen y el puerto de esa conexión.

5.2.2. - Udplogger

Es semejante al anterior, pero para los servicios sobre UDP.

Los archivos que generan estas dos herramientas pueden ser útiles también para detectar ataques de tipo SATAN o ISS, ya que en los archivos de trazas se aprecian intentos de conexión muy cortos en el tiempo a puertos (tcp o udp) de forma consecutiva.

5.2.3. - Icmplogger

Se encarga de trazar el tráfico de icmp.

Estos programas pueden guardar su información en ASCII o en formato binario.

En este segundo caso, el programa dispone de una herramienta (extract) que permite consultar los archivos de trazas dándole patrones de búsqueda, como puede ser el tráfico desde una red concreta, los intentos de conexión a puertos específicos, etc.

5.2.4. - Etherscan

Es una herramienta que monitorea la red buscando ciertos protocolos con actividad inusual, como puedan ser conexiones tftp - en este caso, si se han realizado con éxito nos indica qué archivos se han llevado -, comandos en el puerto de sendmail

(25 tcp) como vrfy, expn, algunos comandos de rpc como rpcinfo, peticiones al servidor de NIS (algunas herramientas utilizan este tipo de servidores para obtener el archivo de

Contraseña, ej: ypx), peticiones al demonio de mountd, etc. Etherscan se ejecuta en modo promiscuo en la máquina utilizando (al igual que las anteriores) el NIT (Network

Interface Tap de SunOs 4.1.x), y también el "Packet Filtering Interface" para realizar esas capturas.

5.2.5. - nstat

Esta herramienta que originariamente fue diseñada para obtener estadísticas de uso de varios protocolos, se puede utilizar para detectar cambios en los patrones de uso de la red, que nos puedan hacer sospechar que algo raro está pasando en la misma.

Esta herramienta viene acompañada por dos utilidades que nos permiten analizar la salida que origina nstat, a saber: nsum, nload. La primera de ellas, nos da información de ciertos periodos de tiempo. La segunda, es un programa awk que produce una salida que puede ser vista de forma gráfica por herramientas como xvgr.

Para concluir este apartado, podemos decir que esta herramienta es muy útil para detectar ciertos tipos de ataques, tal como hemos reflejado anteriormente (con

etherscan), así como dar una idea de qué tipo de protocolos están viajando por la red.

Además, tiene la ventaja de que al estar en modo promiscuo, con sólo tenerlo en una máquina del segmento se puede tener monitoreado todo el segmento en el que esté conectado.

5.3. - argus

Es una herramienta de dominio público que permite auditar el tráfico IP que se produce en nuestra red, mostrándonos todas las conexiones del tipo indicado que descubre.

Este programa se ejecuta como un demonio, escucha directamente la interfaz de red de la máquina y su salida es mandada bien a un archivo de trazas o a otra máquina para allí ser leída. En la captura de paquetes IP se le puede especificar condiciones de filtrado como protocolos específicos, nombres de máquinas, etc.

A la hora de leer esa información disponemos de una herramienta que incluye el software (llamado ra) y que nos permite también realizar filtros de visualización. Una característica de esta herramienta es la posibilidad de filtrar paquetes de acuerdo a las listas de acceso de los routers CISCO. Es posible por tanto decirle que nos capture aquellos paquetes que no cumplen las reglas de la lista de acceso definida para esa interfaz del router. Como en el caso anterior (netlog) es posible ejecutar el comando en modo promiscuo (si lo que queremos es auditar todo nuestro segmento). Este programa divide las transacciones en cuatro grupos: TCP, UDP/DNS, MBONE, ICMP.

Algunos ejemplos de captura pueden ser:

argus -w NombreArchivoTraza &

Seguridad en Redes 5-8

En este ejemplo le indicamos que nos capture todas las transacciones que se producen en nuestra subred y que lo almacene en un archivo.

argus -w ArchivoSalida ip and not icmp &

Todo el tráfico ip pero no el icmp.

Como decíamos antes, el ra es el programa para leer la información generada por

argus.

Veamos algunos ejemplos de utilización:

ra -r ArchivoSalida tcp and host galileo

Vemos todo el tráfico tcp (tanto de entrada como salida) en la máquina galileo.

ra -C lista_acceso dst net 163.117.1.0

Vemos en tiempo real todas las transacciones a la red 163.117.1.0 que violan la lista de acceso de ese interfaz del router.

Para terminar, podemos decir que este software está disponible para SunOs 4.1.x,

Solaris 2.3 y SGI IRIX5.2

5.4. - tcpdump

Es un software de dominio público que imprime las cabeceras de los paquetes que pasan por una interfaz de red. Este programa es posible ejecutarlo en modo promiscuo con lo que tendremos las cabeceras de los paquetes que viajan por la red. Seguridad en Redes 5-9

Tanto en la captura como en la visualización de la información, es posible aplicar filtros por protocolo (TCP, UDP, IP, ARP, RARP...), puertos (en este caso el puerto puede ser un número o un nombre especificado en el archivo/etc/services), direcciones fuente, direcciones destino, direcciones de red, así como realizar filtros con operadores

(=, <, >, !=, and, not, ...). En la última versión, es posible ver también los paquetes de

datos.

5.5. - SATAN (Security Administrator Tool for Analyzing Networks)

Es un software de dominio público creado por Dan Farmer que chequea máquinas conectadas en red y genera información sobre el tipo de máquina, qué servicios da cada máquina y avisa de algunos fallos de seguridad que tengan dichas máquinas.

Una de las ventajas de SATAN frente a otros paquetes, es que utiliza una interfaz de WWW (como Mosaic, Netscape,..), va creando una base de datos de todas las máquinas chequeadas y las va relacionando entre ellas (de forma que si encuentra una máquina insegura, y chequea otra máquina que está relacionada con ésta, automáticamente esta segunda quedará marcada también como insegura).

Además, tiene la posibilidad de poder chequear las máquinas con tres niveles

("light", normal y "heavy"). Una vez realizado el chequeo de la máquina se genera una salida en formato html, y en el caso de encontrar fallos, da una pequeña explicación sobre el fallo en concreto. Cuando existe algún documento sobre ese fallo recogido en el CERT (advisory) tiene un enlace a ese documento, para que sobre la marcha pueda ser consultado. Asimismo, en el caso de que el fallo de seguridad sea debido a versiones antiguas de software da la posibilidad (mediante un enlace) de instalar una versión nueva de ese software.

Algunos de los servicios chequeados por SATAN son: finger, NFS, NIS, ftp, DNS,

rexd, así como tipo de sistema operativo, versión de sendmail, etc. La base de datos generada por SATAN puede ser luego consultada por varios campos: tipo de sistema operativo, tipo de servicio (servidores de NIS, ftp, NFS, X, etc).

SATAN ha sido diseñado como una herramienta de seguridad para ayudar a administradores de sistemas y redes, pero también puede ser utilizada para atacar a sistemas y descubrir la topología de la red de una organización. SATAN es capaz de chequear máquinas por subredes, con lo que quedan al descubierto todas las máquinas que se encuentran conectadas en dicha subred.

Para poder compilar y ejecutar SATAN basta con poseer la versión 5 de perl y un visualizador de WWW.

Para terminar, algunos de los fallos de seguridad que SATAN es capaz de detectar son:

- Acceso vía rexec
- Vulnerabilidad en el sendmail
- Acceso vía tftp
- Seguridad en Redes 5-10
- Accesos vía rsh
- Acceso a servidores X no restringido
- Exportar sistemas de archivos no restringido
- Acceso a archivos de contraseña vía NIS
-

5.6. - ISS (Internet Security Scanner)

Es una herramienta de la cual existe versión de dominio público que chequea una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. ISS es capaz de chequear una dirección IP o un rango de direcciones IP (en este caso se indican dos direcciones IP e ISS chequeará todas las máquinas dentro de ese rango).

El programa viene acompañado de dos utilidades que son ypx y strobe. La primera, nos permite la transferencia de mapas NIS a través de la red y la segunda, chequea y describe todos los puertos TCP que tiene la máquina que chequeamos. Como podemos ver, con la primera herramienta es posible la transferencia de los archivos de

"contraseña" en aquellas máquinas que hayan sido configuradas como servidores de NIS.

ISS se puede ejecutar con varias opciones y la salida se deja en un archivo.

Además, si ha podido traerse el archivo de "contraseña" de la máquina chequeada, creará un archivo aparte con la dirección IP de la máquina

5.7. - Courtney

Este software de dominio público sirve para identificar la máquina origen que intenta realizar ataques mediante herramientas de tipo SATAN.

El programa es un script perl que trabaja conjuntamente con tcpdump. Courtney recibe entradas desde tcpdump y controla la presencia de peticiones a nuevos servicios del stack TCP/IP (las herramientas de este tipo realizan ataques, chequeando de forma ordenada todos los puertos TCP y UDP que tiene el sistema, para poder ver qué servicios tiene instalados dicha máquina). Si se detecta que se está produciendo un continuo chequeo de estos puertos en un breve intervalo de tiempo, Courtney da un aviso. Este aviso se manda vía syslog.

Courtney puede generar dos tipos de alarmas dependiendo del ataque que se esté produciendo (normal o "heavy", las herramientas como SATAN dispone de distintos grados de chequeo de la máquina).

Esta herramienta necesita el intérprete de PERL y el tcpdump.

5.8. - Gabriel

Software desarrollado por "Los Altos Technologies Inc" que permite detectar

"ataques" como los generados por SATAN.

Gabriel identifica el posible ataque y de forma inmediata lo notifica al administrador o responsable de seguridad. La notificación se puede realizar de varias

Seguridad en Redes 5-11 formas (e-mail, cu, archivo de trazas). Este programa existe, en este momento, para

SunOs 4.1.x y Solaris, y está formado por un cliente y un servidor. El cliente se instala en cualquier máquina de la red, recoge la información que se está produciendo y la envía al servidor vía syslog. Estos clientes además envían de forma regular información al servidor para indicarle que están en funcionamiento.

En el caso de SunOs 4.1.x (Solaris 1), Gabriel utiliza el programa etherfind para realizar su trabajo. Una característica interesante de este software es que no necesita programas adicionales (como en el caso anterior PERL y tcpdump). El software viene con los ejecutables para SunOs 4.1.x y Solaris (cliente y servidor) así como un programa para realizar un test de funcionamiento.

Veamos un ejemplo de una alerta generada por el programa ante un ataque con

SATAN. Además de este archivo, se genera un mensaje de correo alertando del ataque.

Mon 07/24/95 14:15:01 restrained attacks from acme

Tue 07/25/95 10:15:01 restrained attacks from acme

Tue 07/25/95 14:00:01 restrained attacks from acme

5.9. - tcplist

Es un pequeño programa de dominio público que nos informa acerca de todas las conexiones TCP desde o hacia la máquina donde lo estamos ejecutando.

5.10. - nocol (Network Operations Center On-Line)

Es un conjunto de programas de monitoreo de sistemas y redes. El software es un conjunto de agentes que recogen información y escriben la salida en un formato que se puede, luego, procesar. Cada dato procesado recibe el nombre de evento y cada evento tiene asociado una gravedad.

Existen cuatro niveles de gravedad: CRITICAL, ERROR, WARNING, INFO.

Cada uno de estos niveles es controlado de forma independiente por cada agente.

Existe un conjunto de herramientas que nos permite ver toda la información generada por los agentes y que puede ser filtrada dependiendo de la gravedad del evento.

Entre las cosas que pueden ser controladas por este software tenemos:

- Monitor de ICMP (usando ping o multiping)
- Carga en la red (ancho de banda)
- Monitor de puertos TCP.
- Monitor de SNMP y SNMP traps.
- Monitor de servidor de Nombres.
- Monitor de rpc.
- Chequeo del bootpd

6. - Herramientas que chequean la integridad del sistema (Conceptos)

Con estas herramientas que nos ayudarán a proteger nuestro sistema. Para conseguirlo, tenemos dos tipos de herramientas. Las primeras, se basan en chequeos a los archivos. Las segundas, nos alertan de posibles modificaciones de archivos y de programas "sospechosos" que puedan estar ejecutándose en la máquina de forma camuflada.

Veremos, en primer lugar, las que chequean la integridad de los sistemas de archivos.

6.1. - COPS (Computer Oracle and Contraseña System)

Cops es un conjunto de programas diseñado por la Universidad de Purdue que chequea ciertos aspectos del sistema operativo UNIX relacionados con la seguridad.

Existen dos versiones de este paquete: una versión escrita en "sh" y "C" y otra versión escrita en "perl", aunque su funcionalidad es similar. Este programa es fácil de instalar y configurar y se ejecuta en gran cantidad de plataformas UNIX.

6.2. - Tiger

Es un software desarrollado por la Universidad de Texas que está formado por un conjunto de shell scripts y código C que chequean el sistema para detectar problemas de seguridad de forma parecida a COPS.

Una vez chequeado el sistema, se genera un archivo con toda la información recogida por el programa. Tiger dispone de una herramienta (tigexp) que recibe como parámetro dicho archivo y da una serie de explicaciones adicionales de cada línea que generó el programa anterior. El programa viene con un archivo de configuración donde es posible informarle qué tipo de chequeo se quiere realizar. Podemos comentar las operaciones más lentas y ejecutar éstas de forma menos continuada, mientras que las más rápidas pueden ser ejecutadas más frecuentemente.

6.3. - Crack

Este paquete de dominio público realizado por Alex Muffet permite chequear el archivo de contraseñas de UNIX y encontrar contraseñas triviales o poco seguras.

Para ello, usa el algoritmo de cifrado (DES) utilizado por el sistema UNIX y va comprobando a partir de reglas y de diccionarios las contraseñas que se encuentran en el archivo de contraseñas, creando un archivo con todos los usuarios y palabras descubiertas. Se realiza una serie de pasadas sobre el archivo de contraseñas, aplicando la secuencia de reglas que se especifique. Estas reglas se encuentran en dos archivos (gecos.rules y dicts.rules) y pueden ser modificadas utilizando un lenguaje bastante simple. Para una mayor efectividad pueden utilizarse diccionarios complementarios (existen en gran diversidad servidores ftp) en diferentes idiomas y sobre diversos temas.

6.4. - Tripwire

Este software de dominio público desarrollado por el Departamento de Informática de la Universidad de Purdue, es una herramienta que comprueba la integridad de los sistemas de archivos y ayuda al administrador a monitorizar éstos frente a modificaciones no autorizadas.

Esta herramienta avisa al administrador de cualquier cambio o alteración de archivos en la máquina (incluido binarios). El programa crea una base de datos con un identificador por cada archivo analizado y puede comparar, en cualquier momento, el actual con el registrado en la base de datos, avisando ante cualquier alteración, eliminación o inclusión de un nuevo archivo en el sistema de archivos.

6.5 .- chkwtmp

Es un pequeño programa que chequea el archivo "/var/adm/wtmp" y detecta entradas que no tengan información (contienen sólo bytes nulos).

Estas entradas son generadas por programas tipo "zap" que sobreescriben la entrada con ceros, para, de esta manera, ocultar la presencia de un usuario en la máquina. Este programa detecta esa inconsistencia y da un aviso de modificación del archivo y entre qué espacio de tiempo se produjo.

6.6. - chklastlog

Es parecido al programa anterior. Éste chequea los archivos "/var/adm/wtmp" y

"/var/adm/lastlog". El primero, es la base de datos de login, y el segundo, la información del último login de un usuario. En el segundo archivo nos indica qué usuario ha sido eliminado del archivo.

6.7.- spar

Software de dominio público diseñado por CSTC (Computer Security Technology

Center) realiza una auditoría de los procesos del sistema, mucho más flexible y potente que el comando lastcomm de UNIX.

El programa lee la información recogida por el sistema y puede ser consultada con una gran variedad de filtros como usuario, grupo, dispositivo, admitiendo también operadores (=, >, <, >=, &&...).

Por defecto, el programa obtiene la información del archivo "/var/adm/pacct". No obstante, se le puede indicar otro archivo. La información puede ser mostrada en ASCII o en binario para su posterior proceso con spar.

6.8.- lsof (List Open Files)

Este programa de dominio público creado por Vic Abell, nos muestra todos los archivos abiertos por el sistema, entendiendo por archivo abierto: un archivo regular, un directorio, un archivo de bloque , archivo de carácter, un archivo de red (socket, archivo NFS).

6.9. - cpm (Check Promiscuous Mode)

Este pequeño programa realizado por la Universidad de Carnegie Mellon, chequea la interfaz de red de la máquina descubriendo si está siendo utilizada en modo promiscuo (escuchando todo el tráfico de la red).

Está herramienta es muy útil, porque nos alerta de la posible existencia de un

"sniffer" (olfateador) que intente capturar información en nuestra red como puedan ser las contraseñas. Este programa debería ser ejecutado de forma periódica para detectar lo antes posible el estado promiscuo en la placa de red. Una forma útil de utilizarlo es mandarnos el resultado vía correo electrónico.

Es importante tener en cuenta que muchos de los programas descritos en este documento, pueden poner la placa en modo promiscuo con lo que deberemos asegurarnos que no son nuestros programas los que producen esa alerta.

Generalmente los programas tipo "sniffer" suelen estar ejecutándose como procesos camuflados en el sistema.

6.10. - ifstatus

Software de dominio público creado por Dave Curry, permite, al igual que el anterior, descubrir si un interfaz de red está siendo utilizada en modo promiscuo para capturar información en la red. Sirven todas las recomendaciones mencionadas anteriormente.

Veamos un ejemplo del mensaje que genera ésta aplicación, cuando encuentra una interfaz de red ejecutada en modo promiscuo:

Checking interface le0... flags = 0x163

WARNING: ACME INTERFACE le0 IS IN PROMISCUOUS MODE.

Checking interface le0... flags = 0x49

6.11. - osh (Operator Shell)

Creado por Mike Neuman, este software de dominio público es una Shell restringida con “setuid root”, que permite indicar al administrador mediante un archivo de datos qué comandos puede ejecutar cada usuario.

El archivo de permisos está formado por nombres de usuario y una lista de los comandos que se permite a cada uno de ellos. También es posible especificar comandos comunes a todos ellos. Este shell deja una auditoría de todos los comandos ejecutados por el usuario, indicando si pudo o no ejecutarlos. Dispone, además, de un editor (vi) restringido.

Este programa es de gran utilidad para aquellas máquinas que dispongan de una gran cantidad de usuarios y no necesiten ejecutar muchos comandos, o para dar privilegios a determinados usuarios “especiales” que tengan algún comando que en circunstancias normales no podrían con un shell normal.

6.12. - noshell

Este programa permite al administrador obtener información adicional sobre intentos de conexión a cuentas canceladas en una máquina.

Para utilizarlo basta sustituir el shell del usuario en el archivo /etc/contraseña por éste programa. A partir de ahí, cada intento de conexión generará un mensaje (vía email o syslog) indicando: usuario remoto, nombre de la computadora remota, dirección

IP, día y hora del intento de login y tty utilizado para la conexión.

Todas estas herramientas se pueden bajar de lince.uc3m.es o de cualquier

sunsite.

6.13. - trinux

Trinux contiene las últimas versiones de las más populares herramientas de seguridad en redes y es usado para mapear y monitorear redes TCP/IP.

El paquete es muy interesante pues, básicamente, se compone varios discos, con los cuales se bootea la máquina que se va a dedicar a realizar el trabajo y corre enteramente en RAM.

Las aplicaciones que trae, principalmente, son:

mail -soporte simple de correo saliente usando smail.

netbase - utilitarios estándar de redes, tales como ifconfig, arp, ping, etc.

netmap - herramientas de escaneo de red, tal como fyodor's, strobe, nmap y netcat.

netmon - herramientas de monitoreo y sniffers, tal como sniffit, tcpdump y iptraf

perlbase - base del lenguaje Perl.

perli386 - archivos del sistema Perl.

perlmods - módulos de Perl.

pcmcia - soportes de módulos de kernel y scripts para laptop

snmp - herramientas seleccionadas desde CMU SNMP.

web - cliente Lynx.

win32 - herramientas de seguridad para Windows95/NT.

Obtenible en www.trinux.org

7. Bibliografias

http://es.wikipedia.org/wiki/Red_de_computadoras

http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-risk.html

http://www.slideshare.net/contiforense/seguridad-informtica-y-policia-informtica-4667479

http://www.slideshare.net/cesbarahona/introduccin-2045973

Políticas_generales_de_seguridad.pdf (tomado del material de apoyo SENA)

Vulnerabilidades_y_soluciones.pdf (tomado del material de apoyo SENA)

http://es.ccm.net/contents/593-proteccion-introduccion-a-la-seguridad-de-redes